

# Obstructions to Hasse principe. Another point of view.

Hubert Schaetzel

**Abstract** To answer to the Hasse principle is the same as to make sure about the existence or not of solutions for a system of diophantine equations. There are numerous obstructions to this principle with non-linear and non-quadratic equations. However, this principle is applied usually to formal variables representing integers. We extend here this framework to prime numbers variables causing a deep modification of the obstruction concept. We then observe that behind the existence problem associated with this principle, one can find the ingredients, mainly by replacing "global" variables by "local" variables, to enumerate the solutions of the asymptotic branches of diophantine equations.

## Obstructions au principe de Hasse : une perspective différente.

**Résumé** Répondre au principe de Hasse est la garantie de l'existence ou non de solutions pour un système d'équations diophantines. Il existe de nombreux cas d'obstruction à ce principe pour des équations qui ne sont ni linéaires, ni quadratiques. Cependant, ce principe est appliqué habituellement à des variables formelles représentant des nombres entiers. Nous élargissons ici ce cadre à des variables représentant des nombres premiers ce qui a pour conséquence une large remise en cause de la notion même d'obstruction. Nous observons ensuite que derrière le problème d'existence de solutions associé à ce principe se découvrent les ingrédients, notamment le remplacement des variables « globales » par des variables « locales », permettant de dénombrer les solutions des branches asymptotiques des équations diophantines.

**Status** Preprint  
**Date** Vesrion 1 : September 01, 2012  
 Version 2 : November 18, 2012  
 Version 3 : October 23, 2013

## Summary

1	Part I : Existence of solutions	3
1.1	Local global Hasse principle. Obstruction to the principle.	3
1.2	Local variables	3
1.2.1	Chebotarev density theorem	3
1.2.2	Prime number density theorem	3
1.2.3	Corollary on prime numbers variables	3
1.2.4	Case of variables of integers	4
1.2.5	Definition of local variables	4
1.2.6	Two available presentations : by congruency classes of or deployed list	4
1.2.7	Essential concept of stability.	4
1.2.7.1	Generalities	4
1.2.7.2	Stability degree of a monomial of prime numbers	5
1.2.7.3	Degree of stability of a monomial of integers	5
1.3	Obstruction to the Hasse principle with a new point of view	5
1.3.1	A trail to reconsider	5
1.3.2	Redefining obstructions	7
1.3.3	Relevance of weak obstruction : a very narrow domain	7
1.3.4	Relevance of strong obstruction : an a priori empty domain	8
1.3.5	Evaluation strategies	8
2	Part II : Solutions enumerations	8
2.1	Introduction to local-global enumerations	8
2.1.1	The solutions density factor	8
2.1.2	The available volume factor	9
2.2	Theorem of Chinese remainder	9
2.2.1	Statement	9
2.2.2	Application to enumerations	9
2.3	Related concepts indispensable to enumerations	10
2.3.1	Concept of stability (or stationarity)	10
2.3.2	Information contained in local variables	10
2.4	One variable local-global enumeration	10
2.4.1	Generalities on monomials	10
2.4.2	The example of $x$	11
2.4.3	The examples of $x^2$ and $x^4$	11
2.4.4	The example of $x^n$	12
2.4.4.1	Singular series	12
2.4.4.2	Function volume and cardinal product	14
2.4.5	Second degree polynomial equations	15

2.4.6	Third degree polynomial equations	17
2.4.6.1	Exposition of the general context	17
2.4.6.2	Proof of equiprobability at degree 3	20
2.4.6.3	Study of supernumerary cardinals	21
2.4.7	Higher degrees polynomial equations	21
2.4.7.1	Decomposition in ring $\mathbb{Z}/p^b\mathbb{Z}[X]$	21
2.4.7.2	Direct resolution	22
2.4.7.3	Discriminant	23
2.4.7.4	Cardinals relative frequencies	27
2.4.7.5	Application to equiprobability	32
2.4.7.6	Study of supernumerary cardinals	33
2.4.8	Reconstruction of the set of prime numbers	33
2.4.8.1	Minimal needs	33
2.4.8.2	Implementation	33
2.4.8.3	Theorem of prime numbers local - global reconstruction	34
2.4.9	The example of $y^n$	34
2.4.9.1	Singular series	34
2.4.9.2	Function volume and cardinal of product	36
2.4.10	Case of polynomials.	37
2.5	Local-global enumerations with two or more variables	37
2.5.1	Case of arithmetic series	37
2.5.2	Polignac, Vinogradov and relatives	38
2.5.3	Case of polynomials with more than two variables	39
2.6	Obstructions to enumerations	40
2.6.1	The examples to exclude	40
2.6.2	The remaining examples	40
2.6.2.1	Cassels et Guy equation	40
2.6.2.2	Borovoi equation	42
2.6.2.3	Reduction of equations	45
2.6.3	Obstruction or influx	45
2.7	Conclusion and prelude	45
Appendix 1		47
Appendix 2		49
Appendix 3		50
Appendix 4		55
Appendix 5		56
Appendix 6		58
Appendix 7		62
Appendix 8		67

## SIGNS AND ABBREVIATIONS

$n$	Natural integer
$\mathbb{N}$	Set of natural integers
$\mathbb{Z}$	Set of relative integers
$p$	Any prime number
$\mathbb{P}$	Set of prime numbers
$\#\{(x_1, \dots, x_n)\}$	Cardinal (quantity, multiplicity...) of $n$ -th $(x_1, \dots, x_n)$ , also noted $\#(x_1, \dots, x_n)$ .
$(, )$	Greatest common divisor of $(, )$
$\text{Si}(x, y, z)$	If $x$ true then $y$ if not $z$ . The condition can be overlapping : $\text{if}(x, \text{if}(y, z, t), \dots)$
$^$	Sign of exponentiation ( $x^n = x^n$ )
$\backslash$	Such as
$\forall$	Whatever
$\in$	Sign of membership to a set ( $n \in \mathbb{N}$ , $p \in \mathbb{P}$ )
$\subset$	Sign of inclusion

### 1.1 Local global Hasse principle. Obstruction to the principle.

The local-global principle consists in trying to reconstruct an information on a global object from information on associated local objects, easier to get [16].

Trivially

$$R(x_1, x_2, \dots) = 0 \Rightarrow \forall p \in P, \forall k \in N, R(x_1, x_2, \dots) = 0 \pmod{p^k} \quad (1)$$

The Hasse principle is verified if the logical implication in the opposite direction is also true (with the condition  $R(x_1, x_2, \dots) = 0$  has a solution in  $R$ , the real numbers field).

The Hasse Minkowski theorem [3] applies on quadratic forms (and therefore also the linear forms) on the (global) field of the rational numbers. It stipulates that such a form will take the value 0 if and only if the form is set to 0 for each of the local field associated with the field of the rational numbers, that is within  $R$  the field of the real numbers, and within any of the  $p$ -adic numbers field  $Q_p$ ,  $p$  a prime,. This is an example where the local-global principle is perfectly verified [16].

Otherwise, it is customary to speak of obstructions to the Hasse principle.

As a first step, we will dedicate ourselves to redefine the framework of these obstructions with a new approach of the local tests.

### 1.2 Local variables

#### 1.2.1 Chebotarev density theorem

Through the preliminary work of Frobenius, Chebotarev [2] shows the following :

Let us have a Galois extension  $L/K$  of a number field, of Galois group  $G$ . Let us have  $\mathfrak{p}|p$  a prime ideal of  $L$  over  $p$ . Let us have the Frobenius conjugation class  $(\mathfrak{p}, L/K)$ , yet noted  $\sigma_p$ . Let us have  $C$  a class of conjugation in  $G$ . Then, the set of prime ideals  $p$  of  $K$ , unramified in  $L$ , and such as  $\sigma_p = C$ , has natural density  $|C|/|G|$ .

This theorem extends the Dirichlet's theorem on the infinitude of the primes in arithmetic progression by trivial application to a  $Q$  cyclotomic extension.

It follows from the theorem :

#### 1.2.2 Prime number density theorem

If  $c$  and  $a \geq 1$  are coprime integers, the natural density of the set of primes  $p = c \pmod{a}$  is equal to  $1/\phi(a)$ .

#### 1.2.3 Corollary on prime numbers variables

Let us have  $p$  a prime number.

We project the set of prime numbers  $P$  on modulo  $p$  congruency classes :

$$\begin{array}{ccc} & \text{mod } p & \\ P & \rightarrow & \{0, 1, 2, \dots, p-1\} \\ p_i & & p_i \pmod{p} \end{array}$$

This application projects a unique number to 0. It is  $p$ . Other classes are images in same density of all other primes. By setting a probability density to quantities projected onto each of congruencies  $0, 1, 2, \dots, p-1$  and by arbitrarily summing all densities to  $p$  (that is an average density of 1 per class), we get the correspondence

Congruencies	0	1	2	...	$p-1$
Normalized densities	$\rightarrow 0$	$\rightarrow p/(p-1)$	$\rightarrow p/(p-1)$		$\rightarrow p/(p-1)$

This means that modulo  $p$ , the set of prime numbers is equivalent to the series of classes called here temporarily the representative of  $P$  at sequence  $p$  :

$$\{1, 2, \dots, p-1\} \quad (2)$$

Indeed, the probability density of 0 is 0, we can ignore this value 0 and we can then ignore the other congruencies relative weights as of equal values (the interest of normalization will be mentioned below in the part concerning the enumeration).

The set  $\{1, 2, \dots, p-1\}$  is precisely the Galois group  $(Z/pZ)^*$ . This group is generated by any primitive root  $g$  de  $p$ .

$$\{g^0, g^1, \dots, g^{p-2}\} \quad (3)$$

We can make similar projections on any set of congruencies modulo  $p^k$ .

$$\begin{array}{ccc} & \text{mod} & \\ P & \rightarrow & \{0, 1, 2, \dots, p^k-1\} \\ p_i & & p_i \text{ mod } p^k \end{array}$$

Then, the table will be (with still the same average value of 1) :

Congruencies	0 mod p	$\neq 0 \text{ mod } p$
Densities	$\rightarrow 0$	$\rightarrow p/(p-1)$

(4)

The corresponding group (with  $\phi(p) = p^{(k-1)}(p-1)$ ) will be :

$$\{g^0, g^1, \dots, g^{\phi(p)-1}\} \quad (5)$$

#### 1.2.4 Case of variables of integers

In a similar and trivial routine, the sets  $\mathbb{Z}$ ,  $\mathbb{N}$  or  $\mathbb{N}^*$  will project in equiprobable way modulo  $p^k$  on :

$$\{0, 1, 2, \dots, p^k-1\} \quad (6)$$

Then, the table of correspondence of congruencies densities will be (taking an average density of 1 per class) :

Congruencies	0 mod p	$\neq 0 \text{ mod } p$
Densities	$\rightarrow 1$	$\rightarrow 1$

(7)

Note : Moreover here, the exact value of the density is obtained within a  $p^k$  period when are added gradually new integers.

#### 1.2.5 Definition of local variables

We will call "asymptotic representative" or "local variable" of a variable at sequence  $p$  and exponent  $k$  (a term which is implied when  $k = 1$ ), the equiprobable projection modulo  $p^k$  of the elements of non-null density of this variable. This can also be viewed as the classes of congruencies modulo  $p^k$  associated with these classes probability densities (before having confirmed the equidensity of the probabilities).

#### 1.2.6 Two available presentations : by congruency classes of or deployed list

The local variable (or asymptotic representative) is usable either as the finite series of congruencies affected of probability densities or as an infinite series (called deployed) also assigned with the densities of probabilities corresponding to this variable.

For example, for all primes  $P$  in the simplest modulo  $p$  case, it is either the finite series  $\{1, 2, \dots, p-1\}$  or the infinite sequence (called deployed)  $\{1, 2, \dots, p-1, p+1, p+2, \dots, 2p-1, 2p+1, 2p+2, \dots, 3p-1, \dots\}$  with equidensity, the list can be deployed also left to negative numbers.

Later, in asymptotic enumeration, we use variables in deployed form.

#### 1.2.7 Essential concept of stability.

##### 1.2.7.1 Generalities

Let us have a variable  $X$  or  $Y$  depending on whether one is in the presence of integers and prime numbers. For representatives of  $X^n$  or  $Y^n$ , we use the same method of projection on the set of congruencies  $\{0, 1, 2, \dots, p^k-1\}$

$$\begin{array}{ccc} & \text{modulo} & \\ X^n & \rightarrow & \{0, 1, 2, \dots, p^k-1\} \\ x^n & & x^n \text{ mod } p^k \end{array} \quad (8)$$

This lead in the same way to zero density classes and given densities classes families. If beyond a given  $k$ , there is no more evolution in the relative proportions between two classes  $c$  and  $c+p^k$  densities for any  $c$ , the representative is then said stable (and the good representative is obtained) or stationary (later term which can borrow at similar concepts that one will discover in the  $p$ -adic field theory and that the reader can find in peculiar in [15] page 26).

We give below these representatives for  $X^n$  or  $Y^n$ , with the convention of writing that  $X$  is a variable of integers and  $Y$  is a variable of prime numbers.

By adding different degrees or more complex monomials, we obtain polynomials of variables of integers or variables of prime numbers. Let us have  $R(X,Y,...)$  such a polynomial.

We then conduct the projection (with  $\phi(p) = p^{(k-1)}(p-1)$ ) :

$$\begin{array}{ccc} R(X,Y,...) & \xrightarrow{\text{modulo}} & \{0, 1, 2, \dots, p^k-1\} \\ R(x,y,...) & & R(x,y,...) \bmod p^k \\ x = 0 \text{ to } p^k-1 & & \\ y = g^0, g^1, \dots \text{ to } g^{\phi(p)-1} & & \\ \dots & & \end{array} \quad (9)$$

Collected frequencies on  $\{0, 1, 2, \dots, p^k-1\}$  depend on the data  $R(X, Y, \dots)$  and the local parameters  $p$  and  $k$ .

Let us set the sequence  $p$  and let us increase by integer increment  $k$  starting with 1. Possibly, the relative proportions of the collected frequencies stabilize at a certain rank  $k_p$ . If this happens, the relative proportions remain constant for all  $k \geq k_p$  and we refer  $k_p$  as the degree of stability of  $R(x, y, \dots)$  at the sequence  $p$ .

All the sequences are passed in review in this way and we go to the next sequence as soon as stable relative proportions are recognized.

### 1.2.7.2 Stability degree of a monomial of prime numbers

Let us have  $\delta b$  the positive integer  $\delta$  from which the greatest common divisor of  $n$  et  $p^{\delta-1}(p-1)$  remains unchanged ( $n$  is the exponent in  $Y^n$ ) :

$$\delta b(p,n) = \min(\delta \setminus d_\delta = d_{\delta+j} \quad \forall j \in \mathbb{N}^*, d_1 = (n, p^{i-1}(p-1)))$$

The degree of stability  $\delta c$  of a monomial is the minimal value  $\delta$  such as the normalized representative of the monomial modulo  $p^\delta$  will no longer evolve when exponent  $\delta$  increases.

Let us consider the monomial  $y^n$ .

Let us have the sequence  $p$  and  $d_\delta = (n, \Phi(\delta)) = (n, p^{\delta-1} \cdot (p-1))$

We get then :

$$\delta c(p = 2, y^n) = 1 + \min(\delta \setminus d_\delta = d_{\delta+j} \quad \forall j \in \mathbb{N}^*) = 1 + \delta b \quad (10)$$

$$\delta c(p \neq 2, y^n) = \min(\delta \setminus d_\delta = d_{\delta+j} \quad \forall j \in \mathbb{N}^*) = \delta b \quad (11)$$

The reader will find in appendix 2 an illustration with the prime numbers variable  $y^6$ . This example highlights the proof of results (10) et (11) which follows.

#### Proof

Let us have  $g$  a primitive root of  $p$ . The representative of a variable  $y^n$ , at sequence  $p \neq 2$ ,  $g$  being a primitive root of  $p$  and with  $d = (n, p^{\delta-1} \cdot (p-1))$ , is  $\{g^{0,d}, g^{1,d}, g^{2,d}, \dots, g^{(\Phi(\delta)/d-1),d}\} \bmod p^\delta$ . For  $p = 2$ , the representative is  $\{5^{0,d}, 5^{1,d}, \dots, 5^{(\Phi(\delta)/d-1),d}\} \cup \{(-5)^{0,d}, (-5)^{1,d}, \dots, (-5)^{(\Phi(\delta)/d-1),d}\}$  where  $d = (n, \Phi(\delta)/2) = (n, 2^{\delta-2} \cdot (2-1))$ . Thus the result.

#### Function « rho »

The degree of stability cuts behaviour modulo  $p^\delta$  of an expression into two zones : the "unpredictable" zone  $\delta < \delta c$  to be explored in a case by case way and the  $\delta \geq \delta c$  zone having the characteristics observed at  $\delta = \delta c$ .

### 1.2.7.3 Degree of stability of a monomial of integers

The degree of stability of the monomial  $X^n$  is infinite in the sense that the frequencies (densities) gathered on  $\{0, 1, 2, \dots, p^k-1\}$  evolve permanently on the first  $\{0\}$  term in regard to other terms  $\{1, 2, \dots, p^k-1\}$  when  $k$  increases (and tends to infinity). However, even if the representative cannot therefore be completely expressed, it is possible to examine its evolution with  $k$  (in the expression given in (8)) and infer useful features at infinity as appropriate.

We shall see, by further developments in part II, that this non-stability of  $\{0\}$  is host key reason of "obstructions" to the Hasse principle.

## 1.3 Obstruction to the Hasse principle with a new point of view

### 1.3.1 A trail to reconsider

For the forms of greater than 2 degrees, counterexamples have been given by different authors to the Hasse principle. These counter-examples are called "obstructions" in the dedicated language. However, these obstructions are observed recklessly only for integer variables. The local variable (of congruency classes) takes in this case successively each of the values between 0 and  $p^k-1$  and one gets, in case of "obstruction", solutions modulo  $p^k$ , ( $k \geq k_p$ ) to the studied diophantine equation at all sequences  $p$ .

However, if a diophantine equation, for example  $3x^3 + 4y^3 + 5z^3 = 0$  has no solution in  $\mathbb{Z}$ , except the trivial solution (0,0,0), it

has neither if variables x, y and z take only values in the set of prime numbers. Formally, the overall equation with integers or with prime numbers is exactly the same. But it is not so in the local situations with integers on one side and prime numbers on the other side.

Thus, we could not find any obstructions to the Hasse principle after this "change of point of view" which is to replace the local variables of integers by local variables of prime numbers in all the examples of the mathematical literature that we tested. Below, we call "prohibitions" the sequences p that entails the denial of the obstruction (in prime numbers). In the table below, the prohibitions are not necessarily limited to the given sequences (even if these lists are a priori exhaustive), but it is sufficient to find a single value, as we have done, to prove the absence of obstructions to the Hasse principle (according to our new perspective).

Table (1)

References	Equations (x, y, z and t prime numbers variables)	Prohibitions p =
[6] Cassels et Guy (1968)	$5x^3+9y^3-10z^3-12t^3=0$	7
[10]	$9x^2-2x.y-7y^2-2z^2+1=0$	2
[5] A.Schinzler	$x^4+17y^4-2(4z^2+t^2)^2=0$	3
[7] E.S.Selmer	$3x^3+4y^3+5z^3=0$	3 et 7
[7]	$x^3+3y^3+20z^3=0$	7
[7]	$x^3+4y^3+15z^3=0$	7
[7]	$x^3+5y^3+12z^3=0$	7 et 13
[11], [7]	$x^3+11y^3+43z^3=0$	2, 3 et 7
[6] V.A.Iskovskikh (1970)	$x^2+y^2+(z^2-3).(z^2-2)=0$	2 et 3
[4]	$x^2+y^2+(z^2+1).(z^2+3).(z^2-3)^2.(z^2+23)=0$	2 et 3

Briefly, let's go back for a proper understanding of the subject, on how to obtain this table. We do a calculation with overlapping loops according to the routine of the relationship (9). For the equation of Cassels and Guy, this is written for example :

```

From p = 2 to pi
From x = 0 to pk-1
If x/p = int(x/p) goto next x otherwise
From y = 0 to pk-1
If y/p = int(y/p) goto next y otherwise
From z = 0 to pk-1
If z/p = int(z/p) goto next z otherwise
From t = 0 to pk-1
If x/p = int(x/p) goto next x otherwise
c = 5x3+9y3-10z3-12t3 mod p
#(c) = #(c)+1
Next t
Next z
Next y
Next x
Next p
Spread out of cardinals # (duplications modulo pk)

```

We get then the following tables :

Tables (2)

k = 1													
p \ c	0	1	2	3	4	5	6	7	8	9	10	11	12
2	1	1	1	1	1	1	1	1	1	1	1	1	1
3	8	4	4	8	4	4	8	4	4	8	4	4	8
5	64	48	48	48	48	64	48	48	48	48	64	48	48
7	0	243	324	81	81	324	243	0	243	324	81	81	324
Product	0	≠ 0	≠ 0	≠ 0	≠ 0	≠ 0	≠ 0	0	≠ 0	≠ 0	≠ 0	≠ 0	≠ 0

k = 2													
p \ c	0	1	2	3	4	5	6	7	8	9	10	11	12
2	8	0	8	0	8	0	8	0	8	0	8	0	8
3	324	162	162	162	0	0	162	162	162	324	162	162	162
5	8000	6000	6000	6000	6000	8000	6000	6000	6000	6000	8000	6000	6000
7	0	83349	111132	27783	27783	111132	83349	0	83349	111132	27783	27783	111132
Product	0	0	≠ 0	0	0	0	≠ 0	0	≠ 0	0	≠ 0	0	≠ 0

k = 3													
p \ c	0	1	2	3	4	5	6	7	8	9	10	11	12
2	64	0	64	0	64	0	64	0	64	0	64	0	64
3	8748	4374	4374	4374	0	0	4374	4374	4374	8748	4374	4374	4374
5	1000000	750000	750000	750000	750000	1000000	750000	750000	750000	750000	1000000	750000	750000
7	0	28588707	38118276	9529569	9529569	38118276	28588707	0	28588707	38118276	9529569	9529569	38118276
Product	0	0	≠0	0	0	0	≠0	0	≠0	0	≠0	0	≠0

The cardinals (numbers) of solutions  $\#(c)$  are within the double framework. As required, we call these cardinals the factors of abundance of  $c$ . The modulo  $p^k$  spread outs are indicated with red wavy edges.

For  $c = 0$ , we find indeed a ban due to the sequence  $p = 7$ . We can also view the concept of stability by looking at ratios of cardinals from a target  $c$  to another. Thus, for  $p = 2, 3$  and  $5$ , stability is reached from  $k = 2$ . For  $p = 7$ , it intervenes even from  $k = 1$  (precisely on the fact that  $\#(c) = 0$  for  $c = 0$  modulo  $7$  and that in general stability occurs for  $c \neq 0$  modulo  $p$  from  $k = 1$  on what we will see later in part II).

In addition, returning to the table of obstructions examples, we can note that a priori any equation  $ax^3+by^3+cz^3 = 0$  with  $a+b+c \neq 0$  has a prohibition testing prime numbers local variables and has not for integer variables.

The temporary absence of "obstruction with prime numbers" in the literature does not mean his absence regardless of the chosen diophantine problem.

Thus

$$x^2+2y^2+3z^2+18t^2 = 0 \quad (12)$$

which has of course only a trivial solution  $(0,0,0,0)$  has no prohibition, using prime numbers variables, regardless of the sequence  $p$ .

However,  $x^2+2y^2+3z^2+18t^2 = c$  has a finite number of solutions (and often none) regardless of the target  $c$ . In this world of scarcity or lack of solutions, a single solution as  $(0,0,0,0)$  is to be regarded as a source of abundance. Therefore, there is no place for a ban at  $c = 0$ .

This example shows that if one wishes to acquire some understanding of what interests us here, it is necessary to have an overall vision, namely study not an equation but a family of equations at the same time. Thus, we introduce the concept of target which is the use of a  $c$  parameter :

$$R(x,y,\dots) = c$$

Deeper information is obtained when we get interested, in this framework, with the enumeration of solutions what we will do in the second part of the article.

### 1.3.2 Redefining obstructions

In the light of the foregoing, we are led to define a notion of more gradual obstruction. We call weak obstruction that observed with variables of integers and strong obstruction that observed with variables of prime umbers. There is of course the possibility of mixing in a diophantine equation, integer variables and variables of primes. In this case, we can speak of intermediate obstruction when it occurs, but this concept is flawed (as a result of the number of variables of each category without quantification with the terminology "intermediate") and has certainly little of interest.

	Types of global et local variables
Strong obstruction	Prime numbers
Weak obstruction	Integers
Intermediate obstruction	The two types

Within this new framework, we highlight the concept of trivial solutions and non-trivial solutions by its banning. There are no trivial solutions. There is a solution or there is none. For the homogeneous equations,  $0$  is a solution and even more. We will see that, far from being trivial, it is instead of great importance for the coherence of the results observed while enumerating solutions. For example, the existence of a single trivial solution allows to justify the consistency with a general enumeration which anticipates an infinite number of solutions, simply by arbitrary assignment of an appropriate multiplicity as  $0^n = 0$  for any  $n$  (similar to the solution at infinity in a projective space).

### 1.3.3 Relevance of weak obstruction : a very narrow domain

As noted at paragraph 1.2.7.3, the degree of stability of an integer variable can be infinite (in particular for the monomials of degree greater than  $1$ ). However, the non-stability affects only target  $c = 0$  in the local equation  $P(x) = c \pmod{p^k}$  where  $P(x)$  is a polynomial without constant term. It is the unique case of the weak prohibition phenomenon. This will be discussed in more detail in part II of this article.

For this exception, the weak obstruction may then be "lifted" somehow by studying what happens when changing variable type.

### 1.3.4 Relevance of strong obstruction : an a priori empty domain

We could not highlight a one variable equation strong obstruction which made sense, that is with the remarks of the example of the diophantine equation (12) in the background.

### 1.3.5 Evaluation strategies

We have two possible options.

Option 1 : Search for the origin of the obstructions by the study of Bauer-Manin groups and other bielliptic objects taking into account different types of variables (of integers and of prime numbers to start with...).

Option 2 : Examine the selected diophantine equation within a target  $c$  parameterized family of equations,  $c$  varying on  $\mathbb{Z}$ . Reasoning within simultaneous enumerations ( $c$  axis forming an additional dimension of the initial affine space) as we indicated in paragraph 1.3.2 while keeping in mind the possibility of exceptions (ex  $p-q = 0$  among  $p-q = 2n$ ).

We adopt this second option because it allows to give another perspective to the concept of "obstruction", but also to unveil an opposite concept, that we have called the "influx", and then discard both in the way proposed in part II.

## 2 Part II : Solutions enumerations

### 2.1 Introduction to local-global enumerations

We reuse in this paragraph title the terminology (local-global) associated with the Hasse principle, but converting a problem of existence into a counting exercise.

We will discover that the notion of obstruction is much less determined as usually sought. According to the choice of the diophantine equation and what we called above the target, it is not about a question of all or none, but it appears rather a gradation of exceptions to the a priori expected results (enumerations), with straight "obstruction", with low values, but also with high values, or even infinite ones.

We are interested in the enumeration of solutions of either integers or prime numbers diophantine equations (or a mixture of the two). Following equations, we will have one finite number (possibly zero) or an infinite number of solutions. Our ultimate goal is the count of the last class of equations. For them, known formulas (demonstrated or supposed) are usually written in the form of a product with a "density of solutions" oriented factor and an "available volume" oriented factor.

$$\#\{(x,y,\dots) \mid R(x,y,\dots) = c\} \approx \text{fan}(c) \cdot V'(c) \quad (13)$$

It is the kind of expression that is found, for example, with the "circle method", where the solutions density factor  $\text{fan}(c)$  is called the singular series (or fudge product) or even Euler product. The formulas associated of this method do however apply only when the number of variables is great towards the degree of the equation, which excluded the most "interesting" cases. We will reduce this barrier of the number of variables by taking a different path sieving the appropriate impacts on one variable (monomials and polynomials) diophantine equations.

Thus, we will gradually show how to reach the type of relationship (13) not by the top (many variables) but from the bottom down (one single variable) without meanwhile forgetting the concept of "obstruction" by checking its relevance (or not).

#### 2.1.1 The solutions density factor

Let us have a diophantine equation and a given target  $c$  :

$$R(x,y,\dots) = c$$

Variables  $x$ , respectively  $y$ , are taking values in the set of integers, respectively prime numbers.

Then, trivially

$$R(x,y,\dots) = c \Rightarrow \forall p \in P, \forall k \in \mathbb{N}, R(x,y,\dots) = c \pmod{p^k} \quad (14)$$

but also, and this is the most useful relationship (by adding the product sign),

$$R(x,y,\dots) = c \Rightarrow \forall p_i \in P, \forall k_i \in \mathbb{N}, R(x,y,\dots) = c \pmod{\prod p_i^{k_i}} \quad (15)$$

so that by adding the notion of enumeration

$$\#\{(x,y,\dots) \mid R(x,y,\dots) = c\} \Rightarrow \#\{(x,y,\dots) \mid \forall p_i \in P, \forall k_i \in \mathbb{N}, R(x,y,\dots) = c \pmod{\prod p_i^{k_i}}\} \quad (16)$$

Let us note that the variables in the second member are local variables, in other words congruency classes. It would be more appropriate to write :

$$\#\{(x,y,\dots) \mid R(x,y,\dots) = c\} \Rightarrow \#\{(cx,cy,\dots) \mid \forall p_i \in P, \forall k_i \in N, R(cx,cy,\dots) = c \bmod \prod p_i^{k_i}\} \quad (17)$$

where  $cx$  belongs to classes  $\{0, 1, \dots, \prod p_i^{k_i} - 1\}$  and  $cy$  to classes  $\{g^0, g^1, \dots, g^{\varphi(t)-1}\}$  with  $\varphi(t) = \varphi(\prod p_i^{k_i}) = \prod p_i^{k_i-1} \cdot (p_i - 1)$ .

Later on in this paper, when there is no ambiguity on the preliminary choice of  $p_i$  and of  $k_i$ , we will use eventually the shortened expression  $\#(c)$  for :

$$\#(c) = \#\{(cx,cy,\dots) \mid \forall p_i \in P, \forall k_i \in N, R(cx,cy,\dots) = c \bmod \prod p_i^{k_i}\} \quad (18)$$

The term "abundance factor" is also used on this occasion for cardinal  $\#(c)$ , these factors being natural numbers.

Let us have  $n$  the number of integers variables (type  $x$ ) and  $m$  the number of prime numbers variables (type  $y$ ). When the  $k_i$  are incremented, the number of classes increases in the presence of several variables. To reduce the term to a density, we divide the expression by the total number of classes. We call this the normalization operation.

Then :

$$\text{fan}(c, p_i) = p_i^{k_i} \cdot \frac{\#\{(x,y,\dots) \mid \forall p_i \in P, \forall k_i \in N, R(x,y,\dots) = c \bmod \prod p_i^{k_i}\}}{(p_i^{k_i})^n \cdot (\varphi(p_i^{k_i}))^m} \quad (19)$$

Multiplication by  $p_i^{k_i}$  brings back to an average value of 1 the  $\text{fan}(c, p_i)$  instances.

For the moment, the used earlier implication involvement (relation17) has a rather fuzzy meaning. It essentially says that if there are solutions to the global equation, they are reflected in the local equations. In other words, we return at this stage without major progress towards a problem of solutions existence. To go further, we will examine the right member of the implication and determine whether the arrow in the other direction is lawful and what may be its significance from the point of view of enumeration.

Before that, however, it is necessary to have related results based in particular on the Chinese theorem that we will discuss after the paragraph "available volume factor".

### 2.1.2 The available volume factor

This second ingredient is obtained as follows. Let us write again :

$$R(x,y,\dots) = c$$

Let us consider the affine space  $(x, y, \dots)$  landmarked by the axis  $x, y, \dots$  that is constructed as follows. The axis coordinates are integers. The coordinates are defined by the subscripts of  $x$  and  $y$ , that is for  $x$  an integer variable  $x_0 = 0, x_1 = 1, x_2 = 2, \dots$  and for  $y$  prime numbers variable  $y_0 = 2, y_1 = 3, y_2 = 5, y_3 = 7, y_4 = 11, \dots$  (according to specific need, subscripts and numbers can be also negative). The volume of the affine space is then equal to all solutions of  $R(x,y,\dots) = c$ ,  $c$  describing all (possibly negative) integers. For a given  $c$ , the number of solutions of  $R(x,y,\dots) \leq c$  is given by the volume of a "slice" of the space noted  $V(c)$ . For the nearby  $c+1$  target, the number of solutions is given by the nearby "slice"  $V(c+1)$ . If  $V(c)$  is a sufficiently regular function (such as a polynomial), the volume between two targets is then :

$$V'(c) \approx V(c+1) - V(c) \quad (20)$$

Note that asymptotically, we can use equality.

## 2.2 Theorem of Chinese remainder

The Chinese remainder theorem is a result of arithmetic dealing with the resolution of systems of congruencies. This result, initially established for  $\mathbb{Z}/n\mathbb{Z}$ , what suffices here, generalizes in ring theory. The Chinese origin is on the mathematician Qin Jiushao for a book published in 1247, but there is also a version dating from the 3rd century by Sun Zi, the Sunzi Suanjing [16].

### 2.2.1 Statement

Let us have  $m_1, m_2, \dots, m_r$  relative primes and  $m$  their product. For any succession of given integers  $x_1, x_2, \dots, x_r$ , there is a single integer  $x$  between 0 and  $m-1$  such as  $x = x_i \bmod m_i$  for  $i = 1$  to  $r$ .

In modern terms, this is written as : If  $m_1, m_2, \dots, m_r$  are relative primes,  $m = m_1 \cdot m_2 \cdot \dots \cdot m_r$ , then the ring  $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$  is isomorphic to the  $\mathbb{Z}/m\mathbb{Z}$  ring.

### 2.2.2 Application to enumerations

Let us have  $m_1$  et  $m_2$  two relative prime numbers. Let us have  $R(x_1, x_2, \dots)$  a polynomial expression with one or more variables. We do vary  $x_1, x_2, \dots$  from 0 to  $m_1-1$ , respectively from 0 to  $m_2-1, \dots$  and collect the number  $\#(cm)$ , respectively  $\#(cm_1)$ , respectively  $\#(cm_2)$  solutions  $(x_1, x_2, \dots)$  such as  $R(x_1, x_2, \dots) = c \bmod m$ .

Then

$$\#(cm) = \#(cm_1) \cdot \#(cm_2) \quad (21)$$

### Proof

The reader, somewhat unfamiliar with Chinese theorem, will find two examples in appendix 1 as illustrations.

The  $R(x_1, x_2, \dots)$  expression induces the values of  $c$  such as  $c = R(x_1, x_2, \dots)$  in the second column of the appendix standard table that can be written for any choice of  $m$ ,  $m_1$  and  $m_2$  and any polynomial expression. For the column of the modulo  $m_1$  values, the results of the  $m_1$ -th first lines are duplicated  $m_2$  times. One proceeds in the same way in the column corresponding to  $m_2$  with systematic permutations of subscripts 1 and 2. Then for a given target  $cm \bmod m$  (second column) is corresponding a distinct  $(cm_1, cm_2)$  modulo  $m_1$  and modulo  $m_2$  respectively (third and fourth columns). As  $m_1$  et  $m_2$  are relative primes and by the Chinese theorem, we have an equality between the "frequency"  $m/\#cm$  of  $cm$  and its "frequency of coincidence" with the previous couple  $(cm_1, cm_2)$  and is thus the product  $(m_1/\#cm_1) \cdot (m_2/\#cm_2)$ . As  $m = m_1 \cdot m_2$ , the said result follows.

For equations containing the prime numbers variables, we first make up a truth table (as in appendix 1) temporarily keeping integer variables. The transition to the new variables leads to a simple deletion of certain rows in this truth table without changing the remaining rows (see again the example of l'appendix 1. Thus the acquired result remains unchanged.

By induction, we then have with  $cx_i$  et  $cy_i$  the relevant classes corresponding to either integer variables or prime numbers variables ( $p_2 = 2, p_3 = 3, p_4 = 5, p_5 = 7, p_6 = 11 \dots$ ) :

$$\{\#(cx_1, \dots, cy_1, \dots) \setminus R(cx_1, \dots, cy_1, \dots) = c \bmod 2^{i^2} \dots p_k^{ik}\} = \prod_{m=2}^k \{\#(cx_1, \dots, cy_1, \dots) \setminus R(cx_1, \dots, cy_1, \dots) = c \bmod p_m^{im}\} \quad (22)$$

## 2.3 Related concepts indispensable to enumerations

### 2.3.1 Concept of stability (or stationarity)

We start with

$$\#\{(x, y, \dots) \setminus R(x, y, \dots) = c\} \Rightarrow \#\{(cx, cy, \dots) \setminus \forall p_i \in P, \forall k_i \in N, R(cx, cy, \dots) = c \bmod \prod p_i^{k_i}\} \quad (23)$$

So that according to the Chinese theorem

$$\#\{(x, y, \dots) \setminus R(x, y, \dots) = c\} \Rightarrow \prod_{p_i \in P} \#\{(cx, cy, \dots) \setminus \forall k_i \in N, R(cx, cy, \dots) = c \bmod p_i^{k_i}\} \quad (24)$$

The second member will only give relevant information if increasing  $k_i$  leads to a stability of the proportions between classes or if the trends of these proportions can be inferred at infinity.

The concept of stability is thus fundamental.

### 2.3.2 Information contained in local variables

A local variable is the projection of an infinite number of values on a finite set. To get back the global variable from the finite sets assumes therefore an infinite number of information, that is all the sequences  $p_i$  must be reviewed. However, even with all these data available, it is not sure that the initial information can be found completely or in a useful manner. We will therefore proceed by stage starting from the most basic cases.

## 2.4 One variable local-global enumeration

### 2.4.1 Generalities on monomials

The  $x^n$  monomials are the basic building blocks of a diophantine equation. Their behaviour towards the Hasse principle supports all the remainder. If they respond in a certain way to such principle, the said principle spreads in a natural way in any equation formed with these bricks. If they are not, we can predict failure in advance.

To enumerate the number of integer solutions of a unique variable diophantine equation, in peculiar  $z^n = c$ , is a priori easy. This is an opportunity that must be taken. Thus, we propose to find the link, in relation to enumeration, between the global equation  $z^n = c$  and the set of equations local  $z^n = c \bmod p^\delta$ , for a finite given  $c$  and  $z$  a variable either of whole numbers or of prime numbers.

If relevant results for one variable are highlighted and if literature proved results in three or more variables (Vinogradov for three prime numbers, Friendlander and Iwaniec for  $p = x^2 + y^4, \dots$ ) are deduced by the same construction, a bridge is thrown then to valid conjectures concerning two variables (twin primes, Goldbach problem...)

We shall seek an expression in the usual form of the asymptotic enumerations, that is the product of a singular series (Euler product) by a volume :

$$\#(c) = \left( \prod_{p_i=2}^{p=\infty} \frac{\#(c) \bmod p_i^{\delta_i}}{p_i^{a_i}} \right) \cdot V'(c) \quad (25)$$

Here  $\delta_i$  is chosen large enough to ensure the concept of stability, the constant  $a_i$ , properly chosen, ensures on his side what may called normalization and  $V'(c) \approx V(c) - V(c-1)$  is the available volume between neighbouring targets.

### Main objective

In what follows, we do need only a minimal information concerning the number of solutions of the equation diophantine  $z^n = c$ . That is, for a given  $n$ , this number is equal to zero if  $c \neq a^n$  and  $c \neq 0$ , is constant if  $c = a^n$  and  $a \neq 0$  (equal to 1 or 2 according to the parity of  $n$ ) and is equal to 1 for  $c = 0$ . This last assertion is questionable as we will see below. These numbers of solutions being thus determined, our goal is to find them back in with the help of the relation 25.

### 2.4.2 The example of x

The equation  $x = c$  has a unique solution for any  $c$  (integer or not).

Locally,  $x = c \bmod p$  (or  $\bmod p^k$ ) has a unique solution for any  $p$ . Thus, trivially, with  $V'(c) = x' = 1$  :

$$\#\{(x) \setminus x = c\} = \prod_{p_i \in P} \#\{cx \setminus cx = c \bmod p_i\} \cdot V'(c) = 1 \cdot 1 = 1 \quad (26)$$

This may seem so simple, but things are less trivial to the higher degrees.

### 2.4.3 The examples of $x^2$ and $x^4$

Dealing with the general case further, we are concerned for the moment only by the numerical examples in order to familiarizes with the concepts.

We begin with  $x^2$ . We seek the evolution of the values of  $\#(c) \bmod p^\delta$  with  $\delta$ , then of  $V'(c)$  which is deduced from  $c = x^2$ , that is  $x = c^{1/2}$ , and so  $V'(c) = x' = 1/2 \cdot c^{-1/2}$ . The numerical example taking some place, we have leaved it in appendix 3. We observe that the problem is actually solved for  $c = 1$  to 64 targets by using the formula :

$$\#(c) = V'(c) \cdot \prod_{p=2}^{p=7} \frac{\#(c) \bmod p^9}{2} \quad (27)$$

In appendix 3, we have given a somewhat broader numerical table with a review of the cardinals for a range of sequences  $p = 2$  to 29 for  $\delta < 6$  and  $p = 2$  to 7 for  $6 \leq \delta \leq 9$ . When subsequent sequences are examined, the multiplicative ratio is  $2/2 = 1$  and does not alter the results for each target. Of course, when  $c$  is greater than 64, the range of  $p$  sequences and of powers  $\delta$  is to extend. On the range of examples on display, we see that we arrive for a right member to a cardinal of 2 when  $c$  is actually square and to a cardinal of 0 otherwise, which corresponds to the actual number of solutions. Note however that the result in  $c = 0$  does not coincide with such a formula if we consider having only a single solution.

We did the same with the example of the monomial  $x^4$  we present below. There, we have formally  $c = x^4$ , so that  $x = c^{1/4}$  and  $V'(c) = x' = 1/4 \cdot c^{-3/4} = 1/(4 \cdot x^3)$ .

Table (3)

x	1	2	3	4	/	/	/	/	/
p \ c = x <sup>4</sup>	1	16	81	256	2	3	4	5	6
2	8	64	8	512	0	0	0	0	0
3	2	2	54	2	0	0	2	0	0
5	4	4	4	4	0	0	0	0	4
7	2	2	2	2	2	0	2	0	0
11	2	2	2	2	0	2	2	2	0
13	4	4	4	4	0	4	0	0	0
17	4	4	4	4	0	0	4	0	0
19	2	2	2	2	0	0	2	2	2
23	2	2	2	2	2	2	2	0	2
29	4	4	4	4	0	0	0	0	0
31	2	2	2	2	2	0	2	2	0
Product	131072	1048576	3538944	8388608	0	0	0	0	0
Product/#(1)	1	8	27	64					
4.adjust = 1/V'(c) = 4.x <sup>3</sup>	4	32	108	256	/	/	/	/	/

x	1	2	3	4	/	/	/	/	/
p	1	16	81	256	2	3	4	5	6
Product/#(1)/ajust	1	1	1	1					

The results in the red framework are equal to  $\#(c) \bmod p^\delta$  with a large enough  $\delta$  (up to get a constant term). We check again that the evaluation method sieves targets without solutions giving a zero value and that the result of the targets with solutions can be put in the form  $\text{fan}(c).V'(c)$  since the last line is a constant (equal to 1). To achieve this result, we note that for the case where  $c = x^4$ , the terms are the same for one target to another except when  $p$  sequences are not relative primes with the power of  $x$  (here  $p = 2$  and  $n = 4$ ) or with targets  $c$  ( $p = 3$  and  $c = 3$ ).

We now consider the general case taking into account any target, using sequences 2 to infinite, and this to any power  $n$ . We find again the remark concerning the sequences  $p$ , the power of  $x$  and targets  $c$ .

## 2.4.4 The example of $x^n$

### 2.4.4.1 Singular series

Let us have to solve

$$x^n = c \bmod p^\delta$$

We note systematically by  $g$ , later in the text, one of the primitive roots of the prime number  $p$ .

#### 2.4.4.1.1 Case $p$ odd

Let us have  $d_i = (n, \Phi(\delta-i))$  where  $\Phi(\delta-i) = p^{\delta-i-1} \cdot (p-1)$  and  $\delta n = \text{int}((\delta-1)/n)$  the integer part of  $(\delta-1)/n$ .

Nous pouvons alors dresser le tableau suivant :

We can then compile the following table :

Table (4)

x	$c = x^n \bmod p^\delta$	$\#(c)$	$\#(\text{variant of } c)$	Types
0	0	$p^{\delta-\delta n-1}$	1	Supernumerary cardinals
$p^{\delta-1} \cdot \{g^0, g^1, \dots, g^{\Phi(1)-1}\}$ $p^{\delta-2} \cdot \{g^0, g^1, \dots, g^{\Phi(2)-1}\}$ ...				
$p^{\delta n+1} \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-(\delta n+1))-1}\}$				
$p^{\delta n} \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-\delta n)-1}\}$	$p^{\delta n} \cdot \{g^{0.d[\delta n]}, g^{1.d[\delta n]}, \dots, g^{(\Phi(\delta-\delta n)/d[\delta n]-1).d[\delta n]}\}$	$d_{\delta n, n} \cdot p^{\delta n \cdot (n-1)}$	$\Phi(\delta-\delta n, n)/d_{\delta n, n}$	
...	...	...	...	
$p^i \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-i)-1}\}$	$p^{i, n} \cdot \{g^{0.d[i, n]}, g^{1.d[i, n]}, \dots, g^{(\Phi(\delta-i)/d[i, n]-1).d[i, n]}\}$	$d_{i, n} \cdot p^{i \cdot (n-1)}$	$\Phi(\delta-i, n)/d_{i, n}$	
...	...	...	...	Std
$p^1 \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-1)-1}\}$	$p^n \cdot \{g^{0.d[n]}, g^{1.d[n]}, \dots, g^{(\Phi(\delta-n)/d[n]-1).d[n]}\}$	$d_n \cdot p^{(n-1)}$	$\Phi(\delta-n)/d_n$	
$p^0 \cdot \{g^0, g^1, \dots, g^{\Phi(\delta)-1}\}$	$p^0 \cdot \{g^{0.d[0]}, g^{1.d[0]}, \dots, g^{(\Phi(\delta)/d[0]-1).d[0]}\}$	$d_0$	$\Phi(\delta)/d_0$	

We have adopted above the writing convention  $[i]$  which means that integers  $i$  are subscripts. Moreover  $p^i \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-i)-1}\}$  is to be read  $\{p^i \cdot g^0, p^i \cdot g^1, \dots, p^i \cdot g^{\Phi(\delta-i)-1}\}$ .

We recall also that  $\#(c)$  is the number of solutions corresponding to a given target  $c$ . For example, for the first line (except the title line),  $c = 0 \bmod p^\delta$  when  $x$  takes one of the first column values and we have  $1 + \Phi(1) + \Phi(2) + \dots + \Phi(\delta-(\delta n+1)) = 1 + p^0 \cdot (p-1) + p^1 \cdot (p-1) + \dots + p^{\delta-(\delta n+1)-1} \cdot (p-1) = p^{\delta-\delta n-1}$  distinct values of  $x$ .

Thus, equation  $x^n = c \bmod p^\delta$  admits  $d_{i, n} \cdot p^{i \cdot (n-1)}$  solutions for  $c$  likewise  $p^{i, n} \cdot g^{i.d[i, n]}$  and  $i \leq \delta n$ , admits  $p^{\delta-\delta n-1}$  solutions for  $c = 0$ , otherwise there is no solution.

### Proof

Replacing  $x$  in  $x^n \bmod p^\delta$ , the reader verifies immediately column 2 of the preceding table. All numbers in the first column are distinct when  $g$  is a primitive root of  $p$  (by definition of a primitive root). It is necessary and it suffices then to show that all the cases  $x = 0$  to  $p^{\delta-1}$  are given in the first column. Indeed, counting from top to bottom, we have  $1 + \Phi(1) + \Phi(2) + \dots + \Phi(\delta-(\delta n+1)) + \Phi(\delta-\delta n) + \dots + \Phi(\delta-i) + \dots + \Phi(\delta-1) + \Phi(\delta) = p^{\delta-\delta n-1} + p^{\delta-\delta n-1} \cdot (-1+p) + \dots + p^{\delta-i-1} \cdot (-1+p) + \dots + p^{\delta-1} \cdot (-1+p) = p^{\delta-\delta n-1} - p^{\delta-\delta n-1} + p^{\delta-\delta n} - p^{\delta-\delta n} + \dots + p^{\delta-i-1} - p^{\delta-i-1} + \dots + p^{\delta-1} - p^{\delta-1} + p^\delta = p^\delta$ , then the result.

Evaluation of the set  $\{g^{0.d[i, n]}, g^{1.d[i, n]}, \dots, g^{(\Phi(\delta-i)/d[i, n]-1).d[i, n]}\}$

There are  $\Phi(\delta)/d_0$  variants (distinct numbers).

The whole set is described by :

$\{g^0, g^n, g^{2n}, \dots, g^{\Phi(\delta-i, n)/d[i, n]-1, n} \cdot g^{\Phi(\delta-i)-1}\} + m \cdot p^i$  with  $m = 0$  to  $\Phi(\delta-i, n)/d_{i, n}-1$ .

In peculiar, for  $i = 1$

$\{g^{0.d[0]}, g^{1.d[0]}, \dots, g^{\Phi(\delta) \cdot g^{0.d[0]}, g^{1.d[0]}, \dots}\} + i \cdot p$  with  $m = 0$  to  $\Phi(\delta-\delta n)$ .

## Terminology

It will be useful later in this article to distinguish some of the  $c$  target and their factors of abundance  $\#(c)$ . We call them "supernumerary cardinals". For the monomials, they identify to objects called that way in table (4).

### 2.4.4.1.2 Case $p$ even ( $p=2$ )

Here, there is no primitive root but we can take the generating couple  $(5, -5)$ .

Let us have  $d_i = (n, \Phi(\delta-i)/2)$  where  $\Phi(\delta-i) = 2^{\delta-i-1}$  and  $\delta n = \text{int}((\delta-1)/n)$ .

We can draw again the table of residues cardinals as in the case of odd sequences :

Table (5)

x	$x^n = c \bmod 2^\delta$	$\#(c)$	Types
$0$ $2^{\delta-1} \cdot \{5^0\}$ $2^{\delta-2} \cdot \{5^0, 5^1, \dots, 5^{\Phi(2)-1}\}$ $2^{\delta-2} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(2)-1}\}$ $\dots$ $2^{\delta n+1} \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-(\delta n+1))-1}\}$ $2^{\delta n+1} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-(\delta n+1))-1}\}$	$0$	$2^{\delta-\delta n-1}$	Supernumerary cardinals
$2^{\delta n} \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-\delta n)-1}\}$ $2^{\delta n} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-\delta n)-1}\}$	$2^{\delta n, n} \cdot \{5^0, 5^1, \dots, 5^{(\Phi(\delta-\delta n)/d[\delta n]-1)}\}$ $2^{\delta n, n} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{(\Phi(\delta-\delta n)/d[\delta n]-1)}\}$	$2^{\delta-\delta n-1}$	
$\dots$	$\dots$	$\dots$	
$2^i \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-i)-1}\}$ $2^i \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-i)-1}\}$	$2^{i, n} \cdot \{5^{0, d[i, n]}, 5^{1, d[i, n]}, \dots, 5^{(\Phi(\delta-i)/d[i, n]-1), d[i, n]}\}$ $2^{i, n} \cdot \{(-5)^{0, d[i, n]}, (-5)^{1, d[i, n]}, \dots, (-5)^{(\Phi(\delta-i)/d[i, n]-1), d[i, n]}\}$	$d_{i, n} \cdot 2^{i, (n-1)}$	
$\dots$	$\dots$	$\dots$	
$2^1 \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-1)-1}\}$ $2^1 \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-1)-1}\}$	$2^n \cdot \{5^{0, d[n]}, 5^{1, d[n]}, \dots, 5^{(\Phi(\delta-n)/d[n]-1), d[n]}\}$ $2^n \cdot \{(-5)^{0, d[n]}, (-5)^{1, d[n]}, \dots, (-5)^{(\Phi(\delta-n)/d[n]-1), d[n]}\}$	$d_n \cdot 2^{(n-1)}$	
$2^0 \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta)-1}\}$ $2^0 \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta)-1}\}$	$2^0 \cdot \{5^{0, d[0]}, 5^{1, d[0]}, \dots, 5^{(\Phi(\delta)/d[0]-1), d[0]}\}$ $2^0 \cdot \{(-5)^{0, d[0]}, (-5)^{1, d[0]}, \dots, (-5)^{(\Phi(\delta)/d[0]-1), d[0]}\}$	$d_0$	

Again, the writing convention  $[i]$  means that integers  $i$  are subscripts.

The equation  $x^n = c \bmod 2^\delta$  admits  $d_{i, n} \cdot 2^{i, (n-1)}$  solutions for  $c$  likewise  $2^{i, n} \cdot 5^{i, d[i, n]}$  et  $i \leq \delta n$ , admits  $2^{\delta-\delta n-1}$  solutions for  $c = 0$ , admits  $2^{\delta-\delta n-1}$  solutions for  $c = 2^{\delta n, n}$ , otherwise, it has no solution.

Let us have  $c$  a residue mod  $2^\delta$  et let us have  $m$  the multiplicity of factor 2 in  $n$ . We get then the following table (the values of column  $x$  are verified by substitution in  $x^n = c \bmod 2^\delta$ ) :

Table (6)

x	conditions on $k, i$ et $n$	c	$\#\{c\}$	$\#\{\text{variants of } c\}$
$2^{\delta n} \cdot (2k)$	$k = 0, 1, \dots, 2^{\delta-\delta n-1}-1$	0	$2^{\delta-\delta n-1}$	1
$2^{\delta n} \cdot (1+2k)$	$k = 0, 1, \dots, 2^{\delta-\delta n-1}-1$	$2^{\delta n, n}$	$2^{\delta-\delta n-1}$	1
$2^i \cdot (1+2 \cdot (\#\{1\}) \cdot k)^{1/n}$ $+ 2^{\delta-i, (n-1)} / (\#\{1\}) k$	$k = 0, 1, \dots, 2^{\delta-1-i, n} / (\#\{1\}) - 1$ $i = 0 \text{ to } \delta n - 1$ $k' = 0 \text{ to } 2^{i, (n-1)} \cdot (\#\{1\}) - 1$	$2^{i, n} (1+2 \cdot \#\{1\} \cdot k)$	$2^{1, (n-1)} \cdot (\#\{1\})$	$2^{\delta-1-i, n} / (\#\{1\})$

The particularity of case  $p = 2$  is on the second data line of the preceding table ( $\#\{2^{\delta n, n}\} = 2^{\delta-\delta n-1}$ ) which does not exist in the odd  $p$  cases.

To summarize, in a slightly different manner than above, the equation  $x^n = c \bmod 2^\delta$  admits  $2^{i, (n-1)} \cdot (\#\{1\})$  solutions for  $c$  different from 0 and  $2^{\delta n, n}$ , admits  $2^{\delta-\delta n-1}$  solutions for  $c = 0$  and  $c = 2^{\delta n, n}$ , otherwise it has no solution.

## Proof

By replacing  $x$  in  $x^n \bmod 2^\delta$ , the reader finds immediately the values for each target  $c$ . All numbers in the first column are distinct. Making up then the sum  $\sum \#\{c\} \cdot \#\{\text{variants of } c\}$ , we get  $2^\delta$ , which proves that all solutions are described.

### 2.4.4.1.3 Number of solutions of $x^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}$

We shall see in the next paragraph the basis for distinguishing the  $c = 0$  and  $c \neq 0$  cases.

## Case $c \neq 0, c \neq x^n$

We use the Chinese theorem :

$$\#\{x^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = \#\{x^n = c \bmod 2^\delta\} \cdot \prod \#\{x^n = c \bmod p_i^{\delta_i}\} \quad (28)$$

As  $c \neq x^n$ , one at least of the terms is zero (and indeed an infinite number of them if all sequences  $p_i$  are reviewed), so the product is null.

$$\#\{x^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = 0 \quad (29)$$

Case  $c \neq 0, c = x^n$

We use again the Chinese theorem :

$$\#\{x^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = \#\{x^n = c \bmod 2^\delta\} \cdot \prod \#\{x^n = c \bmod p_i^{\delta_i}\}$$

The number of solutions of  $x^n = c \bmod p_i^{\delta_i}$  is given by the tables presented in paragraphs 2.4.4.1.1 et 2.4.4.1.2. If  $c = (2^r \cdot p_1^{k_1} \cdot p_2^{k_2} \dots p_j^{k_j})^n$ , the last index is here  $j$  (and not  $i$ ), we have  $d_{k_i, n} \cdot p_i^{k_i \cdot (n-1)}$  classes of solutions each time that  $p_i$  is equal to one of the numbers  $p_1, p_2, \dots$  or  $p_j$  (with  $d_{k_i, n} = 1$  in the case of factor 2), otherwise we have  $d_0$  classes of solutions when  $p_i$  is different from the set of the numbers  $p_1, p_2, \dots$  and  $p_j$ .

Thus :

$$1 = \frac{\#\{x^n = c \bmod p_1^{\delta_1}\}}{d_{k_1, n} \cdot p_1^{k_1 \cdot (n-1)}} = \frac{\#\{x^n = c \bmod p_2^{\delta_2}\}}{d_{k_2, n} \cdot p_2^{k_2 \cdot (n-1)}} = \dots = \frac{\#\{x^n = c \bmod p_j^{\delta_j}\}}{d_{k_j, n} \cdot p_j^{k_j \cdot (n-1)}} \quad (30)$$

and

$$1 = \frac{\#\{x^n = c \bmod p_i^{\delta_i}\}}{d_0} \quad (31)$$

It is necessary, further on, to review all sequences  $p_i$ . However, only sequences that divide  $c$  have a form of the type (30). All other ones are of the type (31).

Let us interest then the  $d_{k, n}$ . We have first  $d_0 = \#\{x^n = 1 \bmod p_i^{\delta_i}\}$ , still referring to the same tables, which is a constant from a higher  $\delta_i$  that a certain  $\delta_s$ . This large enough  $\delta_i$  hypothesis is capital and is adopted systematically in the following text. We simplify also the writing of  $\#\{x^n = 1 \bmod p_i^{\delta_i}\}$  as  $\#\{1\}$  when no confusion results. We then have :

$$d_{k, n} = (n, \Phi(\delta_i - k \cdot n)) = (n, p_i^{\delta_i - k \cdot n - 1} \cdot (p_i - 1))$$

and in peculiar

$$d_0 = (n, p_i^{\delta_i - 1} \cdot (p_i - 1))$$

It is clear that, for  $\delta_i$  sufficient large instances, on one side  $p^k$ ,  $k$  any positive integer, and on the other side all the factors of  $(p-1)$  are taken into account in the common factor operation  $(n, \dots)$  and this factor cannot therefore evolve. Thus we have

$$d_{k, n} = d_0$$

so that still adding its effective value

$$d_{k, n} = d_0 = \#\{x^n = 1 \bmod p_i^{\delta_i}\} = \#\{1\}$$

Thus for large enough  $\delta_i$ , the factors  $d_{k, n}$  are constants (thus the local stability).

Then :

$$\frac{\#\{x^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}\}}{\#\{1\}^{j+1}} = 2^{r \cdot (n-1)} \cdot p_1^{k_1 \cdot (n-1)} \cdot p_2^{k_2 \cdot (n-1)} \dots p_j^{k_j \cdot (n-1)} = c^{(n-1)/n} \quad (32)$$

Case  $c = 0$

$$\#\{x^n = 0 \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = \#\{x^n = 0 \bmod 2^\delta\} \cdot \prod \#\{x^n = 0 \bmod p_i^{\delta_i}\} = 2^{\delta-1} \cdot \prod p_i^{\delta_i} \quad (33)$$

#### 2.4.4.2 Function volume and cardinal product

As  $x^n = c$ , it follows  $x = c^{1/n}$ , so that also :

$$V'(c) = x'(c) = (1/n) \cdot c^{1/n-1} = (1/n) \cdot c^{-(n-1)/n}$$

We assume the generality of the use of this formula even when it does not make obvious sense.

Case  $c \neq 0, c \neq x^n$

The singular series is null.

We have therefore :

$$\#\{x^n = c\} = 0 \cdot V'(c) = 0 \quad (34)$$

This is the sought result.

Case  $c \neq 0, c = x^n$

We have

$$\#\{x^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = 2^{r.(n-1)} \cdot p^{k1.(n-1)} \cdot p^{k2.(n-1)} \dots p^{kj.(n-1)} = c^{(n-1)/n} \cdot \#\{1\}^{j+1}$$

Then

$$\#\{x^n = c\} = c^{(n-1)/n} \cdot \#\{1\}^{j+1} \cdot V'(c) = c^{(n-1)/n} \cdot \#\{1\}^{j+1} \cdot (1/n) \cdot c^{1/n-1} = \#\{1\}^{j+1}/n$$

It is the search result as  $(1/n) \cdot \#\{1\}^{j+1}$  is a constant when  $c$  is given in advance.

#### Case $c = 0$ : Obstruction or indetermination

$$\#\{x^n = 0 \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = 2^{\delta-1} \cdot \prod p_i^{\delta_i}$$

Le product, bearing on all sequences from 2 to  $\infty$ , diverges.

Le volume associated to target 0 is ( $n > 1$ ) :

$$V'(c \rightarrow 0) = (1/n) \cdot c^{1/n-1} \rightarrow \infty \quad (35)$$

Then, assuming the product :

$$\#\{x^n \rightarrow 0\} = \text{singular series} \cdot \text{volume} \rightarrow \infty \quad (36)$$

However equation  $x^n = 0$  has a unique solution  $x = 0$ . The results are not matching.

We are facing an "obstruction". It's the unique exception when we solve equation  $x^n = c$ ,  $c$  parameter of the global-local method.

However, for any positive integer  $m$ ,

$$0^m = 0 \quad (37)$$

Therefore the multiplicity of 0 is itself quite arbitrary. What makes somewhat acceptable the observed exception.

We can thus replace here the notion of obstruction in favour of the concept of indetermination.

We can also support this indeterminacy noting that the calculation of  $V'(c)$  in (35) is quite cavalier and has no obvious mathematical sense at  $c = 0$  because  $V(c) = c^{1/n}$  ( $n > 1$ ) is not differentiable at this point.

We will return to the proper way to deal with this case at the end of the article at paragraph 2.6.2.3.

#### **2.4.5 Second degree polynomial equations**

Let us have the diophantine equation ( $u$  and  $v$  non-null)

$$c = u \cdot x^2 + v \cdot x$$

The solutions to this equation are given by  $x = (-v + (v^2 + 4uc)^{1/2})/2$  in the complex plane. In  $\mathbb{Z}$ , the existence of solutions is related to the discriminant  $\text{Disc} = v^2 + 4u \cdot c$  which must be a square of an integer for solutions to exist, and in this case, we have 2 solutions (double root if null discriminant).

We track again this remarkable point in what follows.

#### Function volume

When  $x$  increases,  $c = u \cdot x^2 + v \cdot x \approx u \cdot x^2$ , thus  $x = V(c) \approx (c/u)^{1/2}$ . Then :

$$V'(c) \approx (1/2) \cdot u^{-1/2} \cdot (c)^{-1/2} \quad (c \neq 0) \quad (38)$$

Strictly  $c$  must be different from zero.

The factor  $(1/2) \cdot u^{-1/2}$ , without impact on equiprobability, can eventually be forgotten.)

#### Singular series

Let us have to solve the local equation

$$c = u \cdot x^2 + v \cdot x \bmod p^\delta$$

$$p > 2$$

Single root :

Table (7)

Conditions			#(c)
	$u = 0 \bmod p$	$u \neq 0 \bmod p^\delta$	1
$k \geq \delta c$	$\text{Disc} = 0 \bmod p^k$		Case dependent
$k < \delta c$	$\text{Disc} = g^0 \cdot g^{2n} \cdot p^{2i}$	$\text{Disc} \neq 0 \bmod p^{2i+1}$	$2 \cdot p^i$
	$\text{Disc} = g^1 \cdot g^{2n} \cdot p^{2i}$	$\text{Disc} \neq 0 \bmod p^{2i+1}$	0
	$\text{Disc} = 0 \bmod p^{2i}$	$\text{Disc} \neq 0 \bmod p^{2i+1}$	0
	$\text{Disc} = 0 \bmod p^{2i-1}$	$\text{Disc} \neq 0 \bmod p^{2i}$	0

We meet again with the importance of square discriminant in the computation of the singular series. This point by itself is already remarkable.

Proof

The integer 2 is invertible modulo  $p^\delta$  and let us have  $k2$  as such  $g^{k2} = 2^{-1}$  modulo  $p^\delta$ .

Let us have  $x$  a solution of  $c = u \cdot x^2 + v \cdot x \bmod p^\delta$ , that is such as  $u \cdot x^2 + v \cdot x = c + k \cdot p^\delta$  for some integer  $k$ .

Then formally  $x = (-v \pm (v^2 + 4 \cdot u \cdot c + 4k \cdot u \cdot p^\delta)^{1/2}) / 2$ .

If  $\text{Disc} = 0 \bmod p^{2i}$  and  $\text{Disc} \neq 0 \bmod p^{2i+1}$ , then  $v^2 + 4 \cdot u \cdot c = m \cdot p^{2i}$  for a given integer  $m$  with  $m \neq 0 \bmod p$ . We have then  $x = (-v \pm (m \cdot p^{2i} + 4k \cdot u \cdot p^\delta)^{1/2}) / 2$ , so that

$$x = -v \cdot g^{k2} \pm p^i \cdot g^{k2} \cdot (m + 4k \cdot u \cdot p^{\delta-2i})^{1/2} \quad (39)$$

For  $p \neq 2$  and  $u \neq 0 \bmod p$ , the set  $A = \{m + 4k \cdot u \cdot p^{\delta-2i} \bmod p^\delta, k = 0 \text{ to } p^{\delta-1} - 1\}$ , is equal to the set  $B = \{m + k \cdot p^{\delta-2i}, k = 0 \text{ to } p^{\delta-2i} - 1\}$  with multiplicity  $p^{2i}$ . As  $m \neq 0 \bmod p$ , there is a primitive root  $g$  of  $p$  and an integer  $s$  such as  $g^s \bmod p^\delta$ .

If  $s$  is even then, for any  $k$ , there exists an integer  $ks$  as  $m + k \cdot p^{\delta-2i} = g^{2ks} \bmod p^\delta$ . The integers  $s/2$  and  $ks$  are all distinct, otherwise their squares would be equal, which would be in contradiction with the distinct elements of  $B$ . Thus the extraction of roots square  $b$  provides  $p^{\delta-2i}$  distinct numbers distant of  $p^{\delta-2i}$ . What is important here is not the cardinal of the distinct numbers but the interval  $p^{\delta-2i}$  between these numbers. We inject again the found values in the relation (39) which gives  $x = -v \cdot g^{k2} \pm p^i \cdot g^{k2} \cdot (g^s + r \cdot p^{\delta-2i})$ ,  $r = 0$  to  $p^{\delta-2i} - 1$ . So that also  $x = -v \cdot g^{k2} \pm p^i \cdot g^{k2+s} + r \cdot g^{k2} \cdot p^{\delta-i}$ ,  $r = 0$  à  $p^{\delta-2i} - 1$ . Modulo  $p^\delta$ , we have redundant values that we eliminate :

$$x = -v \cdot g^{k2} \pm p^i \cdot g^{k2+s} + r \cdot g^{k2} \cdot p^{\delta-i}, r = 0 \text{ to } p^i - 1 \quad (40)$$

We have therefore two alternatives :

$i \geq \delta$ or $\delta = 2i$	$p^i$
$i < \delta$ and $\delta \neq 2i$	$2 \cdot p^i$

On account of the search for stability,  $\delta$  is large enough and thus only the second alternative does present in fact

If  $s$  is odd,  $m + k \cdot p = g^s + k \cdot p$  admits no square root and the case  $\delta - 2i = 0$  being dismissed for imperative of stability, there is no solutions to the equation under consideration.

If  $\text{Disc} = 0 \bmod p^{2i+1}$  and  $\text{Disc} \neq 0 \bmod p^{2(i+1)}$ , then  $v^2 + 4 \cdot u \cdot c = p \cdot m \cdot p^{2i}$ . The factor  $p$  is distinct from any number  $g^n$ . It is thus impossible to extract a root square of the discriminant and the local equation has no solution.

Double root :

When the selected equation in the form  $u \cdot (z - a)^2 = c$ ,  $z$  being the indeterminate, we make the change of variable  $x = z - a$ . If  $u \neq 0 \bmod p$ ,  $u$  has a reverse and there is a bijection between  $c$  and  $u \cdot c$  modulo  $p^\delta$ . The equation, as far as enumeration is concerned, is then the same as the base case :

$$c = x^2$$

$$p = 2$$

This case is to deal with apart because of the absence of primitive root. However, the conclusions remain the same using the two roots 5 and -5. For not overloading the text with this digression, we go ahead.

Table discussion

Let us have first  $u = 0 \bmod p$ . Then  $\#(c)$  is constant and can be ignored thanks to equiprobability.

Let us have then a given target  $c$  such as, for all  $x$ ,  $P(x) \neq c$ . Then, there is a  $p$  such as  $v^2 + 4 \cdot u \cdot c = m \cdot p^{2i}$  where  $m$  is not a

square (a case on two on average). Therefore, many factors of the singular series corresponding to  $c$  are null and singular series of target  $c$  is zero.

Finally, consider a target  $c$  such as  $P(x) = c$ . Then trivially, we have always locally at least one solution to the equation  $P(x) = c \pmod{p^\delta}$  (for all  $p$  and  $\delta$ ). We seek then  $i$  such that  $\text{Disc} = 0 \pmod{p^{2i}}$  and  $\text{Disc} \neq 0 \pmod{p^{2i+1}}$  which exists necessarily. Returning to the previous table, we then  $2p^i$  solutions to the local equation at sequence  $p$ . The target  $c$  being fixed, the discriminant  $\text{Disc}$  is a constant, the sequence  $p$  variant, we have 2 solutions to the local equations except for a finite number of cases where  $p$  coincides with possible squares of  $\text{Disc}$ . Thus, when  $c$  increases,  $\text{Disc}$  increases linearly in  $c$  (with multiplicative factor  $4u$ ), the number of local solutions in these cases increases as  $\text{Disc}^{1/2}$  and therefore as  $r.c^{1/2}$ ,  $r$  a constant. For the other sequences, we take  $2/2 = 1$  solution to avoid divergence of singular series while retaining equiprobability.

Once again, for given  $p$ , the degree of stability of target  $c$  is not the same for each target  $c$ . We write this number  $\delta c$ . When enumerating modulo  $p^\delta$ , it is imperative to be in conditions like  $\delta > \delta c$  in such a way to get the good local value of  $\#(c) = \#(x \text{ as } c = P(x) \pmod{p^\delta}, x = 0 \text{ à } p^\delta - 1)$ .

The reader interested in a numerical, around the origin, verification will take care to offset it by using not the polynomial  $P(x) = u.x^2 + v.x$  but  $P(x) = u.x^2 + v.x + \text{int}(v^2/4u)$  and will use the generic equation :

$$P(x) = u.x^2 + v.x + \text{int}(v^2/4u) = c$$

## Global enumeration

Let us come back to the product

$$\#(c) \approx \text{singular series} \times \text{volume} \approx r.c^{1/2} \cdot (1/2) \cdot u^{-1/2} \cdot (c)^{-1/2} \approx (1/2) \cdot r \cdot u^{-1/2} \quad (\text{for } c \neq 0) \quad (41)$$

The result is therefore a constant at any point  $c \neq 0$ .

At  $c = 0$ , the value is indeterminate and we may intend to extend by continuity.

Thus, the global-local count is feasible without ambiguity for any equation of second degree.

## Theorem

There is no "obstructions" to the global-local count for second degree equations except possibly at a single origin point where indetermination can be remove by continuity.

### 2.4.6 Third degree polynomial equations

#### 2.4.6.1 Exposition of the general context

The previous theorem recalls and confirms the Hensel lemma which claims the absence of obstructions for equations of the second degree in terms of existence of solutions (part I context).

Beyond this degree 2, "troubles" are reckoned if we refer to the mathematical literature (since the famous lemma stops at degree 2). We have seen that as long as we confine ourselves to the monomials of degree 3, contrary events reduce to the target  $c = 0$ . For polynomials, this may be quite another thing that we address here.

Let us go back first to the numerical example of the monomial with equation  $x^3 - c = 0 \pmod{p^\delta}$ .

Table (8)

p	2	3	5	7	11	13	17	19
$\delta$	19	11	8	5	3	3	3	3
$p^\delta$	524288	177147	390625	16807	1331	2197	4913	6859
c	#(c)							
0	4096	2187	3125	343	121	169	289	361
1	1	3	1	3	1	3	1	3
8	4	3	1	3	1	3	1	3
27	1	27	1	3	1	3	1	3
64	16	3	1	3	1	3	1	3
125	1	3	25	3	1	3	1	3
216	4	27	1	3	1	3	1	3
343	1	3	1	147	1	3	1	3
512	64	3	1	3	1	3	1	3
729	1	243	1	3	1	3	1	3
1000	4	3	25	3	1	3	1	3
10648	4	3	1	3	121	3	1	3
32768	1024	3	1	3	1	3	1	3

p	2	3	5	7	11	13	17	19
$\delta$	19	11	8	5	3	3	3	3
$p^\circ$	524288	177147	390625	16807	1331	2197	4913	6859
c	#(c)							
74088	4	27	1	147	1	3	1	3

In this table, we kept only in the first column of the table the c values that are cubes. For any other c, there is at least one sequence (and indeed an infinity) for which #(c) shall be null and the product  $\prod \#(c)$  thus equal to zero.

We find a vertical alignment of cardinals equal to 3 to comply with the general case of monomials studied above. According to the concept of equiprobability modulo  $p^\delta$  widely developed above, it is equivalent to divide by 3 these columns, (the interest being that the infinite product versus lines do no more diverge more and can be compared between themselves) :

Table (9)  
(derived from the previous by abuse of writing)

p	2	3	5	7	11	13	17	19	
$\Delta$	19	11	8	5	3	3	3	3	
$p^\circ$	524288	177147	390625	16807	1331	2197	4913	6859	
c	#(c)								$(\prod \#(c))^{3/2}$
0	4096	729	3125	114,33	121	56,3	289	120,33	$\rightarrow \infty$
1	1	1	1	1	1	1	1	1	1
8	4	1	1	1	1	1	1	1	8
27	1	9	1	1	1	1	1	1	27
64	16	1	1	1	1	1	1	1	64
125	1	1	25	1	1	1	1	1	125
216	4	9	1	1	1	1	1	1	216
343	1	1	1	49	1	1	1	1	343
512	64	1	1	1	1	1	1	1	512
729	1	81	1	1	1	1	1	1	729
1000	4	1	25	1	1	1	1	1	1000
10648	4	1	1	1	121	1	1	1	10648
32768	1024	1	1	1	1	1	1	1	32768
74088	4	9	1	49	1	1	1	1	74088

As we have seen above (relation 32), we get a constant ratio (reduced to 1 here) between the value of the target c and the product  $(\prod \#(c))^{n/(n-1)}$ .

By an example, let us then compare the situation of a third-degree polynomial to the monomial of even degree. We choose :

$$P(x) = x^3 + x^2 + x - c$$

We get to this equation the following table :

Table (10)

p	2	3	5	7	11	13	17	19
$\delta$	9	10	3	3	5	3	3	5
$p^\circ$	512	59049	125	343	161051	2197	4913	2476099
c	#(c)							
0	1	1	1	3	1	3	1	3
3	2	7	1	1	3	1	3	3
14	1	1	3	3	3	1	35	1
39	2	1	3	1	1	3	35	1
84	1	7	3	3	1	1	3	39
155	2	1	1	1	1	3	1	3
258	1	1	1	1	243	1	3	1
399	2	163	3	3	3	1	1	3
584	1	1	3	1	23	3	1	39
819	2	1	3	3	1	3	3	1
1110	1	7	1	1	1	1	1	1
1463	2	1	1	3	1	1	1	3
1884	1	1	3	1	3	3	1	3
2379	2	7	3	1	3	3	3	1
2954	1	1	3	3	1	1	1	1
3615	2	1	1	1	1	1	1	1
4368	1	19	1	3	1	3	3	1
5219	2	1	3	1	23	1	1	1

p	2	3	5	7	11	13	17	19
$\delta$	9	10	3	3	5	3	3	5
$p^0$	512	59049	125	343	161051	2197	4913	2476099
c	#(c)							
6174	1	1	3	3	3	3	3	1
7239	2	7	3	1	23	1	35	3
8420	1	1	1	1	1	1	35	3
9723	2	7	1	3	1	3	3	1
11154	1	7	3	1	1	3	1	1
12719	2	1	3	3	3	1	3	39
14424	1	1	3	1	3	1	1	3
16275	2	19	1	3	1	3	1	1
18278	1	1	1	1	1	3	3	3
20439	2	1	3	1	1	1	1	39
22764	1	7	3	3	23	1	1	1
25259	2	1	3	1	3	3	1	1
27930	1	1	1	3	23	1	3	3
30783	2	7	1	1	1	3	1	3
33824	1	1	3	3	1	1	1	1
37059	2	1	3	1	1	1	3	1
40494	1	55	3	1	3	3	1	1
44135	2	1	1	3	3	3	3	1
47988	1	1	1	1	1	1	35	1
52059	2	7	3	3	1	1	35	1
56354	1	1	3	1	1	3	3	3
60879	2	1	3	3	23	3	1	3
65640	1	7	1	1	3	1	3	1
70643	2	1	1	1	23	1	1	1
75894	1	1	3	3	1		1	39

Again, in this table, we accept only the c values that are of the form  $n^3+n^2+n$ , n an integer. For any other c, there are at least one sequence (indeed an infinity) for which #(c) shall be null and the product  $\prod \#(c)$  will be equal to zero.

For this table to be usable, we must complete it with all supernumerary cardinals (in red in the table above) to greater sequences than p =19. We give them while recalling supernumerary cardinals for lower sequences than p = 19 in the following table :

Table (11)

Targets	Sequences	# super numerary cardinals	Sequences	# super numerary cardinals	Sequences	# super numerary cardinals	Disc	Lines
0	/	/	/	/	/	/	3	0
3	3	7	/	/	/	/	$3^2.2^5$	1
14	17	35	/	/	/	/	$17^2.19$	1
39	17	35	/	/	/	/	$2^4.3^2.17^2$	1
84	3	7	19	39	/	/	$3^2.19^2.59$	2
155	43	87	/	/	/	/	$2^5.43^2.11$	1
258	11	243	/	/	/	/	$3.11^4.41$	1
399	3	163	/	/	/	/	$3^8.2^4.41$	1
584	11	23	19	39	/	/	$11^2.19^2.211$	2
819	131	263	/	/	/	/	$2^5.3.11.131^2$	1
1110	3	7	107	215	/	/	$3^2.17.19.107^2$	2
1463	193	387	/	/	/	/	$2^4.97.193^2$	1
1884	457	915	/	/	/	/	$3^3.17.457^2$	1
2379	3	7	89	179	/	/	$2^5.3^2.67.89^2$	2
2954	617	1235	/	/	/	/	$617^2.619$	1
3615	353	707	/	/	/	/	$2^4.3.59.353^2$	1
4368	3	19	89	179	/	/	$3^4.11.73.89^2$	2
5219	11	23	41	83	/	/	$2^5.11^2.41^2.113$	2
6174	1009	2019	/	/	/	/	$3.337.1009^2$	1
7239	3	7	11	23	17	35	$2^4.3^2.11^2.17^2.281$	3
8420	17	35	73	147	/	/	$11.17^2.73^2.113$	2
9723	3	7	683	1367	/	/	$2^5.3^2.19.683^2$	(3)
11154	3	7	499	999	/	/	$3^2.499^2.1499$	2
12719	19	39	43	87	/	/	$2^4.19^2.43^2.409$	2

Targets	Sequences	# super numerary cardinals	Sequences	# super numerary cardinals	Sequences	# super numerary cardinals	Disc	Lines
14424	1777	3555	/	/	/	/	$3.593.1777^2$	1
16275	3	19	107	315	/	/	$2^5.3^4.107^2.241$	2
18278	2081	4163	/	/	/	/	$2081^2.2083$	1
20439	19	39	59	119	/	/	$2^4.3.11.17.19^2.59^2$	2
22764	3	7	11	23	73	147	$3^2.11^2.73^2.2411$	3
25259	1291	2583	/	/	/	/	$2^5.17.19.1291^2$	1
27930	11	23	251	503	/	/	$3^2.11^2.251^2.307$	2
30783	3	7	491	983	/	/	$2^4.3^2.11.67.491^2$	2
33824	3137	6275	/	/	/	/	$43.73.3137^2$	1
37059	1667	3335	/	/	/	/	$2^5.3.139.1667^2$	1
40494	3	55	131	263	/	/	$3^6.131^2.3539$	2
44135	1873	3747	/	/	/	/	$2^4.937.1873^2$	1
47988	17	35	233	467	/	/	$3.17^2.233^2.1321$	2
52059	3	7	17	35	41	83	$2^5.3^2.17^2.41^2.523$	3
56354	4409	8819	/	/	/	/	$11.401.4409^2$	1
60879	11	23	211	423	/	/	$2^4.3^3.11^2.43.211^2$	2
65640	3	7	1627	3255	/	/	$3^2.19.257.1627^2$	2
70643	11	23	233	467	/	/	$2^5.11^2.233^2.641$	2
75894	19	39	283	567	/	/	$3.11.19^2.163.283^2$	2

We immediately see the link between supernumerary cardinals equal to  $1+2p^{\text{ent}(i/2)}$  and prime factors  $p^i$  of the discriminant (for odd p). We will return to it later to explain the presence of exception to this link (such as systematically for  $p = 2$  and for  $p = 3$  for example when  $c = 39$ ,  $c = 1884$ ,  $c = 27930$  or  $c = 60879$ ).

Let us go back to the last but one table. The main change from the case of the monomial  $x^3-c$  is the loss of alignment of the cardinals worth 3. Previously, we could easily divide the supernumerary cardinals by the appropriate value (1 or 3) to reach the constant ratio that is our ultimate goal. Here, because of the loss of alignment, we cannot decide without rule on the position of the cardinals worth 1 and the cardinals worth 3 (on condition that the choice 1 or 3 is actually relevant). We will return to this point later on.

Admitting that a rule exists, it is necessary also, and this is the most important point, that there may exist an equiprobability of the cardinals worth 3 (and the cardinals worth 1) from one target to the other (that is in each row of the table). In the absence of equiprobability, the products of the local abundance factor (Euler products) would diverge when comparing of one target to another and our construction would be doomed to failure. In the case of the monomial, we had vertical alignment of the cardinals worth 3 for  $p = 1$  modulo 6 sequences. Here, but this is by chance, we have the same rule at  $c = 0$  (thus a probability of 1/2 of such cardinals) and we need to ask if this equiprobability is retained for other targets. The proof of this point follows.

#### 2.4.6.2 Proof of equiprobability at degree 3

We consider the general case of a degree 3 polynomial with parameter target  $c$ . Let us have  $P(x,c) = a_3.x^3 + a_2.x^2 + a_1.x - c$ . Since the only  $c$  targets which we are concerned with are of the form  $a_3.n^3 + a_2.n^2 + a_1.n$ ,  $n$  an integer (other cases corresponding to an impossibility at the global level with some cardinals locally null), we can rewrite thanks to a simple Euclidean division, the polynomial in the form  $P(x,c) = P(x,n) = (x-n).Q(x,n)$  with  $Q(x,n)$  an degree 2 polynomial with parameter  $n$ .

Equation  $P(x,n) = 0 \pmod{p^\delta}$  writes then :

$$x-n = 0 \pmod{p^i} \quad \text{and} \quad Q(x,n) = 0 \pmod{p^{\delta-i}}$$

The  $x-n = 0 \pmod{p^{\delta-i}}$  equation resolves without difficulty and has always one and only one solution.

Consider the second equation and let us have  $\Delta(n)$  the determinant of polynomial  $Q(x,n)$ . If  $\Delta(n)$  is a non-null square modulo  $p^{\delta-i}$  then this equation has two solutions. If  $\Delta(n)$  is not a square modulo  $p^{\delta-i}$  then this equation has no solution. Finally, if  $\Delta(n)$  is zero modulo  $p^{\delta-i}$  then this equation has a single (double) solution.

For a given  $n$ , we seek the relative frequency of these three cases according to  $p$ . We note first that the third case has no bearing on the frequency, since  $\Delta(n)$  is set, these cases are in finite quantity.

We note then that the “ $\Delta(n)$  is a square modulo  $p$ ” property is inherited by  $\Delta(n)$  modulo  $p^j$  for any  $j$ . Similarly, if  $\Delta(n)$  is not a square modulo  $p$  then  $\Delta(n)$  is not a square modulo  $p^j$  for any  $j$ . Indeed, let us reason by the absurd. Let  $g$  a primitive root of  $p$ . Suppose that  $\Delta(n) = g^{2r}$  modulo  $p$  and  $\Delta(n) = g^{2s+1}$  modulo  $p^j$ . Then  $g^{2s+1} - g^{2r} = 0$  modulo  $p$ , then  $g^{2r} \cdot (g^{2(s-r)+1} - 1) = 0$  modulo  $p$ , so that also  $g^{2(s-r)+1} = 1$  modulo  $p$ . But a non-square (quadratic non-residue) can be a square (quadratic residue) modulo the same value  $p$ , thus a contradiction. The result is the same taking  $\Delta(n)$  a non-square modulo  $p$  and  $\Delta(n)$  a square modulo  $p^j$ .

It leaves us only to determine the frequency of the modulo  $p$  property. The proof of this point taking some space, we have postponed it in appendix 7 page 62 showing that solutions  $p$  are of the form

$$p = cl \pmod{\Delta(n)} \quad (42)$$

with as many classes  $c_1$  of one type as the other. Then one can conclude thanks to Dirichlet.

Returning to  $P(x)$ , for a given  $c$  of the form  $a_3.n^3 + a_2.n^2 + a_1.n$ , we either have 1 solution, 3 solutions with equiprobability of these cases or a finite number of exceptions. We will return to these exceptions below.

### 2.4.6.3 Study of supernumerary cardinals

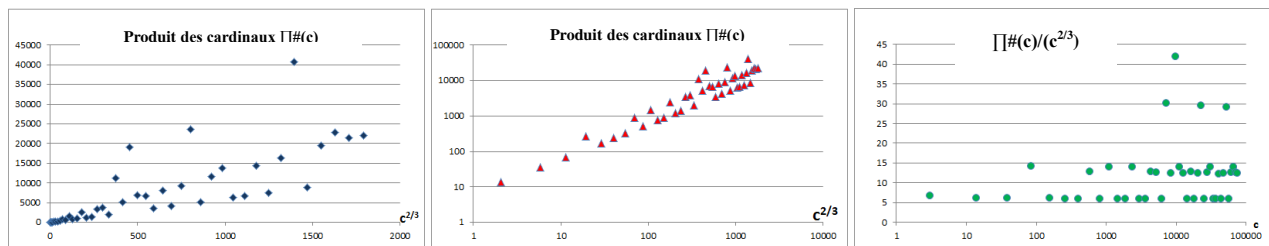
Nous avons ainsi établi l'essentiel pour ce qui concerne le degré 3. Nous pouvons comparer le produit des cardinaux obtenus localement en divisant les incidences à cardinaux 3 par 3. Si, nous faisons cela sans nous préoccuper en même temps des cardinaux, nous obtenons une dispersion très marquée vis-à-vis de notre objectif, cité plusieurs fois, d'obtention d'un rapport constant.

Traçons par exemple, toujours pour  $P(x) = x^3 + x^2 + x - c$ ,  $\prod \#(c)$  en fonction de  $c^{(n-1)/n}$  suivant des coordonnées linéaires, puis logarithmiques (pour mieux montrer les valeurs près de l'origine), puis  $\prod \#(c)/c^{(n-1)/n}$  en fonction de  $c$ .

We have established the essential so much as regards the degree 3. We can compare the product of cardinals achieved locally by dividing the incidences to cardinals 3 by 3. If we do this without concern at the same time of the supernumerary cardinals, we get a dispersion very marked with our goal, noticed several times, to obtain a constant ratio.

Let us chart for example, always for  $P(x) = x^3 + x^2 + x - c$ ,  $\prod \#(c)$  according to  $c^{(n-1)/n}$  with linear and logarithmic coordinates (to better view in the second case the values close to the origin), then  $\prod \#(c)/c^{(n-1)/n}$  with  $c$ .

Graphics (1)



The objective of the constant ratio is to find, of course, in the last chart. We find there three candidates of "constant" ratios as we have not yet divided at this stage the supernumerary cardinals by appropriate values as had proceed from table (8) to table (9). It is obvious, that as  $n$  increases, the determinant  $\Delta(n)$  may contain many multiple factors and new lines of points will then appear. A fourth candidate corresponds here to the particular point  $c = 9723$  who is not, a priori, of the same nature as the other points as discussed below.

The appearance of the chart immediately tells us about one important fact. The appropriate divisions are not "monolithic" as in the case of the monomial  $x^3$  (that is 1 or 3). Indeed, if lower points are relatively well aligned, the points above are less well (as for the next three points, offering few examples, it is difficult to comment the alignment). In fact, to align these points, it is necessary to proceed one after another. To a supernumerary cardinal, it is necessary to assign a division by an intermediate value between 1 and 3 (very roughly in the order of 2) for all non-special cases (here where  $c \neq 9723$ ) to align all points on a horizontal line. We can nevertheless speculate about the behaviour at infinity ( $c \rightarrow +\infty$ ) of these points which we believe that the alignment would be quite remarkable (but this is not essential).

Let us come back on the case  $c = 9723$ . It is unique in that the factor of 2 in the discriminant  $2^5 \cdot 3^2 \cdot 19 \cdot 683^2$  is active contrary to what is happening elsewhere in our numerical example. To obtain an alignment it is necessary to resort to a division of approximately  $2^{3/2}$ .

We must therefore conclude here that there is no simple rules for alignment following a constant (cte) which was our objective. This does not mean that there is no more sophisticated way (which can be found a posteriori by simple division of cte by  $\#(c)$ ).

Now we ought to ask the question of our ultimate goal : this is the enumeration of asymptotic diophantine equations in several variables. What is the impact for a given target of the supernumerary cardinals (finite number what we proved earlier) inherited from each of the variables compared with the impact of the non- supernumerary cardinals (in infinite number) ? To know more about this, the simplest is to review the case to two variables  $c = x_1^3 + x_2^3$  which means to look locally at  $c_1 = x_1^3$  modulo  $p$  and  $c - c_1 = c_2 = x_2^3$  modulo  $p$ . The crossing of the supernumerary cardinals remains finite number events. Thus only accounts the notion of equiprobability that we analysed in detail (see appendix 7). The rules of division of supernumerary cardinals contributions of each variable are thus secondary. There are not really required and they can be chosen freely to always find an adequate if not satisfactory consistency.

The equiprobability is present for degree 3. What is with higher degrees ?

### 2.4.7 Higher degrees polynomial equations

#### 2.4.7.1 Decomposition in ring $\mathbb{Z}/p^\delta \mathbb{Z}[X]$

When we are looking for the number of solutions of  $P(x) = c \pmod{p^\delta}$ , we get in fact the problem of decomposition of  $P(x)$  in ring  $K[X]$  where  $K = \mathbb{Z}/p^\delta \mathbb{Z}$  is a perfect field (field where all extensions are separable). Although  $K$  is perfect, the field has

the distinction of non-unique decompositions according to the chosen case.  $P(x)$  is a polynomial of degree  $n$ , equation  $P(x) = c \pmod{p^\delta}$  has either 0 solution,  $n$  solutions or other cardinals less or greater than  $n$ . When the number of solutions  $(x_1, x_2, \dots, x_k)$  is less than or equal to  $n$ , the decomposition is unique and is obtained by simple Euclidean division of the polynomial  $P(x)$  by  $x - x_i$  modulo  $p^\delta$ . When the number of solutions is strictly greater than  $n$ , the decomposition cannot be unique. For example, with  $K = \mathbb{Z}/43^2\mathbb{Z}$ , we have :

$$\begin{aligned} x^5 + x^4 + x^3 + x^2 + x - 62 \pmod{43^2} &= (x-1723).(x^4 - 125x^3 - 890x^2 - 648x + 293) \pmod{43^2} \\ &= (x-1723).(x-2+43k).(x^3 - (123+43k)x^2 + (713-8.43k)x + 778+2.43k) \pmod{43^2}, k = 0 \text{ à } 42 \end{aligned}$$

There are thus  $1+43 = 44$  solutions to this equation of degree 5.

The variants occur as pairs of polynomial solutions with polynomial coefficients of indeterminate  $k$  of degree  $\delta-1$ . In the example, these pairs are  $(x-2+43k, x^3 - (123+43k)x^2 + (713-8.43k)x + 778+2.43k)$  with  $k = 0$  to 42.

Note that the irreducibility of polynomials can be a factor conducive to many solutions (which may seem contradictory), since if the polynomial is completely reducible (to the first degree), we wouldn't have only 5 solutions.

This is a classical result with basic dating back to Lagrange who demonstrated that a polynomial of degree  $n$  admits no more than  $n$  non-congruent roots mod  $p$ , to Kummer, and to Dirichlet. Here, it is essential to find a method related to all of this and in order to detect the number of local solutions.

#### 2.4.7.2 Direct resolution

Let us find the integer solutions of  $P(x) = c \pmod{p^\delta}$ ,  $p > 2$ , with  $P(x)$  not a monomial. To this end, we have made some numerical tests. We have for examples :

Ex 1 :  $P(x) = x^3 + x^2 + x$ ,  $p = 11$ ,  $g = 2$ ,  $\delta = 6$

#(c)	Matching of #(c)	x	Matching of x
1	1	0 0+mod(2 <sup>k</sup> ,11).11 <sup>4</sup> , k = 1 to 10 0+mod(2 <sup>k</sup> ,11).m.11 <sup>3</sup> , k = 1 to 10, m = 1 to 11 0+mod(2 <sup>k</sup> ,11).m.11 <sup>2</sup> , k = 1 to 10, m = 1 to 121 0+mod(2 <sup>k</sup> ,11).m.11, k = 1 to 10, m = 1 to 1331 5+11k+121m, k = 0, 2 to 10 (k ≠ 1), m = 0 to 11 <sup>3</sup> -1 16+121k+1331m, k = 0,3,5,6 or 7, m = 0 to 11 <sup>2</sup> -1 258+1331k+14641m, k = 1 to 10, m = 0 to 11 <sup>1</sup> -1 258+14641k, k = 2,4,5,6 or 10 1+11k+121m, k = 0 to 8, 10 (k ≠ 9), m = 0 to 11 <sup>3</sup> -1 221+121k+1331m, k = 0,1,2,4 or 7, m = 0 to 11 <sup>2</sup> -1 826+1331k+14641m, k = 1 to 10, m = 0 to 11 <sup>1</sup> -1 826+14641k, k = 0, 2,5,9 or 10 (6,7 or 10)+11.k, k = 0 to 11 <sup>4</sup> -1	r <sub>1</sub> r <sub>1</sub> +mod(g <sup>k</sup> ,p).p <sup>4</sup> , k = 1 to p-1 r <sub>1</sub> +mod(g <sup>k</sup> ,p).p <sup>3</sup> , k = 1 to p-1, m = 1 to p r <sub>1</sub> +mod(g <sup>k</sup> ,p).p <sup>2</sup> , k = 1 to p-1, m = 1 to p <sup>2</sup> r <sub>1</sub> +mod(g <sup>k</sup> ,p).p <sup>1</sup> , k = 1 to p-1, m = 1 to p <sup>3</sup> r <sub>2</sub> +k.p+m.p <sup>2</sup> , some k, m = 0 to p <sup>3</sup> -1 r <sub>3</sub> +k.p <sup>2</sup> +m.p <sup>3</sup> , some k, m = 0 to p <sup>2</sup> -1 r <sub>4</sub> +k.p <sup>3</sup> +m.p <sup>4</sup> , k = 1 to p-1, m = 0 to p <sup>1</sup> -1 r <sub>5</sub> +k.p <sup>4</sup> , some k r <sub>2</sub> ' +k.p+m.p <sup>2</sup> , some k, m = 0 to p <sup>3</sup> -1 r <sub>3</sub> ' +k.p <sup>2</sup> +m.p <sup>3</sup> , some k, m = 0 to p <sup>2</sup> -1 r <sub>4</sub> ' +k.p <sup>3</sup> +m.p <sup>4</sup> , k = 1 to p-1, m = 0 to p <sup>1</sup> -1 r <sub>5</sub> ' +k.p <sup>4</sup> , some k r <sub>6</sub> +k.p, some r <sub>6</sub> , k = 0 to p <sup>4</sup> -1
3	n or 1+2p <sup>0</sup>	3+11.k, k = 0 to 11 <sup>4</sup> -1	r <sub>7</sub> +p.k, k = 0 to p <sup>4</sup> -1
23	1+2p	137+(mod(2 <sup>2k+1</sup> ,11)-2).m.11 <sup>4</sup> , k = 0 to 4, m = 0 to 11 <sup>2</sup> -1 100+(mod(2 <sup>2k</sup> ,11)-1).11 <sup>4</sup> , k = 0 to 4, m = 11 <sup>2</sup> -1	r <sub>8</sub> +(mod(g <sup>2k+1</sup> ,p)-g <sup>1</sup> ).m.p <sup>4</sup> , k = 0 to (p-1)/2-1, m = 0 to p <sup>2</sup> -1 r <sub>9</sub> +(mod(g <sup>2k</sup> ,p)-g <sup>0</sup> ).p <sup>4</sup> , k = 0 to (p-1)/2-1, m = p <sup>2</sup> -1
122	1+p <sup>2</sup>	14899, 44749	r <sub>10</sub> , r <sub>11</sub>
243	1+2p <sup>2</sup>	(258 or 15467)+(2 <sup>2k+1</sup> -2).11 <sup>4</sup> , k = 0 to 4	r <sub>12</sub> +(g <sup>2k+1</sup> -g <sup>1</sup> ).p <sup>4</sup> , k = 0 to (p-1)/2-1

Ex 2 :  $P(x) = x^4 + x^3 + x^2 + x$ ,  $p = 13$ ,  $g = 2$ ,  $\delta = 6$

#(c)	Rapprochement #(c)	x	Rapprochement x
1	1	(2, 3, 7, 8, 9 or 10)+13.k, k = 0 to 13 <sup>4</sup> -1	r <sub>1</sub> +p.k, k = 0 to p <sup>4</sup> -1
2	2	4+13.k, k = 0 to 13 <sup>4</sup> -1	r <sub>2</sub> +p.k, k = 0 to p <sup>4</sup> -1
4	n	0+13.k, k = 0 to 13 <sup>4</sup> -1	r <sub>3</sub> +p.k, k = 0 to p <sup>4</sup> -1
26	2p	1110+(g <sup>k</sup> -1), k = 0 to p <sup>2</sup> .(p-1)/2-1	r <sub>4</sub> +(g <sup>k</sup> -1), k = 0 to p <sup>2</sup> .(p-1)/2-1
338	2p <sup>2</sup>	214388+(g <sup>k</sup> -1), k = 0 to (p-1)/2-1	r <sub>5</sub> +(g <sup>k</sup> -1), k = 0 to (p-1)/2-1
169	p <sup>2</sup>	772	r <sub>6</sub>

The "matching" columns are simple assumptions of generalization of the associated columns that precede them.

In fact, the possibilities for solutions are not limited to these two types of results at all. We see in the first example that direct research results are relatively "messy". It seems futile to seek a general outcome. However results have a homogeneous form under one aspect : solutions are in arithmetic progressions (by modulo  $p^\delta$  construction) with insertion of supernumerary cardinals for square powers.

When  $c$  varies, it is important to us that the non-supernumerary cardinals be equiprobable.

### 2.4.7.3 Discriminant

#### 2.4.7.3.1 Generalities

The degree 2 and degree 3 examples show the importance of the polynomial discriminant, which can no longer surprise us. It remains however to see until which point its knowledge can be effectively useful.

The discriminant of a polynomial  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ,  $a_n \neq 0$ , is defined according to the usual formula :

$$\text{Disc} = (-1)^{n(n-1)/2} \cdot (1/a_n) \cdot \text{Res} \quad (43)$$

Here  $n$  is the degree of the polynomial  $P(x)$ ,  $a_n$  is the dominant coefficient and  $\text{Res}$  is the resultant of  $P(x)$  and its derivate  $P'(x)$ . We set up as usual our equations by the target  $c$  parameter. Thus, we replace  $P(x)$  by removing the constant  $a_0$  and we write :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x = c$$

The discriminant, which concerns us, is thus that of  $P(X)-c$  and the resultant is a matrix of Sylvester  $M_S(c) = \text{Res}(c)$ , square matrix of size  $2n-1$ , defined by :

$$M_S(c) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_1 & -c & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & -c & 0 & \dots & 0 \\ 0 & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & -c & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & a_n & a_{n-1} & a_{n-2} & \dots & -c \\ n.a_n & (n-1).a_{n-1} & (n-2).a_{n-2} & \dots & a_1 & 0 & 0 & 0 & \dots & 0 \\ 0 & n.a_n & (n-1).a_{n-1} & (n-2).a_{n-2} & \dots & a_1 & 0 & 0 & \dots & 0 \\ 0 & 0 & n.a_n & (n-1).a_{n-1} & (n-2).a_{n-2} & \dots & a_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & n.a_n & (n-1).a_{n-1} & (n-2).a_{n-2} & \dots & a_1 \end{vmatrix}$$

The coefficients of  $P(X)$  occupy the first  $n-1$  lines and those of  $P'(X)$  are in the following  $n$  lines.

The determinant of this resultant is a polynomial of degree  $n-1$  with the  $c$  parameter.

The  $aa_i$  being integers (of any sign), we then have :

$$\text{Disc} = (-1)^{n(n-1)/2} \cdot (1/a_n) \cdot (aa_{n-1} \cdot c^{n-1} + aa_{n-2} \cdot c^{n-2} + \dots + aa_1 \cdot c + aa_0) \quad (44)$$

#### 2.4.7.3.2 Multiple roots

The discriminant of a polynomial is zero for multiple roots.

##### Proof

Let us have  $\alpha_1, \alpha_2, \dots, \alpha_n$  the solutions split in the field of complex numbers of polynomial  $P(x) = c$  of degree  $n$ . We have the following result [16] :

$$\text{Disc} = (-1)^{n(n-1)/2} \cdot a_n^{2n-1} \cdot \prod_{i < j} (\alpha_i - \alpha_j)^2 \quad (45)$$

Thus, if there are distinct  $i$  and  $j$  such as  $\alpha_i = \alpha_j$ , then  $\text{Disc} = 0$  and vice versa if  $\text{Disc} = 0$ , there is  $i$  and  $j$  as  $\alpha_i = \alpha_j$  (because  $a_n \neq 0$ ). Which completes the proof.

Let us consider then the extension  $K(i)$  the (local) perfect field  $K = \mathbb{Z}/p^\delta \mathbb{Z}$  in order to manipulate the complex roots. In this local field, considering a primitive root  $g$ , to write  $g^m = t^{1/d}$  means to solve  $g^{m \cdot d} = t$ . By this process, we go back from roots  $\alpha_i$  global to local roots  $\beta_i$  of the studied equation. The cancellation of the discriminant writes then

$$\text{Disc} = 0 \mod p^\delta \quad (46)$$

Let us have  $\beta_1, \beta_2, \dots, \beta_i$  the local roots of the polynomial  $P(x)-c = 0 \mod p^\delta$ . If  $\beta_{i1} = \beta_{i2} \mod p^k$ , corresponding to multiple roots, then

$$\text{Disc} = t \cdot p^{2k} \cdot (-1)^{n(n-1)/2} \cdot a_n^{2(n-1)} \cdot \prod_{i < j, i \neq i_1, j \neq i_2} (\beta_i - \beta_j)^2 = 0 \mod p^{2k} \quad (47)$$

Here  $t$  is the part of expression (45) for which the local decomposition is impossible.

Multiple roots imply a locally null discriminant with square modulus (in  $p^2$ ) for each root instance. This evolution with the square can be verified in the example in the table (11).

However, the converse is false as  $(\alpha_i - \alpha_j)^2$  can be an integer without that the roots  $\alpha_i$  or  $\alpha_j$  are themselves integers (what we check in the table just mentioned for the sequence  $p = 3$  and  $c = 39, c = 1884, c = 27930$  and  $c = 60879$  targets). Similarly, the discriminant may be either multiple of  $p^{2k}$  or only multiple of  $p^{2i}$ , with  $i$  smaller than  $k$ , difference which will impact the expression of the cardinal  $\#(c)$  (but this possibility has not appeared in our numerical examples).

#### 2.4.7.3.3 Number of solutions associated to the discriminant

We are interested in the relationship between the values of the discriminant and the number of solutions  $\#(c)$  of local equations parameterized by  $c$  :

$$P(x) = c \bmod p^\delta$$

Let us recall that Disc is analysed for each target  $c$  and each  $p$  sequence :

$$\text{Disc} = \text{Disc}(c, p)$$

We observe, for a given target  $c$ , that the degree of stability  $\delta$  of  $c$  is equal at sequence  $p$  to the multiplicity of  $p$  in Disc. The degree of stability of  $c$  is infinite only if :

$$\text{Disc} \equiv 0$$

The degree of stability is then infinite for all  $p$  and we have a good candidate for "obstruction".

The discriminant of an equation detects double roots of an global or local equation. It is null when such roots exist. Null value locally means that

$$\text{Disc} = 0 \bmod p^\delta$$

and thus that the sequences, for which the supernumerary cardinals appear, are among the divisors of Disc.

Finally, when  $\text{Disc} \neq 0 \bmod p^\delta$ , we write the discriminant under the form ( $i < \delta$ )

$$\text{Disc} = g^m \cdot p^i$$

We observe then systematically, for equations of degree 3 and 4, a dependency of the enumerations to the parity of  $m$  and  $i$ .

Locally, we distinguished thus the events relating to  $\text{Disc} = \text{Disc}(c, p)$  :

Case	Lower case
Disc = 0	
Disc = 0 mod $p^\delta$	
Disc $\neq 0 \bmod p^\delta$	Disc = $g^m \cdot p^i \bmod p^\delta$

In the following tables we used  $\{\emptyset\}$  to mean that the corresponding condition has not been observed. The special case  $p = 2$  is not treated here. In header of each table, we have indicated the number of  $\mathbb{Z}$  roots of  $P(x)$ . As  $P(x)$  is of the form  $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x$ , we always have at least the root  $x = 0$ . Here are some of the results that we get then :

##### 2.4.7.3.3.1 Degree 3

It is essential to take into account the concept of stability in the study. Here  $\delta$  is the value which allows achieving it. The particular case of  $p = 3$ , concerning several tables, is not treated below.

Conditions	$\#(c = P(x))$
Dominant coefficient of $P(X) = 0 \bmod p$	See lower degree polynomial

Single roots :

Conditions	$\#(c = P(x))$
Disc = 0 mod $p^0$ , Disc = $g^0 \cdot g^{2k} \bmod p^1$	3
Disc = 0 mod $p^0$ , Disc = $g^1 \cdot g^{2k} \bmod p^1$	1
Disc = 0 mod $p^1$ , $i > 0$	$\{\emptyset\}$

Double root :

Conditions	#(c = P(x))
$i \geq \delta$	Case dependent
$0 < i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^0 \cdot g^{2k} \bmod p^{2i+1}$	$1+2 \cdot p^i$
$0 < i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^1 \cdot g^{2k} \bmod p^{2i+1}$	1
$i < \delta$ , Disc = $p^{2i+1}$	1
$i = 0$ , Disc = $p^0$ , Disc = $g^0 \cdot g^{2k} \bmod p^1$	$\{\emptyset\}$
$i = 0$ , Disc = $p^0$ , Disc = $g^1 \cdot g^{2k} \bmod p^1$	1

Triple root :

Conditions	#(c = P(x))
$i \geq \delta$	Case dependent
$0 < i < \delta$ , Disc = 0 mod $p^{3i}$ , Disc = $g^0 \cdot g^{2k} \bmod p^{3i+1}$	$\{\emptyset\}$
$0 < i < \delta$ , Disc = 0 mod $p^{3i}$ , Disc = $g^1 \cdot g^{2k} \bmod p^{3i+1}$	$(3, p-1) \cdot p^i$
$0 < i < \delta$ , $j = 1$ or $j = 2$ , Disc = 0 mod $p^{3i+j}$	$\{\emptyset\}$
Disc = 0 mod $p^0$ , Disc $\neq 0 \bmod p^1$	$\{\emptyset\}$

Clearly, without the need for proof, local enumerations are related to the existence or not of multiple roots. For the case of a "simple root", given the result of section 2.4.6.2, we demonstrate the equiprobability, when the targets  $c$  vary from  $-\infty$  to  $+\infty$ , for a given polynomial  $P(X)$ , between discriminants equal to  $g^0 \cdot g^{2k} \bmod p$  on one hand and discriminants equal to  $g^1 \cdot g^{2k} \bmod p$  on the other hand.

#### 2.4.7.3.3.2 Degree 4

Trends

Conditions	#(c = P(x))
Dominant coefficient of $P(X) = 0 \bmod p$	See lower degree polynomial

Single roots :

Conditions	#(c = P(x))
$i \geq \delta$	Case dependent
$0 < i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^0 \cdot g^{2k} \bmod p^{2i+1}$	$p$ (or $4p$ ?)
$0 < i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^1 \cdot g^{2k} \bmod p^{2i+1}$	$\{\emptyset\}$ (or $2 \cdot p^i$ ?)
Disc = 0 mod $p^2$ , Disc $\neq 0 \bmod p^3$ ,	$2p$
Disc = 0 mod $p^1$ , Disc $\neq 0 \bmod p^2$ ,	2
Disc = 0 mod $p^0$ , Disc = some $g^0 \cdot g^{2k} \bmod p^1$	1
Disc = 0 mod $p^0$ , Disc = some $g^0 \cdot g^{2k} \bmod p^1$ , $k$ odd	4
Disc = 0 mod $p^0$ , Disc = $g^1 \cdot g^{2k} \bmod p^1$	2
Disc = 0 mod $p^1$ , $i > 0$	$\{\emptyset\}$

See examples with  $P(x) = x^4 + x^3 + x^2 + x$  at appendix 4

1 double root, 2 single roots :

Conditions	#(c = P(x))
$i \geq \delta$	Case dependent
$0 < i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^0 \cdot g^{2k} \bmod p^{2i+1}$	$2 \cdot (1 + p^i)$
$i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^1 \cdot g^{2k} \bmod p^{2i+1}$	2
$i < \delta$ , Disc = $p^{2i+1}$	2
$i = 0$ , Disc = $p^0$ , Disc = $g^0 \cdot g^{2k} \bmod p^1$	$\{\emptyset\}$

2 double roots :

Conditions	#(c = P(x))
$i \geq \delta$	Case dependent
$0 < i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^0 \cdot g^{2k} \bmod p^{2i+1}$	$\{\emptyset\}$
$i < \delta$ , Disc = 0 mod $p^{2i}$ , Disc = $g^1 \cdot g^{2k} \bmod p^{2i+1}$	$2 \cdot p^i$
$i < \delta$ , Disc = $p^{2i+1}$	$\{\emptyset\}$
$i = 0$ , Disc = $p^0$ , Disc = $g^0 \cdot g^{2k} \bmod p^1$	Case dependent
$i = 0$ , Disc = $p^0$ , Disc = $g^1 \cdot g^{2k} \bmod p^1$	$\{\emptyset\}$

Triple root :

Conditions	#(c = P(x))
$i \geq \delta$	Case dependent
$0 < i < \delta$ , Disc = 0 mod $p^{3i}$ , Disc = $g^0 \cdot g^{2k}$ mod $p^{3i+1}$	1
$0 < i < \delta$ , Disc = 0 mod $p^{3i}$ , Disc = $g^1 \cdot g^{2k}$ mod $p^{3i+1}$	1
$0 < i < \delta$ , $j = 1$ ou $j = 2$ , Disc = 0 mod $p^{3i+j}$	$\{\emptyset\}$
Disc = 0 mod $p^0$ , Disc = $g^0 \cdot g^{2k}$ mod $p^1$	1
Disc = 0 mod $p^0$ , Disc = $g^1 \cdot g^{2k}$ mod $p^1$	$\{\emptyset\}$

Quadruple root :

Conditions	#(c = P(x))
$i \geq \delta$	Case dependent
$0 < i < \delta$ , Disc = 0 mod $p^{4i}$ , Disc = $g^0 \cdot g^{2k}$ mod $p^{4i+1}$	$(4, p-1) \cdot p^i$
$0 < i < \delta$ , Disc = 0 mod $p^{4i}$ , Disc = $g^1 \cdot g^{2k}$ mod $p^{4i+1}$	$\{\emptyset\}$
$0 < i < \delta$ , $j = 1$ , $j = 2$ or $j = 3$ , Disc = 0 mod $p^{4i+j}$	$\{\emptyset\}$
Disc = 0 mod $p^0$ , Disc $\neq 0$ mod $p^1$	$\{\emptyset\}$

### Numerical example

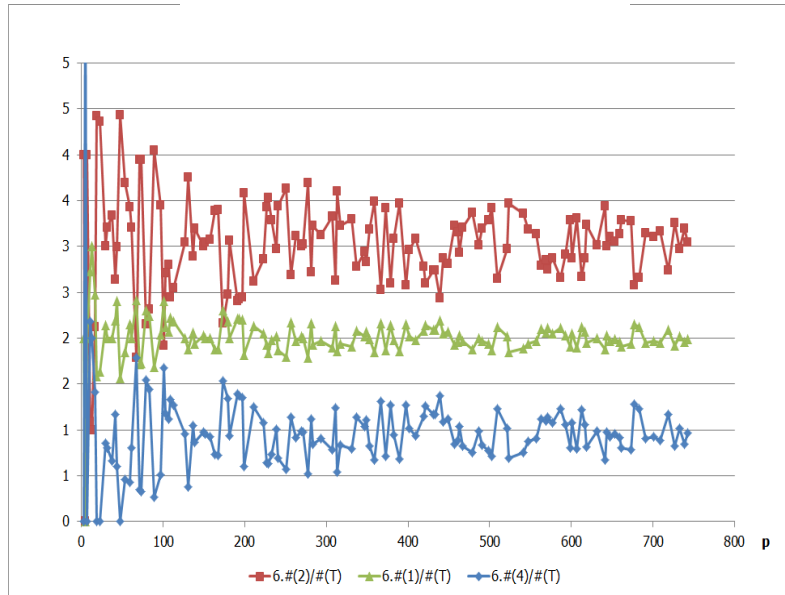
The following table is corresponding to the number of solutions of the equation  $P(x) = c \text{ mod } p^2$  with  $P(x) = x^4 + x^3 + x^2 + x$  varying from 0 to  $p^2 - 1$  and target  $c$  accordingly chosen. Another numerical example with  $P(x) = x^4 + 3x^3 + 4x^2 + 7x$  is given at appendix 8. We see that the sought equiprobability in this case, given at the end of the table, seems difficult to establish a priori by studying one after the other the prime numbers  $p$  with the objective of finding a possible rule of counting. The non-integer ratios  $\#(i)/p$  correspond to contributions of supernumerary cardinals. In addition, we define  $\#(T) = \sum \#(i)$ .

Table (12)

p	#(1)	#(2)	#(4)		6.#(1)/#(T)	6.#(2)/#(T)	6.#(4)/#(T)
3	3	6	0		2	4	0
5	0	0	20		0	0	6
7	14	28	0		2	4	0
11	55	22	44		2,73	1,09	2,18
13	78	26	52		3	1	2
17	119	102	68		2,47	2,12	1,41
19	95	266	0		1,58	4,42	0
23	138	368	0		1,64	4,36	0
29	290	406	116		2,14	3	0,86
31	310	496	124		2	3,2	0,8
37	444	740	148		2	3,33	0,67
41	615	738	328		2,20	2,63	1,17
43	688	854	172		2,41	2,99	0,60
47	564	1598	0		1,57	4,43	0
53	848	1696	212		1,85	3,69	0,46
59	1180	1882	236		2,15	3,42	0,43
61	1220	1952	488		2	3,2	0,8
67	1809	1340	1340		2,42	1,79	1,79
71	1420	3266	284		1,71	3,94	0,34
73	1533	3504	292		1,73	3,95	0,33
79	2370	2212	1580		2,31	2,15	1,54
83	2573	2656	1660		2,24	2,31	1,45
89	2225	5340	356		1,69	4,04	0,27
97	3104	5232	776		2,04	3,45	0,51
101	4040	3232	2828		2,4	1,92	1,68
103	3708	4738	2060		2,12	2,71	1,18
107	3959	5350	2140		2,07	2,80	1,12
109	4360	4796	2616		2,22	2,44	1,33
113	4633	5424	2712		2,18	2,55	1,27
127	5334	8128	2540		2	3,05	0,95
131	5240	10474	1048		1,88	3,75	0,38
Etc.							
				$\Sigma$			
Total	52969	76872	24240	154081			
Mean value					2,0233	2,9599	1,0168
Ratio	2,063	2,993	0,944	6			
At infinity awaited value	2	3	1	6	2	3	1
Difference	3,13%	-0,22%	-5,61%		1,16%	-1,34%	1,68%

## Graphics (2)

### Evolution of proportions with sequence p



Assuming the law of distribution of enumeration as a random draw, we are outlining a trend with proportions (2,3,1), corresponding to irreducible or single root degree 4 polynomials, easily readable on the graph for which we have extended here until the  $p = 743$  sequence the data. Rather than by an average phenomenon (who also plays a rule), we believe that it is an asymptotic trend (which would be the right track to a demonstration in our view) to the values (2,3,1) that the "equiprobability" is carried out, small sequences being without incidence as negligible before infinity. The result "product" is realised to a given target because the result is almost aligned with the expected value to each  $p$  sequence provided that  $p$  is extremely large. This asymptotic trend is, however, very slow and only suspected here. We will see later on (in paragraphs 2.4.7.4.2 and 2.4.7.5) a simple heuristic approach for these proportions for the polynomials without double roots in  $\mathbb{Z}$  (here, this is the case with  $P(x) = x.(x+1).(x^2+1)$ ).

#### 2.4.7.3.4 Degree 5 and more

The expression of the discriminant is the result of a great number of "degrees of freedom" to integer roots or not involved in  $(-1)^{n(n-1)/2} \cdot a_n^{2n-1} \cdot \prod (\alpha_i - \alpha_j)^2$ . The relationship to the parity of power of the primitive root  $g$  is observed only very partially when the degree of the polynomial increases. Some numerical tests announce the following table (the last line being a trivial one) :

#(c = P(x))	Conditions
n	$\text{Disc} = g^0 \cdot g^{2k} \pmod p$ or $\text{Disc} = 0 \pmod p$
n-1	$\{\emptyset\}$
n-2	$\text{Disc} = g^1 \cdot g^{2k} \pmod p$ or $\text{Disc} = 0 \pmod p$
n-3	$\text{Disc} = g^0 \cdot g^{2k} \pmod p$ or $\text{Disc} = 0 \pmod p$
< n-3	$\text{Disc} = g^k \pmod p$ or $\text{Disc} = 0 \pmod p$

In the absence of immediate interest, we do not seek a proof of these lines. We simply observe the alternated parities as soon as  $P(x) = c$  has at least  $n-3$  integer solutions,  $n$  is the degree of  $P(x)$ . For lower cardinals, the parity of the power of  $g$  is completely random and other arithmetic series (as 2-based) would be to look for. On a general level (any polynomial  $P(x)$ ), this has the aspect of a major difficulty.

Let us note also that the alternated parities between  $n-2$  and  $n$  solutions logically corresponds to  $n-1$  solutions, additional solution (to arrive at  $n$  solutions) is somehow free.

Finally, our study does not provide important results on the determinant precise incidence but to obvious impact of square of primitive roots  $g$ . For a more ambitious study, our tool with 14 significant digits is not sufficient.

#### 2.4.7.4 Cardinals relative frequencies

We already said it. The essential is to have a relative frequency of cardinals which is not dependent on targets  $c$ . Previously, let us go back again on the following fundamental case. If we admit that there are as many cases of type  $\text{Disc} = g^0 \cdot g^{2k} \pmod p$  that  $\text{Disc} = g^1 \cdot g^{2k} \pmod p$ , we find the case of the equiprobability at degree 3, that we have proven otherwise. By the same argument, this extends also to degree 4. In the higher degrees, we have not apparently this kind of simplicity that a rule on the powers of  $g$  could produce (and also the study of the discriminant becomes difficult on an software that has only 14 significant digits). So, we have below a more rudimentary approach.

#### 2.4.7.4.1 Case of monomials

We start from table (4) with a representative line :

$x$	$c = x^n \bmod p^\delta$	$\#\{c\}$	$\#\{\text{variants of } c\}$
$p^i \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-1)-1}\}$	$p^{i \cdot n} \cdot \{g^{0 \cdot d[i,n]}, g^{1 \cdot d[i,n]}, \dots, g^{(\Phi(\delta-1 \cdot n)/d[i,n]-1) \cdot d[i,n]}\}$	$d_{i,n} \cdot p^{i \cdot (n-1)}$	$\Phi(\delta-i \cdot n)/d_{i,n}$

Let us have a diophantine equation  $x^n = c \bmod p^\delta$ . The target  $c$ , being given in advance, has only a finite number of factors  $p_i$ . Therefore, there is only a finite number of solutions to the proposed equation such as  $\#(c) = d_{i,n} \cdot p^{i \cdot (n-1)}$  and  $i > 0$  (that we called supernumerary cardinals). When  $p$  varies from 2 to infinity, the supernumerary cardinals are therefore of density (or frequency) zero. The factors of abundance with non-zero frequency depend only on  $(n, p-1) \neq 1$ , that is meet the arithmetic progression  $p = 1 + kp_i$  with  $p_i$  dividing  $n$ .

The alignments (bijections) between the values  $\#(c)$  are obvious in the case of the monomials. When we turn to the polynomials which are clusters of monomials, the machinery of the previous alignments (bijections) is always in action, but the obvious trace of the alignments is lost.

The following table, which concerns the monomials of degree  $n$ , derives from the table (4):

Table (13)

Degree (n)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Nb solutions (m)	Card(n,m) = Proportions of solutions (before ratio to total of proportions)														
0	0	1	2	5	4	8	6	16	20	24	10	27	12	48	56
1	1	0	3	0	15	0	35	21	27	0	99	12	143	0	45
2		1	0	2	0	3	0	0	0	15	0	0	0	35	0
3			1	0	0	0	0	8	6	0	0	0	0	0	15
4				1	0	0	0	0	0	0	0	6	0	0	0
5					1	0	0	2	0	0	0	0	0	0	3
6						1	0	0	0	0	0	2	0	0	0
7							1	0	0	0	0	0	0	0	0
8								1	0	0	0	0	0	0	0
9									1	0	0	0	0	0	0
10										1	0	0	0	0	0
11											1	0	0	0	0
12												1	0	0	0
13													1	0	0
14														1	0
15															1
Total proportions	1	2	6	8	20	12	42	48	54	40	110	48	156	84	120

We give some general formulas for higher degrees next. In these, we reduced the proportions  $\#( )$  in such a way that their sum is equal to 1. To find the values in the preceding table, simply multiply each of the proportions by  $1/\#(n)$ .

Case  $n = p$ ,  $p$  a prime number (Table (14)) :

div \ #	0	1	...	p	Proportions	Arithmetic progressions
p	$(p-1)/p$			$1/p$	$1/(p-1)$	$1 \bmod p$
...						
1	0	1			$(p-2)/(p-1)$	$1 \bmod 1, \neq 1 \bmod p$

So that :

$$\#(0) = 1/p$$

$$\#(1) = (p-2)/(p-1)$$

$$\#(p) = 1/(p \cdot (p-1))$$

$$\#(\text{others}) = 0$$

Case  $n = 2p$ ,  $p$  a prime number (Table (15)) :

div \ #	0	...	2	...	2p	Proportions	Arithmetic progressions
2p	$(2p-1)/(2p)$				$1/(2p)$	$1/(p-1)$	$1 \bmod 2p$
...							
2	$1/2$		$1/2$			$(p-2)/(p-1)$	$1 \bmod 2, \neq 1 \bmod 2p$

So that :

$$\#(0) = (p+1)/(2p)$$

$$\#(2) = (p-2)/(2(p-1))$$

$$\#(2p) = 1/(2p.(p-1))$$

$$\#(\text{others}) = 0$$

Case  $n = p^2$ ,  $p$  a prime number (Table (16)) :

div \ #	0	1	...	p	...	$p^2$	Proportions	Arithmetic progressions
$p^2$	$(p^2-1)/p^2$					$1/p^2$	$1/(p.(p-1))$	$1 \bmod p^2$
...								
p	$(p-1)/p$			$1/p$			$1/p$	$1 \bmod p, \neq 1 \bmod p^2$
...								
1	0	1					$(p-2)/(p-1)$	$1 \bmod 1, \neq 1 \bmod p$

So that :

$$\#(0) = (p^2+1)/p^3$$

$$\#(1) = (p-2)/(p-1)$$

$$\#(p) = 1/p^2$$

$$\#(p^2) = 1/(p^3.(p-1))$$

$$\#(\text{others}) = 0$$

Case  $n = p.q$ ,  $q > p > 2$  two prime numbers (Table (17)) :

div \ #	0	1	...	p	...	q	...	p.q	Proportions	Arithmetic progressions
p.q	$(p.q-1)/(p.q)$							$1/(p.q)$	$1/((p-1)(q-1))$	$1 \bmod p.q$
...										
q	$(q-1)/q$					$1/q$			$(p-2)/((p-1)(q-1))$	$1 \bmod q, \neq 1 \bmod p.q$
...										
p	$(p-1)/p$			$1/p$					$(q-2)/((p-1)(q-1))$	$1 \bmod p, \neq 1 \bmod p.q$
...										
1	0	1							$(p.q-2.(p+q)+4)/((p-1)(q-1))$	$1 \bmod 1, \neq 1 \bmod p, \neq 1 \bmod q$

So that :

$$\#(0) = ((p+q).(p.q+2)-(p^2+q^2)-3p.q-1)/(p.q.(p-1).(q-1))$$

$$\#(1) = (p.q-2(p+q)+4)/((p-1).(q-1))$$

$$\#(p) = (q-2)/(p.(p-1).(q-1))$$

$$\#(q) = (p-2)/(q.(p-1).(q-1))$$

$$\#(p.q) = 1/(p.q.(p-1).(q-1))$$

$$\#(\text{others}) = 0$$

Case  $n = p^r.q^s$ ,  $q > p > 2$  two prime numbers :

We use here Euler's totient function  $\phi$ . We have  $\phi(p^r) = (p-1).p^{r-1}$ ,  $\phi(q^s) = (q-1).q^{s-1}$  and  $\phi(n) = (p-1).(q-1).p^{r-1}.q^{s-1}$ .

We also the writing shortcuts  $\phi p = \phi(p^r)$ ,  $\phi s = \phi(q^s)$  et  $\phi n = \phi(n)$ .

The corresponding table is then (Table (18))

div \ #	0	1	...	$p^r$	...	$q^s$	...	n	Proportions	Arithmetic progressions
n	$1-1/n$							$1/n$	$1/\phi n$	$1 \bmod n$
...										
$q^s$	$1-1/q^s$					$1/q^s$			$1/\phi q-1/\phi n$	$1 \bmod q^s, \neq 1 \bmod n$
...										
$p^r$	$1-1/p^r$			$1/p^r$					$1/\phi p-1/\phi n$	$1 \bmod p^r, \neq 1 \bmod n$
...										
1	0	1							$1-1/\phi p-1/\phi q+1/\phi n$	$1 \bmod 1, \neq 1 \bmod p^r, \neq 1 \bmod q^s$

So that :

$$\#(0) = (1-1/p^r)/\phi p + (1-1/q^s)/\phi q - (1+1/n-1/p^r-1/q^s)/\phi n$$

$$\#(1) = 1-1/\phi p-1/\phi q+1/\phi n$$

$$\#(p^r) = (1/\phi p-1/\phi n)/p^r$$

$$\#(q^s) = (1/\phi q-1/\phi n)/q^s$$

$$\#(n) = 1/(n.\phi n)$$

$$\#(\text{others}) = 0$$

The formulations are then complicated with the multiplication of the number of factors of n. Is it possible to obtain a general expression (including also the even factors) from the previous examples ? If so, it would certainly require still more than a little effort. However, the essential is to have seen that the existence of solutions following arithmetic progressions do pilot

cardinals and obtained proportions. In the case of the polynomials (under conditions of single roots given further), a priori more complex, we will instead produce such a general expression (without proof however).

#### 2.4.7.4.2 Case of polynomials

Let us have  $P$  a given polynomial of degree  $n$ . Let us have  $\#(c, p, \delta)$  the number of integer solutions of  $P(x) = c \pmod{p^\delta}$ . We seek the relative frequency  $\text{freq}(n, ve)$  of

$$\#(c, p, \delta) = ve \quad (48)$$

We first have a fundamental result. Namely, the number of integer solutions of  $P(x) = c \pmod{p^\delta}$  is equal to the number of integer solutions of  $P(x) = c \pmod{p}$  except for a finite number of sequences  $p$ . Indeed, the supernumerary cardinals occur for  $p$  dividing the discriminant of the equation (as discussed later), discriminant that is a constant for a given target  $c$  and has thus trivially only finite number of divisors. Except supernumerary cardinals, exceptions are possible for  $p = 2$  (only 1 case) and for  $p \nmid n$ , then still in finite number. Let us have  $q$  the number of these cases. Their relative frequency is therefore  $q/\infty \equiv 0$ .

It is therefore sufficient to study  $P(x) = c \pmod{p}$  ( $\delta = 1$ ). As the supernumerary cardinals have a null relative frequency, it only remains to study the cases  $ve = 0$  to  $n$ .

We then have:

$$\text{freq}(n, m = n) = 1/m! = 1/n! \quad (49)$$

$$\text{freq}(n, m = n-1) = 0 \quad (50)$$

$$\text{freq}(n, m < n-1) = \frac{1}{m!} \left( \frac{1}{2} - \frac{1}{2.3} + \frac{1}{2.3.4} - \dots + \frac{(-1)^n}{(n-m)!} \right) \quad (51)$$

#### Very incomplete proof

Let us have  $m$  the number of solutions of  $P(x) - c = 0 \pmod{p}$ . In the absence of supernumerary cardinals, we can write uniquely (to the permutations) the polynomial in the form  $(x-s_1).(x-s_2).(x-s_m).Q(x) = 0 = 0 \pmod{p}$  where  $Q(x)$  is of degree  $n-m$  and cannot be split more (in  $\mathbb{Z}/p\mathbb{Z}$ ).

Obviously, if  $P(x) = c \pmod{p}$  has  $n-1$  solutions, the polynomial then splits completely, so  $\text{freq}(n, n-1) = 0$ .

The remainder of our approach is based on a set of heuristic arguments, current process in the presence of prime numbers. Let us suppose so that to find the number of solutions of a randomly selected degree  $n$  polynomial come up to a blind drawing of cubes loose or sticking together and of all eligible configurations within a black box.

We have the following injection :

split initial configuration

$1_1$	$1_2$	$1_3$	...	$1_n$
1	1	1	...	1



effective configuration of the polynomial

1	...	1	$m-n$	1	...	1
1	...	1	$\#(m-n)$	1	...	1

Degrees (total = $n$ )
Lengths

We do match here on one side a cube of length 1 with a split solution (distinct or not to others) and on the other side a brick of length  $\#(n-m)$  with a non-split part of  $Q(x)$  of degree  $n-m$ . The dimensions of the bricks, other than the length, are identical and are therefore ignored. To each of the initial configurations, which are permutations of  $1_i$ ,  $i = 1$  to  $n$  and which are therefore in quantity  $n!$ , we do match a split brick or a not-split brick, the relative weight of the non-split brick being correlated in an "adapted" length.

The determinative hypothesis for this heuristic evaluation is that the length  $\#(n-m)$  is in no way dependent on  $n$  but only the difference  $n-m$ . It follows, at the right of underneath equality, the first term card  $(n-m)$ . To draw randomly the brick of length  $\#(n-m)$  also depends on the position of the brick, for which there are  $n-m$  combinations among  $n$ . It follows the second term below.

We have thus:

$$\text{card}(n, m) = \text{card}(n-m, 0) \cdot \binom{n-m}{n} \quad (52)$$

We can then deduce all of the cardinals by the following construction :

Table (19)

Nb solutions \ Degree	1	2	3	4
0	0	1	2	...
1	1	0	3	...
2		1	0	...
3			1	...
...				...

Each of the cardinals on a diagonal is obtained from the cardinal of the first line in correspondence (or the previous element by a combinatorial ratio). The cardinals of degree 1 and 2 are known (and proved). We after that proceed step by step according to a diagonal, then the next to his right. At the stage of degree n, there is only a single unknown value (here marked in red for the degree 3 stage). This value is obtained simply by difference to the sum of cardinals according to the current column, sum which is n!.

Obtaining the formula (51) request some additional calculations that we report after the more complete numerical table given below.

Table (20)

Degrees (n)	1	2	3	4	5	6	7	8	9	10	11	12...
Nb solutions (m)	Card(n,m) = Proportions of solutions (before dividing by total of proportions)											
0	0	1	2	9	44	265	1854	14833	133496	1334961	14684570	176214841
1	1	0	3	8	45	264	1855	14832	133497	1334960	14684571	176214840
2		1	0	6	20	135	924	7420	66744	667485	7342280	88107426
3			1	0	10	40	315	2464	22260	222480	2447445	29369120
4				1	0	15	70	630	5544	55650	611820	7342335
5					1	0	21	112	1134	11088	122430	1468368
6						1	0	28	168	1890	20328	244860
7							1	0	36	240	2970	34848
8								1	0	45	330	4455
9									1	0	55	440
10										1	0	66
11											1	0
12												1
Total card. = n!	1	2	6	24	120	720	5040	40320	362880	3628800	39916800	479001600

Let us recall that, the chosen polynomial being suitable indeed to this table (without proof, the factorization of the polynomial P(x) and the sign of the discriminant of P(x) c do intervene), a number of targets will in general make exception (and fairly systematically the target c = 0).

Numerical tests confirm the evaluation of these relative frequencies, with calculation errors in focus, because we ought to note large saw teeth variations in these values (in the range of available calculations on a standard computer). These tests also confirm that the polynomial expression occurs according to the presence of given multiple integer roots, the frequency corresponding either to table 20 (single root or irreducibility), either to table 13 (monomials), either to an another form (varying according to the multiple roots decomposition).

The table can then be read in different ways :

- according to the lines,
- according to the main diagonal,
- according to the columns.

Let us deal successively with these different approaches.

Let us start with the first line. The expression for the degree n is deduced at the previous column by the basic formula :

$$\text{card}(n,0) = n.\text{card}(n-1,0) + (-1)^n \quad (53)$$

Let us suppose that this is the case. We have then under a developed form by adding the case n = 1 and n = 2 :

$$\begin{aligned} \text{card}(1,0) &= 0 \\ \text{card}(2,0) &= 1 \\ \text{card}(n > 2,0) &= n.(n-1).(n-2) \dots 3 - n.(n-1).(n-2) \dots 4 + n.(n-1).(n-2) \dots 5 + (-1)^{n-1}.n + (-1)^n \end{aligned} \quad (54)$$

Let us then examine the finite differences according to (non-trivial) diagonals :

Tables (21)

#(diag 2)	1	3	6	10	15	21	28	36	45	55
dif1		2	3	4	5	6	7	8	9	10
dif2			1	1	1	1	1	1	1	1

#(diag 3)	2	8	20	40	70	112	168	240	330	440
dif1		6	12	20	30	42	56	72	90	110
dif2			6	8	10	12	14	16	18	20
dif3				2	2	2	2	2	2	2

#(diag 4)	9	45	135	315	630	1134	1890	2970	4455	6435
dif1		36	90	180	315	504	756	1080	1485	1980
dif2			54	90	135	189	252	324	405	495
dif3				36	45	54	63	72	81	90
dif4					9	9	9	9	9	9

#(diag 5)	44	264	924	2464	5544	11088	20328	34848	56628	88088
dif1		220	660	1540	3080	5544	9240	14520	21780	31460
dif2			440	880	1540	2464	3696	5280	7260	9680
dif3				440	660	924	1232	1584	1980	2420
dif4					220	264	308	352	396	440
dif5						44	44	44	44	44

This shows that the proportion of solutions following diagonals is represented by a degree n polynomial. More specifically, using the choice of m elements among n, it is of the above mentioned form :

$$\text{card}(n + m, m) = \text{card}(n, 0) \cdot \binom{m}{n} \quad (55)$$

So that for  $n > 2$  :

$$\text{card}(n + m, m) = (n(n-1)(n-2) \dots 3 - n(n-1)(n-2) \dots 4 + \dots + (-1)^{n-1} \cdot n + (-1)^n) \cdot \binom{m}{n}$$

So that also :

$$\text{card}(n, m) = ((n-m)(n-m-1) \dots 3 - (n-m)(n-m-1) \dots 4 + \dots + (-1)^{n-1} \cdot (n-m) + (-1)^n) \cdot \binom{m-n}{n}$$

At the degree n, the frequency for m solutions is finally obtained by dividing the cardinal by all possible drawings (here n!), so that :

$$\text{freq}(n, m) = \frac{(n-m)(n-m-1) \dots 3 - (n-m)(n-m-1) \dots 4 + (n-m)(n-m-1) \dots 5 - \dots + (-1)^{n-1} (n-m) + (-1)^n}{(n-m)!m!}$$

or otherwise

$$1/m! \cdot \frac{(n-m)(n-m-1) \dots 3 - (n-m)(n-m-1) \dots 4 + (n-m)(n-m-1) \dots 5 - \dots + (-1)^{n-1} (n-m) + (-1)^n}{(n-m)!m!}$$

So that finally (for  $m < n-1$ ) :

$$\text{freq}(n, m < n-1) = \frac{1}{m!} \left( \frac{1}{2} - \frac{1}{2 \cdot 3} + \frac{1}{2 \cdot 3 \cdot 4} - \dots + \frac{(-1)^n}{(n-m)!} \right) \quad (56)$$

Let us note also the limit case :

$$\lim_{n-m \rightarrow \infty} \text{freq}(n, m) = \frac{1}{e \cdot m!} \quad (57)$$

#### 2.4.7.5 Application to equiprobability

Let us note again, as for an above remark for degree 3 polynomials, that for  $P(x, c) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x - c$ , the only targets c, which we are concerned with, are of the form  $a_n \cdot i^n + a_{n-1} \cdot i^{n-1} + \dots + a_1 \cdot i$ , with i an integer (the other cases corresponding to locally null cardinal cases), we can rewrite the polynomial P(x) form by simple Euclidean division  $P(x, i) = (x-i) \cdot Q(x, i)$  with Q(x, i) a polynomial of degree n-1.

This requires a simple translation (with regard of the polynomial degree) of the data in the table (20) and the addition of the "free" solution :

Table (22)

Degree (n)	2	3	4	5	6	...
n-1	1	2	3	4	5	...
Nb solutions (m)	Card(n,m)					
0+1	0	1	2	9	44	...
1+1	1	0	3	8	45	...
2+1		1	0	6	20	...
3+1			1	0	10	...
4+1				1	0	...
5+1					1	...

Of course, as we already indicate, there exist polynomials which do not meet this cardinal distribution. We have noticed the monomials, but all sorts of intermediate forms can be considered such as  $x^{n-r}(x+a)^r$ . Nevertheless, the essential conclusion on equiprobability remains for these intermediate cases (still waiting of demonstration).

This being established, we can eliminate reducing them to 1 by simple division (as in the case de monomials) all the non-supernumerary cardinals factors of abundance.

Thus, the product of local factors depends only on the supernumerary cardinals that we study below.

#### 2.4.7.6 Study of supernumerary cardinals

The discriminant of an equation detects multiple roots of a global or local equation. It is null when such roots exist. The null value means locally that

$$\text{Disc} = 0 \bmod p^\delta$$

But the converse is false as we saw earlier.

The main difficulty in the handling of the supernumerary cardinals is to identify the standard cardinals they replace.

So even if we completely dominate the subject of the cardinals for the standard targets and those of supernumerary cardinals, the impossibility of identifying the underlying replacement is insurmountable. What saves us at least is the simple and consensual finitude of cases. This allows us to force the expression "factor x volume" to meet our requirement by simple case by case adaptation. We must, however, observe that these supernumerary cardinals are finite numbers (null density) and will be without impact at the passage to several variables. The said forcing becomes unnecessary.

All these considerations give us a sufficient basis to address asymptotic equations in several variables. Prior to this, it is useful to consider the second category of equations with one variable: the monomials and polynomials of one variable of prime numbers.

### 2.4.8 Reconstruction of the set of prime numbers

#### 2.4.8.1 Minimal needs

We have conducted projections of prime numbers on modulo  $p^\delta$  classes in paragraph 1.2.3. We want now to do the reverse and restore this set. It is an essential step without which to reach more generality would be impossible. The equiprobability greatly simplifies operations.

#### 2.4.8.2 Implementation

Let us have  $\varepsilon$  a positive real. Let us build the table below in which we consider a variable "y" describing the set of natural numbers. We wish to extract the set of prime umbers via a multiplicative modulo p process. To do this, whenever p divides y, we make a weighting  $\varepsilon$  with a power equal to the valuation of p in y, otherwise we make a weighting of 1, except when  $y = 1$  and in which case the weighting will be  $1-\varepsilon$ .

Table (23)

p \ y	0	1	2	3	4	5	6	7	8	9	10	11	...	$\infty$
2	0	$1-\varepsilon$	$\varepsilon$	1	$\varepsilon^2$	1	$\varepsilon$	1	$\varepsilon^3$	1	$\varepsilon$	1	...	...
3	0	$1-\varepsilon$	1	$\varepsilon$	1	1	$\varepsilon$	1	1	$\varepsilon^2$	1	1	...	...
5	0	$1-\varepsilon$	1	1	1	$\varepsilon$	1	1	1	1	$\varepsilon$	1	...	...
7	0	$1-\varepsilon$	1	1	1	1	1	$\varepsilon$	1	1	1	1	...	...
11	0	$1-\varepsilon$	1	1	1	1	1	1	1	1	1	$\varepsilon$	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
p	0	$1-\varepsilon$	1	1	1	1	1	1	1	1	1	1	...	...
Product $\Pi$	0	$(1-\varepsilon)^t$	$\varepsilon$	$\varepsilon$	$\varepsilon^2$	$\varepsilon$	$\varepsilon^2$	$\varepsilon$	$\varepsilon^3$	$\varepsilon^2$	$\varepsilon^2$	$\varepsilon$	...	...
$\Pi/\varepsilon$	0	$(1-\varepsilon)^t/\varepsilon$	1	1	$\varepsilon$	1	$\varepsilon$	1	$\varepsilon^2$	$\varepsilon$	$\varepsilon$	1	...	...

The weighting in the column of the element 0 is zero because  $p^k$  divides 0 for all  $k$  et we write then  $\varepsilon^{k \rightarrow +\infty} = 0$  (for  $0 < \varepsilon \ll 1$ ). If  $t > 2\text{Ln}(\varepsilon)/\text{Ln}(1-\varepsilon)$  then  $(1-\varepsilon)^t/\varepsilon < \varepsilon$ . As  $t$  tends to infinity, it results that  $(1-\varepsilon)^t/\varepsilon$  tends to 0 for any  $\varepsilon$  such as  $0 < \varepsilon \ll 1$ .

When  $\varepsilon$  tends towards 0, the row in the table corresponding to the sequence  $p$  tends towards the local variable  $\{1, 2, \dots, p-1\}$  by assignment of 0 or 1.

After multiplication of the elements of the columns, and division by  $\varepsilon$ , the last line of the table shows 1 for any prime number and a near zero value otherwise when  $\varepsilon$  is near zero. We realise thus our initial goal. In this way, we can get the list of prime numbers with a weighting of 1 and the other numbers with a residual weighting as small as wanted.

#### 2.4.8.3 Theorem of prime numbers local - global reconstruction

The list of prime numbers is asymptotically the product after deployment of (following columns) components of the local variables from sequence 2 to  $\infty$  with the same coefficient of density for the entire list.

Note :

One must keep in memory the shade of writing  $\varepsilon \rightarrow 0$  (instead of  $\varepsilon = 0$ ). Otherwise, all of the set  $P$  disappears with the product of the representatives. However, in the presence of additional variables, it is not generally useful to maintain this subtlety (and then simply take  $\varepsilon = 0$ ).

#### 2.4.9 The example of $y^n$

##### 2.4.9.1 Singular series

Let us have to solve

$$y^n = c \bmod p^\delta$$

##### 2.4.9.1.1 Case of odd p

Let us have  $d_i = (n, \Phi(\delta-i))$  where  $\Phi(\delta-i) = p^{\delta-i-1} \cdot (p-1)$  and  $\delta n = \text{int}((\delta-1)/n)$  the integer part of  $(\delta-1)/n$ .

We can then set up the following table :

Table (24)

y	$c = y^n \bmod p^\delta$	$\#\{c\}$	$\#\{\text{variants de } c\}$
0	0	$\varepsilon^{\delta n+1} \cdot p^{\delta-\delta n-1}$	1
$p^{\delta-1} \cdot \{g^0, g^1, \dots, g^{\Phi(1)-1}\}$ $p^{\delta-2} \cdot \{g^0, g^1, \dots, g^{\Phi(2)-1}\}$ ...			
$p^{\delta n+1} \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-(\delta n+1))-1}\}$ $p^{\delta n} \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-\delta n)-1}\}$	$p^{\delta n} \cdot \{g^{0.d[\delta n]}, g^{1.d[\delta n]}, \dots, g^{(\Phi(\delta-\delta n)/d[\delta n]-1).d[\delta n]}\}$	$\varepsilon^{\delta n} \cdot d_{\delta n} \cdot p^{\delta n-(n-1)}$	$\Phi(\delta-\delta n)/d_{\delta n}$
...	...	...	...
$p^i \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-i)-1}\}$	$p^{i.n} \cdot \{g^{0.d[i.n]}, g^{1.d[i.n]}, \dots, g^{(\Phi(\delta-i)/d[i.n]-1).d[i.n]}\}$	$\varepsilon^i \cdot d_{i.n} \cdot p^{1-(n-1)}$	$\Phi(\delta-i)/d_{i.n}$
...	...	...	...
$p^1 \cdot \{g^0, g^1, \dots, g^{\Phi(\delta-1)-1}\}$ $p^0 \cdot \{g^0, g^1, \dots, g^{\Phi(\delta)-1}\}$	$p^n \cdot \{g^{0.d[n]}, g^{1.d[n]}, \dots, g^{(\Phi(\delta-n)/d[n]-1).d[n]}\}$ $p^0 \cdot \{g^{0.d[0]}, g^{1.d[0]}, \dots, g^{(\Phi(\delta)/d[0]-1).d[0]}\}$	$\varepsilon^1 \cdot d_n \cdot p^{(n-1)}$ $\varepsilon^0 \cdot d_0$	$\Phi(\delta-n)/d_n$ $\Phi(\delta)/d_0$

It is a simple copy of the table in paragraph 2.4.4.1.1 adding to  $\#(c)$  the weighting  $\varepsilon^i$  where  $i$  is the valuation of  $p$  in  $y$ . We have, for non-zero  $\varepsilon$ ,  $\varepsilon^0 = 1$ . The significance of  $\varepsilon^{\delta n+1}$  in the previous table is  $\varepsilon^{\delta n+i}$  with  $i \geq 1$  and it does not matter in fact the precise value of  $i$ . When we give to  $\varepsilon$  an infinitesimal, the variable  $y$  tends then towards the representative  $\{g^0, g^1, \dots, g^{\Phi(\delta)-1}\}$  which is our goal.

##### 2.4.9.1.2 Case of even p (p=2)

We use the couple of generators (5,-5).

Let us have  $d_i = (n, \Phi(\delta-i)/2)$  where  $\Phi(\delta-i) = 2^{\delta-i-1}$  and  $\delta n = \text{int}((\delta-1)/n)$ .

We can set up again the table of the cardinals of the residues as in the case of odd sequences :

Table (25)

y	$y^n = c \bmod 2^\delta$	$\#\{c\}$
0 $2^{\delta-1} \cdot \{5^0\}$ $2^{\delta-2} \cdot \{5^0, 5^1, \dots, 5^{\Phi(2)-1}\}$ $2^{\delta-2} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(2)-1}\}$ ... $2^{\delta n+1} \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-(\delta n+1))-1}\}$ $2^{\delta n+1} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-(\delta n+1))-1}\}$	0 $2^{\delta n} \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-\delta n)/d[\delta n]-1}\}$ $2^{\delta n} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-\delta n)/d[\delta n]-1}\}$	$\varepsilon^{\delta n+1} \cdot 2^{\delta-\delta n-1}$
$2^{\delta n} \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-\delta n)-1}\}$ $2^{\delta n} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-\delta n)-1}\}$	$2^{\delta n} \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-\delta n)/d[\delta n]-1}\}$ $2^{\delta n} \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-\delta n)/d[\delta n]-1}\}$	$\varepsilon^{\delta n} \cdot 2^{\delta-\delta n-1}$
...	...	...
$2^i \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-i)-1}\}$ $2^i \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-i)-1}\}$	$2^{i.n} \cdot \{5^{0.d[i.n]}, 5^{1.d[i.n]}, \dots, 5^{\Phi(\delta-i.n)/d[i.n]-1}\}$ $2^{i.n} \cdot \{(-5)^{0.d[i.n]}, (-5)^{1.d[i.n]}, \dots, (-5)^{\Phi(\delta-i.n)/d[i.n]-1}\}$	$\varepsilon^i \cdot d_{i.n} \cdot 2^{i.(n-1)}$
...	...	...
$2^1 \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta-1)-1}\}$ $2^1 \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta-1)-1}\}$	$2^n \cdot \{5^{0.d[n]}, 5^{1.d[n]}, \dots, 5^{\Phi(\delta-n)/d[n]-1}\}$ $2^n \cdot \{(-5)^{0.d[n]}, (-5)^{1.d[n]}, \dots, (-5)^{\Phi(\delta-n)/d[n]-1}\}$	$\varepsilon^1 \cdot d_n \cdot 2^{(n-1)}$
$2^0 \cdot \{5^0, 5^1, \dots, 5^{\Phi(\delta)-1}\}$ $2^0 \cdot \{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta)-1}\}$	$2^0 \cdot \{5^{0.d[0]}, 5^{1.d[0]}, \dots, 5^{\Phi(\delta)/d[0]-1}\}$ $2^0 \cdot \{(-5)^{0.d[0]}, (-5)^{1.d[0]}, \dots, (-5)^{\Phi(\delta)/d[0]-1}\}$	$\varepsilon^0 \cdot d_0$

Let us have  $c \bmod 2^\delta$  residue and let us have  $m$  the multiplicity of factor 2 in  $n$ . We then have the following summary table (the values of column  $y$  can be verified by substitution in  $y^n = c \bmod 2^\delta$ ) :

Table (26)

y	Conditions on $k, i$ and $n$	c	$\#\{c\}$	$\#\{\text{variants of } c\}$
$2^{\delta n} \cdot (2k)$	$k = 0, 1, \dots, 2^{\delta-\delta n-1}-1$	0	$\varepsilon^{\delta n} \cdot 2^{\delta-\delta n-1}$	1
$2^{\delta n} \cdot (1+2k)$	$k = 0, 1, \dots, 2^{\delta-\delta n-1}-1$	$2^{\delta n}$	$\varepsilon^{\delta n} \cdot 2^{\delta-\delta n-1}$	1
$2^1 \cdot (1+2 \cdot (\#\{1\}) \cdot k)^{1/n}$ $+ 2^{\delta-i \cdot (n-1)} / (\#\{1\})k$	$k = 0, 1, \dots, 2^{\delta-1-i \cdot n} / (\#\{1\})-1$ $i = 0 \text{ to } \delta n-1$ $k' = 0 \text{ to } 2^{i \cdot (n-1)} \cdot (\#\{1\})-1$	$2^{1 \cdot n} \cdot (1+2 \cdot \#\{1\}) \cdot k$	$\varepsilon^1 \cdot 2^{i \cdot (n-1)} \cdot (\#\{1\})$	$2^{\delta-1-i \cdot n} / (\#\{1\})$

When we give to  $\varepsilon$  an infinitesimal weighting, the variable is then tends towards the representative  $\{5^0, 5^1, \dots, 5^{\Phi(\delta)-1}\}$ ,  $\{(-5)^0, (-5)^1, \dots, (-5)^{\Phi(\delta)-1}\}$  which is our goal.

#### 2.4.9.1.3 Number of solutions of $y^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}$ .

As in the case of an integer variable equation, we will see in the next paragraph the purpose of the below individual cases  $c = 1$  and  $c \neq 1$ .

Case  $c \neq 0, c \neq 1, c \neq y^n$

We apply the Chinese theorem :

$$\#\{y^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = \#\{y^n = c \bmod 2^\delta\} \cdot \prod \#\{y^n = c \bmod p_i^{\delta_i}\}$$

As  $c \neq y^n$ , one at least of the terms is zero so the product is zero.

Case  $c \neq 0, c \neq 1, c = y^n$

We still apply the Chinese theorem :

$$\#\{y^n = c \bmod 2^\delta \cdot \prod p_i^{\delta_i}\} = \#\{y^n = c \bmod 2^\delta\} \cdot \prod \#\{y^n = c \bmod p_i^{\delta_i}\}$$

The number of solutions of  $y^n = c \bmod p_i^{\delta_i}$  is given by the tables presented in paragraphs 2.4.9.1.1 et 2.4.9.1.2. If  $c = (2^r \cdot p_1^{k_1} \cdot p_2^{k_2} \dots p_j^{k_j})^n$ , we have  $\varepsilon^{k_i} \cdot d_{k_i,n} \cdot p^{k_i \cdot (n-1)}$  classes of solutions each time that  $p_i$  is equal to one of the numbers  $p_1, p_2, \dots$  or  $p_j$  (with  $d_{k_i,n} = 1$  in the case of factor 2), otherwise we have  $d_0$  classes of solutions when  $p_i$  is different from the set of the numbers  $p_1, p_2, \dots$  et  $p_j$ .

Thus :

$$1 = \frac{\#\{y^n = c \bmod p_1^{\delta_i}\}}{\varepsilon^{k_1} \cdot d_{k_1,n} \cdot p^{k_1 \cdot (n-1)}} = \frac{\#\{y^n = c \bmod p_2^{\delta_i}\}}{\varepsilon^{k_2} \cdot d_{k_2,n} \cdot p^{k_2 \cdot (n-1)}} = \dots = \frac{\#\{y^n = c \bmod p_i^{\delta_i}\}}{\varepsilon^{k_j} \cdot d_{k_j,n} \cdot p^{k_j \cdot (n-1)}} = \frac{\#\{y^n = c \bmod p_i^{\delta_i}\}}{\varepsilon^0 \cdot d_0}$$

Let us look at the  $d_{k,n}$ . We have first of all  $d_0 = \#\{y^n = 1 \mod p_i^{\delta_i}\}$  which is a constant for  $\delta_i$  large enough. This hypothesis (large enough  $\delta_i$ ) is well understood now. We simplify the writing of  $\#\{y^n = 1 \mod p_i^{\delta_i}\}$  into  $\#\{1\}$  when no confusion results. We always have :

$$d_{k,n} = (n, \Phi(\delta_i - k, n)) = (n, p_i^{\delta_i - k, n-1} \cdot (p-1))$$

and in peculiar

$$d_0 = (n, p_i^{\delta_i-1} \cdot (p-1))$$

It is clear that, for large enough  $\delta_i$ ,  $p$  and  $(p-1)$  factors are in the given gcd  $(n, \dots)$ , and therefore again :

$$d_{k,n} = d_0 = \#\{y^n = 1 \mod p_i^{\delta_i}\}$$

So that :

$$\frac{\#\{y^n = c \mod 2^\delta \cdot \prod p_i^{\delta_i}\}}{\#\{1\}^{j+1}} = \varepsilon^r \cdot \varepsilon^{k_1} \cdot \varepsilon^{k_2} \dots \varepsilon^{k_j} \cdot 2^{r \cdot (n-1)} \cdot p^{k_1 \cdot (n-1)} \cdot p^{k_2 \cdot (n-1)} \dots p^{k_j \cdot (n-1)} = \varepsilon^r \cdot \varepsilon^{k_1} \cdot \varepsilon^{k_2} \dots \varepsilon^{k_j} \cdot c^{(n-1)/n} \quad (58)$$

Case  $c = 1$

$$\#\{y^n = 1 \mod 2^\delta \cdot \prod p_i^{\delta_i}\} = \#\{y^n = 1 \mod 2^\delta\} \cdot \prod \#\{y^n = 1 \mod p_i^{\delta_i}\} \quad (59)$$

The product is used as a reference  $\#(1)$ . Its actual value is not of significant importance.

Case  $c = 0$

The product is null.

#### 2.4.9.2 Function volume and cardinal of product

Again, as in paragraph 2.4.4.2, we assume the generality of the formula that follows, even in a field where this does not make sense. Thus as  $y^n = c$ , it just  $y = c^{1/n}$ . As  $y$  is a prime numbers variable, we have the classic formula of enumeration in  $y/\ln(y)$  given by Gauss, so that :

$$V(c) \approx c^{1/n} / \ln(c^{1/n}) = n \cdot c^{1/n} / \ln(c)$$

Then, neglecting the logarithmic square term :

$$V'(c) \approx n \cdot c^{1/n-1} / \ln(c)$$

This is obviously strictly applicable only when  $c$  tends towards infinity (asymptotic model).

Case  $c \neq 0, c \neq 1, c \neq y^n$

The singular series is null. We thus have :

$$\#\{x^n = c\} = 0. V'(c) = 0 \quad (60)$$

It is the sought result.

Case  $c \neq 0, c \neq 1, c = y^n$

With  $\#\{y^n = c \mod 2^\delta \cdot \prod p_i^{\delta_i}\} = \varepsilon^r \cdot \varepsilon^{k_1} \cdot \varepsilon^{k_2} \dots \varepsilon^{k_j} \cdot c^{(n-1)/n} \cdot \#\{1\}^{j+1}$  and  $V'(c) = (1/n) \cdot c^{-(n-1)/n} / \ln(c)$ , it follows :

$$\#\{y^n = c\} = \varepsilon^r \cdot \varepsilon^{k_1} \cdot \varepsilon^{k_2} \dots \varepsilon^{k_j} \cdot (1/n) \cdot \#\{1\}^{j+1} / \ln(c)$$

The expression right member tends towards 0 when  $\varepsilon$  is an infinitesimal unless  $r + k_1 + k_2 + \dots + k_j = 0$ , that is if  $c$  has no prime factor, that is if  $c = 1$ . For discussion of this case, we refer to the next paragraph.

The expression has no meaning either if  $c = 0$ .

The cases  $c = 0$  or  $c = 1$  being eliminated, there remains the situation where  $r + k_1 + k_2 + \dots + k_j \geq 1$ , then :

$$\#\{y^n = c\} / \varepsilon = \varepsilon^{r+k_1+k_2+\dots+k_j-1} \cdot (1/n) \cdot \#\{1\}^{j+1} \cdot c^{1/n-1} / \ln(c)$$

Now the second member is different from an infinitesimal and is equal to a constant  $(1/n) \cdot \#\{1\}^{j+1}$  only when  $r + k_1 + k_2 + \dots + k_j = 1$ , that is when  $c$  is a prime number.

It is the constant sought result. Thus the global-local process sieves well the variable  $y$  as a variable of prime numbers with equiprobability.

### Case $c = 0$

The  $y^n = 0$  equation makes no sense since  $y$  is a prime number.

In fact, the case  $c = 0$  has no peculiar state in the  $y^n = c$  exercise. It is simply a case without solution like so many.

### Case $c = 1$

Like the case  $c = 0$  for the equation  $x^n = 0$ , the  $c = 1$  case is an "obstruction" to the resolution of  $y^n = c$ . Still, this exception is unique. On one hand, the reason for this exception is similar to the one given above and can be translated by

$$1^n = 1$$

for all  $n$ . It is therefore impossible to assign to this target a multiplicity, which can be arbitrary. As said above for the equation with integer variable, there is no obstruction but rather an indeterminacy. On the other hand, "obstruction" comes also from the volume expression which shows  $\ln(c) = \ln(1) = 0$  in the denominator which has no meaning.

We will address once more this exception at the end of the article in paragraph 2.6.2.3. Let us note however that in practice, this exception is of quite marginal interest as 1 does not have the status of a prime number to start with and we can say that the equation has no solution from the starting point.

### **2.4.10 Case of polynomials.**

Studies on the polynomials, similar to those of paragraphs 2.4.5, 2.4.6 and 2.4.7, could be conducted here for prime numbers variables. However, they do not gender new discoveries and are thus of minor importance. We therefore happily drop out these rough layouts to lighten the text (already sufficiently long after all).

Our study on one variable diophantine equations summarizes to two points, somewhat to the antipodes, concerning the phenomenon of obstruction :

- It is latent, meaning it arises as soon as the first variable is on the paper.
- It is marginal, even in this case (with one variable) where the difficulties were foreseen as the rule (statistical distributions are favourable to the enumerations of solutions when the number of variables increases and vice versa).

### **2.5 Local-global enumerations with two or more variables**

We make a review, to start with, for cases whose behaviour is clearly established to validate the applicability of the concept of local variables.

#### **2.5.1 Case of arithmetic series**

Let us recover the equiprobability in arithmetic series from local variables. The formal equation writes as :

$$p = a.n + c \quad (61)$$

Here  $a$  is a given positive number,  $n$  is a variable taking values in the set  $N$ ,  $p$  is a variable taking values across prime numbers. We are seeking then the average arithmetic equivalent of  $c$  modulo  $a$ .

Let us have a prime number  $p$ . The congruency classes formed from  $a.n$  modulo  $p$  are :

$a.N \bmod p$	$0.a$	$1.a$	$2.a$	$\dots$	$(p-1).a$
---------------	-------	-------	-------	---------	-----------

We have two cases :

$a = 0 \bmod p$	0	0	0	$\dots$	0
$a \neq 0 \bmod p$	0	1	2	$\dots$	$p-1$

Let us have  $R_p$  the local variable representing  $P$  at sequence  $p$ .  $R_p = \{1, 2, \dots, p-1\}$ .

Let us have  $c$  an element of the classes modulo  $p$  obtained by subtractive crossing of  $R_p$  and  $a.N$ .

Then, if  $a \not\equiv 0 \pmod p$

Table (27)

$R_p - a.N \pmod p$	0	1	...	$p-1$
1	1	0		2
2	2	1		3
...	...	...		...
$p-2$	$p-2$	$p-3$		1
$p-1$	$p-1$	$p-2$		0

so that

$$\#\{c\} = p-1$$

which means equidensity of the classes of congruencies for all  $c$ .

Then, if  $a \equiv 0 \pmod p$

Table (28)

$R_p - a.N \pmod p$	0	0	...	0
1	1	1		1
2	2	2		2
...	...	...		...
$p-2$	$p-2$	$p-2$		$p-2$
$p-1$	$p-1$	$p-1$		$p-1$

so that

$$\begin{aligned}\#\{c = 0\} &= 0 \\ \#\{c \neq 0\} &= p\end{aligned}$$

which means equidensity of the classes of congruencies for all  $c$  except  $c = 0$  with to zero density.

What can be written also :

$$\#\{c \setminus R_p - a.N = c \text{ modulo } 2.3 \dots p\} = \prod_{q|a}^p q \prod_{q \nmid a}^{P} q-1 \quad (62)$$

or :

$$\#\{c \setminus R_p - a.N = c \text{ modulo } 2.3 \dots p\} = \prod_{q|a} q/(q-1) \prod_{q \nmid a}^{P} q-1 \quad (63)$$

The second product of the relation (63) is identical, as normalization is concerned, for all sequence  $c$ . At given  $a$ , we again find the expected equidensity. The first product allows also to find density  $1/\varphi(a)$  by writing  $a = \prod_{q|a} q^k$ ,  $\varphi(a) = \prod_{q|a} q^{k-1} \cdot (q-1)$ , so that  $a/\varphi(a) = \prod_{q|a} q/(q-1)$ .

Note: There is no need to consider cases modulo  $p^k$ ,  $k > 1$ , the degree of stability being  $k = 1$ .

### 2.5.2 Polignac, Vinogradov and relatives

A this stage of development of our tools, it takes little effort to solve this degree 1 type of exercises. We seek the singular series corresponding to :

$$p_1 + p_2 + \dots + p_i = c \quad (64)$$

This is to establish the standardized factors of abundance of targets  $c$  generated in a table having two axis crossing  $p_1 + p_2 + \dots + p_{i-1}$  and  $p_i$  :

Table (29)

	$\#(p_i)$	$1/(p-1)$	$1/(p-1)$	$1/(p-1)$	$1/(p-1)$
$\#(p_1+p_2+\dots+p_{i-1})$	$p_1+p_2+\dots \bmod p$	1	2	...	$p-1$
$\#(0)$	0	1	2		$p-1$
$\#(1)$	1	2	3		0
$\#(2)$	2	3	4		1
...	...	...	...		...
$\#(p-2)$	$p-2$	$p-1$	0		$p-3$
$\#(p-1)$	$p-1$	0	1		$p-2$

Let us note again that, to make this calculation, we use the fact that the degree of stability of the variables  $p_k$  is 1.

Let us then proceed by induction to find these occurrences.

For  $i = 1$ , we have two cases for targets :

c	$\#(c)$
$c = 0 \bmod p$	0
$c \neq 0 \bmod p$	$p/(p-1)$

Let us suppose made  $i-1$  crossings and let us still assume two cases for targets. Let us note also that the case  $i = 1$  meets the hypothesis :

c	$\#(c)$
$c = 0 \bmod p$	$1-(-1)^{i-1}/(p-1)^{i-1}$
$c \neq 0 \bmod p$	$1-(-1)^i/(p-1)^i$

This means that  $\#(c \neq 0 \bmod p) = \#(1)$ .

Let us note  $\#(c)$  the new values to the stage  $i$  and by  $\#(c)$  the previous ones. We also write to simplify  $\#(c = 0 \bmod p) = \#(0)$  and  $\#(c \neq 0 \bmod p) = \#(1)$ .

We will have then :

$$\begin{aligned}\#(0) &= \#(0) \cdot (p-1)/(p-1) \\ \#(1) &= \#(0) \cdot 1/(p-1) + \#(1) \cdot (p-2)/(p-1)\end{aligned}$$

So that also

$$\begin{aligned}\#(0) &= 1-(-1)^{i+1-1}/(p-1)^{i+1-1} \\ \#(1) &= (1-(-1)^{i-1}/(p-1)^{i-1})/(p-1) + (1-(-1)^i/(p-1)^i) \cdot (p-2)/(p-1) = 1-(-1)^{i+1}/(p-1)^{i+1}\end{aligned}$$

We check well the hypothesis of recurrence.

Thus, taking account of the volume available  $V'(c) = (1/c) \cdot (c/\ln(c))^i$  for the target  $c$  :

$$\lim_{c \rightarrow \infty} \# \{ (p_1, p_2, \dots, p_i) \setminus p_1+p_2+\dots+p_i = c \} = \prod_{p \nmid c} \left(1 - \frac{(-1)^i}{(p-1)^i}\right) \prod_{p \mid c} \left(1 - \frac{(-1)^{i-1}}{(p-1)^{i-1}}\right) \cdot c^{i-1}/\ln^i(c) \quad (65)$$

This is the formula of the mathematical literature. It is only true asymptotically, the enumerations for finite  $c$  and a small number of variables being very far away from this formula.

### 2.5.3 Case of polynomials with more than two variables

When three variables, or more, appear in a diophantine equation with non-symmetrical asymptotic branches, numerical verifications fail in general. Indeed, in the numerical approach to three variables or more, there are multiple ways (an infinite) to define the volume in its progression to infinity. If the distribution of solutions is not homogeneous following the various axis (that is the different variables), all choices of volumes are not suitable.

The choice of a given volume in the search for the number of solutions comes up to add new equations in the original equation  $R(x,y,z,\dots) = c$ , hence the system of equations :

$$\begin{aligned}R(x,y,z,\dots) &= c \\ L(x,y,z,\dots) &= 0 \\ &\dots\end{aligned}$$

However, the proposed method is not made for these cases.

We have developed the point, in another article, some sophisticated matrix methods to evaluate the singular series in the presence of multiple variables. One must keep in memory the present reserve on the choice of the volume in the case of failures in numerical verifications as volume choice must be adapted.

## 2.6 Obstructions to enumerations

In part I devoted to the problem of existence of solutions, we could not highlight strong obstruction, making sense, taking into account the trivial solutions, nor for a few examples of mathematical literature, neither for a particular case of our own production.

Now, we are going to go back to the cases described in table (1) with an aim to enumerate solutions.

### 2.6.1 The examples to exclude

The enumerations, that we aim, use the identification of variables with representatives by projection of an infinite number of values. Only asymptotic branches equations allow using the chosen method. The examples to exclude are therefore already :

Table (30)

$a.x^3+b.y^3+e.z^3 = c$ for any triplet of integers (a,b,e)
$x^2+y^2+(z^2-3).(z^2-2) = c$
$x^2+y^2+(z^2+1).(z^2+3).(z^2-3)^2.(z^2+23) = c$
$x^4+17y^4-2(4z^2+t^2)^2 = c$

### 2.6.2 The remaining examples

The remaining examples include :

Table (31)

Equations
$5x^3+9y^3-10z^3-12t^3 = c$
$9x^2-2x.y-7y^2-2z^2+1 = c$

#### 2.6.2.1 Cassels et Guy equation

That is :

$$5x_1^3+9x_2^3 = 10x_3^3+12x_4^3$$

Here we have an equation with more than two variables. Despite the subject to subsection 2.5.3, it is simple enough to bend to a consistent numerical verification.

We therefore study target c parameterized equations  $c = 5x_1^3+9x_2^3-(10x_3^3+12x_4^3)$ . We seek the approximated abundance factors for different values of c as well as the number of solutions for quadruplets  $(x_1, x_2, x_3, x_4)$  limited to the field of values  $-u \leq x_1 \leq u, -u \leq x_2 \leq u, -u \leq x_3 \leq u, -u \leq x_4 \leq u$ .

Table (32)

		targets c									
		0	1	2	3	4	5	6	7	8	9
p	$\delta$	Number of local solutions (nsl)									
2	1	8	8	8	8	8	8	8	8	8	8
3	2	729	729	729	729	729	729	729	729	729	729
5	3	2265625	1953125	1953125	1953125	1953125	1953125	1953125	1953125	1953125	1953125
7	2	76489	129654	151263	93639	93639	151263	129654	74088	129654	151263
11	1	1331	1331	1331	1331	1331	1331	1331	1331	1331	1331
13	2	4853173	4541199	4969614	4969614	4969614	4541199	4969614	4969614	4541199	4969614
17	1	4913	4913	4913	4913	4913	4913	4913	4913	4913	4913
19	1	6859	6726	6726	6726	7125	6726	7125	6726	6726	7125
23	1	12167	12167	12167	12167	12167	12167	12167	12167	12167	12167
29	1	24389	24389	24389	24389	24389	24389	24389	24389	24389	24389
31	1	27001	30132	30132	30783	30132	28737	30783	30783	30132	28737
37	1	50653	51060	49839	51060	51060	51060	51060	51060	51060	49839
41	1	68921	68921	68921	68921	68921	68921	68921	68921	68921	68921
43	1	74089	78948	78948	81657	78948	81657	81657	78303	78948	78303
47	1	103823	103823	103823	103823	103823	103823	103823	103823	103823	103823
53	1	148877	148877	148877	148877	148877	148877	148877	148877	148877	148877
p	$\delta$	normalized proportions (pn = nsl/p <sup>26</sup> )									
2	1	1	1	1	1	1	1	1	1	1	1
3	2	1	1	1	1	1	1	1	1	1	1

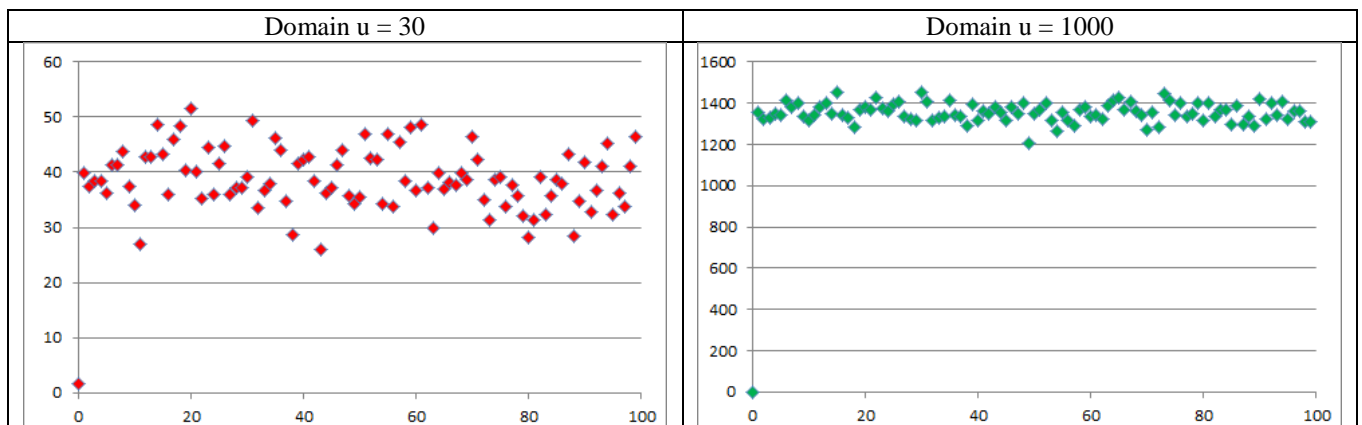
5	3	1,1600	1	1	1	1	1	1	1	1	1
7	2	0,6501	1,1020	1,2857	0,7959	0,7959	1,2857	1,1020	0,6297	1,1020	1,2857
11	1	1	1	1	1	1	1	1	1	1	1
13	2	1,0055	0,9408	1,0296	1,0296	1,0296	0,9408	1,0296	1,0296	0,9408	1,0296
17	1	1	1	1	1	1	1	1	1	1	1
19	1	1	0,9806	0,9806	0,9806	1,0388	0,9806	1,0388	0,9806	0,9806	1,0388
23	1	1	1	1	1	1	1	1	1	1	1
29	1	1	1	1	1	1	1	1	1	1	1
31	1	0,9063	1,0114	1,0114	1,0333	1,0114	0,9646	1,0333	1,0333	1,0114	0,9646
37	1	1	1,0080	0,9839	1,0080	1,0080	1,0080	1,0080	1,0080	1,0080	0,9839
41	1	1	1	1	1	1	1	1	1	1	1
43	1	0,9319	0,9930	0,9930	1,0270	0,9930	1,0270	1,0270	0,9849	0,9930	0,9849
47	1	1	1	1	1	1	1	1	1	1	1
53	1	1	1	1	1	1	1	1	1	1	1

c	0	1	2	3	4	5	6	7	8	9
	singular series = $\prod p_n$									
	0,6404	1,0293	1,2828	0,8596	0,8618	1,1846	1,2609	0,6522	1,0293	1,2854
domain u	#(effective solutions)									
1000	1	1398	1697	1142	1160	1592	1783	902	1445	1719
300	1	411	476	334	333	454	505	260	444	481
100	1	134	164	100	102	152	163	78	153	158
30	1	41	48	33	33	43	52	27	45	48

domain u	ratio singular series / #(effective solutions)									
1000	1,6	1358,2	1322,9	1328,5	1346,0	1343,9	1414,1	1383,0	1403,8	1337,4
300	1,6	270,1	244,0	268,7	242,5	272,7	274,4	243,8	286,6	259,8
100	1,6	130,2	127,8	116,3	118,4	128,3	129,3	119,6	148,6	122,9
30	1,6	39,8	37,4	38,4	38,3	36,3	41,2	41,4	43,7	37,3

By extending the range of targets c from 0 to 99, we obtain the two graphs that follow :

Graphics (3)



The dispersion of the values is related to at least three reasons :

- the test sample  $(x_1, x_2, x_3, x_4)$  is finite (with no hope to test one day the non-finite sample)
- the singular series is an approximation (sequences  $p \leq 53$  instead of  $p = 2 \rightarrow \infty$ )
- some degrees of stability  $\delta_s$  are here possibly not achieved for certain sequences (for example  $p = 5$ )

With sample increases and more accurate singular series (the reader may look at our article on asymptotic enumerations which will give all the ingredients to calculate it with the desired accuracy), the dispersion will be reduced (a priori given reason one).

The only exception to the anticipated enumeration is here the target  $c = 0$ . However, we can then write  $5(x_1^3 - 2x_3^3) = 3(3x_2^3 - 4x_4^3)$ , and thus reformulate a system of two (homogeneous) equations :

$$\begin{aligned}x_1^3-2x_3^3 &= 3r \\ 3x_2^3-4x_4^3 &= 5r\end{aligned}$$

Thus, the initial equation writes down another way which is an explanation of the noted exception. The Cassels and Guy equation is not isolated. We can see the same phenomenon, for example, with  $c = a.x_1^3+9x_2^3-(2a.x_3^3+12x_4^3)$  where  $a = 5, 13, 19, 23, 31, 41$  or  $43$ , but not with  $a = 7, 17, 29$  or  $37$  (where the solution  $c$  is not unique). These cases may seem less convincing on the matter of decomposition in several equations, but the following example, with richer exceptions, will feed our argument.

## 2.6.2.2 Borovoi equation

### 2.6.2.2.1 Variables of integers

The proposed equation is extracted from a Jean-Louis Colliot-Thélène and Fei Xu article and attributed to Mikhail Borovoi. It is the diophantine equation  $-9x^2+2x.y+7y^2+2z^2-1 = 0$  which has no integer solution and, there again, has more than two variables. It is a most interesting example as we shall discover.

To do this, we have  $c = -9x^2+2x.y+7y^2+2z^2-1$  and are looking for the number of local solutions (modulo  $p^\delta$ ) according to target  $c$ . We get the following table :

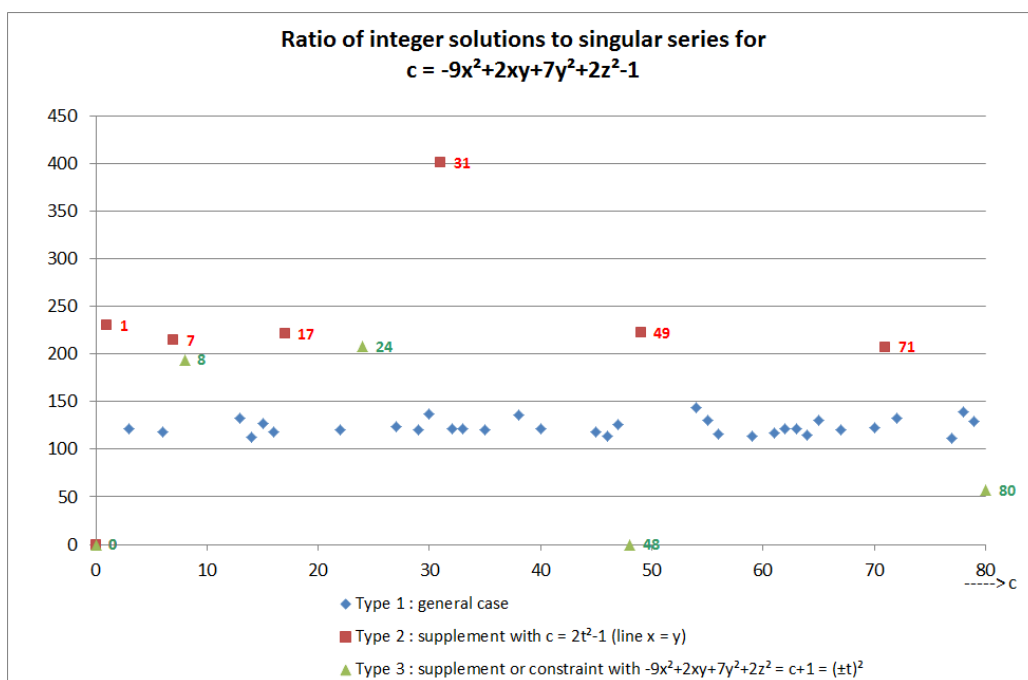
Table (33)

p	2	3	5	7	11	13	17	19	23	2	3	5	7	11	13	17	19	23	Singular series = $\prod p_n$	#(effective solutions)	Ratio singular series / #
$\delta$	6	5	3	2	2	2	2	2	2	6	5	3	2	2	2	2	2	2			
c	number of local solutions (nsl)									normalized proportions (pn = nsl/p <sup>2<math>\delta</math></sup> )											
0	8192	39366	12500	2744	13310	26364	88434	123462	292008	2	0,667	0,8	1,143	0,909	0,923	1,059	0,947	1,043	1,071	0	0
1	8192	78732	18750	2744	15972	30758	88434	137180	292008	2	1,333	1,2	1,143	1,091	1,077	1,059	1,053	1,043	4,997	1148	230
2	0	52488	18750	2058	13310	26364	78608	137180	292008	0	0,889	1,2	0,857	0,909	0,923	0,941	1,053	1,043	0	0	
3	8192	39366	12500	2744	13310	26364	88434	123462	292008	2	0,667	0,8	1,143	0,909	0,923	1,059	0,947	1,043	1,071	130	121
4	0	78732	15000	2058	13310	30758	78608	123462	267674	0	1,333	0,960	0,857	0,909	1,077	0,941	0,947	0,957	0	0	
5	0	52488	12500	2058	15972	30758	78608	123462	292008	0	0,889	0,8	0,857	1,091	1,077	0,941	0,947	1,043	0	0	
6	8192	39366	18750	2352	15972	30758	78608	123462	267674	2	0,667	1,2	0,980	1,091	1,077	0,941	0,947	0,957	1,570	185	118
7	8192	78732	18750	2744	15972	30758	88434	137180	292008	2	1,333	1,2	1,143	1,091	1,077	1,059	1,053	1,043	4,997	1070	214
8	8192	65610	12500	2744	13310	26364	88434	123462	292008	2	1,111	0,8	1,143	0,909	0,923	1,059	0,947	1,043	1,785	346	194
...																					

In the preceding table, #(effective solutions) are the number of solutions of the proposed equation limiting triplets  $(x,y,z)$  to  $-2000/3 \leq x \leq 2000/3, -2000/\sqrt{7} \leq y \leq 2000/\sqrt{7}, -2000/\sqrt{2} \leq z \leq 2000/\sqrt{2}$ , which is enough to expose our case.

The results, for target 0 to 81, are graphically more speaking (see also a more complete table in appendix 5) :

Graphic (4)



If we do not take into account the sorting in three types made in this graph, we may regard that as a "messy thing". But this case is interesting precisely because this hotch-potch gets good reasons.

First, we detect type 1 (diamond-shaped blue characters). It is corresponding to an a priori expected result, which is a ratio "#(effective solutions) / singular series" reasonably fluctuating around a constant value (here in the order of 125, but this very value as little immediate interest), the differences to the average being due, as in the Cassels and Guy example, to the rough calculation (finite sample (x, y, z), approximate singular series, stability degrees not possibly achieved). We observe this constant ratio for the majority of the targets.

Then, we also find many exceptions that we have identified above indicating the abscissa values c on the chart. These exceptions are explained as follows after rewriting the equation in the form :

$$c = -9x^2 + 2xy + 7y^2 + 2z^2 - 1 = (y-x)(9x+7y) + 2z^2 - 1 \quad (66)$$

The first type of exceptions (in red squares) corresponds to :

$$c = 2t^2 - 1 \quad (67)$$

We then have  $(y-x)(9x+7y) + 2z^2 - 1 = 2t^2 - 1$  and there is a line of "trivial" solution of degree 1

$$\begin{aligned} t &= \pm z \\ \text{and} \\ \{x &= y \text{ or } 9x+7y = 0\} \end{aligned}$$

who strengthen thus the "normal" value at degree 2.

The second type of exceptions (in green triangles) is a little better hidden. It corresponds to the target of the form :

$$c = (1+2t)^2 - 1 \quad (68)$$

We then write  $(y-x)(9x+7y) + 2z^2 - 1 = (1+2t)^2 - 1$ , so that  $(y-x)(9x+7y) + 2z^2 - (1+2t)^2 = 0$ . If  $z = \pm(1+2t)$ , then  $(x-y)(9x+7y) = z^2 = (z/r).(z.r)$ . In the latter part of equality, r is any divisor of z. Hence the new first degree equations :  $x-y = (z/r)$  and  $9x+7y = (z.r)$ , and hence the system of equations in integers :

$$\begin{aligned} x &= (7(z/r) + (z.r))/16 \\ \text{and} \\ y &= (-9(z/r) + (z.r))/16 \end{aligned}$$

There is a constraint because of the divisions by r and 16, where a possibility of lesser quantity of solutions (even with respect to an second degree equation).

The first type always displays an excess of solutions. But, it is important to note that the reduction to the lower level (here the level 2 to level 1 passage) is not necessarily accompanied with a surplus as shows the second type at  $c = 0$ ,  $c = 48$  and  $c = 80$ . The explanation for target  $c = 0$  without solution was already given in part I by considering the point of view of the prime number variables. The case of target  $c = 48$  is described in same manner. However, if a target c is prohibited for the prime numbers variables, solutions are possible (in integers) which allows a case like  $c = 80$  with non-zero number of solutions.

Let us note that other exceptions may be present which we do not suspect here the linearization.

La position à adopter, à la fois la plus simple et la plus adaptée, par rapport à toutes ces exceptions est en fait de dire que le procédé global-local ne s'applique en aucune manière, dès lors qu'une réduction de l'équation initiale est possible :

The position to be adopted, both the simplest and the most suitable, to all these exceptions is in fact to say that the global-local process applies in no way as soon as a reduction of the initial equation is possible :

- reduction into several equations (2 or more) of lower degrees
- discriminant of the equation equal to zero
- ...

#### 2.6.2.2.2 Variables of prime numbers

We can confirm this approach using the same diophantine equation but considering not integer variables, but prime numbers variables. We still studied the target 0 to 81.

Here, they are divided into four categories :

- Cat. 1 : those, the more numerous, for which no solution is detected and the singular series is zero ( $c = 0, 2, 3, 4, 5, 6, 9, 10, 11, 12, 14, 15, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39, 41, 42, 43, 44, 47, 48, 50, 51, 52, 53, 54, 55, 57, 58, 59, 60, 62, 63, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79$  and  $80$ ),

- Cat. 2 : those for which the number of solutions is low and appears to be reduced to this small number (and therefore finite quantities) and whose singular series is zero ( $c = 8, 16, 40, 46, 56$  and  $64$ ),
- Cat. 3 : those for which the number of solutions increases with the volume (and therefore a priori in infinite amount) and the singular series is non-null ( $c = 1, 13, 33, 45, 49, 61$  and  $81$ ),
- Cat. 4 : those for which the number of solutions increases with the volume (and therefore a priori in infinite amount) and the singular series is null ( $c = 7$  and  $17$ ).

The first category is in the logic of things. It is the main stream because the number of variables is small relative to the degree of the equation.

For a finite number of solutions, it is expected to have a singular series equal to zero, which is expressed in the second category of targets.

The third category is the "reverse" of the first one.

We examine the very particular case of the fourth category a little later on.

We excluded trivial (zero) results of the first category in the table below representing the ratio of the number of solutions versus singular series :

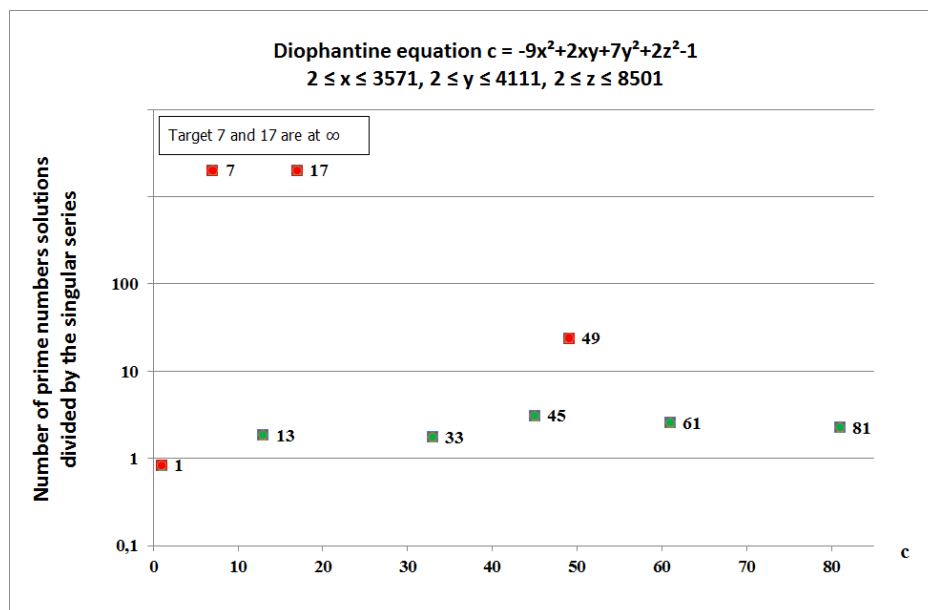
Table (34)

Targets	1	7	8	13	16	17	33	40	45	46	49	56	61	64	81
Singular series	54,197	0	0	4,330	0	0	6,348	0	7,810	0	21,679	0	16,559	0	13,021
Definition domain # solutions															
$2 \leq x \leq 229, 2 \leq y \leq 263, 2 \leq z \leq 577$	4	50	1	1	1	50	1	1	5	1	52	2	11	1	6
$2 \leq x \leq 983, 2 \leq y \leq 1123, 2 \leq z \leq 2381$	21	166	1	4	1	166	3	1	10	1	172	2	19	1	18
$2 \leq x \leq 3571, 2 \leq y \leq 4111, 2 \leq z \leq 8501$	45	500	1	8	1	500	11	1	24	1	520	2	42	1	29
Ratio															
$2 \leq x \leq 229, 2 \leq y \leq 263, 2 \leq z \leq 577$	0,07	$\infty$	$\rightarrow \infty$	0,23	$\rightarrow \infty$	$\infty$	0,16	$\rightarrow \infty$	0,64	$\rightarrow \infty$	2,40	$\rightarrow \infty$	0,66	$\rightarrow \infty$	0,46
$2 \leq x \leq 983, 2 \leq y \leq 1123, 2 \leq z \leq 2381$	0,39	$\infty$	$\rightarrow \infty$	0,92	$\rightarrow \infty$	$\infty$	0,47	$\rightarrow \infty$	1,28	$\rightarrow \infty$	7,93	$\rightarrow \infty$	1,15	$\rightarrow \infty$	1,38
$2 \leq x \leq 3571, 2 \leq y \leq 4111, 2 \leq z \leq 8501$	0,83	$\infty$	$\rightarrow \infty$	1,85	$\rightarrow \infty$	$\infty$	1,73	$\rightarrow \infty$	3,07	$\rightarrow \infty$	23,99	$\rightarrow \infty$	2,54	$\rightarrow \infty$	2,23

Appendix 6 provides more details on how to obtain this table.

The report on a graph of the precedent results gives, when excepting category 2 :

Graphic (5)



The fourth category is incoherent. This is however not an event of type "obstruction", namely a lack of solutions with a non-zero singular series, but precisely the opposite, namely, a phenomenon of "influx" (an infinite number of solutions with a singular zero, what the numerical example makes understand without proving it). We can again give an "simple explanation" since these targets correspond to the type  $c = 2t^2 - 1$  family identified in the case of the variables of integers and therefore to

be rejected in our method at the same time as targets  $c = 1$  and  $c = 49$  which on the chart are either in a too low positions (for  $c = 1$ ), or a too high position (for  $c = 49$ ). After elimination (of the red points), we see that the positions of the remaining targets (in green) are close to a horizontal line, what is expected a priori. Moreover, when the chosen volume for numerical computation increases, we ought to see an evolution towards a smaller dispersion.

Let us note also, that the case of the Borovoi equation is not isolated among the equations of the type  $c = \alpha.x^2 + \beta.x.y + \gamma.y^2 + \delta.z^2$  where many similar cases can be easily obtained (for example among the equation  $c = (y-x)(9x+(7+16.a).y)+2z^2-1$  where  $a$  is an integer parameter (but without all integers suitable for  $a$ )). The principle of accurate enumeration of these equations is developed in another of our articles.

### 2.6.2.3 Reduction of equations

The Borovoi equation shows that apart from the reduction to specific systems of equations, the points describing the number of solutions are placed on a horizontal line in charts (or, what is the same thing, obey the relation  $\#(c) = \text{singular series } x \text{ volume}$ ). For Borovoi equation, recalling exceptions, the two found types belong, according to relations (67) and (68), to second degree curves, for which we verified in paragraph 2.4.5 an equivalent Hensel lemma applied to enumeration (and therefore such as  $\#(c) = \text{singular series } x \text{ volume}$ ). For the Cassels and Guy equation of, the alignment of the exception point is trivial (since we have only one point).

Let us recall, before ending up this article the imbroglio, at paragraphs 2.4.4.2 and 2.4.9.2, to treat the two cases  $x^n = c$  with  $c = 0$  for the variable of integers  $x$  and  $y^n = c$  with  $c = 1$  for the prime numbers variable  $y$ . The example of Mikhail Borovoi fully provides the way to process these cases "correctly".

To write down

$$x^n = c \quad (69)$$

comes up to write down a system of equations

$$x = 0, x = 0, \dots, \text{ ou } x = 0 \quad (70).$$

To write down

$$y^n = 1 \quad (71)$$

again comes up to write down a system of equations

$$y = 1, y = 1, \dots, \text{ ou } y = 1 \quad (72).$$

According to our discussion, it can no longer be question to solve the initial equations (69) et (71) because they decompose into systems of equations and it can be neither to solve systems of equations because we do not know how to establish singular series of systems of equations (nor volumes for systems).

Correct treatment therefore normally leads to a stalemate.

By chance here, the equations are identical and boil down to

$$x = 0$$

on one side and

$$y = 1$$

on the other side, which allows however to finish the job.

### 2.6.3 Obstruction or influx

Our examples have highlighted a whole field of standards expected results from obstruction to influx with all possible intermediaries but only when the studied diophantine equation can be rewritten in a different way. Obstruction (strong) cases are only obvious, a priori, when equations are formed with integer variables, while cases of influx occur in those formed with prime numbers variables (related to weak obstruction).

Outside this context (that is for equations that we will call "irreducible"), we have lost track of any exception.

## 2.7 Conclusion and prelude

Our approach is against the current common approach. It seems natural to erect the global equation as the centre of a given problem and to "pester" against obstructions that are found in the local equations (while studying them thoroughly). The global equation is an absolute, the road is one-way with no return, and there is no questioning of hypothesis (the global equation).

We prefer an alternative way. We always start from the global equation but it is the local equations, infinitely more numerous, that form our reference centre. For a given target, they indicate if the way to write the global equation is sound or not. In fact, "obstructions" disappear since any particular target (and thus the corresponding equation) enacted locally as non-legitimate is being "scrapped" or the less classified in a new special family for enumeration.

More precisely, it turns out that there is no obstruction into asymptotic branches diophantine equations but situations where

the choice of the target  $c$  reduces the given equation to one or more smaller degree equations (that is with members of smaller degree). The problem is then to be reconsidered in this new situation. The concept of obstruction with that point of view has more meaning. One of the simplest example is  $p-q = 2c$  corresponding to the problem of twin and relative primes. If  $c = 0$ , then  $p = q$ , so that  $p = p$ , or also  $0.p = 0$ . So the equation is no more of degree 1 but of degree 0. For any other integer  $c$ , we cannot do this reduction and the result is that of Pólya.

We should pursue our investigations in a third part by further developing the tools for evaluation of the number of solutions of diophantine equations. We have seen that, a priori, according to the chosen method, only the resolution of diophantine equations with asymptotic branches offers a fertile ground. Even so, it is customary to think that each of these diophantine equations is a specific problem. In fact, this is not the case. It is possible to construct basic bricks of results and assemble them relying on special matrices. The ranks and the terms of these matrices can be studied in an environment of classes modulo  $p_i^{k_i}$  and depend on degrees of stability of the chosen equations. However, their evolution with  $k_i$  is "easily" described by the terms of the said matrices or by their eigenvalues and eigenvectors and is deduced at infinity if necessary. The aggregation of variables in a diophantine equation comes up to mere products of these matrices. This construction is fascinating. Euler products are extracted from these matrices responding to many types of problems such as  $p = x^2 + x^4 + c$  with any  $c$ , generalizing the results found by Friedlander and Iwaniec for  $c = 0$ , such as  $p^j = \sum x_i^{(j)} + \sum y_i^{(j)} + c$  where the sums relate to any number of terms and the integer powers are distinct or not, or even such as more general polynomial expressions (with more development required). The interested reader can refer to our paper "Asymptotic enumerations. Hypervolumes method" for this purpose. It is necessary of course to remember that thus found formulas are meaningful only "off reduction" of the proposed equation.

## Appendix 1

### Product of cardinals relative to integers

Let us have an example for the clarity of the presentation:  $P(n) = n^2$ ,  $m_i = 2^2$ ,  $m_j = 3^2$ .

Table 1

Truth table 1

n	P(n) mod 36	P(n) mod 4	P(n) mod 9	P(n)	#P(n) mod 36	#P(n) mod 4	#P(n) mod 9	
0	0	0	0	0	6	2	3	True
1	1	1	1	1	4	2	2	True
2	4	0	4	2	0	0	0	True
3	9	1	0	3	0	0	0	True
4	16	0	7	4	4	2	2	True
5	25	1	7	5	0	2	0	True
6	0	0	0	6	0	0	0	True
7	13	1	4	7	0	0	2	True
8	28	0	1	8	0	2	0	True
9	9	1	0	9	6	2	3	True
10	28	0	1	10	0	0	2	True
11	13	1	4	11	0	0	0	True
12	0	0	0	12	0	2	0	True
13	25	1	7	13	4	2	2	True
14	16	0	7	14	0	0	0	True
15	9	1	0	15	0	0	0	True
16	4	0	4	16	4	2	2	True
17	1	1	1	17	0	2	0	True
18	0	0	0	18	0	0	3	True
19	1	1	1	19	0	0	2	True
20	4	0	4	20	0	2	0	True
21	9	1	0	21	0	2	0	True
22	16	0	7	22	0	0	2	True
23	25	1	7	23	0	0	0	True
24	0	0	0	24	0	2	0	True
25	13	1	4	25	4	2	2	True
26	28	0	1	26	0	0	0	True
27	9	1	0	27	0	0	3	True
28	28	0	1	28	4	2	2	True
29	13	1	4	29	0	2	0	True
30	0	0	0	30	0	0	0	True
31	25	1	7	31	0	0	2	True
32	16	0	7	32	0	2	0	True
33	9	1	0	33	0	2	0	True
34	4	0	4	34	0	0	2	True
35	1	1	1	35	0	0	0	True

### Product of cardinals relative to prime numbers

Let us reuse the precedent example removing the multiples of the divisors of  $m_i$  and  $m_j$  (that is of 2 and 3).

Table 2

Truth table 2 (identical to 1 with lines without objet (W.O.))

n	P(n) mod 36	P(n) mod 4	P(n) mod 9	P(n)	#P(n) mod 36	#P(n) mod 4	#P(n) mod 9	
0	0	0	0	0	6	2	3	True → W.O.
1	1	1	1	1	4	2	2	True
2	4	0	4	2	0	0	0	True → W.O.
3	9	1	0	3	0	0	0	True → W.O.
4	16	0	7	4	4	2	2	True → W.O.
5	25	1	7	5	0	2	0	True
6	0	0	0	6	0	0	0	True → W.O.
7	13	1	4	7	0	0	2	True
8	28	0	1	8	0	2	0	True → W.O.
9	9	1	0	9	6	2	3	True → W.O.
10	28	0	1	10	0	0	2	True → W.O.
11	13	1	4	11	0	0	0	True
12	0	0	0	12	0	2	0	True → W.O.
13	25	1	7	13	4	2	2	True
14	16	0	7	14	0	0	0	True → W.O.
15	9	1	0	15	0	0	0	True → W.O.
16	4	0	4	16	4	2	2	True → W.O.
17	1	1	1	17	0	2	0	True
18	0	0	0	18	0	0	3	True → W.O.
19	1	1	1	19	0	0	2	True
20	4	0	4	20	0	2	0	True → W.O.
21	9	1	0	21	0	2	0	True → W.O.
22	16	0	7	22	0	0	2	True → W.O.
23	25	1	7	23	0	0	0	True
24	0	0	0	24	0	2	0	True → W.O.
25	13	1	4	25	4	2	2	True
26	28	0	1	26	0	0	0	True → W.O.
27	9	1	0	27	0	0	3	True → W.O.
28	28	0	1	28	4	2	2	True → W.O.
29	13	1	4	29	0	2	0	True
30	0	0	0	30	0	0	0	True → W.O.
31	25	1	7	31	0	0	2	True
32	16	0	7	32	0	2	0	True → W.O.
33	9	1	0	33	0	2	0	True → W.O.
34	4	0	4	34	0	0	2	True → W.O.
35	1	1	1	35	0	0	0	True

## Appendix 2

Stability of the variable of prime numbers  $y^6$ .

$p = 2$	
$y = [1] \bmod 2$	
$y^6 = [1] \bmod 2$	Initial
$y = [1,3] \bmod 4 \equiv [1] \bmod 2$	
$y^6 = [1,1] \bmod 4 \equiv [1] \bmod 4$	Evolution1
$y = [1,3,5,7] \bmod 8 \equiv [1] \bmod 2$	
$y^6 = [1,1,1,1] \bmod 8 \equiv [1] \bmod 8$	Evolution2
$y = [1,3,5,7,9,11,13,15] \bmod 16 \equiv [1] \bmod 2$	
$y^6 = [1,9,9,1,1,9,9,1] \bmod 16 \equiv [1] \bmod 8$	Stabilized
$y = [1,3,5,\dots,2^6-1] \bmod 2^6 \equiv [1] \bmod 2$	
$y^6 \equiv [1] \bmod 2^3$ si $\delta \geq 3 = 1+2$ ( $2^1 = \max(6,2^{\delta-1})$ , $\delta b = 2$ )	

$p = 3$	
$y = [1,2] \bmod 3$	
$y^6 = [1,1] \bmod 3 \equiv [1] \bmod 3$	Initial
$y = [1,2,4,5,7,8] \bmod 9 \equiv [1,2] \bmod 3$	
$y^6 = [1,1,1,1,1,1] \bmod 9 \equiv [1] \bmod 9$	Evolution1
$y = [1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26] \bmod 27 \equiv [1,2] \bmod 3$	
$y^6 = [1,10,19,19,10,1,1,10,19,19,10,1,1,10,19,19,10,1] \bmod 27 \equiv [1,10,19] \bmod 27 \equiv [1] \bmod 9$	Stabilized
$y = [1,2,4,5,\dots] \bmod 3^6 \equiv [1,2] \bmod 3$	
$y^6 \equiv [1] \bmod 3^2$ if $\delta \geq 2 = 2+0$ ( $3^1 \cdot 2 = \max(6,3^{\delta-1} \cdot (3-1))$ , $\delta b = 2$ )	

$p = 5$	
$y = [1,2,3,4] \bmod 5$	
$y^6 = [1,4,4,1] \bmod 5 \equiv [1,4] \bmod 5$	Initial
$y = [1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24] \bmod 25 \equiv [1,2,3,4] \bmod 5$	
$y^6 = [1,14,4,21,6,24,19,16,11,9,9,11,16,19,24,6,21,4,14,1] \bmod 25 \equiv [1,4,6,9,11,14,16,19,21,24] \bmod 25 \equiv [1,4] \bmod 5$	Stabilized
$y = [1,2,3,4,\dots] \bmod 5^6 \equiv [1,2,3,4] \bmod 5$	
$y^6 \equiv [1,4] \bmod 5^1$ $\delta \geq 1 = 1+0$ ( $5^0 \cdot 2 = \max(6,5^{\delta-1})$ , $\delta b = 1$ )	

The sign of equivalence is placed here whenever the proportion of occurrences of each element remains the same.

### Appendix 3

c	p	2	3	5	7	11	13	17	19	23	29
0	#(c)	1	1	1	1	1	1	1	1	1	1
1	mod p <sup>1</sup>	1	2	2	2	2	2	2	2	2	2
2		1	0	0	2	0	0	2	0	2	0
3		1	1	0	0	2	2	0	0	2	0
4		1	2	2	2	2	2	2	2	2	2
5		1	0	1	0	2	0	0	2	0	2
6		1	1	2	0	0	0	0	2	2	2
7		1	2	0	1	0	0	0	2	0	2
8		1	0	0	2	0	0	2	0	2	0
9		1	1	2	2	2	2	2	2	2	2
10		1	2	1	0	0	2	0	0	0	0
11		1	0	2	2	1	0	0	2	0	0
12		1	1	0	0	2	2	0	0	2	0
13		1	2	0	0	0	1	2	0	2	2
14		1	0	2	1	2	2	0	0	0	0
15		1	1	1	2	2	0	2	0	0	0
16		1	2	2	2	2	2	2	2	2	2
17		1	0	0	0	0	2	1	2	0	0
18		1	1	0	2	0	0	2	0	2	0
19		1	2	2	0	0	0	2	1	0	0
20		1	0	1	0	2	0	0	2	0	2
21		1	1	2	1	0	0	2	0	0	0
22		1	2	0	2	1	2	0	0	0	2
23		1	0	0	2	2	2	0	2	1	2
24		1	1	2	0	0	0	0	2	2	2
25		1	2	1	2	2	2	2	2	2	2
26		1	0	2	0	2	1	2	2	2	0
27		1	1	0	0	2	2	0	0	2	0
28		1	2	0	1	0	0	0	2	0	2
29		1	0	2	2	0	2	0	0	2	1
30		1	1	1	2	0	2	2	2	0	2
31		1	2	2	0	2	0	0	0	2	0
32		1	0	0	2	0	0	2	0	2	0
33		1	1	0	0	1	0	2	0	0	2
34		1	2	2	0	2	0	1	0	0	2
35		1	0	1	1	0	2	2	2	2	2
36		1	1	2	2	2	2	2	2	2	2
37		1	2	0	2	2	0	0	0	0	0
38		1	0	0	0	2	2	2	1	0	2
39		1	1	2	2	0	1	0	2	2	0
40		1	2	1	0	0	2	0	0	0	0
41		1	0	2	0	0	0	0	0	2	0
42		1	1	0	1	2	2	2	2	0	2
43		1	2	0	2	0	2	2	2	0	0
44		1	0	2	2	1	0	0	2	0	0
45		1	1	1	0	2	0	0	2	0	2
46		1	2	2	2	0	0	0	0	1	0
47		1	0	0	0	2	0	2	2	2	0
48		1	1	0	0	2	2	0	0	2	0
49		1	2	2	1	2	2	2	2	2	2
50		1	0	1	2	0	0	2	0	2	0
51		1	1	2	2	0	2	1	0	0	2
52		1	2	0	0	0	1	2	0	2	2
53		1	0	0	2	2	2	2	0	0	2
54		1	1	2	0	0	0	0	2	2	2
55		1	2	1	0	1	2	2	2	2	0
56		1	0	2	1	2	2	0	0	0	0
57		1	1	0	2	0	0	0	1	0	2
58		1	2	0	2	2	0	0	2	2	1
59		1	0	2	0	2	0	2	0	2	2
60		1	1	1	2	2	0	2	0	0	0
61		1	2	2	0	0	2	0	2	0	0
62		1	0	0	0	0	2	0	2	2	2
63		1	1	0	1	0	0	0	2	0	2
64		1	2	2	2	2	2	2	2	2	2

c	p	2	3	5	7	11	13	17	19	23	29
0	#(c)	2	3	5	7	11	13	17	19	23	29
1	mod p <sup>2</sup>	2	2	2	2	2	2	2	2	2	2
2		0	0	0	2	0	0	2	0	2	0
3		0	0	0	0	2	2	0	0	2	0
4		2	2	2	2	2	2	2	2	2	2
5		2	0	0	0	2	0	0	2	0	2
6		0	0	2	0	0	0	0	2	2	2
7		0	2	0	0	0	0	0	2	0	2
8		2	0	0	2	0	0	2	0	2	0
9		2	3	2	2	2	2	2	2	2	2
10		0	2	0	0	0	2	0	0	0	0
11		0	0	2	2	0	0	0	2	0	0
12		2	0	0	0	2	2	0	0	2	0
13		2	2	0	0	0	0	2	0	2	2
14		0	0	2	0	2	2	0	0	0	0
15		0	0	0	2	2	0	2	0	0	0
16		2	2	2	2	2	2	2	2	2	2
17		2	0	0	0	0	2	0	2	0	0
18		0	3	0	2	0	0	2	0	2	0
19		0	2	2	0	0	0	2	0	0	0
20		2	0	0	0	2	0	0	2	0	2
21		2	0	2	0	0	0	2	0	0	0
22		0	2	0	2	0	2	0	0	0	2
23		0	0	0	2	2	2	0	0	2	2
24		2	0	2	0	0	0	0	2	2	2
25		2	2	5	2	2	2	2	2	2	2
26		0	0	2	0	2	0	2	2	2	0
27		0	3	0	0	2	2	0	0	2	0
28		2	2	0	0	0	0	0	2	0	2
29		2	0	2	2	0	2	0	0	2	0
30		0	0	0	2	0	2	2	2	0	2
31		0	2	2	0	2	0	0	0	2	0
32		2	0	0	2	0	0	2	0	2	0
33		2	0	0	0	0	0	2	0	0	2
34		0	2	2	0	2	0	0	0	0	2
35		0	0	0	0	0	2	2	2	2	2
36		2	3	2	2	2	2	2	2	2	2
37		2	2	0	2	2	0	0	0	0	0
38		0	0	0	0	2	2	2	0	0	2
39		0	0	2	2	0	0	0	2	2	0
40		2	2	0	0	0	2	0	0	0	0
41		2	0	2	0	0	0	0	0	2	0
42		0	0	0	0	2	2	2	2	0	2
43		0	2	0	2	0	2	2	2	0	0
44		2	0	2	2	0	0	0	2	0	0
45		2	3	0	0	2	0	0	2	0	2
46		0	2	2	2	0	0	0	0	0	0
47		0	0	0	0	2	0	2	2	2	0
48		2	0	0	0	2	2	0	0	2	0
49		2	2	2	7	2	2	2	2	2	2
50		0	0	5	2	0	0	2	0	2	0
51		0	0	2	2	0	2	0	0	0	2
52		2	2	0	0	0	0	2	0	2	2
53		2	0	0	2	2	2	2	0	0	2
54		0	3	2	0	0	0	0	2	2	2
55		0	2	0	0	0	2	2	2	2	0
56		2	0	2	0	2	2	0	0	0	0
57		2	0	0	2	0	0	0	0	0	2
58		0	2	0	2	2	0	0	2	2	0
59		0	0	2	0	2	0	2	0	2	2
60		2	0	0	2	2	0	2	0	0	0
61		2	2	2	0	0	2	0	2	0	0
62		0	0	0	0	0	2	0	2	2	2
63		0	3	0	0	0	0	0	2	0	2
64		2	2	2	2	2	2	2	2	2	2

c	p									
	#(c) mod $p^3$									
0	2	3	5	7	11	13	17	19	23	29
1	4	2	2	2	2	2	2	2	2	2
2	0	0	0	2	0	0	2	0	2	0
3	0	0	0	0	2	2	0	0	2	0
4	2	2	2	2	2	2	2	2	2	2
5	0	0	0	0	2	0	0	2	0	2
6	0	0	2	0	0	0	0	2	2	2
7	0	2	0	0	0	0	0	2	0	2
8	2	0	0	2	0	0	2	0	2	0
9	4	6	2	2	2	2	2	2	2	2
10	0	2	0	0	0	2	0	0	0	0
11	0	0	2	2	0	0	0	2	0	0
12	2	0	0	0	2	2	0	0	2	0
13	0	2	0	0	0	0	2	0	2	2
14	0	0	2	0	2	2	0	0	0	0
15	0	0	0	2	2	0	2	0	0	0
16	2	2	2	2	2	2	2	2	2	2
17	4	0	0	0	0	2	0	2	0	0
18	0	0	0	2	0	0	2	0	2	0
19	0	2	2	0	0	0	2	0	0	0
20	2	0	0	0	2	0	0	2	0	2
21	0	0	2	0	0	0	2	0	0	0
22	0	2	0	2	0	2	0	0	0	2
23	0	0	0	2	2	2	0	2	0	2
24	2	0	2	0	0	0	0	2	2	2
25	4	2	10	2	2	2	2	2	2	2
26	0	0	2	0	2	0	2	2	2	0
27	0	3	0	0	2	2	0	0	2	0
28	2	2	0	0	0	0	0	2	0	2
29	0	0	2	2	0	2	0	0	2	0
30	0	0	0	2	0	2	2	2	0	2
31	0	2	2	0	2	0	0	0	2	0
32	2	0	0	2	0	0	2	0	2	0
33	4	0	0	0	0	0	2	0	0	2
34	0	2	2	0	2	0	0	0	0	2
35	0	0	0	0	0	2	2	2	2	2
36	2	6	2	2	2	2	2	2	2	2
37	0	2	0	2	2	0	0	0	0	0
38	0	0	0	0	2	2	2	0	0	2
39	0	0	2	2	0	0	0	2	2	0
40	2	2	0	0	0	2	0	0	0	0
41	4	0	2	0	0	0	0	0	2	0
42	0	0	0	0	2	2	2	2	0	2
43	0	2	0	2	0	2	2	2	0	0
44	2	0	2	2	0	0	0	2	0	0
45	0	0	0	0	2	0	0	2	0	2
46	0	2	2	2	0	0	0	0	0	0
47	0	0	0	0	2	0	2	2	2	0
48	2	0	0	0	2	2	0	0	2	0
49	4	2	2	14	2	2	2	2	2	2
50	0	0	0	2	0	0	2	0	2	0
51	0	0	2	2	0	2	0	0	0	2
52	2	2	0	0	0	0	2	0	2	2
53	0	0	0	2	2	2	2	0	0	2
54	0	3	2	0	0	0	0	2	2	2
55	0	2	0	0	0	2	2	2	2	0
56	2	0	2	0	2	2	0	0	0	0
57	4	0	0	2	0	0	0	0	0	2
58	0	2	0	2	2	0	0	2	2	0
59	0	0	2	0	2	0	2	0	2	2
60	2	0	0	2	2	0	2	0	0	0
61	0	2	2	0	0	2	0	2	0	0
62	0	0	0	0	0	2	0	2	2	2
63	0	6	0	0	0	0	0	2	0	2
64	2	2	2	2	2	2	2	2	2	2

c	p									
	#(c) mod $p^4$									
0	4	9	25	49	121	169	289	361	529	841
1	4	2	2	2	2	2	2	2	2	2
2	0	0	0	2	0	0	2	0	2	0
3	0	0	0	0	2	2	0	0	2	0
4	4	2	2	2	2	2	2	2	2	2
5	0	0	0	0	2	0	0	2	0	2
6	0	0	2	0	0	0	0	2	2	2
7	0	2	0	0	0	0	0	2	0	2
8	0	0	0	2	0	0	2	0	2	0
9	4	6	2	2	2	2	2	2	2	2
10	0	2	0	0	0	2	0	0	0	0
11	0	0	2	2	0	0	0	2	0	0
12	0	0	0	0	2	2	0	0	2	0
13	0	2	0	0	0	0	2	0	2	2
14	0	0	2	0	2	2	0	0	0	0
15	0	0	0	2	2	0	2	0	0	0
16	4	2	2	2	2	2	2	2	2	2
17	4	0	0	0	0	2	0	2	0	0
18	0	0	0	2	0	0	2	0	2	0
19	0	2	2	0	0	0	2	0	0	0
20	4	0	0	0	2	0	0	2	0	2
21	0	0	2	0	0	0	2	0	0	0
22	0	2	0	2	0	2	0	0	0	2
23	0	0	0	2	2	2	0	2	0	2
24	0	0	2	0	0	0	0	2	2	2
25	4	2	10	2	2	2	2	2	2	2
26	0	0	2	0	2	0	2	2	2	0
27	0	0	0	0	2	2	0	0	2	0
28	0	2	0	0	0	0	0	2	0	2
29	0	0	2	2	0	2	0	0	2	0
30	0	0	0	2	0	2	2	2	0	2
31	0	2	2	0	2	0	0	0	2	0
32	4	0	0	2	0	0	2	0	2	0
33	4	0	0	0	0	0	2	0	0	2
34	0	2	2	0	2	0	0	0	0	2
35	0	0	0	0	0	2	2	2	2	2
36	4	6	2	2	2	2	2	2	2	2
37	0	2	0	2	2	0	0	0	0	0
38	0	0	0	0	2	2	2	0	0	2
39	0	0	2	2	0	0	0	2	2	0
40	0	2	0	0	0	2	0	0	0	0
41	4	0	2	0	0	0	0	0	2	0
42	0	0	0	0	2	2	2	2	0	2
43	0	2	0	2	0	2	2	2	0	0
44	0	0	2	2	0	0	0	2	0	0
45	0	0	0	0	2	0	0	2	0	2
46	0	2	2	2	0	0	0	0	0	0
47	0	0	0	0	2	0	2	2	2	0
48	4	0	0	0	2	2	0	0	2	0
49	4	2	2	14	2	2	2	2	2	2
50	0	0	0	2	0	0	2	0	2	0
51	0	0	2	2	0	2	0	0	0	2
52	4	2	0	0	0	0	2	0	2	2
53	0	0	0	2	2	2	2	0	0	2
54	0	0	2	0	0	0	0	2	2	2
55	0	2	0	0	0	2	2	2	2	0
56	0	0	2	0	2	2	0	0	0	0
57	4	0	0	2	0	0	0	0	0	2
58	0	2	0	2	2	0	0	2	2	0
59	0	0	2	0	2	0	2	0	2	2
60	0	0	0	2	2	0	2	0	0	0
61	0	2	2	0	0	2	0	2	0	0
62	0	0	0	0	0	2	0	2	2	2
63	0	6	0	0	0	0	0	2	0	2
64	4	2	2	2	2	2	2	2	2	2

p		2	3	5	7	11	13	17	19	23	29
c											
0	#(c)	4	9	25	49	121	169	289	361	529	841
1	mod $p^5$	4	2	2	2	2	2	2	2	2	2
2		0	0	0	2	0	0	2	0	2	0
3		0	0	0	0	2	2	0	0	2	0
4		8	2	2	2	2	2	2	2	2	2
5		0	0	0	0	2	0	0	2	0	2
6		0	0	2	0	0	0	0	2	2	2
7		0	2	0	0	0	0	0	2	0	2
8		0	0	0	2	0	0	2	0	2	0
9		4	6	2	2	2	2	2	2	2	2
10		0	2	0	0	0	2	0	0	0	0
11		0	0	2	2	0	0	0	2	0	0
12		0	0	0	0	2	2	0	0	2	0
13		0	2	0	0	0	0	2	0	2	2
14		0	0	2	0	2	2	0	0	0	0
15		0	0	0	2	2	0	2	0	0	0
16		4	2	2	2	2	2	2	2	2	2
17		4	0	0	0	0	2	0	2	0	0
18		0	0	0	2	0	0	2	0	2	0
19		0	2	2	0	0	0	2	0	0	0
20		0	0	0	0	2	0	0	2	0	2
21		0	0	2	0	0	0	2	0	0	0
22		0	2	0	2	0	2	0	0	0	2
23		0	0	0	2	2	2	0	2	0	2
24		0	0	2	0	0	0	0	2	2	2
25		4	2	10	2	2	2	2	2	2	2
26		0	0	2	0	2	0	2	2	2	0
27		0	0	0	0	2	2	0	0	2	0
28		0	2	0	0	0	0	0	2	0	2
29		0	0	2	2	0	2	0	0	2	0
30		0	0	0	2	0	2	2	2	0	2
31		0	2	2	0	2	0	0	0	2	0
32		4	0	0	2	0	0	2	0	2	0
33		4	0	0	0	0	0	2	0	0	2
34		0	2	2	0	2	0	0	0	0	2
35		0	0	0	0	0	2	2	2	2	2
36		8	6	2	2	2	2	2	2	2	2
37		0	2	0	2	2	0	0	0	0	0
38		0	0	0	0	2	2	2	0	0	2
39		0	0	2	2	0	0	0	2	2	0
40		0	2	0	0	0	2	0	0	0	0
41		4	0	2	0	0	0	0	0	2	0
42		0	0	0	0	2	2	2	2	0	2
43		0	2	0	2	0	2	2	2	0	0
44		0	0	2	2	0	0	0	2	0	0
45		0	0	0	0	2	0	0	2	0	2
46		0	2	2	2	0	0	0	0	0	0
47		0	0	0	0	2	0	2	2	2	0
48		4	0	0	0	2	2	0	0	2	0
49		4	2	2	14	2	2	2	2	2	2
50		0	0	0	2	0	0	2	0	2	0
51		0	0	2	2	0	2	0	0	0	2
52		0	2	0	0	0	0	2	0	2	2
53		0	0	0	2	2	2	2	0	0	2
54		0	0	2	0	0	0	0	2	2	2
55		0	2	0	0	0	2	2	2	2	0
56		0	0	2	0	2	2	0	0	0	0
57		4	0	0	2	0	0	0	0	0	2
58		0	2	0	2	2	0	0	2	2	0
59		0	0	2	0	2	0	2	0	2	2
60		0	0	0	2	2	0	2	0	0	0
61		0	2	2	0	0	2	0	2	0	0
62		0	0	0	0	0	2	0	2	2	2
63		0	6	0	0	0	0	0	2	0	2
64		4	2	2	2	2	2	2	2	2	2

p		2	3	5	7
#(c)					
mod $p^6$		8	27	125	343
		4	2	2	2
		0	0	0	2
		0	0	0	0
		8	2	2	2
		0	0	0	0
		0	0	2	0
		0	2	0	0
		0	0	0	2
		4	6	2	2
		0	2	0	0
		0	0	2	2
		0	0	0	0
		0	2	0	0
		0	0	2	0
		0	0	0	2
		8	2	2	2
		4	0	0	0
		0	0	0	2
		0	2	2	0
		0	0	0	0
		0	0	2	0
		0	2	0	2
		0	0	0	2
		0	0	2	0
		0	2	2	0
		0	0	0	2
		4	0	0	0
		0	2	2	0
		0	0	0	2
		0	2	0	0
		0	0	2	0
		0	2	0	0
		0	0	2	2
		0	2	2	2
		0	0	0	0
		0	2	0	2
		0	0	0	0
		0	0	2	2
		0	2	0	0
		0	0	2	0
		4	0	0	2
		0	2	0	2
		0	0	0	0
		0	2	2	0
		0	0	2	0
		0	6	0	0
		8	2	2	2

	p	2	3	5	7
c					
0	#(c)	8	27	125	343
1	mod $p^7$	4	2	2	2
2		0	0	0	2
3		0	0	0	0
4		8	2	2	2
5		0	0	0	0
6		0	0	2	0
7		0	2	0	0
8		0	0	0	2
9		4	6	2	2
10		0	2	0	0
11		0	0	2	2
12		0	0	0	0
13		0	2	0	0
14		0	0	2	0
15		0	0	0	2
16		16	2	2	2
17		4	0	0	0
18		0	0	0	2
19		0	2	2	0
20		0	0	0	0
21		0	0	2	0
22		0	2	0	2
23		0	0	0	2
24		0	0	2	0
25		4	2	10	2
26		0	0	2	0
27		0	0	0	0
28		0	2	0	0
29		0	0	2	2
30		0	0	0	2
31		0	2	2	0
32		0	0	0	2
33		4	0	0	0
34		0	2	2	0
35		0	0	0	0
36		8	6	2	2
37		0	2	0	2
38		0	0	0	0
39		0	0	2	2
40		0	2	0	0
41		4	0	2	0
42		0	0	0	0
43		0	2	0	2
44		0	0	2	2
45		0	0	0	0
46		0	2	2	2
47		0	0	0	0
48		0	0	0	0
49		4	2	2	14
50		0	0	0	2
51		0	0	2	2
52		0	2	0	0
53		0	0	0	2
54		0	0	2	0
55		0	2	0	0
56		0	0	2	0
57		4	0	0	2
58		0	2	0	2
59		0	0	2	0
60		0	0	0	2
61		0	2	2	0
62		0	0	0	0
63		0	6	0	0
64		8	2	2	2

	p	2	3	5	7
c					
0	#(c)	16	81	625	2401
1	mod $p^8$	4	2	2	2
2		0	0	0	2
3		0	0	0	0
4		8	2	2	2
5		0	0	0	0
6		0	0	2	0
7		0	2	0	0
8		0	0	0	2
9		4	6	2	2
10		0	2	0	0
11		0	0	2	2
12		0	0	0	0
13		0	2	0	0
14		0	0	2	0
15		0	0	0	2
16		16	2	2	2
17		4	0	0	0
18		0	0	0	2
19		0	2	2	0
20		0	0	0	0
21		0	0	2	0
22		0	2	0	2
23		0	0	0	2
24		0	0	2	0
25		4	2	10	2
26		0	0	2	0
27		0	0	0	0
28		0	2	0	0
29		0	0	2	2
30		0	0	0	2
31		0	2	2	0
32		0	0	0	2
33		4	0	0	0
34		0	2	2	0
35		0	0	0	0
36		8	6	2	2
37		0	2	0	2
38		0	0	0	0
39		0	0	2	2
40		0	2	0	0
41		4	0	2	0
42		0	0	0	0
43		0	2	0	2
44		0	0	2	2
45		0	0	0	0
46		0	2	2	2
47		0	0	0	0
48		0	0	0	0
49		4	2	2	14
50		0	0	0	2
51		0	0	2	2
52		0	2	0	0
53		0	0	0	2
54		0	0	2	0
55		0	2	0	0
56		0	0	2	0
57		4	0	0	2
58		0	2	0	2
59		0	0	2	0
60		0	0	0	2
61		0	2	2	0
62		0	0	0	0
63		0	6	0	0
64		16	2	2	2

	p	2	3	5	7
c					
0	#(c)	16	81	625	2401
1	mod $p^9$	4	2	2	2
2		0	0	0	2
3		0	0	0	0
4		8	2	2	2
5		0	0	0	0
6		0	0	2	0
7		0	2	0	0
8		0	0	0	2
9		4	6	2	2
10		0	2	0	0
11		0	0	2	2
12		0	0	0	0
13		0	2	0	0
14		0	0	2	0
15		0	0	0	2
16		16	2	2	2
17		4	0	0	0
18		0	0	0	2
19		0	2	2	0
20		0	0	0	0
21		0	0	2	0
22		0	2	0	2
23		0	0	0	2
24		0	0	2	0
25		4	2	10	2
26		0	0	2	0
27		0	0	0	0
28		0	2	0	0
29		0	0	2	2
30		0	0	0	2
31		0	2	2	0
32		0	0	0	2
33		4	0	0	0
34		0	2	2	0
35		0	0	0	0
36		8	6	2	2
37		0	2	0	2
38		0	0	0	0
39		0	0	2	2
40		0	2	0	0
41		4	0	2	0
42		0	0	0	0
43		0	2	0	2
44		0	0	2	2
45		0	0	0	0
46		0	2	2	2
47		0	0	0	0
48		0	0	0	0
49		4	2	2	14
50		0	0	0	2
51		0	0	2	2
52		0	2	0	0
53		0	0	0	2
54		0	0	2	0
55		0	2	0	0
56		0	0	2	0
57		4	0	0	2
58		0	2	0	2
59		0	0	2	0
60		0	0	0	2
61		0	2	2	0
62		0	0	0	0
63		0	6	0	0
64		32	2	2	2

One uses  $x^2 = c$ ,  $x = c^{1/2}$ ,  $x'(c) = V'(c) = (1/2).c^{-1/2}$

delta		1	2	3	4	5	6	7	8	9	$V'(c) = (1/2).c^{-1/2}$	Product.V'(c)/8
c												
0	product #(c) sequences 2, 3, 5 et 7	1	210	210	44100	44100	9261000	9261000	1944810000	1944810000	$\infty$	$\infty$
1		8	16	32	32	32	32	32	32	32	0,500	<b>2</b>
2		0	0	0	0	0	0	0	0	0	0,354	0
3		0	0	0	0	0	0	0	0	0	0,289	0
4		8	16	16	32	64	64	64	64	64	0,250	<b>2</b>
5		0	0	0	0	0	0	0	0	0	0,224	0
6		0	0	0	0	0	0	0	0	0	0,204	0
7		0	0	0	0	0	0	0	0	0	0,189	0
8		0	0	0	0	0	0	0	0	0	0,177	0
9		4	24	96	96	96	96	96	96	96	0,167	<b>2</b>
10		0	0	0	0	0	0	0	0	0	0,158	0
11		0	0	0	0	0	0	0	0	0	0,151	0
12		0	0	0	0	0	0	0	0	0	0,144	0
13		0	0	0	0	0	0	0	0	0	0,139	0
14		0	0	0	0	0	0	0	0	0	0,134	0
15		2	0	0	0	0	0	0	0	0	0,129	0
16		8	16	16	32	32	64	128	128	128	0,125	<b>2</b>
17		0	0	0	0	0	0	0	0	0	0,121	0
18		0	0	0	0	0	0	0	0	0	0,118	0
19		0	0	0	0	0	0	0	0	0	0,115	0
20		0	0	0	0	0	0	0	0	0	0,112	0
21		2	0	0	0	0	0	0	0	0	0,109	0
22		0	0	0	0	0	0	0	0	0	0,107	0
23		0	0	0	0	0	0	0	0	0	0,104	0
24		0	0	0	0	0	0	0	0	0	0,102	0
25		4	40	160	160	160	160	160	160	160	0,100	<b>2</b>
26		0	0	0	0	0	0	0	0	0	0,098	0
27		0	0	0	0	0	0	0	0	0	0,096	0
28		0	0	0	0	0	0	0	0	0	0,094	0
29		0	0	0	0	0	0	0	0	0	0,093	0
30		2	0	0	0	0	0	0	0	0	0,091	0
31		0	0	0	0	0	0	0	0	0	0,090	0
32		0	0	0	0	0	0	0	0	0	0,088	0
33		0	0	0	0	0	0	0	0	0	0,087	0
34		0	0	0	0	0	0	0	0	0	0,086	0
35		0	0	0	0	0	0	0	0	0	0,085	0
36		4	24	48	96	192	192	192	192	192	0,083	<b>2</b>
37		0	0	0	0	0	0	0	0	0	0,082	0
38		0	0	0	0	0	0	0	0	0	0,081	0
39		4	0	0	0	0	0	0	0	0	0,080	0
40		0	0	0	0	0	0	0	0	0	0,079	0
41		0	0	0	0	0	0	0	0	0	0,078	0
42		0	0	0	0	0	0	0	0	0	0,077	0
43		0	0	0	0	0	0	0	0	0	0,076	0
44		0	0	0	0	0	0	0	0	0	0,075	0
45		0	0	0	0	0	0	0	0	0	0,075	0
46		8	0	0	0	0	0	0	0	0	0,074	0
47		0	0	0	0	0	0	0	0	0	0,073	0
48		0	0	0	0	0	0	0	0	0	0,072	0
49		4	56	224	224	224	224	224	224	224	0,071	<b>2</b>
50		0	0	0	0	0	0	0	0	0	0,071	0
51		4	0	0	0	0	0	0	0	0	0,070	0
52		0	0	0	0	0	0	0	0	0	0,069	0
53		0	0	0	0	0	0	0	0	0	0,069	0
54		0	0	0	0	0	0	0	0	0	0,068	0
55		0	0	0	0	0	0	0	0	0	0,067	0
56		0	0	0	0	0	0	0	0	0	0,067	0
57		0	0	0	0	0	0	0	0	0	0,066	0
58		0	0	0	0	0	0	0	0	0	0,066	0
59		0	0	0	0	0	0	0	0	0	0,065	0
60		2	0	0	0	0	0	0	0	0	0,065	0
61		0	0	0	0	0	0	0	0	0	0,064	0
62		0	0	0	0	0	0	0	0	0	0,064	0
63		0	0	0	0	0	0	0	0	0	0,063	0
64		8	16	16	32	32	64	64	128	256	0,063	<b>2</b>

Thus if  $c \neq 0$ ,

$$\#(c) = V'(c) \cdot \prod_{p=2}^{p=7} \frac{\#(c) \bmod p^9}{2}$$

## Appendix 4

Numerical examples with  $P(x) = x^4 + x^3 + x^2 + x$  :

$p = 3$

Conditions	$\#(c = P(x))$
Disc = $\{1\} \bmod 3$	1
Disc = $\{2\} \bmod 3$	2
Disc = $\{\emptyset\}$	4
Disc = $\{(0)\} \bmod 3$	$\{\emptyset\}$

$p = 5$

Conditions	$\#(c = P(x))$
Disc = $\{\emptyset\}$	1
Disc = $\{\emptyset\}$	2
Disc = $\{4\} \bmod 5$	4
Disc = $\{(0), 1, 2, 3\} \bmod 5$	$\{\emptyset\}$

$p = 7$

Conditions	$\#(c = P(x))$
Disc = $\{4\} \bmod 7$	1
Disc = $\{5, 6\} \bmod 7$	2
Disc = $\{\emptyset\}$	4
Disc = $\{(0), 1, 2, 3\} \bmod 7$	$\{\emptyset\}$
Disc = $\{3, 5, 6\} \bmod 7$	14
Disc = $\{5\} \bmod 7$	49

$p = 11$

Conditions	$\#(c = P(x))$
Disc = $\{1, 3, 9\} \bmod 11$	1
Disc = $\{6\} \bmod 11$	2
Disc = $\{4\} \bmod 11$	4
Disc = $\{(0), 2, 5, 7, 8, 10\} \bmod 11$	$\{\emptyset\}$

$p = 13$

Conditions	$\#(c = P(x))$
Disc = $\{3, 4, 10\} \bmod 13$	1
Disc = $\{7\} \bmod 13$	2
Disc = $\{10\} \bmod 13$	4
Disc = $\{(0), 1, 2, 5, 6, 8, 9, 11, 12\} \bmod 13$	$\{\emptyset\}$
Disc = $\{1\} \bmod 13, k = 3$	13
Disc = $\{2, 5, 7, 8, 11\} \bmod 13, k = 2$	26

$p = 17$

Conditions	$\#(c = P(x))$
Disc = $\{2, 8, 9, 13, 15\} \bmod 17$	1
Disc = $\{5, 6\} \bmod 17$	2
Disc = $\{1\} \bmod 17$	4
Disc = $\{(0), 3, 4, 7, 10, 11, 12, 14, 16\} \bmod 17$	$\{\emptyset\}$

$p = 19$

Conditions	$\#(c = P(x))$
Disc = $\{1, 6, 7, 9\} \bmod 19$	1
Disc = $\{3, 8, 14, 15, 18\} \bmod 19$	2
Disc = $\{\emptyset\} \bmod 19$	4
Disc = $\{(0), 1, 2, 4, 5, 7, 10, 11, 12, 13, 16, 17\} \bmod 19$	$\{\emptyset\}$

$p = 23$

Conditions	$\#(c = P(x))$
Disc = $\{2, 8, 9, 12, 16\} \bmod 23$	1
Disc = $\{5, 7, 10, 15, 20, 21\} \bmod 23$	2
Disc = $\{\emptyset\} \bmod 23$	4
Disc = $\{(0), 1, 3, 4, 6, 11, 13, 14, 17, 18, 19, 22\} \bmod 23$	$\{\emptyset\}$
Disc = $\{5\} \bmod 23$	23

$p = 29$

Conditions	#(c = P(x))
Disc = {4, 13, 16, 22, 23, 24, 28} mod 29	1
Disc = {2, 3, 10, 15, 17, 26, 27} mod 29	2
Disc = {13} mod 29	4
Disc = {(0), 1, 5, 6, 7, 8, 9, 11, 12, 14, 17, 18, 19, 20, 21, 25} mod 29	{Ø}
Disc = {25} mod 29	29

$p = 31$

Conditions	#(c = P(x))
Disc = {1, 4, 7, 10, 16, 18, 20, 24, 28} mod 31	1
Disc = {3, 6, 15, 17, 21, 26, 29} mod 31	2
Disc = {1, 11} mod 31	4
Disc = {(0), 2, 5, 8, 9, 12, 13, 14, 19, 22, 23, 25, 27, 30} mod 31	{Ø}

## Appendix 5

Equation of Borovoi. Case of variables of integers

p	2	3	5	7	11	13	17	19	23	2	3	5	7	11	13	17	19	23	=	pn	#(effective solutions)	ratio singular series / #
δ	6	5	3	2	2	2	2	2	2	6	5	3	2	2	2	2	2					
c	Number of local solutions (nsl)									Normalized proportions (pn = nsl/p <sup>2δ</sup> )												
0	8192	39366	12500	2744	13310	26364	88434	123462	292008	2,000	0,667	0,800	1,143	0,909	0,923	1,059	0,947	1,043	1,071	0	0	
1	8192	78732	18750	2744	15972	30758	88434	137180	292008	2,000	1,333	1,200	1,143	1,091	1,077	1,059	1,053	1,043	4,997	1148	230	
2	0	52488	18750	2058	13310	26364	78608	137180	292008	0,000	0,889	1,200	0,857	0,909	0,923	0,941	1,053	1,043	0,000	0		
3	8192	39366	12500	2744	13310	26364	88434	123462	292008	2,000	0,667	0,800	1,143	0,909	0,923	1,059	0,947	1,043	1,071	130	121	
4	0	78732	15000	2058	13310	30758	78608	123462	267674	0,000	1,333	0,960	0,857	0,909	1,077	0,941	0,947	0,957	0,000	0		
5	0	52488	12500	2058	15972	30758	78608	123462	292008	0,000	0,889	0,800	0,857	1,091	1,077	0,941	0,947	1,043	0,000	0		
6	8192	39366	18750	2352	15972	30758	78608	123462	267674	2,000	0,667	1,200	0,980	1,091	1,077	0,941	0,947	0,957	1,570	185	118	
7	8192	78732	18750	2744	15972	30758	88434	137180	292008	2,000	1,333	1,200	1,143	1,091	1,077	1,059	1,053	1,043	4,997	1070	214	
8	8192	65610	12500	2744	13310	26364	88434	123462	292008	2,000	1,111	0,800	1,143	0,909	0,923	1,059	0,947	1,043	1,785	346	194	
9	0	39366	15000	2058	15972	26364	78608	137180	267674	0,000	0,667	0,960	0,857	1,091	0,923	0,941	1,053	0,957	0,000	0		
10	0	78732	12500	2744	14520	30758	78608	123462	267674	0,000	1,333	0,800	1,143	0,992	1,077	0,941	0,947	0,957	0,000	0		
11	0	52488	18750	2058	13310	26364	78608	137180	292008	0,000	0,889	1,200	0,857	0,909	0,923	0,941	1,053	1,043	0,000	0		
12	0	39366	18750	2058	15972	28392	88434	137180	292008	0,000	0,667	1,200	0,857	1,091	0,994	1,059	1,053	1,043	0,000	0		
13	8192	78732	12500	2352	13310	26364	78608	137180	267674	2,000	1,333	0,800	0,980	0,909	0,923	0,941	1,053	0,957	1,662	220	132	
14	8192	52488	15000	2744	13310	30758	88434	137180	267674	2,000	0,889	0,960	1,143	0,909	1,077	1,059	1,053	0,957	2,036	229	112	
15	4096	39366	12500	2744	13310	26364	88434	123462	292008	1,000	0,667	0,800	1,143	0,909	0,923	1,059	0,947	1,043	0,535	68	127	
16	8192	78732	18750	2058	15972	26364	83232	123462	267674	2,000	1,333	1,200	0,857	1,091	0,923	0,997	0,947	0,957	2,494	295	118	
17	8192	78732	18750	2744	15972	30758	88434	137180	292008	2,000	1,333	1,200	1,143	1,091	1,077	1,059	1,053	1,043	4,997	1104	221	
18	0	39366	12500	2058	15972	30758	88434	129960	267674	0,000	0,667	0,800	0,857	1,091	1,077	1,059	0,997	0,957	0,000	0		
19	0	78732	15000	2058	13310	30758	78608	123462	267674	0,000	1,333	0,960	0,857	0,909	1,077	0,941	0,947	0,957	0,000	0		
20	0	52488	12500	2352	15972	30758	88434	137180	267674	0,000	0,889	0,800	0,980	1,091	1,077	1,059	1,053	0,957	0,000	0		
21	0	39366	18750	2744	14520	26364	78608	137180	267674	0,000	0,667	1,200	1,143	0,992	0,923	0,941	1,053	0,957	0,000	0		
22	8192	78732	18750	2744	13310	26364	78608	123462	279312	2,000	1,333	1,200	1,143	0,909	0,923	0,941	0,947	0,998	2,731	330	121	
23	0	52488	12500	2058	15972	30758	78608	123462	292008	0,000	0,889	0,800	0,857	1,091	1,077	0,941	0,947	1,043	0,000	0		
24	8192	39366	17500	2744	13310	26364	88434	123462	292008	2,000	0,667	1,120	1,143	0,909	0,923	1,059	0,947	1,043	1,499	312	208	
25	0	78732	12500	2058	13310	28392	88434	123462	292008	0,000	1,333	0,800	0,857	0,909	0,994	1,059	0,947	1,043	0,000	0		
26	0	69984	18750	2058	13310	26364	78608	137180	292008	0,000	1,185	1,200	0,857	0,909	0,923	0,941	1,053	1,043	0,000	0		
27	8192	39366	18750	2352	15972	30758	78608	123462	267674	2,000	0,667	1,200	0,980	1,091	1,077	0,941	0,947	0,957	1,570	194	124	
28	0	78732	12500	2744	15972	26364	78608	137180	292008	0,000	1,333	0,800	1,143	1,091	0,923	0,941	1,053	1,043	0,000	0		
29	8192	52488	15000	2744	15972	26364	88434	123462	267674	2,000	0,889	0,960	1,143	1,091	0,923	1,059	0,947	0,957	1,885	226	120	
30	8192	39366	12500	2058	13310	30758	78608	137180	292008	2,000	0,667	0,800	0,857	0,909	1,077	0,941	1,053	1,043	0,925	127	137	
31	4096	78732	18750	2744	15972	30758	88434	137180	292008	1,000	1,333	1,200	1,143	1,091	1,077	1,059	1,053	1,043	2,498	1002	401	
32	8192	52488	18750	2058	14520	30758	88434	137180	267674	2,000	0,889	1,200	0,857	0,992	1,077	1,059	1,053	0,957	2,082	252	121	
33	8192	39366	12500	2058	13310	30758	83232	137180	267674	2,000	0,667	0,800	0,857	0,909	1,077	0,997	1,053	0,957	0,898	109	121	
34	0	78732	15000	2352	15972	26364	88434	123462	292008	0,000	1,333	0,960	0,980	1,091	0,923	1,059	0,947	1,043	0,000	0		
35	8192	65610	12500	2744	13310	26364	88434	123462	292008	2,000	1,111	0,800	1,143	0,909	0,923	1,059	0,947	1,043	1,785	214	120	

36	0	39366	18750	2744	13310	30758	78608	137180	267674	0,000	0,667	1,200	1,143	0,909	1,077	0,941	1,053	0,957	0,000	0	
37	0	78732	18750	2058	13310	26364	88434	129960	267674	0,000	1,333	1,200	0,857	0,909	0,923	1,059	0,997	0,957	0,000	0	
38	8192	52488	12500	2744	15972	28392	78608	123462	292008	2,000	0,889	0,800	1,143	1,091	0,994	0,941	0,947	1,043	1,640	222	135
39	0	39366	15000	2058	15972	26364	78608	137180	267674	0,000	0,667	0,960	0,857	1,091	0,923	0,941	1,053	0,957	0,000	0	
40	8192	78732	12500	2058	15972	30758	78608	137180	292008	2,000	1,333	0,800	0,857	1,091	1,077	0,941	1,053	1,043	2,221	270	122
41	0	52488	18750	2352	13310	26364	88434	123462	267674	0,000	0,889	1,200	0,980	0,909	0,923	1,059	0,947	0,957	0,000	0	
42	0	39366	18750	2744	15972	26364	88434	123462	267674	0,000	0,667	1,200	1,143	1,091	0,923	1,059	0,947	0,957	0,000	0	
43	0	78732	12500	2744	14520	30758	78608	123462	267674	0,000	1,333	0,800	1,143	0,992	1,077	0,941	0,947	0,957	0,000	0	
44	0	78732	15000	2058	13310	30758	78608	123462	267674	0,000	1,333	0,960	0,857	0,909	1,077	0,941	0,947	0,957	0,000	0	
45	8192	39366	12500	2744	15972	30758	78608	137180	279312	2,000	0,667	0,800	1,143	1,091	1,077	0,941	1,053	0,998	1,416	167	118
46	8192	78732	18750	2058	13310	30758	88434	123462	292008	2,000	1,333	1,200	0,857	0,909	1,077	1,059	0,947	1,043	2,811	319	113
47	4096	52488	18750	2058	13310	26364	78608	137180	292008	1,000	0,889	1,200	0,857	0,909	0,923	0,941	1,053	1,043	0,793	100	126
48	8192	39366	12500	2695	13310	26364	88434	123462	292008	2,000	0,667	0,800	1,122	0,909	0,923	1,059	0,947	1,043	1,052	0	0
49	8192	78732	18750	2744	15972	30758	88434	137180	292008	2,000	1,333	1,200	1,143	1,091	1,077	1,059	1,053	1,043	4,997	1109	222
50	0	52488	12500	2744	15972	26364	83232	137180	267674	0,000	0,889	0,800	1,143	1,091	0,923	0,997	1,053	0,957	0,000	0	
51	0	39366	18750	2058	15972	28392	88434	137180	292008	0,000	0,667	1,200	0,857	1,091	0,994	1,059	1,053	1,043	0,000	0	
52	0	78732	18750	2744	13310	26364	88434	137180	267674	0,000	1,333	1,200	1,143	0,909	0,923	1,059	1,053	0,957	0,000	0	
53	0	69984	12500	2058	15972	30758	78608	123462	292008	0,000	1,185	0,800	0,857	1,091	1,077	0,941	0,947	1,043	0,000	0	
54	8192	39366	15000	2058	14520	26364	88434	123462	292008	2,000	0,667	0,960	0,857	0,992	0,923	1,059	0,947	1,043	1,051	151	144
55	8192	78732	12500	2352	13310	26364	78608	137180	267674	2,000	1,333	0,800	0,980	0,909	0,923	0,941	1,053	0,957	1,662	217	131
56	8192	52488	18750	2744	15972	30758	78608	129960	267674	2,000	0,889	1,200	1,143	1,091	1,077	0,941	0,997	0,957	2,571	297	115
57	0	39366	18750	2744	13310	30758	78608	123462	292008	0,000	0,667	1,200	1,143	0,909	1,077	0,941	0,947	1,043	0,000	0	
58	0	78732	12500	2058	13310	30758	88434	137180	292008	0,000	1,333	0,800	0,857	0,909	1,077	1,059	1,053	1,043	0,000	0	
59	8192	52488	15000	2744	13310	30758	88434	137180	267674	2,000	0,889	0,960	1,143	0,909	1,077	1,059	1,053	0,957	2,036	232	114
60	0	39366	12500	2058	15972	26364	78608	123462	267674	0,000	0,667	0,800	0,857	1,091	0,923	0,941	0,947	0,957	0,000	0	
61	8192	78732	18750	2058	15972	26364	78608	123462	292008	2,000	1,333	1,200	0,857	1,091	0,923	0,941	0,947	1,043	2,570	300	117
62	8192	65610	18750	2352	15972	30758	78608	123462	267674	2,000	1,111	1,200	0,980	1,091	1,077	0,941	0,947	0,957	2,617	317	121
63	4096	39366	12500	2744	13310	26364	88434	123462	292008	1,000	0,667	0,800	1,143	0,909	0,923	1,059	0,947	1,043	0,535	65	121
64	8192	78732	15000	2744	15972	28392	78608	137180	267674	2,000	1,333	0,960	1,143	1,091	0,994	0,941	1,053	0,957	3,007	344	114
65	8192	52488	12500	2058	14520	26364	88434	123462	267674	2,000	0,889	0,800	0,857	0,992	0,923	1,059	0,947	0,957	1,071	140	131
66	0	39366	18750	2744	13310	30758	88434	137180	267674	0,000	0,667	1,200	1,143	0,909	1,077	1,059	1,053	0,957	0,000	0	
67	8192	78732	18750	2058	15972	26364	83232	123462	267674	2,000	1,333	1,200	0,857	1,091	0,923	0,997	0,947	0,957	2,494	300	120
68	0	52488	12500	2058	13310	26364	88434	137180	279312	0,000	0,889	0,800	0,857	0,909	0,923	1,059	1,053	0,998	0,000	0	
69	0	39366	15000	2352	13310	30758	88434	137180	292008	0,000	0,667	0,960	0,980	0,909	1,077	1,059	1,053	1,043	0,000	0	
70	8192	78732	12500	2744	13310	30758	78608	137180	292008	2,000	1,333	0,800	1,143	0,909	1,077	0,941	1,053	1,043	2,468	302	122
71	8192	78732	18750	2744	15972	30758	88434	137180	292008	2,000	1,333	1,200	1,143	1,091	1,077	1,059	1,053	1,043	4,997	1036	207
72	8192	39366	18750	2058	15972	30758	78608	123462	292008	2,000	0,667	1,200	0,857	1,091	1,077	0,941	0,947	1,043	1,499	198	132
73	0	78732	12500	2744	15972	26364	78608	123462	267674	0,000	1,333	0,800	1,143	1,091	0,923	0,941	0,947	0,957	0,000	0	
74	0	52488	18750	2058	13310	26364	78608	137180	292008	0,000	0,889	1,200	0,857	0,909	0,923	0,941	1,053	1,043	0,000	0	
75	0	39366	12500	2058	15972	30758	88434	129960	267674	0,000	0,667	0,800	0,857	1,091	1,077	1,059	0,997	0,957	0,000	0	
76	0	78732	18750	2352	14520	26364	88434	123462	292008	0,000	1,333	1,200	0,980	0,992	0,923	1,059	0,947	1,043	0,000	0	
77	8192	52488	18750	2744	13310	28392	78608	137180	292008	2,000	0,889	1,200	1,143	0,909	0,994	0,941	1,053	1,043	2,278	255	112
78	8192	39366	12500	2744	15972	26364	78608	137180	267674	2,000	0,667	0,800	1,143	1,091	0,923	0,941	1,053	0,957	1,163	162	139
79	4096	78732	15000	2058	13310	30758	78608	123462	267674	1,000	1,333	0,960	0,857	0,909	1,077	0,941	0,947	0,957	0,916	118	129
80	8192	74358	12500	2744	13310	26364	88434	123462	292008	2,000	1,259	0,800	1,143	0,909	0,923	1,059	0,947	1,043	2,023	116	57
81	8192	39366	18750	2058	13310	26364	78608	123462	292008	2,000	0,667	1,200	0,857	0,909	0,923	0,941	0,947	1,043	1,071	134	125

## Appendix 6

### Equation of Borovoi. Case of prime numbers variables

		Targets														
p	$\delta$	1	7	8	13	16	17	33	40	45	46	49	56	61	64	81
		Abundance factors														
2	8	65536	0	0	65536	0	65536	65536	0	65536	0	65536	0	65536	0	65536
3	5	26244	26244	0	26244	26244	0	26244	26244	26244	26244	26244	0	26244	26244	26244
5	4	312500	312500	125000	125000	312500	312500	125000	125000	125000	312500	125000	312500	312500	125000	312500
7	3	76832	76832	76832	57624	76832	76832	76832	76832	76832	76832	76832	76832	76832	76832	76832
11	2	12584	12584	9196	9196	12584	12584	9196	12584	12584	9196	12584	12584	12584	12584	9196
13	2	25012	25012	20280	20280	20280	25012	25012	25012	25012	25012	25012	25012	25012	20280	20280
17	2	75140	75140	75140	64736	64736	75140	64736	64736	64736	75140	75140	64736	64736	64736	64736
19	2	118408	118408	103968	118408	103968	118408	118408	118408	118408	103968	118408	103968	103968	118408	103968
23	2	258152	258152	258152	234876	234876	258152	234876	258152	209484	258152	258152	234876	258152	234876	258152
29	2	659344	659344	612248	659344	659344	659344	612248	659344	659344	659344	659344	612248	612248	612248	612248
31	1	904	904	904	904	840	904	840	904	840	904	904	840	840	840	904
37	1	1296	1296	1224	1296	1296	1296	1224	1224	1224	1224	1296	1296	1224	1224	1296
41	1	1604	1604	1604	1520	1520	1604	1520	1520	1520	1604	1520	1604	1604	1520	1520
43	1	1768	1768	1676	1676	1676	1768	1768	1676	1768	1676	1768	1676	1768	1768	1768
47	1	2120	2120	2120	2120	2120	2120	2120	2024	2024	2024	2120	2024	2024	2120	2024
53	1	2704	2704	2600	2704	2600	2704	2704	2704	2600	2600	2704	2600	2600	2704	2600
59	1	3368	3368	3248	3368	3248	3368	3368	3248	3248	3368	3368	3248	3248	3368	3368
61	1	3604	3604	3480	3480	3604	3604	3480	3480	3480	3480	3604	3480	3480	3480	3604
67	1	4360	4360	4220	4220	4220	4360	4360	4360	4360	4220	4360	4360	4220	4220	4220
71	1	4904	4904	4904	4764	4764	4904	4764	4764	4764	4764	4904	4904	4764	4764	4764
73	1	5188	5188	5188	5040	5040	5188	5040	5188	5188	5040	5188	5188	5040	5188	5188
79	1	6088	6088	6088	5932	5932	6088	5932	5932	6088	5932	6088	5932	6088	6088	5932
83	1	6728	6728	6560	6728	6560	6728	6728	6560	6728	6728	6728	6728	6728	6560	6728
89	1	7748	7748	7748	7568	7748	7748	7748	7568	7568	7748	7748	7748	7568	7568	7568
97	1	9220	9220	9220	9024	9024	9220	9024	9024	9024	9220	9220	9024	9220	9220	9024
101	1	10004	10004	9800	9800	9800	10004	10004	10004	10004	9800	10004	10004	10004	9800	9800
103	1	10408	10408	10408	10408	10408	10408	10408	10408	10408	10200	10408	10200	10200	10200	10408
107	1	11240	11240	11020	11020	11240	11240	11020	11020	11240	11020	11240	11020	11020	11240	11240
109	1	11664	11664	11448	11664	11664	11664	11448	11664	11448	11664	11664	11664	11664	11664	11448
113	1	12552	12552	12552	12552	12320	12552	12320	12552	12320	12320	12552	12552	12552	12320	12552
127	1	15880	15880	15880	15628	15880	15880	15880	15880	15628	15880	15880	15628	15880	15628	15880
131	1	16904	16904	16640	16904	16904	16904	16640	16640	16640	16904	16904	16904	16640	16640	16904
137	1	18504	18504	18504	18504	18504	18504	18504	18224	18224	18224	18504	18224	18224	18504	18224
139	1	19048	19048	18768	19048	19048	19048	18768	18768	18768	18768	19048	18768	19048	18768	19048
149	1	21904	21904	21608	21904	21608	21904	21904	21904	21608	21608	21904	21904	21904	21904	21608
151	1	22504	22504	22504	22204	22504	22504	22504	22204	22204	22504	22504	22204	22504	22204	22204
157	1	24340	24340	24024	24024	24024	24340	24340	24340	24024	24024	24340	24024	24340	24340	24024
163	1	26248	26248	25916	25916	26248	26248	25916	25916	25916	25916	26248	25916	25916	25916	26248
167	1	27560	27560	27560	27560	27224	27560	27224	27224	27224	27560	27560	27560	27560	27560	27224
173	1	29588	29588	29240	29240	29588	29588	29240	29240	29588	29240	29588	29240	29588	29588	29588
179	1	31688	31688	31324	31324	31324	31688	31688	31688	31324	31324	31688	31324	31688	31324	31324
181	1	32404	32404	32040	32040	32404	32404	32040	32404	32040	32404	32404	32404	32040	32040	32040
191	1	36104	36104	36104	35724	36104	36104	36104	35724	36104	35724	36104	35724	35724	36104	35724
193	1	36872	36872	36872	36872	36480	36872	36480	36480	36872	36480	36872	36480	36872	36872	36480
197	1	38416	38416	38024	38416	38416	38416	38024	38024	38416	38024	38416	38416	38024	38024	38416
199	1	39208	39208	39208	39208	38808	39208	38808	38808	39208	39208	39208	39208	39208	39208	38808
211	1	44104	44104	43676	43676	44104	44104	43676	44104	43676	43676	44104	44104	43676	43676	43676
223	1	49288	49288	49288	49288	49288	49288	49288	49288	48840	49288	49288	48840	49288	49288	49288
227	1	51080	51080	50624	51080	51080	51080	50624	51080	51080	50624	51080	50624	50624	50624	50624
229	1	51988	51988	51528	51528	51528	51988	51988	51988	51528	51988	51988	51528	51528	51988	51528

233	1	53832	53832	53832	53832	53360	53832	53360	53360	53832	53360	53832	53360	53832	53360	53360
239	1	56648	56648	56648	56172	56648	56648	56648	56172	56172	56172	56648	56172	56648	56172	56172
241	1	57604	57604	57604	57120	57120	57604	57120	57604	57120	57604	57604	57120	57120	57120	57604
251	1	62504	62504	62000	62504	62000	62504	62504	62000	62504	62504	62504	62504	62504	62000	62504
257	1	65540	65540	65540	65024	65540	65540	65540	65024	65540	65024	65540	65540	65540	65024	65024
263	1	68648	68648	68648	68124	68648	68648	68648	68124	68648	68124	68648	68124	68648	68124	68124
269	1	71828	71828	71288	71288	71828	71828	71288	71288	71828	71288	71828	71288	71288	71288	71828
271	1	72904	72904	72904	72904	72904	72904	72904	72904	72360	72360	72904	72904	72904	72360	72904
277	1	76176	76176	75624	76176	76176	76176	75624	75624	76176	75624	76176	75624	75624	76176	76176
281	1	78408	78408	78408	78408	78408	78408	78408	77840	77840	77840	78408	78408	78408	77840	77840
283	1	79528	79528	78960	79528	79528	79528	78960	78960	79528	79528	79528	78960	78960	79528	79528
293	1	85268	85268	84680	84680	84680	85268	85268	85268	84680	85268	85268	84680	85268	84680	84680
307	1	93640	93640	93024	93640	93024	93640	93640	93024	93024	93640	93640	93640	93024	93024	93640
311	1	96104	96104	96104	96104	95480	96104	95480	95480	95480	96104	96104	95480	95480	96104	95480
313	1	97348	97348	97348	96720	96720	97348	96720	96720	96720	96720	97348	97348	96720	96720	96720
317	1	99856	99856	99224	99856	99856	99856	99224	99856	99856	99856	99856	99856	99224	99856	99224
331	1	108904	108904	108236	108236	108236	108904	108904	108904	108236	108904	108904	108904	108904	108904	108236
337	1	112904	112904	112904	112904	112224	112904	112224	112904	112224	112904	112904	112224	112224	112224	112904
347	1	119720	119720	119020	119020	119720	119720	119020	119720	119020	119720	119720	119720	119720	119720	119020
349	1	121108	121108	120408	120408	120408	121108	121108	120408	121108	121108	121108	120408	121108	121108	121108
353	1	123908	123908	123908	123200	123908	123908	123908	123908	123908	123908	123908	123908	123200	123200	123908
359	1	128168	128168	128168	127452	128168	128168	128168	128168	128168	128168	128168	127452	127452	127452	128168
367	1	133960	133960	133960	133960	133224	133960	133224	133960	133960	133960	133960	133960	133960	133224	133960
373	1	138384	138384	137640	138384	137640	138384	138384	137640	137640	138384	138384	138384	138384	138384	138384
379	1	142888	142888	142124	142124	142888	142888	142124	142124	142888	142888	142888	142888	142124	142888	142888
383	1	145928	145928	145928	145928	145928	145928	145928	145160	145928	145160	145928	145928	145928	145928	145160
389	1	150544	150544	149768	150544	149768	150544	150544	149768	149768	150544	150544	150544	149768	149768	150544
397	1	156820	156820	156024	156024	156820	156820	156024	156820	156820	156024	156820	156024	156820	156024	156024
		Targets														
p	$\delta$	1	7	8	13	16	17	33	40	45	46	49	56	61	64	81
		Normalized factors														
2	8	8	0	0	8	0	8	8	0	8	0	8	0	8	0	8
3	5	1,5	1,5	0	1,5	1,5	0	1,5	1,5	1,5	1,5	1,5	0	1,5	1,5	1,5
5	4	1,5625	1,5625	0,625	0,625	1,5625	1,5625	0,625	0,625	0,625	1,5625	0,625	1,5625	1,5625	0,625	1,5625
7	3	1,037	1,037	1,037	0,778	1,037	1,037	1,037	1,037	1,037	1,037	1,037	1,037	1,037	1,037	1,037
11	2	1,144	1,144	0,836	0,836	1,144	1,144	0,836	1,144	1,144	0,836	1,144	1,144	1,144	1,144	0,836
13	2	1,113	1,113	0,903	0,903	0,903	1,113	1,113	1,113	1,113	1,113	1,113	1,113	1,113	0,903	0,903
17	2	1,079	1,079	1,079	0,930	0,930	1,079	0,930	0,930	0,930	1,079	1,079	0,930	0,930	0,930	0,930
19	2	1,069	1,069	0,938	1,069	0,938	1,069	1,069	1,069	1,069	0,938	1,069	0,938	0,938	1,069	0,938
23	2	1,054	1,054	1,054	0,959	0,959	1,054	0,959	1,054	0,855	1,054	1,054	0,959	1,054	0,959	1,054
29	2	1,036	1,036	0,962	1,036	1,036	1,036	0,962	1,036	1,036	1,036	1,036	0,962	0,962	0,962	0,962
31	1	1,038	1,038	1,038	1,038	0,964	1,038	0,964	1,038	0,964	1,038	1,038	0,964	0,964	0,964	1,038
37	1	1,028	1,028	0,971	1,028	1,028	1,028	0,971	0,971	0,971	0,971	1,028	1,028	0,971	0,971	1,028
41	1	1,028	1,028	1,028	0,974	0,974	1,028	0,974	0,974	1,028	0,974	1,028	1,028	1,028	0,974	0,974
43	1	1,026	1,026	0,973	0,973	0,973	1,026	1,026	0,973	1,026	0,973	1,026	0,973	1,026	1,026	1,026
47	1	1,024	1,024	1,024	1,024	1,024	1,024	1,024	0,977	0,977	0,977	1,024	0,977	0,977	1,024	0,977
53	1	1,019	1,019	0,980	1,019	0,980	1,019	1,019	1,019	0,980	0,980	1,019	0,980	0,980	1,019	0,980
59	1	1,018	1,018	0,982	1,018	0,982	1,018	1,018	0,982	0,982	1,018	1,018	0,982	0,982	1,018	1,018
61	1	1,018	1,018	0,983	0,983	1,018	1,018	0,983	0,983	0,983	0,983	1,018	0,983	0,983	0,983	1,018
67	1	1,016	1,016	0,983	0,983	0,983	1,016	1,016	1,016	1,016	0,983	1,016	1,016	0,983	0,983	0,983
71	1	1,015	1,015	1,015	0,986	0,986	1,015	0,986	0,986	0,986	0,986	1,015	1,015	0,986	0,986	0,986
73	1	1,015	1,015	1,015	0,986	0,986	1,015	0,986	1,015	1,015	0,986	1,015	1,015	0,986	1,015	1,015
79	1	1,013	1,013	1,013	0,988	0,988	1,013	0,988	0,988	1,013	0,988	1,013	0,988	1,013	1,013	0,988
83	1	1,013	1,013	0,988	1,013	0,988	1,013	1,013	0,988	1,013	1,013	1,013	1,013	1,013	0,988	1,013
89	1	1,012	1,012	1,012	0,988	1,012	1,012	1,012	0,988	0,988	1,012	1,012	1,012	0,988	0,988	0,988
97	1	1,011	1,011	1,011	0,989	0,989	1,011	0,989	0,989	0,989	1,011	1,011	0,989	1,011	1,011	0,989
101	1	1,010	1,010	0,990	0,990	0,990	1,010	1,010	1,010	1,010	0,990	1,010	1,010	1,010	0,990	0,990

103	1	1,010	1,010	1,010	1,010	1,010	1,010	1,010	1,010	1,010	0,990	1,010	0,990	0,990	0,990	1,010
107	1	1,010	1,010	0,990	0,990	1,010	1,010	0,990	0,990	1,010	0,990	1,010	0,990	0,990	1,010	1,010
109	1	1,009	1,009	0,991	1,009	1,009	1,009	0,991	1,009	0,991	1,009	1,009	1,009	1,009	1,009	0,991
113	1	1,010	1,010	1,010	1,010	0,991	1,010	0,991	1,010	0,991	0,991	1,010	1,010	1,010	0,991	1,010
127	1	1,008	1,008	1,008	0,992	1,008	1,008	1,008	1,008	0,992	1,008	1,008	0,992	1,008	0,992	1,008
131	1	1,008	1,008	0,992	1,008	1,008	1,008	0,992	0,992	0,992	1,008	1,008	1,008	0,992	0,992	1,008
137	1	1,008	1,008	1,008	1,008	1,008	1,008	1,008	0,993	0,993	0,993	1,008	0,993	0,993	1,008	0,993
139	1	1,007	1,007	0,993	1,007	1,007	1,007	0,993	0,993	0,993	0,993	1,007	0,993	1,007	0,993	1,007
149	1	1,007	1,007	0,993	1,007	0,993	1,007	1,007	1,007	0,993	0,993	1,007	1,007	1,007	1,007	0,993
151	1	1,007	1,007	1,007	0,993	1,007	1,007	1,007	0,993	0,993	1,007	1,007	0,993	1,007	0,993	0,993
157	1	1,007	1,007	0,994	0,994	0,994	1,007	1,007	1,007	0,994	0,994	1,007	0,994	1,007	1,007	0,994
163	1	1,006	1,006	0,994	0,994	1,006	1,006	0,994	0,994	0,994	0,994	1,006	0,994	0,994	0,994	1,006
167	1	1,006	1,006	1,006	1,006	0,994	1,006	0,994	0,994	0,994	1,006	1,006	1,006	1,006	1,006	0,994
173	1	1,006	1,006	0,994	0,994	1,006	1,006	0,994	0,994	1,006	0,994	1,006	0,994	1,006	1,006	1,006
179	1	1,006	1,006	0,994	0,994	0,994	1,006	1,006	1,006	0,994	0,994	1,006	0,994	1,006	0,994	0,994
181	1	1,006	1,006	0,994	0,994	1,006	1,006	0,994	1,006	0,994	1,006	1,006	1,006	0,994	0,994	0,994
191	1	1,005	1,005	1,005	0,995	1,005	1,005	1,005	0,995	1,005	0,995	1,005	0,995	0,995	1,005	0,995
193	1	1,005	1,005	1,005	1,005	0,995	1,005	0,995	0,995	1,005	0,995	1,005	0,995	1,005	1,005	0,995
197	1	1,005	1,005	0,995	1,005	1,005	1,005	0,995	0,995	1,005	0,995	1,005	1,005	0,995	0,995	1,005
199	1	1,005	1,005	1,005	1,005	0,995	1,005	0,995	0,995	1,005	1,005	1,005	1,005	1,005	1,005	0,995
211	1	1,005	1,005	0,995	0,995	1,005	1,005	0,995	1,005	0,995	0,995	1,005	1,005	0,995	0,995	0,995
223	1	1,005	1,005	1,005	1,005	1,005	1,005	1,005	1,005	0,995	1,005	1,005	0,995	1,005	1,005	1,005
227	1	1,005	1,005	0,996	1,005	1,005	1,005	0,996	1,005	1,005	0,996	1,005	0,996	0,996	0,996	0,996
229	1	1,004	1,004	0,996	0,996	0,996	1,004	1,004	1,004	0,996	1,004	1,004	0,996	0,996	1,004	0,996
233	1	1,004	1,004	1,004	1,004	0,996	1,004	0,996	0,996	1,004	0,996	1,004	0,996	1,004	0,996	0,996
239	1	1,004	1,004	1,004	0,996	1,004	1,004	1,004	0,996	0,996	0,996	1,004	0,996	1,004	0,996	0,996
241	1	1,004	1,004	1,004	0,996	0,996	1,004	0,996	1,004	0,996	1,004	1,004	0,996	0,996	0,996	1,004
251	1	1,004	1,004	0,996	1,004	0,996	1,004	1,004	0,996	1,004	1,004	1,004	1,004	1,004	0,996	1,004
257	1	1,004	1,004	1,004	0,996	1,004	1,004	1,004	0,996	1,004	0,996	1,004	1,004	1,004	0,996	0,996
263	1	1,004	1,004	1,004	0,996	1,004	1,004	1,004	0,996	1,004	0,996	1,004	0,996	1,004	0,996	0,996
269	1	1,004	1,004	0,996	0,996	1,004	1,004	0,996	0,996	1,004	0,996	1,004	0,996	0,996	0,996	1,004
271	1	1,004	1,004	1,004	1,004	1,004	1,004	1,004	1,004	0,996	0,996	1,004	1,004	1,004	0,996	1,004
277	1	1,004	1,004	0,996	1,004	1,004	1,004	0,996	0,996	1,004	0,996	1,004	0,996	0,996	1,004	1,004
281	1	1,004	1,004	1,004	1,004	1,004	1,004	1,004	0,996	0,996	0,996	1,004	1,004	1,004	0,996	0,996
283	1	1,004	1,004	0,996	1,004	1,004	1,004	0,996	0,996	1,004	1,004	1,004	0,996	0,996	1,004	1,004
293	1	1,003	1,003	0,997	0,997	0,997	1,003	1,003	1,003	0,997	1,003	1,003	0,997	1,003	0,997	0,997
307	1	1,003	1,003	0,997	1,003	0,997	1,003	1,003	0,997	0,997	1,003	1,003	1,003	0,997	0,997	1,003
311	1	1,003	1,003	1,003	1,003	0,997	1,003	0,997	0,997	0,997	1,003	1,003	0,997	0,997	1,003	0,997
313	1	1,003	1,003	1,003	0,997	0,997	1,003	0,997	0,997	0,997	0,997	1,003	1,003	0,997	0,997	0,997
317	1	1,003	1,003	0,997	1,003	1,003	1,003	0,997	1,003	1,003	1,003	1,003	0,997	1,003	0,997	0,997
331	1	1,003	1,003	0,997	0,997	0,997	1,003	1,003	1,003	0,997	1,003	1,003	1,003	1,003	1,003	0,997
337	1	1,003	1,003	1,003	1,003	0,997	1,003	0,997	1,003	0,997	1,003	1,003	0,997	0,997	0,997	1,003
347	1	1,003	1,003	0,997	0,997	1,003	1,003	0,997	1,003	0,997	1,003	1,003	1,003	1,003	1,003	0,997
349	1	1,003	1,003	0,997	0,997	0,997	1,003	1,003	0,997	1,003	1,003	1,003	0,997	1,003	1,003	1,003
353	1	1,003	1,003	1,003	0,997	1,003	1,003	1,003	1,003	1,003	1,003	1,003	0,997	0,997	1,003	1,003
359	1	1,003	1,003	1,003	0,997	1,003	1,003	1,003	1,003	1,003	1,003	1,003	0,997	0,997	0,997	1,003
367	1	1,003	1,003	1,003	1,003	0,997	1,003	0,997	1,003	1,003	1,003	1,003	1,003	1,003	0,997	1,003
373	1	1,003	1,003	0,997	1,003	0,997	1,003	1,003	0,997	0,997	1,003	1,003	1,003	1,003	1,003	1,003
379	1	1,003	1,003	0,997	0,997	1,003	1,003	0,997	0,997	1,003	1,003	1,003	1,003	0,997	1,003	1,003
383	1	1,003	1,003	1,003	1,003	1,003	1,003	1,003	0,997	1,003	0,997	1,003	1,003	1,003	1,003	0,997
389	1	1,003	1,003	0,997	1,003	0,997	1,003	1,003	0,997	0,997	1,003	1,003	1,003	0,997	0,997	1,003
397	1	1,003	1,003	0,997	0,997	1,003	1,003	0,997	1,003	1,003	0,997	1,003	0,997	1,003	0,997	0,997
Targets		1	7	8	13	16	17	33	40	45	46	49	56	61	64	81
p = 2	$\prod$ normalized factors	8	0	0	8	0	8	8	0	8	0	8	0	8	0	8
p = 3	$\prod$ normalized factors	1,5	1,5	0	1,5	1,5	0	1,5	1,5	1,5	1,5	1,5	0	1,5	1,5	1,5

$p = 5 \text{ à } 397$	$\prod$ normalized factors	4,516	4,516	0,494	0,361	1,349	4,516	0,529	0,787	0,651	1,435	1,807	1,535	1,380	0,563	1,085
Singular series $p = 2 \text{ à } 397$		54,197	0	0	4,330	0	0	6,348	0	7,810	0	21,679	0	16,559	0	13,021
Definition domain																
$2 \leq x \leq 229$ , $2 \leq y \leq 263$ , $2 \leq z \leq 577$	# solutions at c	4	50	1	1	1	50	1	1	5	1	52	2	11	1	6
$2 \leq x \leq 983$ , $2 \leq y \leq 1123$ , $2 \leq z \leq 2381$	# solutions at c	21	166	1	4	1	166	3	1	10	1	172	2	19	1	18
$2 \leq x \leq 3571$ , $2 \leq y \leq 4111$ , $2 \leq z \leq 8501$	# solutions at c	45	500	1	8	1	500	11	1	24	1	520	2	42	1	29
Domain of definition	Ratio															
$2 \leq x \leq 229$ , $2 \leq y \leq 263$ , $2 \leq z \leq 577$	#(c)/sing. series	0,07	$\infty$	$\rightarrow \infty$	0,23	$\rightarrow \infty$	$\infty$	0,16	$\rightarrow \infty$	0,64	$\rightarrow \infty$	2,40	$\rightarrow \infty$	0,66	$\rightarrow \infty$	0,46
$2 \leq x \leq 983$ , $2 \leq y \leq 1123$ , $2 \leq z \leq 2381$	#(c)/sing. series	0,39	$\infty$	$\rightarrow \infty$	0,92	$\rightarrow \infty$	$\infty$	0,47	$\rightarrow \infty$	1,28	$\rightarrow \infty$	7,93	$\rightarrow \infty$	1,15	$\rightarrow \infty$	1,38
$2 \leq x \leq 3571$ , $2 \leq y \leq 4111$ , $2 \leq z \leq 8501$	#(c)/sing. series	0,83	$\infty$	$\rightarrow \infty$	1,85	$\rightarrow \infty$	$\infty$	1,73	$\rightarrow \infty$	3,07	$\rightarrow \infty$	23,99	$\rightarrow \infty$	2,54	$\rightarrow \infty$	2,23

## Appendix 7

### Quadratic reciprocal classes

A “cumbersome” item in the research of abundance factors of quadratic equations is the systematic need of evaluation of squares to check existence or not of residues. It would be interesting for more effectiveness to anticipate this existence property. We will devote ourselves to this point in the next course. Thus, we ask the question

$$\exists ? x \text{ integer} \setminus c = x^2 \bmod p$$

and seek a condition on p

$$p \in G(c) \text{ (or } p \in H(c))$$

equivalent to

$$c \in C(p) \text{ (or } c \in D(p))$$

### Inventory of the classes

We observe the following cases for equation  $c = x^2 \bmod p$  :

Case	G(c)	H(c)
$c = 1$	$1 \bmod 1$	vide
$c = -1$	$1 \bmod 4$	$3 \bmod 4$
$c = 2$	$\{1,7\} \bmod 8$	$\{3,5\} \bmod 8$
$c > 0$ prime $1 \bmod 4$	$U\{g_{4c}^{2i}, 2c+g_{4c}^{2i}\} \bmod 4c$ $\equiv$ $U\{g_{4c}^{2i}\} \bmod c$	$U\{g_{4c}^{2i+1}, 2c+g_{4c}^{2i+1}\} \bmod 4c$ $\equiv$ $U\{g_{4c}^{2i+1}\} \bmod c$
$c > 0$ prime $3 \bmod 4$	$U\{g_{4c}^{2i}\} \bmod 4c$	$U\{2c+g_{4c}^{2i}\} \bmod 4c$
$c > 0$ square	$1 \bmod 1$	void
$c = \alpha.\beta$ $(\alpha,\beta) = 1$	$G(\alpha.\beta) = U(\cap(G(\alpha),G(\beta)), \cap(H(\alpha),H(\beta)))$ $\bmod 4\alpha.\beta$	$H(\alpha.\beta) = U(\cap(G(\alpha),H(\beta)), \cap(H(\alpha),G(\beta)))$ $\bmod 4\alpha.\beta$

When the target is formed of more than two relative prime numbers factors, the last relation is put in the form :

$$G(c) = U(\cap(G_i, \dots, H_j, \dots)) \bmod 4c, \{i \dots, j \dots\} \equiv \{1,2,\dots,t\}, \# \{H_j\} \text{ even}$$

$$H(c) = U(\cap(G_i, \dots, H_j, \dots)) \bmod 4c, \{i \dots, j \dots\} \equiv \{1,2,\dots,t\}, \# \{H_j\} \text{ odd}$$

This writing means that G, respectively H, are the union of the set of the t combinations of classes at the same time of type  $G_i$  and  $H_j$  provided that the number of selected  $H_j$  families is even, respectively odd.

The cases deduced from the decomposition  $c = \alpha.\beta$  with  $\gcd(\alpha,\beta) = 1$  (using in particular  $\beta = -1$ ) are :

Case	G(c)	H(c)
$c < 0$ , prime $1 \bmod 4$	$U\{g_{4c}^{2i}\} \bmod 4c$	$U\{2c+g_{4c}^{2i}\} \bmod 4c$
$c < 0$ , prime $3 \bmod 4$	$U\{g_{4c}^{2i}\} \bmod c$	$U\{g_{4c}^{2i+1}\} \bmod c$
$c = \alpha.f^2$	$G(c/f^2)$	$H(c/f^2)$

The first table calls for several observations concerning the use of the operators of union (U), of intersection ( $\cap$ ) and the term with index  $g_{4c}$ .

The intersection of two families of numbers  $G(\alpha)$  modulo q and  $G(\beta)$  modulo r is obtained as follows. Let us have t the greatest common multiple of q and r. We then express  $G(\alpha)$  and  $G(\beta)$  in an equivalent way modulo t. The intersection is obtained by the choice of the elements common to  $G(\alpha)$  modulo t and  $G(\beta)$  modulo t. The union is carried out on the same model except that all the elements modulo t are taken into account.

The table below illustrates the point.

3	$G(3) = \{1,11\} \bmod 12$ $= \{1,11,13,23,25,35,37,47,49,59\} \bmod 60$	$H(3) = \{5,7\} \bmod 12$ $= \{5,7,17,19,29,31,41,43,53,55\} \bmod 60$
5	$G(5) = \{1,9\} \bmod 10$ $= \{1,9,11,19,21,29,31,39,41,49,51,59\} \bmod 60$	$H(5) = \{3,7\} \bmod 10$ $= \{3,7,13,17,23,27,33,37,43,47,53,57\} \bmod 60$
$\cap$	Part $G(3.5) = \{1,11,49,59\} \bmod 60$	Part $H(3.5) = \{7,17,43,53\} \bmod 60$
U	$G(15) = \{1,7,11,17,43,49,53,59\} \bmod 60$	

Let us explain now the meaning of  $g_{4c}$ . We used until now notation g for a prime number p primitive root. The property of primitive roots is to generate by exponentiation the whole set of non-null classes modulo p (1 to p-1). In the case of  $g_{4c}$ , where c is a prime number, we are interested by a behaviour modulo  $4c$ , namely (c prime number replaced by letter p) the values of  $g_{4p}^i \bmod 4p$ ,  $i = 1$  to  $4p-1$ .

The primitive roots modulo  $4p$  are those which generate p-1 distinct classes including 1 and  $4p-1$ .

## Primitive roots modulo 4p

### Definition

The set of the primitive roots modulo 4p is the set of the primitive roots modulo p carried to 3 modulo 4 by successive additions of p (mod 4p).

### Properties

The set  $\{g_{4p}^i\} \text{ mod } 4p$  is a cyclic group of order p-1.

We have  $g_{4p}^{p-1} = 1 \text{ mod } 4p$ .

If  $p \equiv 1 \text{ mod } 4$  then  $g_{4p}^{(p-1)/2} = -1 + 2p \text{ mod } 4p$ .

If  $p \equiv 3 \text{ mod } 4$  then  $g_{4p}^{(p-1)/2} = -1 \text{ mod } 4p$ .

Only primitive roots modulo 4p have all of these properties.

Let us take example  $p = 31$ .

g	3	11	12	13	17	21	22	24
G+p	34	42	43	44	48	52	53	55
G+2p	65	73	74	75	79	83	84	86
G+3p	96	104	105	106	110	114	115	117

For each preceding numbers  $\{3, 11, 43, 75, 79, 83, 115, 55\}$ , we have well  $g_{4p}^{(p-1)/2} = 4p-1$  (but not for example for  $p = 7$ ) and  $g_{4p}^{p-1} = 1$  when  $p = 31$ .

The even numbers of this table cannot, self-evidently, generate 1 mod 4p.

The numbers  $n = \{65, 73, 105, 13, 17, 21, 53, 117\}$  are such as  $n^{p-1} = 1$ , but  $n^{(p-1)/2} = 2p-1$  (for  $p = 31$ ).

In addition among  $\{1, 3, 5, \dots, 123\}$ , we also find the family  $n = \{7, 19, 51, 59, 71, 103, 107, 111\}$  such as  $n^{p-1} = 1$ , but  $n^{(p-1)/2} = 2p+1$ .

After ascending the numbers, only the family  $\{3, 11, 43, 55, 75, 79, 83, 115\}$  is correct.

By exponentiation, all the generated classes  $g_{4p}^i$ ,  $i = 1$  to  $p-1$  is identical to the preceding one whatever the chosen generator in the family of the primitive roots modulo 4p.

Here with  $g_{4p} = 3$ , we get :

$$\{3, 9, 27, 81, 119, 109, 79, 113, 91, 25, 75, 101, 55, 41, 123, 121, 115, 97, 43, 5, 15, 45, 11, 33, 99, 49, 23, 69, 83, 1\}$$

Let us have in ascending order :

$$G(31) = \{1, 3, 5, 9, 11, 15, 23, 25, 27, 33, 41, 43, 45, 49, 55, 69, 75, 79, 81, 83, 91, 97, 99, 101, 109, 113, 115, 119, 121, 123\}$$

The other classes modulo 4p relative prime (which are always odd) to 4p are :

$$H(31) = \{7, 13, 17, 19, 21, 29, 35, 37, 39, 47, 51, 53, 57, 59, 61, 63, 65, 67, 71, 73, 77, 85, 87, 89, 95, 103, 105, 107, 111, 117\}$$

Foot-note: Concepts of primitive roots are possible modulo  $2^n p$ . For lack of a particular utility here, we do not develop this point here. However, it is useful to say, that for current interest, we must work modulo 4p and not modulo 2p.

## Proofs

### Proof 0

Let us start by demonstrating that :

$$\begin{aligned} U\{g_{4c}^{2i}, 2c+g_{4c}^{2i}\} \text{ mod } 4c &\equiv U\{g_{4c}^{2i}\} \text{ mod } c \\ U\{g_{4c}^{2i+1}, 2c+g_{4c}^{2i+1}\} \text{ mod } 4c &\equiv U\{g_{4c}^{2i+1}\} \text{ mod } c \end{aligned}$$

Self-evidently  $U\{g_{4c}^{2i}, 2c+g_{4c}^{2i}\} \text{ mod } 4c \equiv U\{g_{4c}^{2i}\} \text{ mod } 2c$ . The powers of  $g_{4c}$  are odd numbers since this number is 3 mod 4 and does not generate even numbers. Thus  $U\{g_{4c}^{2i}\} \text{ mod } 2c \equiv U\{g_{4c}^{2i}\} \text{ mod } c$ . The same arguments apply to the second expression.

### Proof 1

Let us have to prove if  $p \equiv 1 \text{ mod } 4$  then  $g_{4p}^{(p-1)/2} = -1 + 2p \text{ mod } 4p$ , otherwise if  $p \equiv 3 \text{ mod } 4$  then  $g_{4p}^{(p-1)/2} = -1 \text{ mod } 4p$ .

We have  $g_{4p}^{p-1} = 1 \text{ mod } 4p$  as well if  $g_{4p} \equiv 1 \text{ mod } 4$  or if  $g_{4p} \equiv 3 \text{ mod } 4$ . Indeed,  $g_{4p} = g + t.p$  where t is an integer between 0 and 3. Thus  $g_{4p} \equiv g \text{ mod } p$ , hence  $g_{4p}^{p-1} = g^{p-1} = 1 \text{ mod } p$  what involves self-evidently  $g_{4p}^{p-1} = 1 \text{ mod } 4p$ .

In addition  $g^{(p-1)/2} = -1 \text{ mod } p$ , hence  $g^{(p-1)/2} = -1 + m.p \text{ mod } p$ , m an integer ranging between 0 and 3.

Let us calculate  $g_{4p}^{(p-1)/2} = (3+4u)^{(p-1)/2} = (-1)^{(p-1)/2} + 4n = (g+t.p)^{(p-1)/2} = g^{(p-1)/2} + k.p = -1 + (k+m).p \text{ mod } 4p$

Then if  $(p-1)/2$  is odd,  $(k+m).p = -4n + r.4p = 4q$ , then  $k+m$  is multiple of 4, hence  $g_{4p}^{(p-1)/2} = -1 \text{ mod } 4p$ . If  $(p-1)/2$  is even,  $1+4n = -1 + (k+m).p + r.4p$ , hence  $2 = (k+m).p + 4q$ . Only  $k+m = 2 \text{ mod } 4$  is a solution of this equation. Hence  $g_{4p}^{(p-1)/2} = -1 + 2p \text{ mod } 4p$ .

Then, let us show that  $\{g_{4p}^i\} \bmod 4p$  is cyclic of order  $p-1$  exactly.

We have  $g_{4p}^i = (3+4u)^i = (-1)^i + 4n = (g+t.p)^i = g^i + k.p \bmod 4p$  and  $g^i \neq 1 + m.p \bmod 4p$  if  $0 < i < p-1$  for any  $m$ .

Hence  $g_{4p}^i \neq 1 + (m+k).p \bmod 4p$  if  $0 < i < p-1$ . If at this time  $g_{4p}^i = 1 \bmod 4p$ , that involves  $0 \neq (m+k).p \bmod 4p$ , so that  $m+k \neq 0 \bmod 4$  for any  $m$  what is false. Hence  $g_{4p}^i \neq 1 \bmod 4p$  for any  $i$ ,  $0 < i < p-1$ . As  $g_{4p}^{p-1} = 1 \bmod 4p$ ,  $\{g_{4p}^i\} \bmod 4p$  is cyclic of order  $p-1$  exactly.

## Proof 2

We like to answer the question of existence (or not) of a solution to equation  $x^2 = c \bmod p$  pending on the value of  $c$ .

The case  $c = 1$  is self-evident since  $x = 1$  is always solution, therefore any number  $p$  is appropriate for given  $c$ .

The case  $c = -1$  is written  $x^2 = -1 = g^{(p-1)/2} \bmod p$  which has a solution if  $(p-1)/2$  is square, hence  $p = 1 \bmod 4$ .

The case  $c = 2$  results from Legendre relation  $(2/p) = (-1)^{(p^2-1)/8} \bmod p$ . If  $p = 1 \bmod 8$  or  $p = 7 \bmod 8$  then  $(2/p) = 1 \bmod p$  (existence of a residue), if not if  $p = 3 \bmod 8$  or  $p = 5 \bmod 8$  then  $(2/p) = -1 \bmod p$  (non-existence of a residue).

If  $c$  is an odd prime number, we consider two cases. We check the solutions proposed in the table and we show that there are no others what suffice here. We use for that Legendre notation and the law of quadratic reciprocity where  $c$  and  $p$  are relative primes :

$$\left(\frac{c}{p}\right) = \left(\frac{p}{c}\right)(-1)^{\frac{(c-1)}{2} \cdot \frac{(p-1)}{2}} \bmod p$$

We have the equivalences :

$$p \in G(c) \Leftrightarrow \left(\frac{c}{p}\right) = 1 \bmod p$$

$$p \in H(c) \Leftrightarrow \left(\frac{c}{p}\right) = -1 \bmod p$$

Then, if  $c = 1 \bmod 4$  and if  $G(c) \equiv \{g_{4c}^{2i}, 2c + g_{4c}^{2i}\} \bmod 4c$ , we may write :

$$\left(\frac{c}{p}\right) = \left(\frac{c}{g_{4c}^{2i} + k \cdot 4c}\right) = (-1)^{\frac{(c-1)}{2} \cdot \frac{(g_{4c}^{2i} + k \cdot 4c - 1)}{2}} \cdot \left(\frac{g_{4c}^{2i} + k \cdot 4c}{c}\right) = (-1)^{(0+2n) \cdot t} \left(\frac{g_{4c}^{2i}}{c}\right) = 1 \bmod p$$

Here, as  $(c-1)/2$  is  $0 \bmod 2$ , it does not matter if  $(g_{4c}^{2i}-1)/2$  is even or odd.

In the same way :

$$\left(\frac{c}{p}\right) = \left(\frac{c}{g_{4c}^{2i} + 2c + k \cdot 4c}\right) = (-1)^{\frac{(c-1)}{2} \cdot \frac{(g_{4c}^{2i} + 2c + k \cdot 4c - 1)}{2}} \cdot \left(\frac{g_{4c}^{2i} + 2c + k \cdot 4c}{c}\right) = (-1)^{(0+2n) \cdot (t+c)} \left(\frac{g_{4c}^{2i}}{c}\right) = 1 \bmod p$$

Then, if  $c = 1 \bmod 4$  and if  $H(c) \equiv \{g_{4c}^{2i+1}, 2c + g_{4c}^{2i+1}\} \bmod 4c$ , we may write :

$$\left(\frac{c}{p}\right) = \left(\frac{c}{g_{4c}^{2i+1} + k \cdot 4c}\right) = (-1)^{\frac{(c-1)}{2} \cdot \frac{(g_{4c}^{2i+1} + k \cdot 4c - 1)}{2}} \cdot \left(\frac{g_{4c}^{2i+1} + k \cdot 4c}{c}\right) = (-1)^{(0+2n) \cdot t'} \left(\frac{g_{4c}}{c}\right) = -1 \bmod p$$

This time, in addition to preceding remarks, we use the primitive roots fundamental property :

$$\left(\frac{g}{p}\right) = -1 \bmod p$$

As  $g_{4c} = g + t \cdot c$ ,  $t$  an integer, it follows :

$$\left(\frac{g_{4c} + t \cdot c}{c}\right) = \left(\frac{g_{4c}}{c}\right) = -1$$

In the same way :

$$\left(\frac{c}{p}\right) = \left(\frac{c}{g_{4c}^{2i+1} + 2c + k \cdot 4c}\right) = (-1)^{\frac{(c-1)}{2} \cdot \frac{(g_{4c}^{2i+1} + 2c + k \cdot 4c - 1)}{2}} \cdot \left(\frac{g_{4c}^{2i+1} + 2c + k \cdot 4c}{c}\right) = (-1)^{(0+2n) \cdot (t'+c)} \left(\frac{g_{4c}}{c}\right) = -1 \bmod p$$

Let us examine now  $c = 3 \bmod 4$ .

If  $G(c) \equiv \{g_{4c}^i\} \bmod 4c$ , we may write :

$$\left(\frac{c}{p}\right) = \left(\frac{c}{g_{4c}^i + k \cdot 4c}\right) = (-1)^{\frac{(c-1)}{2} \cdot \frac{(g_{4c}^i + k \cdot 4c - 1)}{2}} \cdot \left(\frac{g_{4c}^i + k \cdot 4c}{c}\right) = (-1)^{(1+2n) \cdot (g_{4c}^i - 1)/2} \left(\frac{g_{4c}^i}{c}\right) = 1 \bmod p$$

Indeed, the parity of the product  $(1+2n).(g_{4c}^i-1)/2$  depends only on the parity of  $(g_{4c}^i-1)/2$ . The primitive  $g_{4c}$  is 3 mod 4 by definition. Thus, if  $i$  is odd,  $(g_{4c}^i-1)/2$  is odd and Legendre symbol  $(g_{4c}^i/c)$  is worth -1. Otherwise, if  $i$  is even,  $(g_{4c}^i-1)/2$  is even, while the Legendre symbol  $(g_{4c}^i/c)$  is worth 1. Hence the preceding result.

If  $H(c) \equiv \{2c+g_{4c}^i\} \bmod 4c$ , we can write:

$$\left(\frac{c}{p}\right) = \left(\frac{c}{g_{4c}^i+2c+k.4c}\right) = (-1)^{\frac{(c-1) \cdot (g_{4c}^i+2c+k.4c-1)}{2}} \cdot \left(\frac{g_{4c}^i+2c+k.4c}{c}\right) = (-1)^{(1+2n).(c+(g_{4c}^i-1)/2)} \left(\frac{g_{4c}^i}{c}\right) = -1 \bmod p$$

Indeed, compared to the expression interesting  $G(c)$ , the last expression presents a multiplication by  $(-1)^{(1+2n).c}$  where  $c$  is 3 mod 4, that is by  $(-1)^{(1+2n).c} = -1$ . Hence the result.

Having checked the inclusion of the candidate families respectively in  $G(c)$  and  $H(c)$ , it remains us to prove that there are no other solutions. Let us consider the case  $c = 3 \bmod 4$  (where  $c$  is a prime number) and the set  $\{g_{4c}^i\} \bmod 4c$ . Let us have  $x = g_{4c}^i \bmod 4c$  and  $y = g_{4c}^j \bmod 4c$ . If  $x = y$ , then  $g_{4c}^i = g_{4c}^j \bmod 4c$ , then  $g_{4c}^{i-j} = 1 \bmod 4c$ . There is  $t$  an integer such as  $g_{4c} = g+t.c$ . Thus  $(g+t.c)^{i-j} = g^{i-j} + m.c = 1 \bmod 4c$ ,  $m$  an integer. Hence  $g^{i-j} = 1 \bmod c$ . Hence  $i = j \bmod p-1$ . The set  $\{g_{4c}^i\} \bmod 4c$  thus has  $c-1$  distinct elements. In the same way  $\{2c+g_{4c}^i\} \bmod 4c$  has  $c-1$  distinct elements.  $U\{G(c), H(c)\}$  gathering all the classes relative prime with  $4c$ , that is  $\phi(4c) = \phi(4)\phi(c) = 2(c-1)$ , there are no other solutions. In the case of  $c = 1 \bmod 4$ , we can use the same arguments without new difficulties.

If  $c$  contains a square, let us have  $\alpha.\beta^2$  its decomposition into non-square and square. The equation becomes  $x^2 = \alpha.\beta^2 \bmod p$ . Existence of a solution with this equation rests self-evidently on existence of a solution, pending on  $p$ , for equation  $(x/\beta)^2 = \alpha \bmod p$  knowing that a reverse always exists mod  $p$  (if the number is non-null), the equation transforms into  $y^2 = \alpha \bmod p$  what proves the previous suggested simplification.

If  $c$  is positive and is the product of two relative primes factors,  $c = \alpha.\beta$ . Then, we study equation  $x^2 = \alpha.\beta \bmod p$  seeking set  $G(\alpha.\beta) = \{p\}$  with residue  $c$ . We suppose equation  $x^2 = \alpha \bmod p$  solved, that is set  $G(\alpha) \bmod 4\alpha$  for existence and set  $H(\alpha) \bmod 4\alpha$  for non-existence of a residue. In the same way, for  $x^2 = \beta \bmod p$ , we have sets  $G(\beta) \bmod 4\beta$  and  $H(\beta) \bmod 4\beta$ . Let us have  $p$  a prime number. If there is  $x$  such as  $x^2 = \alpha \bmod p$ , i.e. if  $\alpha$  is a square modulo  $p$ , and if, for any  $x$ , we have  $x^2 \neq \beta \bmod p$ , i.e.  $\beta$  is not a square modulo  $p$  then clearly  $\alpha\beta$  is not a square modulo  $p$  and, for any  $x$ ,  $x^2 \neq \alpha\beta \bmod p$  (this can be shown rigorously by using the primitive roots of  $p$ ). The reasoning is the same one when permuting  $\alpha$  and  $\beta$ . In addition, self-evidently, if  $\alpha$  and  $\beta$  are squares modulo  $p$ , the product  $\alpha\beta$  is a square modulo  $p$ . If  $\alpha$  and  $\beta$  are non-squares modulo  $p$ , then there is a primitive root  $g$  of  $p$  and an integer  $i$  such as  $\alpha = g^{2i} \bmod p$  and a primitive root  $g'$  of  $p$  and an integer  $j$  such as  $\beta = g'^{2j} \bmod p$ . We express then  $g'$  according to  $g$  by  $g' = g^k \bmod p$ . A primitive root is expressed according to another with  $k$  relative prime with  $p-1$ , therefore  $k$  odd. It follows  $\beta = g^k.g^{2j.k} = g^{2m} \bmod p$ . Thus  $\alpha.\beta = g^{2(1+i+m)} \bmod p$  is a square modulo  $p$ . This argument is summarized according to the table :

$\exists x \setminus x^2 = \alpha.\beta \bmod p \Leftrightarrow$	$\{\exists x \setminus x^2 = \alpha \bmod p \text{ and } \exists x \setminus x^2 = \beta \bmod p\}$
	or $\{\forall x, x^2 \neq \alpha \bmod p \text{ and } \forall x, x^2 \neq \beta \bmod p\}$
$\forall x, x^2 \neq \alpha.\beta \bmod p \Leftrightarrow$	$\{\exists x \setminus x^2 = \alpha \bmod p \text{ and } \forall x, x^2 \neq \beta \bmod p\}$
	or $\{\forall x, x^2 \neq \alpha \bmod p \text{ and } \exists x \setminus x^2 = \beta \bmod p\}$

As  $\exists x \setminus x^2 = \alpha \bmod p$  is equivalent to  $p \in G(\alpha)$  and  $\forall x, x^2 \neq \alpha \bmod p$  is equivalent to  $p \in H(\alpha)$ , it follows immediately with our rules for intersections and unions :

$$G(\alpha.\beta) = U(\cap(G(\alpha), G(\beta)), \cap(H(\alpha), H(\beta)))$$

$$H(\alpha.\beta) = U(\cap(G(\alpha), H(\beta)), \cap(H(\alpha), G(\beta)))$$

In addition, these rules come from modulo  $4\alpha$  and modulo  $4\beta$  results for prime  $\alpha$  and  $\beta$  numbers, results which are naturally prolonged modulo  $4\alpha\beta$  to order  $\alpha\beta$ .

For any  $c$ , we withdraw the set of the square factors and get a decomposition in factors  $c' = \pm \prod f_i$ . We apply the routines to the various factors of this number. It does not matter, except possibly for the size of calculations, the order and the signs used (provided that the product corresponds well to  $c$ ).

Let us approach the passage of  $c$  with  $-c$  when  $c$  is a prime number. We use  $G(-c) = U(\cap(G(c), G(-1)), \cap(H(c), H(-1))) \bmod 4c$  and  $H(-c) = U(\cap(G(c), H(-1)), \cap(H(c), G(-1))) \bmod 4c$ . The table for these cases is easily written recalling that  $g_{4c} = 3 \bmod 4$  :

	$G(c)$	$H(c)$
$c > 0$ prime 1 mod 4	$U\{g_{4c}^{2i} \bmod 4c, 2c+g_{4c}^{2i} \bmod 4c\}$ $e$ $U\{1 \bmod 4, 3 \bmod 4\}$	$U\{g_{4c}^{2i+1} \bmod 4c, 2c+g_{4c}^{2i+1} \bmod 4c\}$ $e$ $U\{3 \bmod 4, 1 \bmod 4\}$
$c > 0$ prime 3 mod 4	$U\{g_{4c}^{2i} \bmod 4c, g_{4c}^{2i+1} \bmod 4c\}$ $e$ $U\{1 \bmod 4, 3 \bmod 4\}$	$U\{2c+g_{4c}^{2i} \bmod 4c, 2c+g_{4c}^{2i+1} \bmod 4c\}$ $e$ $U\{3 \bmod 4, 1 \bmod 4\}$

Then :

$$\begin{aligned} G(-c \text{ (} c \equiv 1 \pmod{4} \text{)}) &= U\{g_{4c}^{2i}, g_{4c}^{2i+1}\} = U\{g_{4c}^i\} \pmod{4c} \\ H(-c \text{ (} c \equiv 1 \pmod{4} \text{)}) &= U\{2c+g_{4c}^{2i}, 2c+g_{4c}^{2i+1}\} = U\{2c+g_{4c}^i\} \pmod{4c} \\ G(-c \text{ (} c \equiv 3 \pmod{4} \text{)}) &= U\{g_{4c}^{2i}, 2c+g_{4c}^{2i}\} \pmod{4c} \\ H(-c \text{ (} c \equiv 3 \pmod{4} \text{)}) &= U\{g_{4c}^{2i+1}, 2c+g_{4c}^{2i+1}\} \pmod{4c} \end{aligned}$$

What shows our matter completely.

### Examples of evaluation

We illustrate our study for the following examples.

For  $c = 3$ , prime number we have only one primitive root modulo 3 which is  $g = 2$ . We reason then modulo 12 ( $4c = 12$ ). Then  $g_{4c} = 2+3p = 11$  is worth  $3 \pmod{4}$ , then  $G(c) = \{11^0, 11^1\} = \{1, 11\} \pmod{12}$ . The other relative primes to 12 are then  $H(c) = \{5, 7\} \pmod{12}$ .

For  $c = -3$ , two possibilities arise. Either the direct reading of the table where  $G(-3) = U\{g_{12}^{2i} \pmod{12}, 6+g_{12}^{2i} \pmod{12}\} = \{1, 7\} \pmod{12}$ , or to consider product  $3.(-1)$ .

Hence :

For  $G(-3)$

3	$G(3) = \{1, 11\} \pmod{12}$	$H(3) = \{5, 7\} \pmod{12}$
-1	$G(-1) = \{1\} \pmod{4} = \{1, 5, 9\} \pmod{12}$	$H(-1) = \{3\} \pmod{4} = \{3, 7, 11\} \pmod{12}$
$\cap$	Part $G(-3) = \{1\} \pmod{12}$	Part $G(-3) = \{7\} \pmod{12}$
U	$G(-3) = \{1, 7\} \pmod{12}$	

For  $H(-3)$

3	$G(3) = \{1, 11\} \pmod{12}$	$H(3) = \{5, 7\} \pmod{12}$
-1	$H(-1) = \{3\} \pmod{4} = \{3, 7, 11\} \pmod{12}$	$G(-1) = \{1\} \pmod{4} = \{1, 5, 9\} \pmod{12}$
$\cap$	Part $H(-3) = \{11\} \pmod{12}$	Part $H(-3) = \{5\} \pmod{12}$
U	$H(-3) = \{5, 11\} \pmod{12}$	

We can form in the same way  $G(5) = \{1, 9, 11, 19\} \pmod{20} = \{1, 9\} \pmod{10}$  and  $G(-5) = \{3, 7, 13, 17\} \pmod{20} = \{3, 7\} \pmod{10}$ . We can then evaluate  $G(15)$  and  $H(15)$ , either by considering that  $15 = 3.5$  or that  $15 = (-3).(-5)$ .

Let us adopt this last way.

For  $G(15)$

-3	$G(-3) = \{1, 7\} \pmod{12}$ $= \{1, 7, 13, 19, 25, 31, 37, 43, 49, 55\} \pmod{60}$	$H(-3) = \{5, 11\} \pmod{12}$ $= \{5, 11, 17, 23, 29, 35, 41, 47, 53, 59\} \pmod{60}$
-5	$G(-5) = \{1, 3, 7, 9\} \pmod{20}$ $= \{1, 3, 7, 9, 21, 23, 27, 29, 41, 43, 47, 49\} \pmod{60}$	$H(-5) = \{11, 13, 17, 19\} \pmod{20}$ $= \{11, 13, 17, 19, 31, 33, 37, 39, 51, 53, 57, 59\} \pmod{60}$
$\cap$	Part $G(-3, -5) = \{1, 7, 43, 49\} \pmod{60}$	Part $G(-3, -5) = \{11, 17, 53, 59\} \pmod{60}$
U	$G(15) = \{1, 7, 11, 17, 43, 49, 53, 59\} \pmod{60}$	

For  $H(15)$

-3	$G(-3) = \{1, 7, 13, 19, 25, 31, 37, 43, 49, 55\} \pmod{60}$	$H(-3) = \{5, 11, 17, 23, 29, 35, 41, 47, 53, 59\} \pmod{60}$
-5	$H(-5) = \{11, 13, 17, 19, 31, 33, 37, 39, 51, 53, 57, 59\} \pmod{60}$	$G(-5) = \{1, 3, 7, 9, 21, 23, 27, 29, 41, 43, 47, 49\} \pmod{60}$
$\cap$	Part $H(-3, -5) = \{13, 19, 31, 37\} \pmod{60}$	Part $H(-3, -5) = \{23, 29, 41, 47\} \pmod{60}$
U	$H(15) = \{13, 19, 23, 29, 31, 37, 41, 47\} \pmod{60}$	

The set  $G(15) \cup H(15)$  contains well the set of relative prime numbers to 15. The reader will be able to verify that we get the same families by using such other decompositions of  $c = 15$  :  $15 = 3.5 = -1.3.(-5) \dots$

If we continue then with the case  $c = 105 = 3.5.7$ , we proceed at the stage  $c = (3.5).7$  knowing that 3.5 and 7 are relative prime numbers, that is using the general formula of intersections and unions :

$$\begin{aligned} G(105) &= U(G(3) \cap G(5) \cap G(7), G(3) \cap H(5) \cap H(7), H(3) \cap G(5) \cap H(7), H(3) \cap H(5) \cap G(7)) \pmod{420} \\ H(105) &= U(G(3) \cap G(5) \cap H(7), G(3) \cap H(5) \cap G(7), H(3) \cap G(5) \cap G(7), H(3) \cap H(5) \cap H(7)) \pmod{420} \end{aligned}$$

## Appendix 8

The following table gives to the number of solutions of equation  $P(x) = c \pmod{p^2}$  with  $P(x) = x^4 + 3x^3 + 4x^2 + 7x$  by varying  $x$  from 0 to  $p^2 - 1$  and adequate. The non-integer ratios  $\#(i)/p$  correspond to contributions of supernumerary cardinals. We define also  $\#(T) = \#(1) + \#(2) + \#(4)$

p	#(1)	#(2)	#(4)		6.#(1)/#(T)	6.#(2)/#(T)	6.#(4) /#(T)
3	3	6	0		2,00	4,00	0,00
5	0	0	20		0,00	0,00	6,00
7	0	26	0		0,00	6,00	0,00
11	44	42	0		3,07	2,93	0,00
13	52	104	0		2,00	4,00	0,00
17	85	136	68		1,76	2,82	1,41
19	114	226	0		2,01	3,99	0,00
23	115	322	92		1,30	3,65	1,04
29	319	522	0		2,28	3,72	0,00
31	279	682	0		1,74	4,26	0,00
37	555	370	444		2,43	1,62	1,95
41	615	902	164		2,20	3,22	0,59
43	774	516	516		2,57	1,71	1,71
47	846	1128	188		2,35	3,13	0,52
53	1166	742	848		2,54	1,62	1,85
59	885	2360	236		1,53	4,07	0,41
61	1525	1708	488		2,46	2,75	0,79
67	1340	2546	536		1,82	3,45	0,73
71	1704	2698	568		2,06	3,26	0,69
73	1898	2774	584		2,17	3,17	0,67
79	2528	2368	1264		2,46	2,31	1,23
83	2406	3318	996		2,15	2,96	0,89
89	2492	3558	1780		1,91	2,73	1,36
97	3104	4266	1940		2,00	2,75	1,25
101	3434	4644	2020		2,04	2,76	1,20
103	3090	5768	1648		1,76	3,29	0,94
107	4494	4280	2568		2,38	2,26	1,36
109	3597	5668	2616		1,82	2,86	1,32
113	4972	4744	2712		2,40	2,29	1,31
127	5461	7112	3556		2,03	2,65	1,32
131	6419	8646	2096		2,24	3,02	0,73
137	6576	7670	4384		2,12	2,47	1,41
139	6116	8618	4448		1,91	2,70	1,39
149	7450	10430	4172		2,03	2,84	1,14
151	7701	12684	2416		2,03	3,34	0,64
157	8792	11302	4396		2,15	2,77	1,08
163	8476	12712	5216		1,93	2,89	1,19
167	10020	14024	3340		2,20	3,07	0,73
173	9861	14532	5536		1,98	2,91	1,11
179	11098	16466	4296		2,09	3,10	0,81
181	11946	14840	5792		2,20	2,73	1,07
191	12797	16044	7640		2,10	2,64	1,26
193	13896	17368	5404		2,27	2,84	0,88
197	12017	21276	5516		1,86	3,29	0,85
199	12935	21890	4776		1,96	3,32	0,72
211	14770	20256	9284		2,00	2,74	1,26
223	14718	29434	5352		1,78	3,57	0,65
227	15663	26786	9080		1,82	3,12	1,06
229	19465	21984	10992		2,23	2,52	1,26
233	17708	28890	7456		1,97	3,21	0,83
239	21032	25332	10516		2,22	2,67	1,11
				$\Sigma$			
Total	297353	424720	147960	870033			
Men value					2,0062	2,9802	1,0136
Ratio	2,051	2,929	1,020	6			
At infinity awaited value	2	3	1	6	2	3	1
Difference	2,53%	-2,37%	2,04%		0,31%	-0,66%	1,36%

We have the same trend towards an equiprobability with proportions (2,3,1) that for equation  $x^4 + x^3 + x^2 + x$  that we have seen above in the body of text.

## REFERENCES

- [1] Jacques Hadamard. Charles-Jean De la Vallée Poussin. (1896)
- [2] Nikolai Chebotarev. Thèse. 1922.
- [3] H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. TeilI. Jahrsbericht d. DMV 35 (1926).
- [4] Emmanuel Peyre. Principe de Hasse. [http ://www-fourier.ujf-grenoble.fr/~peyre/articles](http://www-fourier.ujf-grenoble.fr/~peyre/articles)
- [5] Samir Siksek and Alexei Skorobogatov. On a Shimura curve that is a counterexample to the Hasse principle. Mathematics subject classification (2000): 11G18, 11G05, 11G30.
- [6] David Hariri. Principe local - global en arithmétique. SMF Gazette 107. Janvier 2006.
- [7] A counterexample to a conjecture of Selmer. Tom Fisher. 6 November 2002.
- [8] Class field theory. J.S. Milne. Version 4.00 March 2/ 2008
- [9] J. W. S. Cassels, Rational quadratic forms, London Mathematical Society Monographs, vol. 13 (Academic Press, London, 1978)
- [10] Jean-Louis Colliot-Thélène and Fei Xu. Brauer-Manin obstruction for integral points of homogeneous spaces and representation by integral quadratic forms. Compositio Math. 145 (2009), 309-363
- [11] Carmen Laura Basile and Alexei Skorobogatov. On the Hasse principle for bielliptic surfaces.
- [12] Melvyn B. Nathanson. Additive Number Theory. Springer.
- [13] M. Borovoi, On representations of integers by indefinite ternary quadratic forms, J. Number Theory 90 (2001), 281{293.
- [14] E. S. Selmer. The Diophantine equation  $ax^3+by^3+cz^3=0$ . Acta Math. 85:203-362 (1 plate), 1951.
- [15] Jean Pierre Serre. Cours d'arithmétique. Presses universitaires de France. Le Mathématicien.
- [16] Source Wikipédia. L'encyclopédie libre.