Asymptotic diophantian counting. Hypervolumes method. Summarized version.

Hubert Schaetzel

Abstract We develop a method to get enumeration of diophantine equations asymptotic solutions that we call hypervolumes method by analogy to the famous Hardy-Littlewood circle method. The estimates are based on integral calculus of volumes associated with a corrective evaluation on the surface of the volumes with an "asymptotic sieve". Matrices with remarkable properties are produced, which are an essential contribution of our study. Their usefulness is obvious with recurring terms like Waring sums without limitation to these cases.

Dénombrements asymptotiques d'équations diophantines.
Méthode des hypervolumes. Version courte.

Résumé Nous développons une méthode de dénombrement des solutions d'équations diophantines à branches asymptotiques dite des hypervolumes par analogie à la célèbre méthode du cercle de Hardy-Littlewood. Elle repose sur le calcul de volumes par intégrations multiples associé à des corrections en surface des volumes par un « crible asymptotique ». Les matrices mises en œuvre pour le calcul de ces corrections ont des propriétés remarquables et sont une contribution essentielle de notre étude. Leur utilité est manifeste en abordant aussi bien des équations à termes récurrents, telles les sommes de Waring, que d'autres à termes non récurrents.

Statut Preprint
Date Version V1 : April 24/2010
Version V5 : October 29/2017

Summary

1. Preamble

Let us have a diophantine equation whose number of solutions diverges :

$$R(x_i, y_j, z_k\ldots) = c \qquad (1)$$

The number c is here a constant factor that we call the target and x_i, y_j, z_k… are variables, describing either all natural integer numbers (incidentally all relative numbers), or prime numbers (incidentally of the two signs). We seek the number of n-uplets (x_i, y_j, z_k…) in the form of a mathematical formula. Usually (formulas of De Polignac, of Vinogradov, of Hardy - Littlewood, ...), this type of formulas resembles a product involving the previous variables with assigned integer or fractional exponents, the logarithms of these same variables with appropriate exponents and a constant based on an Euler infinite product [2]. Specifically, to solve (and therefore enumerate) $R(x_i, y_j, z_k\ldots) = c$ is equivalent to solve (and therefore enumerate) :

$$R(x_i, y_j, z_k\ldots) = c \bmod 2^{k2}.3^{k3}\ldots p_i^{ki}\ldots \qquad (2)$$

Here, p_i describes the set of prime numbers, and the k_i tend towards infinity.
We will note in this text the number of solutions by the cardinal sign :

$$\#(x_i, y_j, z_k\ldots) \qquad (3)$$

From the chinese theorem, it follows immediately :

$$\#\{(x, y, z \ldots) / R(x, y, z\ldots) = c \text{ modulo } 2^{i2}.3^{i3} \ldots p_k^{ik}\} = \prod_{m=2 \text{ to } k} \#\{(x, y, z\ldots) / R(x, y, z\ldots) = c \text{ modulo } p_m^{im}\} \qquad (4)$$

This relationship is the basis of what follows. To use it, we will specify how to pass from #{(x, y, z…) / R(x, y, z…) = c modulo p} to #{(x, y, z…) / R(x, y, z…) = c modulo p^δ}. Then we make tend δ towards infinity <u>if necessary</u>. Meanwhile, we will ensure normalizing (the meaning of the word is given underneath) of the expressions.
In practice, it suffices to form multidimensional arrays whose axis are the values of x, y, z... respectively and collect the number of occurrences of given c according to the R(x, y, z…) = c mod p^δ formula. For given c, the collected number is called the (non-normalized) abundance factor at step p. At c, the enumeration from m = 2 to k is proportional to the product of these factors and the searched proportions are obtained when k tends towards infinity.
Subsequently, we will call p the sequence and g will appoint one (among other) primitive root of the prime number p.

2. Asymptotic representatives

Asymptotic representatives are the axis of the above mentioned multidimensional arrays. The asymptotic representative of the variable z is written simply {{z}}. This is an equivalent of z, in the asymptotic enumeration framework, obtained by enumerating all relevant modulo classes of x, y.... If the variable is a variable concerning integers, the modulo p^δ representative is trivially the series of integers 0, 1, 2,..., p^δ-1 (with a weighting of 1 for each of these numbers). When the variable represents the prime numbers, the equivalent is more difficult to clarify. Thus, let us have the table :

p \ y_j	0	1	2	3	4	5	6	7	8	9	10	11	…	∞
2	ε_0	1-ε_1	ε	1	ε^2	1	ε	1	ε^3	1	ε	1	…	…
3	ε_0	1-ε_1	1	ε	1	1	ε	1	1	ε^2	1	1	…	…
5	ε_0	1-ε_1	1	1	1	ε	1	1	1	1	ε	1	…	…
7	ε_0	1-ε_1	1	1	1	1	1	ε	1	1	1	1	…	…
11	ε_0	1-ε_1	1	1	1	1	1	1	1	1	1	ε	…	…
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
p	ε_0	1-ε_1	1	1	1	1	1	1	1	1	1	1	…	…
Π	ε_0^t	$(1-\varepsilon_1)^t$	ε	ε	ε^2	ε	ε^2	ε	ε^3	ε^2	ε^2	ε	…	…
Π/ε	$\varepsilon_0^t/\varepsilon$	$(1-\varepsilon_1)^t/\varepsilon$	1	1	ε	1	ε	1	ε^2	ε	ε	1	…	…

We can choose ε_0, ε_1, ε as infinitesimals such as ε, $\varepsilon_0^t/\varepsilon$, $(1-\varepsilon_1)^t/\varepsilon$ simultaneously tend to 0. So we actually find all of the searched prime numbers (weighting 1 for prime numbers and 0 otherwise). Hence, the asymptotic representatives table, φ being the Euler function :

Variable of integers	$\{\{x\}\}_{p\wedge\delta} = [0,1,2,\ldots,p^\delta-1]$
Variable of prime numbers	$\{\{y\}\}_{p\wedge\delta} = [g^0,g^1,g^2,\ldots,g^{\varphi(p\wedge\delta)-1}]$

The use of a primitive root allows, in a very simple way, to push aside the multiples of p which is necessary to forge the representative of a variable of prime numbers at the sequence p.
Then, more simply modulo p, the asymptotic representative is written as :

Variable of integers	$\{\{x\}\}_p = [0,1,2,\ldots,p-1]$
Variable of prime numbers	$\{\{y\}\}_p = [1,2,\ldots,p-1]$

An alternative entry is to also represent weights :

$\{\{x\}\}_p \equiv$

0	1	2	…	p-1
1	1	1	…	1

$\{\{y\}\}_p \equiv$

1	2	3	…	p-1
1	1	1	…	1

These weightings are going to grow with the introduction of a new variable by crossing with the old ones. The way to avoid this increase of the weightings is to give a global unit weight to additional representatives (two or more variables). Thus :

$\{\{x_i^*\}\}_p \equiv$

0	1	2	…	p-1
1/p	1/p	1/p	1/p	1/p

(so that $\sum = 1$)

$\{\{y_i^*\}\}_p \equiv$

1	2	3	…	p-1
1/(p-1)	1/(p-1)	1/(p-1)	1/(p-1)	1/(p-1)

(so that $\sum = 1$)

This operation, called normalization, extends without difficulty modulo p^δ.

- for a variable of integers, obtained cardinal must be divided by p^δ at sequence p
- for a variable of prime numbers, obtained cardinal must be divided by $p^{\delta-1}(p-1)$ at sequence p

These ratios apply for each variable input : k variables of integers → ratio $1/(p^\delta)^k$, m variables of prime numbers → ratio $1/(p^\delta.(p-1))^m$. To restore the sum to p_i^δ, it is necessary and sufficient to carry out a final multiplication of the ratios by p^δ
Hence the rules :

k variables of integers	→	ratio $1/(p^\delta)^{(k-1)}$
m variables of prime numbers	→	ratio $p^\delta/((p^{\delta-1}(p-1))^m)$
k variables of integers and m variables of prime numbers	→	ratio $1/(p^\delta)^{(k-1)}/((p^{\delta-1}(p-1))^m)$

In these conditions, the average weighting of all the targets c in the interval $]-\infty,+\infty[$ is equal to 1. This remains so if one chooses an interval $]-\infty,a]$ or $[a,+\infty[$. We get then the normalized abundance factor of target c using these ratios :

$$fan(c,p) = \#(c).r \qquad (5)$$

and

$$fan(c) = \prod_{p=2 \text{ to } +\infty} fan(c,p) \qquad (6)$$

The establishment of these factors are thus based on arithmetic considerations with a passage to the limit (required within asymptotic census and compatible with it at the same time). The use of this method gives immediately asymptotic proportions between different targets.

3. Monomial study

The monomials x^n are the elementary bricks of a diophantine equation. Their asymptotic behaviour supports all the rest. The equation $x^n = c$, for finite given c, is not an equation with asymptotic character, but we can extract results of it that fully serve when new variables and operations are added to this basic structure.

3.1. Solutions of the modulo p^δ equation

Case p odd

Let us have $x^n = c \bmod p^\delta$, p an odd prime number. Let us have $d_i = (n,\Phi(\delta\text{-}i))$ where $\Phi(\delta\text{-}i) = p^{\delta-i-1}.(p-1)$ and $\delta n = int((\delta-1)/n)$ the integer part of $(\delta-1)/n$. We can draw the following table :

row	x	$x^n = c \bmod p^\delta$	#{c}
δn+1	0 $p^{\delta-1}.\{g^0, g^1, \dots, g^{\Phi(1)-1}\}$ $p^{\delta-2}.\{g^0, g^1, \dots, g^{\Phi(2)-1}\}$ … $p^{\delta n+1}.\{g^0, g^1, \dots, g^{\Phi(\delta-(\delta n+1))-1}\}$	0	$p^{\delta-\delta n-1}$
δn	$p^{\delta n}.\{g^0, g^1, \dots, g^{\Phi(\delta-\delta n)-1}\}$	$p^{\delta n.n}.\{g^{0.d[\delta n.n]}, g^{1.d[\delta n.n]}, \dots, g^{(\Phi(\delta-\delta n.n)/d[\delta n.n]-1).d[\delta n.n]}\}$	$d_{\delta n.n}.p^{\delta n.(n-1)}$
…	…	…	…
i	$p^i.\{g^0, g^1, \dots, g^{\Phi(\delta-i)-1}\}$	$p^{i.n}.\{g^{0.d[i.n]}, g^{1.d[i.n]}, \dots, g^{(\Phi(\delta-i.n)/d[i.n]-1).d[i.n]}\}$	$d_{i.n}.p^{i.(n-1)}$
…	…		…
1	$p^1.\{g^0, g^1, \dots, g^{\Phi(\delta-1)-1}\}$	$p^n.\{g^{0.d[n]}, g^{1.d[n]}, \dots, g^{(\Phi(\delta-n)/d[n]-1).d[n]}\}$	$d_n.p^{(n-1)}$
0	$p^0.\{g^0, g^1, \dots, g^{\Phi(\delta)-1}\}$	$p^0.\{g^{0.d[0]}, g^{1.d[0]}, \dots, g^{(\Phi(\delta)/d[0]-1).d[0]}\}$	d_0

We can check by simple substitution in the modulo equation that the proposed solutions are correct and verify that we have all of the solutions by a simple enumeration. We have adopted above the writing convention v_i or v[i] which means v_i integer values vary between 0 and $\Phi(\delta-i)/d_i-1$ where $d_i = (n, \Phi(\delta-i))$. Thus, equation $x^n = c \bmod p^\delta$ admits $d_{i.n}.p^{i.(n-1)}$ solutions for c likewise $p^{i.n}.g^{i.d[i.n]}$ and $i \leq \delta n$, admits $p^{\delta-\delta n-1}$ solutions for c = 0, otherwise there is no solution.
This general case simplifies if n has no p factor :

$$p \nmid n \qquad (7)$$

Then :

$$d_i = (n,\Phi(\delta-i)) = (n,p^{\delta-1-i}.(p-1)) = (n,p-1) = d_0 = d \qquad (8)$$

So that :

$$\{g^{0.n}, g^{1.n}, g^{2.n}, \dots, g^{(\Phi(\delta-j)-1).n}\} \equiv U_{d.(p\wedge j.(n-1))\ \text{times}}\ \{g^{0.d}, g^{1.d}, g^{2.d}, \dots, g^{(\Phi(\delta-j.n)/d-1).d}\} \bmod p^{\delta-j.n} \qquad (9)$$

Finally :

$$\begin{vmatrix} \#\{p^\delta\} = \#\{0\} \\ \#\{p^{\delta n.n}.g^0\} \\ \#\{p^{\delta n.n}.g^1\} \\ \dots \\ \#\{p^{\delta n.n}.g^{d-1}\} \\ \dots \\ \#\{p^{j.n}.g^0\} \\ \#\{p^{j.n}.g^1\} \\ \dots \\ \#\{p^{j.n}.g^{d-1}\} \\ \dots \\ \#\{p^0.g^0\} \\ \#\{p^0.g^1\} \\ \dots \\ \#\{p^0.g^{d-1}\} \end{vmatrix} = \begin{vmatrix} p^{\delta-\delta n-1} \\ d.p^{\delta n.(n-1)} \\ 0 \\ \dots \\ 0 \\ \dots \\ d.p^{j.(n-1)} \\ 0 \\ \dots \\ 0 \\ \dots \\ d = \#\{1\} \\ 0 \\ \dots \\ 0 \end{vmatrix} \qquad (10)$$

For each of the lines, it is assumed that the cardinal of $p^{j.n}.g^i$ is also that of $p^{j.n}.g^i.g^{u.d}$.
Let us note that if d = 1, then the d-1 exponent is 0 and rows corresponding to the cardinals $\#\{p^{j.n}.g^1.g^{v[j.n].d[j.n]}\}$ to $\#\{p^{j.n}.g^{d[j.n]-1}.g^{v[j.n].d[j.n]}\}$ do not exist. We have then $\#\{p^{j.n}.g^0\} = \#\{p^{j.n}.g^1\} = \dots = \#\{p^{j.n}.g^{u(j.n)-1}\} = p^{j.(n-1)}$.

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. This detail is however providing nothing substantial to the article. We therefore restrict us to the following :

Equation $x^n = c \bmod 2^\delta$ admits $d_{i.n}.2^{i.(n-1)}$ solutions for c likewise $2^{i.n}.5^{i.d[i.n]}$ and $i \leq \delta n$, admits $2^{\delta-\delta n-1}$ solutions for c = 0, admits $2^{\delta-\delta n-1}$ solutions for $c = 2^{\delta n.n}$, otherwise there is no solution.
If $d_{j.n} = 1$, we have :

$$2 \nmid n \qquad (11)$$

Let us note then #{1} the cardinal of the solutions of $x^n = 1 \bmod 2^\delta$:

$$\#\{1\} = \#\{x / x^n = 1 \bmod 2^\delta, x = 0,1, \dots, 2^\delta-1\} \qquad (12)$$

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

x	conditions on k, i et n	c	#{c}	#{kinds of c}
$2^{\delta n}.(2k)$	$k = 0, 1, \ldots, 2^{\delta-\delta n-1}-1$	0	$2^{\delta-\delta n-1}$	1
$2^{\delta n}.(1+2k)$	$k = 0, 1, \ldots, 2^{\delta-\delta n-1}-1$	$2^{\delta n.n}$	$2^{\delta-\delta n-1}$	1
$2^{i}.(1+2.(\#\{1\}).k)^{1/n}$ $+2^{\delta-i.(.n-1)}/(\#\{1\})k'$	$k = 0, 1, \ldots, 2^{\delta-1-i.n}/(\#\{1\})-1$ $i = 0$ à $\delta n-1$ $k' = 0$ à $2^{i.(n-1)}.(\#\{1\})-1$	$2^{i.n}\ (1+2.\#\{1\}.k)$	$2^{i.(n-1)}.(\#\{1\})$	$2^{\delta-1-i.n}/(\#\{1\})$

Then forming the sum $\sum \#\{c\}.\#\{\text{kinds of c}\}$, we find it equal to 2^{δ}, which proves that all solutions are described. The particularity of the case p = 2 shows at the second row of data in the preceding table ($\#\{2^{\delta n.n}\} = 2^{\delta-\delta n-1}$) which does not exist in the case p is odd.

In summary, said in a slightly different way as above, equation $x^n = c \bmod 2^{\delta}$ admits $2^{i.(n-1)}.(\#\{1\})$ 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 there is no solution

3.2. Matrix formatting

3.2.1. Case of variables of integers modulo p

Let us solve :

$$x_1^n+x_2^n+\ldots+x_k^n = c \bmod p \qquad (13)$$

Each variable of integers x_i^n is replaced by its representative $[0^n, 1^n, 2^n, \ldots, (p-1)^n]$. Thus we get a table of k dimensions and size p along each axis. The elements of this array are obtained by modulo p sums according to operators +. One should count the number of occurrences of each number between 0 and p-1 in the table.

First, we deal with the peculiar case p = 2. This is equivalent to form multidimensional tables with a generator {0,1} on each axis. The reader will easily check that we obtain :

$$\#\{0\} = 2^{k-1} \quad \text{et} \quad \#\{1\} = 2^{k-1} \quad \text{if} \quad p = 2 \qquad (14)$$

For $p \neq 2$, again forming a table with k dimensions, we observe the limited number of distinct cardinals. Different values are no more than d+1 where d = (n, p-1). To achieve this result, we count first the residues of $x^n \bmod p$ which enables us to get straightforward the following table summarizing the different cardinals in the "k = 1" cases. There are here three cases to be considered :

Target c	Cardinal (for k = 1)
{0}	1
$\{g^d, g^{2d}, g^{3d}, \ldots, g^{(p-1)}\} \bmod p$	d = (n, p-1)
Other among {0, 1, 2, …, (p-1)}	0

Then the iteration for k > 1 gives the following table (table 1) :

		$card_0$	$card_1$				$card_2$				…	$card_{d-1}$			
		0	$g^0.g^d$	$g^0.g^{2d}$	…	$g^0.g^{(p-1)}$	$g^1.g^d$	$g^1.g^{2d}$	…	$g^1.g^{(p-1)}$		$g^{d-1}.g^d$	$g^{d-1}.g^{2d}$	…	$g^{d-1}.g^{(p-1)}$
card = 1	0														
card = d	g^d														
	g^{2d}														
	…														
	$g^{(p-1)}$														

Our recurrence hypothesis, implicit in the table above, is that a set of type $g^r.\{g^d, g^{2d}, g^{3d}, \ldots, g^{(p-1)}\} = \{g^r.g^d, g^r.g^{2d}, g^r.g^{3d}, \ldots, g^r.g^{(p-1)}\}$ has the same value for cardinals $card_{r+1}$. It is necessary then to check the property passing from k to k+1 by noting that it is actually true for k = 1 (trivial case).

We observe that the table is formed of the following parts : the first line, the first column except the element of the first line, the first square (under $card_1$) and the other squares (under $card_2$ to $card_{d-1}$). We are thus brought to consider the cases corresponding to each part of the table, in order to get corresponding contributions for given target c, contributions which we must then add.
We call generating vector of table 1 following x, respectively y, the elements 0 and $g^{u.d}$ located on the left first column of this table and the elements 0 and $g^y.g^{v.d}$ located above the first line of this table :

Case 1 : First line of table 1.
This line, where we add 0, simply reproduces, with cardinal 1, each element of the generating vector following y. The contribution to the cardinals is the identity :

$$card'_r = card_r \qquad (15)$$

Case 2 : First column of table 1, except line 1, already mentioned above.
The contribution is $d.card_0$ for each target of the form $g^{u.d}$ and is 0 for each target of the form $g^x.g^{u.d}$ with $x \neq 0$. With adopted rule on cardinal's indexes, we act on $card'_1$, each target $g^{u.d}$ being concerned in an identical way, as :

$$\begin{matrix} card'_1 = d.card_0 \\ card'_i = 0,\ i \neq 1 \end{matrix} \qquad (16)$$

Case 3 : First square of table 1 right of the first column and following squares.
Here a target is written $c = g^{u.d} + g^y.g^{v.d} \bmod p$ and we seek, for y given, the couples (u,v) answering that equation. That is to say $s(c) = \#\{(u,v)\}$. Then, for the target $c.g^d$, we have $c.g^d = g^{(u+1).d} + g^y.g^{(v+1).d} \bmod p$ and the number of couples (u,v) solutions is identical to the number of preceding couples and this with the same contributions by each square of the table. Thus, it suffices to solve respectively each case, possibly distinct, of type $c = g^r$, r = 0 to d-1, to get respectively the identical cases $c = g^r.g^d$, $c = g^r.g^{2d}$, …, $g^r.g^{((p-1)/d-1).d} \bmod p$, with cardinal (p-1)/d (the case $c = g^r$ included). Hence the contribution :

$$card'_{r+1} = \sum_{y=0}^{d-1} d.(\#\{(u,v) / g^r = g^{u.d} + g^y.g^{v.d} \bmod p\}.card_{y+1}) \qquad (17)$$

The argument is identical for c = 0 with multiplicity equal to (p-1)/d to be multiplied by d, that is p-1 what imposes the existence of only one non-null component on the first line of the matrix. We verify this point on the example. The equation of problem is $g^{u.d} + g^y.g^{v.d} = 0$, u and v varying independently from 1 to (p-1) /d, that is also $g^y.g^{v.d} = -g^{u.d}$, then $g^{y+(v-u).d} = -1 \bmod p$. However as g is a primitive root of the sequence p, we have necessarily $g^{(p-1)/2} = -1 \bmod p$. It follows $y+(v-u).d = (p-1)/2 \bmod p-1$, then $y = (p-1)/2+(v-u).d \bmod p-1$. However d divides p-1. We deduce immediately $y = (p-1)/2 \bmod d$. This means that matrix column n° y+2 carries on the first line all the solutions and the cardinal is worth p-1 at indicated position y+2. Hence the contribution :

$$card'_0 = (p-1).card_{(p+1)/2} \qquad (18)$$

Addition of contributions 1, 2 and 3 gives the following matrix. This one, noted [A], is written in a shorter way as (relation 19) :

$$[A(x,y)] = [\text{if}((x,y) = (2,1), d, \text{if}((x,y) = (1,(p+1)/2 \bmod d), p-1, \text{if}((x,y)>(1,1), \#(u,v).d / g^{x-2} = g^{u.d} + g^{y-2}.g^{v.d} \bmod p, 0)))] + [I]$$

where
x is index of row 1 to d+1, y is index of column 1 to d+1,
{u,v} integers describing $[0,(p-1)/d-1]^2$, d = (n, p-1),
[I] is identity matrix dimension d+1.
x axis is directed to the bottom, y axis to the right.
By convention also, (x,y) > (1,1) means x > 1 and y > 1.

Then

$$\begin{vmatrix} \#(0) \\ \#(g^0.g^{u.d}) \\ \#(g^1.g^{u.d}) \\ \dots \\ \#(g^{d-1}.g^{u.d}) \end{vmatrix} = \begin{vmatrix} & & \\ & A & \\ & & \end{vmatrix}^k \begin{vmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{vmatrix} \qquad (20)$$

With d+1 size matrix, one concludes that d+1 is the maximum number of distinct cardinals. The first column of A is the column vector generator of A. This is consistent with the first step of the recurrence hypothesis.

Returning back, we focus the reader's attention, for its theoretical importance, on the equation that follows and that will receive the name of equation of primitive roots :

$$g^r = g^{u.d} + g^y.g^{v.d} \bmod p \qquad (21)$$

3.2.2. Case of variables of prime numbers modulo p

$$y_1^n + y_2^n + \dots + y_m^n = c \bmod p \qquad (22)$$

Here the y_i are positive primes. The case is very similar to the previous one. The representative is no longer $[0^n, 1^n, 2^n, \ldots, (p-1)^n]$ but $[1^n, 2^n, \ldots, (p-1)^n]$. The absence of target {0} makes that the first column of the preceding table disappears (column corresponds to $card_0$).
Thus

$$\{B] = [A]-[I] \qquad (23)$$

where [A] is the matrix obtained previously, [B] the matrix which concerns us here and the identity matrix [I] of size d+1.

The cardinals of order m are :

$$\begin{vmatrix} \#(0) \\ \#(g^0.g^{u.d}) \\ \#(g^1.g^{u.d}) \\ \ldots \\ \#(g^{d-1}.g^{u.d}) \end{vmatrix} = \begin{vmatrix} & & \\ & B & \\ & & \end{vmatrix}^m \begin{vmatrix} 1 \\ 0 \\ 0 \\ \ldots \\ 0 \end{vmatrix} \qquad (24)$$

3.2.3. Case of variables of the two types

One can compose cases of variables of both types, with equal exponents, resulting then to simple multiplications of matrices.

3.2.4. Eigenvalues and eigenvectors of cardinal matrices

Below, the conjugate of an imaginary number or a set of those is noted *. The transposed matrix of A is ${}^tA$.

For the p = 2 sequence, the calculation is carried out directly. When the sequence is odd, in a general way, the cardinal matrix [C] associated with x^n at sequence p is built from a circular matrix [CI] :

$$card'(i) = \sum_{j=0 \text{ à } p-1} \#(i-j \bmod p).card(j) \qquad (25)$$

Here #(i-j) are the components at (i,j) of the matrix [CI] which is a right circular matrix as #(i-j) = #(i+t-(j+t)).
The eigenvalues of such a matrix $[CI_d(c_0,c_1, \ldots, c_{p-1})]$ is :

$$\sigma_v = \sum_{t=0 \text{ to } p-1} c_t.e^{-2\pi i.t.v/p}$$

One will recognize here a discrete Fourier transform (DFT).
To clarify later writing, we use $c_t = c(t)$. We have c(t) = #(t), that is :

$$c(0) = \#(0) = \text{if(variable of integers = ve, 1, 0)}$$
$$c(g^k.g^{u.d}) = \#(g^k.g^{u.d}) = \text{if(k = 0, d, 0)}$$

Hence

$$\sigma_v = \text{if(ve,1,0)} + d.\sum_{r=0 \text{ to } (p-1)/d-1} e^{-2\pi i.(g\hat{}(r.d)).v/p} \qquad (26)$$

We observe the repetition of the eigenvalues related to the c_t coefficients patterns. When $v' = v.g^{u.d}$, u an integer, we have actually $\sigma_{v'} = \sigma_v$.
Furthermore, for [P] a change of base matrix, $[CI] = [P].[\sigma].[P^{-1}]$, we choose the unitary matrix

$$[P(r,s)] = [{}^tP^*(r,s)] = (1/p^{1/2}).[e^{(2\pi i/p).r.s}]$$

We proceed then to a rearrangement of the generating elements different from 0 modulo p (first row and first column outside the table) starting with $g^{u.d}$, u = 0 to (p-1)/d-1, then $g^{u.d+1}$, then $g^{u.d+2}$, etc.
This gives a new matrix with the same rearrangement on [P] (and $[P^{-1}]$). Hence it follows :

$$[CI'] = [P'].[\sigma'].[P'^{-1}]$$

with :

$$[P'(r,s)] = (1/p^{1/2}).[e^{(2\pi i/p).if(r=0,0,(g\hat{}int((r-1)/((p-1)/d))).(g\hat{}d.((r-1) \bmod (p-1)/d))).if(s=0,0,(g\hat{}int((s-1)/((p-1)/d))).(g\hat{}d.((s-1) \bmod (p-1)/d)))}]$$
$$[P'^{-1}(r,s)] = (1/p^{1/2}).[(e^{(-2\pi i/p).if(r=0,0,(g\hat{}int((r-1)/((p-1)/d))).(g\hat{}d.((r-1) \bmod (p-1)/d))).if(s=0,0,(g\hat{}int((s-1)/((p-1)/d))).(gd.\hat{}((s-1) \bmod (p-1)/d)))}]$$
$$[\sigma'(r,s)] = [\text{if}(r \neq s,0,\sigma_{\text{if}(r=0,0,(g\hat{}int((r-1)/((p-1)/d))).(g\hat{}d.((r-1) \bmod (p-1)/d)))}]$$

Progression of the indexes is here of the form :

$$\{\{0\}, \{g^{0.d}, g^{1.d}, \ldots, g^{((p-1)/d-1).d}\}, \{g.g^{0.d}, g.g^{1.d}, \ldots, g.g^{((p-1)/d-1).d}\}, \ldots, \{g^{d-1}.g^{0.d}, g^{d-1}.g^{1.d}, \ldots, g^{d-1}.g^{((p-1)/d-1).d}\}\}$$

We proceed then to the "merger" per blocks of the matrices. The line sums of cardinal matrix must remain unchanged at value p. The first line, out of first column, is merged by summation of (p-1)/d components (without division of the result). The first column, out of first line, is merged by summation of (p-1)/d component and division by (p-1)/d. The square blocks size ((p-1)/d,(p-1)/d) of the matrices are merged by summation and division by (p-1)/d (no division versus lines but versus columns). Indexes u and v are selected to locate the blocks of size ((p-1)/d,(p-1)/d). These indexes vary from 0 to d.
Thus :

$$[CI''] = [P''].[\sigma''].[P''^{-1}]$$

Inside a block (d,d), we get :

$$[P'(r+1 \bmod d, s+1 \bmod d)] = [P'(r \bmod d, s \bmod d)]$$
$$[P'^{-1}(r+1 \bmod d, s+1 \bmod d)] = [P'^{-1}(r \bmod d, s \bmod d)]$$

The sum of a block ((p-1)/d, (p-1)/d) divided by (p-1)/d is therefore the sum of a line (1, (p-1)/d).
Thus, the sum bearing on r = 0 to (p-1)/d-1 :

$$[P''(u,v)] = [\text{if}(v = 0, 1, \text{if}(u = 0, (p-1)/d, (1/p^{1/2}).\sum e^{(2\pi i/p).(g\hat{}(u-1)).(g\hat{}(r.d))}]$$

$$[P''^{-1}(u,v)] = [\text{if}(v = 0, 1, \text{if}(u = 0, (p-1)/d, (1/p^{1/2}).\sum e^{(-2\pi i/p).(g\hat{}(u-1)).(g\hat{}(r.d))}]$$

$$[\sigma''(u,v)] = [\text{if}(u \neq v, 0, \text{if}(ve,1,0)+d.\sum e^{(-2\pi i/p).(g\hat{}(u-1)).(g\hat{}(r.d))}]$$

We have for u > 0 and v > 0 (in a block ((p-1)/d, (p-1)/d) :

$$P''(u,v) = P''(u-1,v+1)$$
$$P''^{-1}(u,v) = P''^{-1}(u-1,v+1)$$

The inner part (that is out of the first line and first column) of these matrices is <u>left circular</u>.
This then translates as follows (the σ''_i shall be replaced by σ_i for readability) :

<u>Theorem : Decomposition of cardinal matrices</u>

The cardinal matrix [C], relative to the operation x^n (with ve = 1), respectively y^n (with ve = 0), at sequence p, of size d+1 where d = (n, p-1), is diagonalisable and :

$$[C] = (1/p) \left| \begin{array}{ccccc} 1 & \lambda_0*/d & \lambda_0*/d & \ldots & \lambda_0*/d \\ 1 & \lambda_1*/d & \lambda_d*/d & \ldots & \lambda_d*/d \\ 1 & \lambda_2*/d & \lambda_3*/d & \ldots & \lambda_1*/d \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_d*/d & \lambda_1*/d & \ldots & \lambda_{d-1}*/d \end{array} \right| \left| \begin{array}{ccccc} \sigma_0 & 0 & 0 & \ldots & 0 \\ 0 & \sigma_1 & 0 & \ldots & 0 \\ 0 & 0 & \sigma_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \sigma_d \end{array} \right| \left| \begin{array}{ccccc} 1 & \lambda_0/d & \lambda_0/d & \ldots & \lambda_0/d \\ 1 & \lambda_1/d & \lambda_2/d & \ldots & \lambda_d/d \\ 1 & \lambda_2/d & \lambda_3/d & \ldots & \lambda_1/d \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_d/d & \lambda_1/d & \ldots & \lambda_{d-1}/d \end{array} \right| \quad (27)$$

with

$$\lambda_u = d.\sum e^{(-2\pi i/p).g\hat{}(u-1+r.d)} \quad (28)$$
$$r = 0 \text{ to } (p-1)/d-1$$

and

$$\sigma_u = \text{if}(ve,1,0)+d.\sum e^{(-2\pi i/p).g\hat{}(u-1+r.d)} \quad (29)$$
$$r = 0 \text{ to } (p-1)/d-1$$

A variety of permutations of indexes is permissible, in particular, we can write:

$$[C] = (1/p) \left| \begin{array}{ccccc} 1 & \lambda_0*/d & \lambda_0*/d & \ldots & \lambda_0*/d \\ 1 & \lambda_1*/d & \lambda_2*/d & \ldots & \lambda_d*/d \\ 1 & \lambda_d*/d & \lambda_1*/d & \ldots & \lambda_{d-1}*/d \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_2*/d & \lambda_3*/d & \ldots & \lambda_1*/d \end{array} \right| \left| \begin{array}{ccccc} \sigma_0 & 0 & 0 & \ldots & 0 \\ 0 & \sigma_1 & 0 & \ldots & 0 \\ 0 & 0 & \sigma_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \sigma_d \end{array} \right| \left| \begin{array}{ccccc} 1 & \lambda_0/d & \lambda_0/d & \ldots & \lambda_0/d \\ 1 & \lambda_1/d & \lambda_d/d & \ldots & \lambda_2/d \\ 1 & \lambda_2/d & \lambda_1/d & \ldots & \lambda_3/d \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_d/d & \lambda_{d-1}/d & \ldots & \lambda_1/d \end{array} \right| \quad (30)$$

We note that the eigenvalues are imaginary or real according to the following cases:

d = (n, p-1) odd	p = 1 mod 2d	real eigenvalues
d = (n, p-1) even	p = 1 mod 2d	real eigenvalues
d = (n, p-1) even	p = 1+d mod 2d	imaginary eigenvalues

3.2.5. Case modulo p^{δ}

The principle of the multidimensional arrays is identical. The wording is more space consuming because of the different combinations of terms like $p^k.g^i.g^{u.d}$ (instead of $g^i.g^{u.d}$) and 0. Because of the primitive roots equations, the blocks inside the matrix, except first row and column concerning target 0 do repeat following the direction of the main diagonal with a multiplicative factor p (the value of the sequence) likewise the relevant targets. The change of base matrix and its inverse deriving of a left circular matrix observe this rearrangement but on opposite diagonal. The eigenvalues thus follow the same multiplicative scheme :

$$p^{\delta}[\sigma_0],\ p^{\delta-1}[\sigma_1],\ p^{\delta-1}[\sigma_2],\ \ldots,\ p^{\delta-1}[\sigma_d],\ p^{\delta-2}[\sigma_1],\ p^{\delta-2}[\sigma_2],\ \ldots,\ p^{\delta-2}[\sigma_d]\ldots$$

where $\sigma_0, \sigma_1, \sigma_2, \ldots, \sigma_d$ are the eigenvalues of the modulo p cardinal matrix.

4. Aggregation modulo p

4.1. Concept of environment

All diophantine equations are not of homogeneous degrees. We may consider the behaviour of x^n appearing other variables $R(x_1, x_2\ldots)$. This again means to compose a two-dimensional table.

		$card_0\ R(x_1, x_2\ldots)$	$card_i\ R(x_1, x_2\ldots)$			
		0	$g^i.g^{d'}$	$g^i.g^{2d'}$	…	$g^i.g^{(p-1)}$
$card_0\ (x^n) = 1$	0	c				
$card_{g\wedge i}\ (x^n) = d$	g^d					
	g^{2d}					
	…					
	$g^{(p-1)}$					

To proceed as above, it is necessary and it suffices to have d = d'. Here d = (n, p-1) and d' is necessarily a divisor of p-1 (possibly 1). It is therefore necessary to break into new classes g^i in such a way to have a "common factor" to d and d'. The smallest suitable value is the lowest common multiple to d and d' taking account of p-1. Hence the adequate value is cm = (lcm(d,d'), p-1).

Thus, if we consider the diophantine equations like :

$$x_1^{(a1)} + x_2^{(a2)} + \ldots + x_k^{(ak)} + y_1^{(b1)} + y_2^{(b2)} + \ldots + y_m^{(bm)} = c \qquad (31)$$

where $(a_1), (a_2), \ldots, (a_k)$ respectively $(b_1), (b_2), \ldots, (b_m)$ are any positive integers and x_i and respectively y_i are variables of integers and prime numbers. At sequence p, we have $d_i = (p\text{-}1,(a_i))$ and $d_j = (p\text{-}1,(b_j))$, then :

$$cm = (p\text{-}1, lcm((a_1), (a_2), \ldots, (a_k), (b_1), (b_2), \ldots, (b_m)) \qquad (32)$$

We will call cm the environment of x^n in the presence of other variables.

4.2. Equations of the primitive roots

We seek the contribution of the monomial $x_i^{(ai)}$ with $d = (p\text{-}1, a_i)$ in the environment cm. Thanks to a two-dimensional table, we get immediately the equations involving primitive roots of p, then the matrices whose first row and first column are distinguished from the other components. The difference between this case and the homogeneous exponents' case is simply on the exponentiation of one of the terms ($g^{u.d}$ instead of $g^{u.cm}$).
The matrix components c(x,y) are indexed in rows and columns, respectively. For a reduced matrix (corresponding to the withdrawal of the first row and first column), the coordinates x and y will start at 2.

First row of matrix

$$c(1,y) = \#\{(u,v) \setminus 0 = g^{u.d} + g^{y-2}.g^{v.cm} \bmod p\} \qquad (33)$$

First column of matrix

$$c(x,1) = \#\{(u,v) \setminus g^{x-2} = g^{u.d} \bmod p\} \qquad (34)$$

Reduced matrix blocks

$$c(x,y) = d\ .\ \#\{(u,v) \setminus g^{x-2} = g^{u.d} + g^{y-2}.g^{v.cm} \bmod p\} \qquad (35)$$

The domain of definition of (u,v) is u = 0 to (p-1)/d-1, v = 0 to (p-1)/cm-1.

4.3. General form of cardinal matrices

We consider the case of the matrices of monomial x^d (matrix [A]) or y^d (matrix [B]) in an environment cm. The matrices are square of size cm+1. These matrices, like standard cardinal matrices show a peculiar first row and first column. The rest of the matrix is composed by repetition (cm/d times) parallel to the main diagonal of cm/d block of size d.

The general form of [A] matrices is :

$$[A]_{d,cm} = \begin{vmatrix} 1 & [L1] & [L1] & [L1] & [L1] & [L1] & [L1] & [L1] & [L1] \\ [C1] & [A(1)] & [A(2)] & [A(3)] & \dots & [A(cm/d-3)] & [A(cm/d-2)] & [A(cm/d-1)] & [A(cm/d)] \\ [C1] & [A(cm/d)] & [A(1)] & [A(2)] & [A(3)] & \dots & [A(cm/d-3)] & [A(cm/d-2)] & [A(cm/d-1)] \\ [C1] & [A(cm/d-1)] & [A(cm/d)] & [A(1)] & [A(2)] & [A(3)] & \dots & [A(cm/d-3)] & [A(cm/d-2)] \\ [C1] & [A(cm/d-2)] & [A(cm/d-1)] & [A(cm/d)] & [A(1)] & [A(2)] & [A(3)] & \dots & [A(cm/d-3)] \\ [C1] & \dots & [A(cm/d-2)] & [A(cm/d-1)] & [A(cm/d)] & [A(1)] & [A(2)] & [A(3)] & \dots \\ [C1] & [A(4)] & \dots & [A(cm/d-2)] & [A(cm/d-1)] & [A(cm/d)] & [A(1)] & [A(2)] & [A(3)] \\ [C1] & [A(3)] & [A(4)] & \dots & [A(cm/d-2)] & [A(cm/d-1)] & [A(cm/d)] & [A(1)] & [A(2)] \\ [C1] & [A(2)] & [A(3)] & [A(4)] & \dots & [A(cm/d-2)] & [A(cm/d-1)] & [A(cm/d)] & [A(1)] \end{vmatrix} \quad (36)$$

And we have :

$$[B]_{d,cm} = [A]_{d,cm} - [I] \quad (37)$$

[C1] is a matrix column of size (1,d) whose first component is d and other components are 0.
[L1] is a row matrix of size (d,1) whose first component (if p = 1 mod 2d) or the d/2+1 component (if p = 1+d mod 2d) is (p-1)/(cm/d) and the other components are 0.
[A(i)] and [B(i)] are square matrices of size d.

Proof

First line of matrix

By division, we get for the characteristic equation of the first line :

$$c(1,y) = \#\{(u,v) \setminus -1 = g^{(p-1)/2} = g^{y-2}.g^{(v.cm/d-u).d} \bmod p\}$$

It follows y-2+(v.cm/d-u).d = (p-1)/2 mod p-1, then y = 2+(p-1)/2 + (v.cm/d-u).d mod p-1. As d divides p-1, we deduce immediately y = 2+(p-1)/2 mod d and (v.cm/d-u) = 0 mod (p-1)/d. This last equation has an equal number of solutions whatever y (because independent of y) and thus (p-1)/d solutions (u,v), hence :

$$c(1,2+(p-1)/2 \bmod d) = (p-1)/d$$
$$c(1,y \neq 2+(p-1)/2 \bmod d) = 0$$

First column of matrix

From $c(x,1) = \#\{(u,v) / g^{x-2} = g^{u.d} \bmod p\}$, it follows x = 2+u.d mod p-1. The equation has only one solution at x = 2 +k.d with d choice for k (k = 0 mod (p-1)/d). So that :

$$c(x,1) = if(x=2 \bmod d, d, 0)$$

Matrix blocks

Reduced matrix characteristic equation is $c(x,y) = d.\#\{(u,v) \setminus g^{x-2} = g^{u.d} + g^{y-2}.g^{v.cm} \bmod p\} = d.\#\{(u,v) \setminus g^{d}.g^{x+d-2} = g^{d}.(g^{u.d} + g^{y-2}.g^{v.cm}) \bmod p\} = d.\#\{(u,v) \setminus g^{x+d-2} = g^{u.d+d} + g^{y-2+d}.g^{v.cm} \bmod p\}$ which is the required principal diagonal property mod d.

The addition of {0} in two-dimensional table involves, as in standard cardinal matrix case, the following relations:

$$[A(i)] = [B(i)] \text{ if } i \neq 1$$
$$[A(1)] = [B(1)] + [I]$$

Property of components average

Let us have $[A]_{d,cm}$ the cardinal matrix of monomial x^d in environment cm and let us have $[A]_{cm,cm}$ the cardinal matrix of monomial x^{cm} in environment cm for integers variable, $[B]_{d,cm}$ and $[B]_{cm,cm}$ being our matrices for prime numbers variables cases. The components of the first matrices ($[A]_{d,cm}$ and $[B]_{d,cm}$) result from the seconds ($[B]_{cm,cm}$ and $[B]_{cm,cm}$) by an average operation :

$$c_{[A](d,cm)}(i,j) = (d/cm).\sum c_{[A](cm,cm)}(i+n.d,j+n.d) \quad n = 0 \text{ to } cm/d-1 \quad i>1,\ j>1 \quad (38)$$

$$c_{[A](d,cm)}(1,j) = (d/cm).\sum_{n=0 \text{ to } cm/d-1} c_{[A](cm,cm)}(1,j+n.d) \quad j>1 \qquad (39)$$

$$c_{[A](d,cm)}(i,1) = (d/cm).\sum_{n=0 \text{ to } cm/d-1} c_{[A](cm,cm)}(i+n.d,1) \quad i>1 \qquad (40)$$

This is an immediate consequence of the equations of primitive roots and we get thus easily the cardinal matrix of monomial x^n in the environment cm from the cardinal matrix of monomial x^{cm} (in the environment cm).

4.4. Diagonalisation of cardinal matrices

We use the theorem of decomposition of the cardinal matrices to get the expression of the change of base matrix and its eigenvalues for :

- x^n in environment n (d = (n,p1)) : $[C]_{d,d} = [P_B]_{d,d}.[\sigma]_{d,d}.[P_B^{-1}]_{d,d}$
- x^n in environment cm : $[C]_{d,cm} = [P_B]_{d,cm}.[\sigma]_{d,cm}.[P_B^{-1}]_{d,cm}$
- x^{cm} in environment cm : $[C]_{cm,cm} = [P_B]_{cm,cm}.[\sigma]_{cm,cm}.[P_B^{-1}]_{cm,cm}$

[C] is either [A] or [B] depending on the type of variables. The first index refers to the exponent of the monomial (which gives d for x^n) and the second is index refers to the environment. The dimension of the square matrix is equal to the second index plus one.
The evaluation of matrices $[P_B]_{d,cm}$ and $[P_B]_{cm,cm}$ by the cardinal matrix decomposition theorem is the same. We thus have :

$$[P_B]_{d,cm} = [P_B]_{cm,cm} \qquad (41)$$

The property of the average of the components immediately causes :

- the eigenvalues of $[\sigma]_{d,cm}$ are those of $[\sigma]_{d,d}$
- the repetition, with step d, except row of #(0), of the eigenvalues of $[\sigma]_{d,cm}$
- the eigenvalues of $[\sigma]_{d,cm}$ are the average at index modulo cm/d of the eigenvalues of $[\sigma]_{cm,cm}$

We will call the common change of base matrix $[P_B]_{cm,cm}$ the <u>environment matrix</u>.

4.5. The example of environment 4. Matrices of Iwaniec and Friedlander

Friedlander and Iwaniec proved in 1996 the infinite number of primes of the type $x_1^2+x_2^4$. We produces here our own way this result and some more. Instead, let us study more generally (c is a constant relative integer not reduced to 0 only, x_1 et x_2 are variables of integers and y a variable of prime numbers) :

$$x_1^2+x_2^4 = y+c$$

We have three principal cases to consider for environment and two lower cases :

p	(p-1,d) variable x^2	(p-1,d) variable x^4	(p-1,d) variable -y	cm	lower cases
2	1	1	1	1	/
1 mod 4	2	4	1	4	p = or(1,5) mod 8
3 mod 4	2	2	1	2	/

To perform the multiplication of matrices, we move variable y towards the left member of the proposed equation. Let us seek the cardinal matrix of -y in the environments 1, 2 and 4 respectively. To do this, we consider first the variables of integers x and -x modulo p whose representatives are [0, 1, 2,..., p-1] and [-0, -1, -2,...,-p+1] and are thus identical. Passing to y and -y, it suffices to remove 0 and representatives modulo p of y and -y are therefore also identical. The cardinals of the cardinal matrices x and -x in the environments 1, 2 and 4 matrices are equally distributed. We have thus :

$$\begin{array}{c|c|c} \text{Var x or -x} & & [A] \\ \#\{0\} & : & 1 \quad p-1 \\ \#\{g^u\} & & 1 \quad p-1 \end{array} \qquad \begin{array}{c|c|c} \text{Var y or -y} & & [B] = [A]-[I] \\ \#\{0\} & : [M0] = & 0 \quad p-1 \\ \#\{g^u\} & & 1 \quad p-2 \end{array}$$

$$\begin{array}{c|c|c} \#\{0\} & & 1 \quad (p-1)/2 \quad (p-1)/2 \\ \#\{g^{2u}\} & : & 1 \quad (p-1)/2 \quad (p-1)/2 \\ \#\{g.g^{2u}\} & & 1 \quad (p-1)/2 \quad (p-1)/2 \end{array} \qquad \begin{array}{c|c|c} \#\{0\} & & 0 \quad (p-1)/2 \quad (p-1)/2 \\ \#\{g^{2u}\} & : [M0] = & 1 \quad (p-3)/2 \quad (p-1)/2 \\ \#\{g.g^{2u}\} & & 1 \quad (p-1)/2 \quad (p-3)/2 \end{array}$$

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} : \begin{vmatrix} 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \end{vmatrix} \begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} : [M0] = \begin{vmatrix} 0 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-5)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-5)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-5)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-5)/4 \end{vmatrix}$$

Cardinal matrices in larger environments are obtained by equal subdivisions of components in the case of variables x and -x (the sum of each line is always p) cases. For variables y and -y, one simply subtract 1 on the diagonal of the matrix as described previously. Then we have :

For p = 2

The case p = 2 is solved easily showing immediately the same abundance factors :

$$\begin{vmatrix} \#\{0\} \\ \#\{g^u\} \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix}^2 \begin{vmatrix} 1 \\ 0 \end{vmatrix} = \begin{vmatrix} 2 \\ 2 \end{vmatrix}$$

For p = 3 mod 4

We have to find the cardinal matrix of x^2 in the environment 2. Thanks to primitive roots equations and thanks to the fact that the sum of each row of the matrix equals p, we can write (the reader will be careful to distinguish between variables (here x_1 and x_2) and matrix components (x_1, x_2, x_3, etc.)) :

$$[M1] = \begin{vmatrix} 1 & 0 & p-1 \\ 2 & x_2+1 & x_2 \\ 0 & x_1 & x_2+1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & p-1 \\ 2 & (p-1)/2 & (p-3)/2 \\ 0 & (p+1)/2 & (p-1)/2 \end{vmatrix}$$

It follows the expression of [M1] and of the abundance factors :

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{2u}\} \\ \#\{g.g^{2u}\} \end{vmatrix} = [M0].[M1]^2.\begin{vmatrix} 1 \\ 0 \\ 0 \end{vmatrix} = [M0]\begin{vmatrix} 1 \\ p+1 \\ p+1 \end{vmatrix} = \begin{vmatrix} p^2-1 \\ p^2-p-1 \\ p^2-p-1 \end{vmatrix}$$

For p = 1 mod 8

We must consider two matrices. The first one corresponding to the monomial x^4 is :

$$[M1] = \begin{vmatrix} 1 & p-1 & 0 & 0 & 0 \\ 4 & x_1-3 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_4+1 & x_5 & x_5 \\ 0 & x_3 & x_5 & x_3+1 & x_5 \\ 0 & x_4 & x_5 & x_5 & x_2+1 \end{vmatrix}$$

where

$$\begin{vmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{vmatrix} = \begin{vmatrix} (p+5)/4+(-1)^{(\beta+1)/2}.(3/2).\beta \\ (p-3)/4+2\alpha.\text{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4-2\alpha.\text{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p+1)/4+(-1)^{(\beta+1)/2}.(1/2).\beta \end{vmatrix}$$

with the decomposition into integers of p

$$p = (2\alpha)^2+\beta^2 \quad \alpha > 0, \beta > 0$$

The general form of matrix [M1] is still easily obtained from primitive roots equations. Values of x_1, x_2, x_3, x_4 and x_5 are however conjectural (but can in principle be obtained by the primitive roots equations). The condition concerning x_2 and x_4 (that is $x_4>x_2$ or $x_2>x_4$) simply depends on the choice of g. The second matrix corresponding to the monomial x^2 when cm = 4. All calculations made, using the method of the average of the components, we have :

$$[M2] = \begin{vmatrix} 1 & (p-1)/2 & 0 & (p-1)/2 & 0 \\ 2 & y_1+1 & y_2 & y_3 & y_4 \\ 0 & y_2 & y_3+1 & y_4 & y_1+2 \\ 2 & y_3 & y_4 & y_1+1 & y_2 \\ 0 & y_4 & y_1+2 & y_2 & y_3+1 \end{vmatrix}$$

where

$$\begin{vmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{vmatrix} = \begin{vmatrix} (x_1+x_3)/2-2 \\ (x_2+x_5)/2 \\ x_3 \\ (x_4+x_5)/2 \end{vmatrix} = \begin{vmatrix} (p-7)/4+(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-1)/4+\alpha.\text{if}(x_4>x_2,-1,1) \\ (p-3)/4-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-1)/4-\alpha.\text{if}(x_4>x_2,-1,1) \end{vmatrix}$$

For the evaluation of the coefficients of abundance, we have (in practice, order of multiplication of matrices is not important as they commute) :

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} = [M0].[M1].[M2]. \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix}$$

So that :

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ 2(x_1+x_3-1) \\ 2(x_2+x_5) \\ 2(2x_3+1) \\ 2(x_4+x_5) \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ p-1+2.(-1)^{(\beta+1)/2}.\beta \\ p-1+4\alpha.if(x_4>x_2,-1,1) \\ p-1-2.(-1)^{(\beta+1)/2}.\beta \\ p-1-4\alpha.if(x_4>x_2,-1,1) \end{vmatrix} = \begin{vmatrix} (p-1)^2 \\ p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1-4\alpha.if(x_4>x_2,-1,1) \\ p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1+4\alpha.if(x_4>x_2,-1,1) \end{vmatrix}$$

For p = 5 mod 8

We must consider two matrices. The first one corresponding to the monomial x^4 which one gets in the same way as for p = 1 mod 8:

$$[M1] = \begin{vmatrix} 1 & 0 & 0 & p-1 & 0 \\ 4 & x_3+1 & x_5 & x_3 & x_5 \\ 0 & x_4 & x_5+1 & x_5 & x_2 \\ 0 & x_1 & x_2 & x_3+1 & x_4 \\ 0 & x_2 & x_4 & x_5 & x_5+1 \end{vmatrix}$$

where

$$\begin{vmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{vmatrix} = \begin{vmatrix} (p+1)/4+(-1)^{(\beta+1)/2}.(3/2).\beta \\ (p+1)/4+2\alpha.if(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-7)/4-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p+1)/4-2\alpha.if(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4+(-1)^{(\beta+1)/2}.(1/2).\beta \end{vmatrix}$$

with still the decomposition into integers of p :

$$p = (2\alpha)^2+\beta^2 \quad \alpha > 0, \beta > 0$$

The second matrix corresponding to the monomial x^2 when cm = 4. All calculations made, with again application of average method, we have :

$$[M2] = \begin{vmatrix} 1 & (p-1)/2 & 0 & (p-1)/2 & 0 \\ 2 & y_3+1 & y_4 & y_1 & y_2 \\ 0 & y_4 & y_1+1 & y_2 & y_3+2 \\ 2 & y_1 & y_2 & y_3+1 & y_4 \\ 0 & y_2 & y_3+2 & y_4 & y_1+1 \end{vmatrix}$$

where

$$\begin{vmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{vmatrix} = \begin{vmatrix} (x_1+x_3)/2 \\ (x_2+x_5)/2 \\ x_3-1 \\ (x_4+x_5)/2 \end{vmatrix} = \begin{vmatrix} (p-3)/4+(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-1)/4+\alpha.if(x_4>x_2,-1,1) \\ (p-7)/4-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-1)/4-\alpha.if(x_4>x_2,-1,1) \end{vmatrix}$$

For the evaluation of the coefficients of abundance, we have then :

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} = [M0].[M1].[M2]. \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ 2(2x_3+3) \\ [2(x_4+x_5) \\ 2(x_1+x_3+1) \\ 2(x_2+x_5) \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ p-1-2.(-1)^{(\beta+1)/2}.\beta \\ p-1-4\alpha.if(x_4>x_2,-1,1) \\ p-1+2.(-1)^{(\beta+1)/2}.\beta \\ p-1+4\alpha.if(x_4>x_2,-1,1) \end{vmatrix} = \begin{vmatrix} (p-1)^2 \\ p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1+4\alpha.if(x_4>x_2,-1,1) \\ p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1-4\alpha.if(x_4>x_2,-1,1) \end{vmatrix}$$

We observe that the passage of the expression $x_2^4+x_1^2 = c$ to $x_2^4+x_1^2 = y+c$, by multiplication by [M0], is equivalent to subtract to p^2 the previously obtained cardinals.

Normalization is done by dividing the cardinals by $p^{2-1}(p-1)^1 = p(p-1)$.

For p = 2

$$\begin{vmatrix} Fan\{c, 2\} \end{vmatrix} = \begin{vmatrix} 1 \end{vmatrix}$$

For p = 3 mod 4

$$\begin{vmatrix} Fan\{0, p\} \\ Fan\{g^u, p\} \end{vmatrix} = \begin{vmatrix} (p+1)/p \\ (p^2-p-1)/(p.(p-1)) \end{vmatrix}$$

For p = 1 mod 8

$$\begin{vmatrix} Fan\{0,\ p\} \\ Fan\{g^{4u},\ p\} \\ Fan\{g.g^{4u},\ p\} \\ Fan\{g^2.g^{4u},\ p\} \\ Fan\{g^3.g^{4u},\ p\} \end{vmatrix} = \begin{vmatrix} (p-1)/p \\ (p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta)\ /(p.(p-1)) \\ (p^2-p+1-4\alpha.if(x_4>x_2,-1,1))\ /(p.(p-1)) \\ (p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta)\ /(p.(p-1)) \\ (p^2-p+1+4\alpha.if(x_4>x_2,-1,1))\ /(p.(p-1)) \end{vmatrix}$$

For p = 5 mod 8

$$\begin{vmatrix} Fan\{0,p\} \\ Fan\{g^{4u},\ p\} \\ Fan\{g.g^{4u},\ p\} \\ Fan\{g^2.g^{4u},\ p\} \\ Fan\{g^3.g^{4u},\ p\} \end{vmatrix} = \begin{vmatrix} (p-1)/p \\ (p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta)\ /(p.(p-1)) \\ (p^2-p+1+4\alpha.if(x_4>x_2,-1,1))\ /(p.(p-1)) \\ (p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta)\ /(p.(p-1)) \\ (p^2-p+1-4\alpha.if(x_4>x_2,-1,1))\ /(p.(p-1)) \end{vmatrix}$$

The changeover of cardinals for p = 1 mod 8 to those for p = 5 mod 8 depends on some changes of signs which have a subtle origin in $i^2 = -1$.
Thus :

$$Fan(0) = \prod_{p=1 \bmod 4} (1-1/p) \quad \prod_{p=3 \bmod 4} (1+1/p)$$

and

$$Fan(c \neq 0) = \prod_{p \setminus c} 1-(-1)^{(p-1)/2}/p \cdot \prod_{p \nmid c,\ p=3 \bmod 4} \left(1-\frac{1}{p.(p-1)}\right).\prod_{p \nmid c,\ p=1 \bmod 4,\ c=g^i.g^{4u}} \left(1+\frac{1+2a}{p.(p-1)}\right)$$

where $a = (-1)^{(p+3)/4+int(i/2)}.if(i \bmod 2 = 0, (-1)^{(\beta+1)/2}.\beta, 2\alpha.if(x_4>x_2,-1,1))$ and $p = (2\alpha)^2+\beta^2 \quad \alpha > 0,\ \beta > 0$.

We can explicit, thanks to the above relations, the abundance factors of a more general diophantine equation :

$$x_1^4+x_2^4 \ldots x_i^4+x_{i+1}^2+x_{i+2}^2 \ldots x_{i+j}^2 + y_1^4+y_2^4 \ldots y_k^4+y_{k+1}^2+y_{k+2}^2 \ldots y_{k+m}^2 = y+c$$

We have immediately :
For p = 2

$$\begin{vmatrix} \#\{c\} \end{vmatrix} = \begin{vmatrix} 2^{i+j-1} \end{vmatrix}$$

For p = 1 mod 4

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} = \begin{vmatrix} p^{i+j}.(p-1)^{k+m} \\ p^{i+j}.(p-1)^{k+m} \\ p^{i+j}.(p-1)^{k+m} \\ p^{i+j}.(p-1)^{k+m} \\ p^{i+j}.(p-1)^{k+m} \end{vmatrix} - [M1]^i.[M2]^j.([M1]-[I])^k.([M2]-[I])^m. \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix}$$

For p = 3 mod 4

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{2u}\} \\ \#\{g.g^{2u}\} \end{vmatrix} = \begin{vmatrix} p^{i+j}.(p-1)^{k+m} \\ p^{i+j}.(p-1)^{k+m} \\ p^{i+j}.(p-1)^{k+m} \end{vmatrix} - [M1]^i.[M2]^j.([M1]-[I])^k.([M2]-[I])^m. \begin{vmatrix} 1 \\ 0 \\ 0 \end{vmatrix}$$

Here [M1] and [M2] are respectively the matrix applying to the monomials x^4 and x^2 when cm = 4 that we got by taking account of the p modulo 8 congruencies. [I] is the identity matrix of size cm+1. It can be shown, in a general way, that adding the variable y in a diophantine equation is equivalent to subtract to $p^{i+j}.(p-1)^{k+m}$ the initially found cardinals with i, j, k and m the number of variables (overlapping or not) of the original equation. We used this result above. The use of the eigenvalues and eigenvectors of the matrices [M1], [M2], [M1]-[I] and [M2]-[I] of course simplifies the literal evaluation of this case which is left to the initiative of the reader.
To finish with, one ought to normalize the cardinals by a division by $p^{i+j-1}.(p-1)^{k+m}$.

4.6. The example of twin and cousin prime numbers

This corresponds simply to the equation

$$y_1-y_2 = c$$

We can use the preceding matrix [M0], which is the same for the variables y and -y. Thus :

$$\begin{vmatrix} \#\{0\} \\ \#\{g^u\} \end{vmatrix} = [M0]^2 \begin{vmatrix} 1 \\ 0 \end{vmatrix} = \begin{vmatrix} 0 & p-1 \\ 1 & p-2 \end{vmatrix}^2 \cdot \begin{vmatrix} 1 \\ 0 \end{vmatrix} = \begin{vmatrix} p-1 & (p-1).(p-2) \\ p-2 & p^2-3p+3 \end{vmatrix} \begin{vmatrix} 1 \\ 0 \end{vmatrix} = \begin{vmatrix} p-1 \\ p-2 \end{vmatrix}$$

Then (with $\delta = 1$) after normalization by $p/(p-1)^2$, we get

$$\begin{vmatrix} \text{Fan}\{c = 0 \bmod p,\ p\} \\ \text{Fan}\{c \neq 0 \bmod p,\ p\} \end{vmatrix} = \begin{vmatrix} p/(p-1) \\ p.(p-2)/(p-1)^2 \end{vmatrix}$$

That is also under the usual Euler product form :

$$\text{Fan}(c) = \prod_{p \nmid c} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \setminus c} \left(1 + \frac{1}{(p-1)}\right)$$

The usual formula holds only because the degree of stability, concept that we develop underneath, of the given diophantine equation is 1 (which is also the case with the Friedlander and Iwaniec equation).

5. Aggregation modulo p^{δ}

5.1. Degree of stability

Let us have R(x, y, …) = c a given diophantine equation. Let us calculate the (normalized) abundance factors of targets c modulo p^{δ} and modulo $p^{\delta+1}$ by forming multidimensional arrays whose axis are {{x}}, {{y}}... and collecting the cardinals for each c throughout the set [0, 1,..., p^{δ}-1] on the one hand and [0, 1,..., $p^{\delta+1}$-1] on the other hand.
If, for any target c,

$$\text{fan}_{(\delta+1)}(c \bmod p^{\delta}, p) = \text{fan}_{(\delta)}(c, p) \qquad (42)$$

that is, if the normalized abundance factors of target c do not evolve starting from rank δ, then rank δ is called the degree of stability of R(x, y, …). We will write it :

$$\delta s = \delta s(p) \qquad (43)$$

The degrees of stability depend on the sequences. If they are finite for all sequences p, the calculation of (normalized) abundance factor is obviously facilitated. If some or all are infinite, then often (if it is not possible to identify recurrent behaviour), the calculation of factor abundance may be impossible (this may also mean that asymptotic oscillation prevail and that a normalized factor does not exist).

The concept can be used for an independent group of variables within a diophantine equation. To each independent group will correspond its set of degrees of stability relative to the sequences). Put together (sums or differences, but not products), we seek at a given sequence the greatest common divisor of the degrees of stability of the existing independent groups. The new set of degrees of stability is thus composed by examining one by one all sequences (or rather sets of peculiar congruencies of the sequences).

An application of interest is the enumeration of an equation like

$$R(\ldots) = p + c \qquad (44)$$

where R(…) is any diophantine expression which does not contain variable p, p is a variable of prime numbers and c is a given constant (the target). The degree of stability of p is 1 and therefore the degree of stability of the whole equation c = R(…)-p is 1. It is then easy to do an approximate evaluation of the proportions between the numbers of solutions for different targets c on the bases of the first sequences.

Example

We choose here an example with overlapping variables on one hand sufficiently complicated so that the asymptotic behaviour cannot be guessed heuristically and on the other hand with relatively different results from a target to another (ratio of 1 to 2.35 here) so that we do not observe systematically only an average behaviour.
Let us thus have the diophantine expression $x^2+xy+y^2+u^3+2u^2v+uv^2+3v^3 = p+c$.
The factors of abundance are obtained by the composition of a multi-dimensional table which axes are x = [0,1,…,p_i], y = [0,1,…,p_i], u = [0,1,…,p_i], v = [0,1,…,p_i], -p = -[1,…,p_i] = [1,…,p_i]. We collect the occurrences of $c = x^2+xy+y^2+u^3+2u^2v+uv^2+3v^3-p$ modulo p_i.

seq \ c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	6	10	6	10	6	10	6	10	6	10	6	10	6	10	6	10
3	54	45	63	54	45	63	54	45	63	54	45	63	54	45	63	54
5	480	505	505	505	505	480	505	505	505	505	480	505	505	505	505	480
7	2016	2065	2065	2065	2065	2065	2065	2016	2065	2065	2065	2065	2065	2065	2016	2065
…																

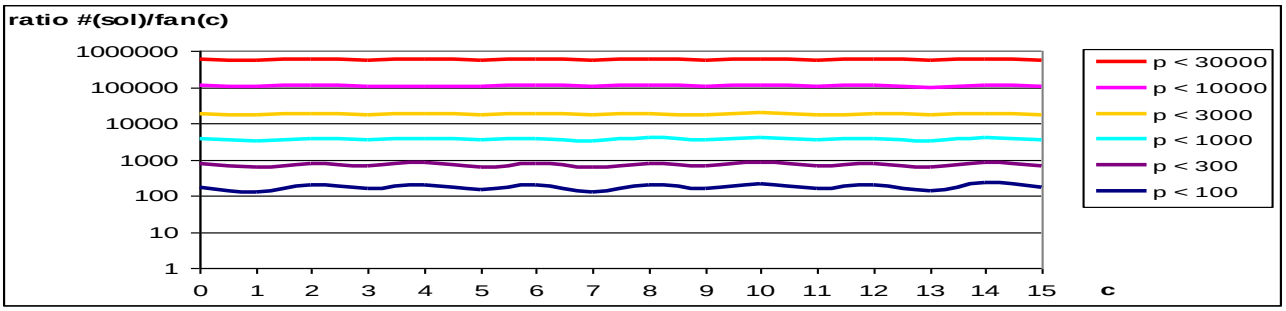
In this case, the $p_i = 2$ sequence shows the most decisive action on the asymptotic behaviour with a deficit of solutions for even targets and an excess for odd targets. Normalization to a given sequence p_i is obtained by dividing by $p_i^{4-1}.(p_i-1)^1$. The normalized abundance factors (modulo p_i) converge quite rapidly as we can see on the numerical evaluation up to sequence 31 :

seq \ c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
≤ 2	0,75	1,25	0,75	1,25	0,75	1,25	0,75	1,25	0,75	1,25	0,75	1,25	0,75	1,25	0,75	1,25
≤ 3	0,75	1,0417	0,875	1,25	0,625	1,4583	0,75	1,0417	0,875	1,25	0,625	1,4583	0,75	1,0417	0,875	1,25
≤ 5	0,72	1,0521	0,8838	1,2625	0,6313	1,4	0,7575	1,0521	0,8838	1,2625	0,6	1,4729	0,7575	1,0521	0,8838	1,2
≤ 7	0,7053	1,0557	0,8868	1,2668	0,6334	1,4048	0,7601	1,0306	0,8868	1,2668	0,602	1,4779	0,7601	1,0557	0,8657	1,2041
≤ 11	0,7111	1,0548	0,886	1,2657	0,6329	1,4036	0,7594	1,0298	0,886	1,2657	0,6015	1,4901	0,7594	1,0548	0,865	1,2031
≤ 13	0,7153	1,0506	0,8878	1,2682	0,6332	1,3981	0,7598	1,0303	0,8825	1,2664	0,6027	1,4931	0,7565	1,061	0,8616	1,2055
≤ 17	0,7153	1,0506	0,8878	1,2682	0,6332	1,3981	0,7598	1,0303	0,8825	1,2664	0,6027	1,4931	0,7565	1,061	0,8616	1,2055
≤ 19	0,7173	1,0503	0,8867	1,2667	0,6339	1,3963	0,7606	1,03	0,8823	1,2677	0,6034	1,4926	0,7562	1,0622	0,8605	1,2068
≤ 23	0,7173	1,0503	0,8867	1,2667	0,6339	1,3963	0,7606	1,03	0,8823	1,2677	0,6034	1,4926	0,7562	1,0622	0,8605	1,2068
≤ 29	0,7165	1,0503	0,8867	1,2667	0,6339	1,3964	0,7607	1,03	0,8823	1,2678	0,6034	1,4927	0,7563	1,0622	0,8606	1,2068
≤ 31	0,7165	1,0499	0,8864	1,2669	0,6337	1,3967	0,7608	1,0301	0,882	1,2681	0,6036	1,493	0,7564	1,0625	0,8607	1,2063

These factors will change little when one will go further towards infinite.
Let us find then the effective number of solutions (in the first quadrant) for the proposed equation varying the range of the values taken by p.

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p < 100	125	135	172	196	127	211	151	131	178	207	131	239	153	148	194	209
p < 300	550	620	696	819	518	884	569	622	696	855	505	961	574	642	714	826
p < 1000	2730	3412	3447	4365	2364	4758	2861	3342	3475	4468	2386	5019	2898	3510	3490	4339
p < 3000	13120	17222	16597	21742	11390	23658	13715	16923	16329	21707	11475	25131	13813	17639	16179	20871
p < 10000	78995	105677	96758	132925	68311	142761	82684	103290	96177	133207	66608	151487	82192	105836	94639	127254
p < 30000	410448	569761	507787	701271	359916	763551	431915	556091	504246	703569	346990	812793	429549	571233	494318	671832

To finish with, let us draw down the ratio of the number of solutions by the abundance factor for each target :



We observe when p increases that we tend towards a horizontal line, which is the awaited result.
Of course, the exact calculation needs whole evaluation of the Euler products which is also the subject of this article.

5.2. Cardinal matrix

As we saw earlier, in a general way, the cardinal matrix [C] of an independent group, (with k variables of integers and m variables of prime numbers), originates in the equation :

$$\text{card'}(i) = \sum_{j=0 \text{ à } n-1 = p^{\delta}.(p-1)-1} \#(i-j).\text{card}(j) \qquad (45)$$

Here #(i-j) are the components at (i,j) of a matrix with leads to the cardinal matrix.
Under this "non-contracted" form, the matrix is right circular :

$$[C] = [C(c_0,c_1, \ldots, c_{n-1})] = \begin{vmatrix} c_0 & c_n & \ldots & c_1 \\ c_1 & c_0 & \ldots & c_2 \\ \ldots & \ldots & \ldots & \ldots \\ c_n & c_3 & \ldots & c_0 \end{vmatrix} \qquad (46)$$

The melting of the targets with identical cardinals, the sorting of the $\#(p^w.g^v.g^{u.cm})$ with ascending v and decreasing w supplies then the expected cardinal matrix.

5.3. Environment matrix

The determinant of matrix [C] is given by :

$$\mathrm{Det}([C]) = \prod_{v=0}^{n-1} \sum_{t=0}^{n-1} c_t.e^{-2\pi i.t.v/n} \qquad (47)$$

with eigenvalues, when taking $[CI_t] = [C(c_0 = 0, \ldots, c_{t-1} = 0, c_t = 1, c_{t+1} = 0, \ldots, c_{n-1} = 0)]$, the components of the trace matrix (v = 0 to n-1) :

$$\sum c_t.[e^{-2\pi i.t.v/n}] \qquad (48)$$

and with eigenvectors matrix (change of base matrix), the special unitary complex group of dimension n ($SU_n(\partial)$) :

$$[P] = (1/n^{1/2}).\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & (e^{2\pi i/n})^{.1} & (e^{2\pi i/n})^{.1.2} & \ldots & (e^{2\pi i/n})^{.1.(n-1)} \\ 1 & (e^{2\pi i/n})^{.2} & (e^{2\pi i/n})^{.2.2} & \ldots & (e^{2\pi i/n})^{.2.(n-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & (e^{2\pi i/n})^{.(n-1)} & (e^{2\pi i/n})^{.(n-1).2} & \ldots & (e^{2\pi i/n})^{.(n-1).(n-1)} \end{vmatrix} \qquad (49)$$

This matrix or equivalent matrix can be used as <u>common</u> change of base matrix. The identical cardinals targets grouping, the sorting of the $\#(p^w.g^v.g^{u.cm})$ with ascending v and decreasing w (or another order) causes the rearrangement of this matrix and of its inverse exactly in the same way (for a given order) for a given environment cm. Hence the existence of a common environment matrix.

5.4. Eigenvalues

Eigenvalues obey a scheme requiring only to research cm values :

$$p^{\delta}, p^{\delta-1}[\sigma_1], p^{\delta-1}[\sigma_2], \ldots, p^{\delta-1}[\sigma_{cm}], p^{\delta-2}[\sigma_1], p^{\delta-2}[\sigma_2], \ldots, p^{\delta-2}[\sigma_{cm}]\ldots$$

where $\sigma_1, \sigma_2, \ldots, \sigma_{cm}$ are the eigenvalues of the modulo p cardinal matrix that are obtained by the products of the independent variables groups eigenvalues, since when forming operations like $\prod [P].[\sigma].[P^{-1}]$ the products $[P^{-1}].[P]$ vanish.

6. Multiplication by an integer constant

The introduction of negative constants shapes effectively asymptotic character to a diophantine equation with a finite target c. We are concerned for example with enumerations in the case of the equations $a_1x_1^n + a_2x_2^n + \ldots + a_kx_k^n = c \bmod p$ or $a_1y_1^n + a_2y_2^n + \ldots + a_my_m^n = c \bmod p$.

Let us have d = (n, p-1). We start with following remarks. If a divides p, then $a = 0 \bmod p$ and $a.x^n = 0 \bmod p$. The abundance factors are then all null except for c = 0 with #{0} = p (or p-1 in the case $a.y^n = 0 \bmod p$). If a does not divide p, then there is i (i < d) and j such as $a = g^i.g^{j.d}$, thus $a.x^n = g^i.g^{j.d}.x^n \bmod p$. This enables us then to proceed to the usual method of two-dimensional tables with an, below illustrated, adequate correction.
For the first line, the incidence of $a = g^i.g^{j.d}$ is null (a.0 = 0). For the other lines, if $c = g^{u.d} + g^j.g^{v.d}$, then $g^i.c = g^i.g^{u.d} + g^i.g^j.g^{v.d}$, which means exactly preceding example result. Let us have thus for a variable of integers (respectively a variable of prime numbers), u varying in the usual field of definition 0 to (p-1)/d-1 :

$$\begin{vmatrix} \mathrm{card'}_0 \\ \mathrm{card'}\{g^i.g^{u.d}\} \\ \mathrm{card'}\{g^{i+1}.g^{u.d}\} \\ \ldots \\ \mathrm{card'}\{g^{i+d-1}.g^{u.d}\} \end{vmatrix} = \begin{vmatrix} \\ [A] \text{ (or } [B]) \\ \\ \\ \\ \end{vmatrix} \begin{Vmatrix} \mathrm{card}_0 \\ \mathrm{card}\{g^i.g^{u.d}\} \\ \mathrm{card}\{g^{i+1}.g^{u.d}\} \\ \ldots \\ \mathrm{card}\{g^{i+d-1}.g^{u.d}\} \end{Vmatrix}$$

In addition, by a trace vector of [I] shift of i columns, except for the first component, we have

$$\begin{vmatrix} \mathrm{card}_0 \\ \mathrm{card}\{g^i.g^{u.d}\} \\ \mathrm{card}\{g^{i+1}.g^{u.d}\} \\ \mathrm{card}\{g^{i+2}.g^{u.d}\} \\ \mathrm{card}\{g^{i+3}.g^{u.d}\} \\ \ldots \\ \mathrm{card}\{g^{i+d-1}.g^{u.d}\} \end{vmatrix} = \left|\begin{array}{ccccccc} 1 & 0 & \ldots & \ldots & & 0 \\ \hline 0 & 0 \rightarrow & 1 & & & \\ & 0 & & 1 & & \\ \ldots & & 0 & & \ldots & \\ \ldots & & & 0 & & 1 \\ & & & & \ldots & \\ 0 & 1 & & & & 0 \end{array}\right| \begin{Vmatrix} \mathrm{card}_0 \\ \mathrm{card}\{g^0.g^{u.d}\} \\ \mathrm{card}\{g^1.g^{u.d}\} \\ \mathrm{card}\{g^2.g^{u.d}\} \\ \mathrm{card}\{g^3.g^{u.d}\} \\ \ldots \\ \mathrm{card}\{g^{d-1}.g^{u.d}\} \end{Vmatrix}$$

In the same way, by a shift of -i columns, we have

$$\begin{vmatrix} card'_0 \\ card' \{g^0.g^{u.d}\} \\ card' \{g^1.g^{u.d}\} \\ card' \{g^2.g^{u.d}\} \\ card' \{g^3.g^{u.d}\} \\ \dots \\ card' \{g^{d-1}.g^{u.d}\} \end{vmatrix} = \left|\begin{array}{c|ccccc} 1 & 0 & \dots & \dots & 0 \\ \hline 0 & 0 & & & 1 \\ & \downarrow & 0 & & \\ \dots & 1 & & 0 & \\ \dots & & 1 & & 0 \\ & & & \dots & \dots \\ 0 & & & 1 & 0 \end{array}\right| \begin{vmatrix} card'_0 \\ card' \{g^i.g^{u.d}\} \\ card' \{g^{i+1}.g^{u.d}\} \\ card' \{g^{i+2}.g^{u.d}\} \\ card' \{g^{i+3}.g^{u.d}\} \\ \dots \\ card' \{g^{i+d-1}.g^{u.d}\} \end{vmatrix}$$

Thus :

$$\begin{vmatrix} card'_0 \\ card' \{g^0.g^{u.d}\} \\ card' \{g^1.g^{u.d}\} \\ card' \{g^2.g^{u.d}\} \\ card' \{g^3.g^{u.d}\} \\ \dots \\ card' \{g^{d-1}.g^{u.d}\} \end{vmatrix} = \left|\begin{array}{c|ccccc} 1 & 0 & \dots & \dots & 0 \\ \hline 0 & 0 & & & 1 \\ & 0 & & & \\ \dots & 1 & 0 & & \\ \dots & & 1 & 0 & \\ & & \dots & \dots & \\ 0 & & & 1 & 0 \end{array}\right| [A] \text{ (or [B])} \left|\begin{array}{c|ccccc} 1 & 0 & \dots & \dots & 0 \\ \hline 0 & 0 & 1 & & \\ & 0 & & 1 & \\ \dots & & 0 & & \dots \\ \dots & & & 0 & 1 \\ & & & & \dots \\ 0 & 1 & & & 0 \end{array}\right| \begin{vmatrix} card_0 \\ card \{g^0.g^{u.d}\} \\ card \{g^1.g^{u.d}\} \\ card \{g^2.g^{u.d}\} \\ card \{g^3.g^{u.d}\} \\ \dots \\ card \{g^{d-1}.g^{u.d}\} \end{vmatrix} \quad (50)$$

The product of three matrices gives the desired transformation.

$$\begin{vmatrix} \\ [A'] \text{ (or [B'])} \\ \\ \\ \\ \end{vmatrix} = \left|\begin{array}{c|ccccc} 1 & 0 & \dots & \dots & 0 \\ \hline 0 & 0 & & & 1 \\ & 0 & & & \\ \dots & 1 & 0 & & \\ \dots & & 1 & 0 & \\ & & \dots & \dots & \\ 0 & & & 1 & 0 \end{array}\right| \left\|\begin{array}{c|ccccc} 1 & 0 & \dots & \dots & 0 \\ \hline 0 & 0 & 1 & & \\ & 0 & & 1 & \\ \dots & & 0 & & \dots \\ \dots & & & 0 & 1 \\ & & & & \dots \\ 0 & 1 & & & 0 \end{array}\right\| [A] \text{ (or [B])}$$

For $a_1x_1^n + a_2x_2^n + \dots + a_kx_k^n = c \bmod p$, respectively $a_1y_1^n + a_2y_2^n + \dots + a_my_m^n = c \bmod p$, we determine abundance factors by matrices products :

$$[A'] = [A_1'].[A_2'] \dots [A_k']$$
and
$$[B'] = [B_1'].[B_2'] \dots [B_m']$$

Let us notice that these matrices commute.
In addition, combinations of integers and prime numbers variables are welcome.

The permutation matrices commute also with the change of base matrices of the cardinal matrices. This means that the multiplication by a constant will translate to a permutation of the eigenvalues (in the matrix of the eigenvalues). Finally, the transition from $a.z^n$ à $-az^n$ is equivalent to a permutation of the eigenvalues (outside of the one corresponding to 0 which stays at its place) by translating indexes by a modulo (p-1)/2 step (since $-1 = g^{(p-1)/2} \bmod cm$).

7. Equations with overlapping variables

To solve a diophantine equation with more complex groups involved (for example $u.x^2+v.x.y+w.y^2$), it is necessary to determine the corresponding specific matrices and find the common environment. Specific rules governing these aggregates, although already addressed (see degrees of stability), are still to be bettered. When the sums of degrees are homogeneous for each independent group (as here the degree 2 respectively for x^2, xy and y^2), the situation can usually be adressed modulo p^δ, with finite δ, and δ the lowest common multiple of the degrees of the whole equation.
As an example, we have for the cardinal matrices of $u.x_1^2+v.x_1.x_2+w.x_2^2$ and its eigenvalues (the proof will be left aside here) in the case of $\Delta = v^2-4uw$ a non-square modulo p ($\Delta \neq 0 \bmod p$) :

δ = 1

$$\begin{vmatrix} 1 & (p-1)(p+1) \\ p+1 & p^2-p-1 \end{vmatrix} \begin{vmatrix} \mu q_0 \\ \mu q_1 \end{vmatrix} = \begin{vmatrix} p^2 \\ -p \end{vmatrix}$$

δ = 2

$$\begin{vmatrix} p^2 & 0 & (p-1).p.p.(p+1) \\ 0 & p.(p) & (p-1).p.p.(p+1) \\ p.(p+1) & (p-1).p.(p-1) & p^2.(p^2-p-1) \end{vmatrix} \begin{vmatrix} \mu q_0 \\ \mu q_1 \\ \mu q_2 \end{vmatrix} = \begin{vmatrix} p^4 \\ -p^3 \\ p^2 \end{vmatrix}$$

δ = 3

$$\begin{vmatrix} p^2 & (p-1).p^2.(p+1) & 0 & (p-1).p^2.p^2.(p+1) \\ p^2.(p+1) & p^2.(p^2-p-1) & 0 & (p-1).p^2.p^2.(p+1) \\ 0 & 0 & P^3.(p) & (p-1).p^2.p^2.(p+1) \\ p^2.(p+1) & (p-1).p^2.(p+1) & (p-1).p.p^2.(p+1) & p^4.(p^2-p-1) \end{vmatrix} \begin{vmatrix} \mu q_0 \\ \mu q_1 \\ \mu q_2 \\ \mu q_3 \end{vmatrix} = \begin{vmatrix} p^6 \\ -p^5 \\ p^4 \\ -p^3 \end{vmatrix}$$

$\delta = 4$

$$\begin{vmatrix} p^4 & 0 & (p-1).p.p^3.(p+1) & 0 & (p-1).p^3.p^3.(p+1) \\ 0 & p^3.(p) & (p-1).p.p^3.(p+1) & 0 & (p-1).p^3.p^3.(p+1) \\ p^3.(p+1) & (p-1).p^3.(p+1) & p^4.(p^2-p-1) & 0 & (p-1).p^3.p^3.(p+1) \\ 0 & 0 & 0 & p^5.(p) & (p-1).p^3.p^3.(p+1) \\ p^3.(p+1) & (p-1).p^3.(p+1) & (p-1).p.p^3.(p+1) & (p-1).p^2.p^3.(p+1) & p^6.(p^2-p-1) \end{vmatrix} \begin{vmatrix} \mu q_0 \\ \mu q_1 \\ \mu q_2 \\ \mu q_3 \\ \mu q_4 \end{vmatrix} = \begin{vmatrix} p^8 \\ -p^7 \\ p^6 \\ -p^5 \\ p^4 \end{vmatrix}$$

$\delta = 5$

$$\begin{vmatrix} p^4 & (p-1).p^4.(p+1) & 0 & (p-1).\ p^2.p^4.(p+1) & 0 & (p-1).p^4.p^4.(p+1) \\ p^4.(p+1) & p^4.(p^2-p-1) & 0 & (p-1).\ p^2.p^4.(p+1) & 0 & (p-1).p^4.p^4.(p+1) \\ 0 & 0 & p^5.(p) & (p-1).\ p^2.p^4.(p+1) & 0 & (p-1).p^4.p^4.(p+1) \\ p^4.(p+1) & (p-1).p^4.(p+1) & (p-1).p.p^4.(p+1) & p^6.(p^2-p-1) & 0 & (p-1).p^4.p^4.(p+1) \\ 0 & 0 & 0 & 0 & p^7.(p) & (p-1).p^4.p^4.(p+1) \\ p^4.(p+1) & (p-1).p^4.(p+1) & (p-1).p.p^4.(p+1) & (p-1).p^2.p^4.(p+1) & (p-1).p^3.p^4.(p+1) & p^8.(p^2-p-1) \end{vmatrix} \begin{vmatrix} \mu q_0 \\ \mu q_1 \\ \mu q_2 \\ \mu q_3 \\ \mu q_4 \\ \mu q_5 \end{vmatrix} = \begin{vmatrix} p^8 \\ -p^7 \\ p^6 \\ -p^5 \\ p^4 \\ -p^3 \end{vmatrix}$$

It is easy to anticipate (jumping one step $\delta \rightarrow \delta+2$) the general form of the matrices and especially that of the eigenvalues when δ increases in these examples. When Δ is a square modulo p, but $\Delta \neq 0 \bmod p$, eigenvalues remain identical except signs which are always positive. The $\Delta = 0 \bmod p$ case is more fancy.
According to the value cm, one needs to choose one or the other of these matrices and sets of eigenvalues.

8. Intégration et dérivation

8.1. Enumeration in a volume

So far, we had attention only for what we called in the preamble the constant based on an Euler infinite product. Thanks to that factor, we can compare the number of solutions of $R(x, y, \ldots) = c$ and $R(x, y, \ldots) = c-1$ and step by step those in the $R(x, y, \ldots) \leq c$ volume. Surfaces (for the equalities) and volume (for the inequality) are always <u>infinite</u> in our (asymptotic) cases and we will note that c may take any positive, null or negative value. The step by step will not meet any exception. In peculiar, the target $c = 0$ case is not a limit case but one among the other ones.
We must now consider the rest of the formula that we will get by multiple integrations [4]. The ability to effectively conduct such integrations seriously limits the field of literal formulas one can get. Generally, the first condition will be having an equation with separated or separable variables (for quadratic equations, variables are not separated but are separable). Furthermore, we use the fact that asymptotically a polynomial is equivalent to its dominant term.

Note that if no literal formula is found, we may just look on the divergence or not of the solutions. This point is not studied here.

Let us have a set of polynomials all crescents, such as:

$$\sum_{n=1}^{i} P_n(x_n) + \sum_{n=1}^{j} Q_n(y_n) \leq c + \sum_{n=1}^{k} R_n(z_n) + \sum_{n=1}^{m} S_n(t_n) \qquad (51)$$

The number of meshes (solutions) in the non-limited volume can be written then, x_n and z_n being variables of integers and y_n et t_n variables of prime numbers, as :

$$\int_0^{z_1} \int_0^{z_k} \int_2^{t_1} \int_2^{t_m} \int_0^{x_1 = P_1^{-1}(c+\sum R_n(z_n)+\sum S_n(t_n))} \cdots \int_2^{y_j = Q_j^{-1}(c-2+\sum R_n(z_n)+\sum S_n(t_n))-\sum P_n(x_n)-\sum Q_n(y_n)))} \frac{dy_1 \ldots dy_j.dt_1 \ldots dt_m \,.\, dx_1 \ldots dx_i.dz_1 \ldots dz_k}{Ln(y_1)\ldots Ln(y_j).Ln(t_1)...Ln(t_m)} \qquad (52)$$

We thus get a volume in the form $V(c, z_1, \ldots, z_k, t_1, \ldots, t_m)$, instead of $V(c)$, including only the variables on the right inequality. We will make tend the variables $z_1, \ldots, z_k, t_1, \ldots, t_m$ towards infinite for the asymptotic enumerations. Of course, as we said earlier, we should replace the polynomials in the integral by the dominant terms (that is when $P(x) \equiv a.x^n$ by $P^{-1}(x) \equiv (x/a)^{1/n}$).

8.2. Average enumeration on the surface of a volume

Let us rewrite the inequality as $R(x_1, \ldots, x_k, y_1, \ldots, y_j, z_1, \ldots, z_k, t_1, \ldots, t_m) \leq c$ with corresponding volume $V(c, z_1, \ldots, z_k, t_1, \ldots, t_m)$. In the enumeration point of view, expression $R(\ldots)$ and variables x_i, y_i, z_i, t_i being given initially, the only parameter of the problem is c. Let us have then :

$$R(x_1, \ldots, x_k, y_1, \ldots, y_j, z_1, \ldots, z_k, t_1, \ldots, t_m) = c$$

The number of potential solutions of this equality is :

$$V(c, z_1, \ldots, z_k, t_1, \ldots, t_m) - V(c-1, z_1, \ldots, z_k, t_1, \ldots, t_m)$$

This operation must be carried out with constant variables z_1, …, z_k, t_1, …, t_m and leads at first approximation to the partial derivative with respect to c :

$$V'(c, z_1, \ldots, z_k, t_1, \ldots, t_m)$$

The asymptotic solution is obtained afterwards while tending the variables z_1, …, z_k, t_1, …, t_m towards infinite (what often makes c negligible in the literal formula we get).

8.3. Balanced enumeration

To finish with, the preceding enumeration has to be corrected with adapted weightings so that the sum of all the enumerations for successive targets in interval]-∞, c] will give back volume V(c). The average weighting in interval]-∞,c] must thus be 1. We realised that in paragraph 2 and we called the resulting weighting factor the normalized abundance factor Fan(c). Thus :

$$\#\{R(\ldots) = c\} \equiv Fan(c).(V'(c)+O(c)) \approx Fan(c).V'(c)$$

8.4. The logarithmic wall-through

We carry out the development by integral parts (u = F(t) where F is the primitive of the function f, an integrable function (in general a polynomial), $v = Ln^n(t)$, $u' = f(t)$, $v' = n.Ln^{n-1}(t)/t$) :

$$\int f(t).Ln^n(t)dt = [F(t).Ln^n(t)] - n.\int f(t)Ln^{(n-1)}(t)dt$$

Then, we can write the succession of equalities :

$$\int f(t).Ln^{n-1}(t)dt = [F(t).Ln^{n-1}(t)] - (n-1).\int f(t)Ln^{(n-1)}(t)dt$$

$$\int f(t).Ln^{n-2}(t)dt = [F(t).Ln^{n-2}(t)] - (n-2).\int f(t)Ln^{(n-2)}(t)dt \qquad \text{and so on …}$$

By successive eliminations between the last term of these expressions and the first term of the following expression multiplied by the adequate factor, it follows :

$$\int f(t).Ln^n(t)dt = [F(t).Ln^n(t)]\left(1- \frac{n}{Ln(t)} + \frac{n(n-1)}{Ln^2(t)} - \frac{n(n-1)(n-2)}{Ln^3(t)} \ldots\right)$$

If n is null, the expression does not include logarithms and does not interest us here. If n is a positive integer, the development admits a finite or infinite number of terms, pending on f(t). In these two cases however :

$$\int f(t).Ln^n(t)dt = [F(t).Ln^n(t)]\,(1+o(1))$$

So that :

$$\int^c f(t).Ln^n(t)dt = [F(t).Ln^n(t)]^{t=c}.(1+o(1)) \qquad (53)$$

We get while tending c towards infinite :

$$\lim_{c\to\infty} \int^c f(t).Ln^n(t)dt = \lim_{c\to\infty} Ln^n(c) \cdot \lim_{c\to\infty} F(c) \qquad (54)$$

Thus :

$$\text{Lim}_{c\to\infty} \int^c f(t).Ln^n(t)dt = \lim_{c\to\infty} Ln^n(c) \lim_{c\to\infty} \int^c f(t)dt \qquad (55)$$

This expression shows again that logarithms can be extracted from integrals taking value of the divergent upper boundary of this integral. In the practical use of the previous result, there should be no singular points neither for f(t), nor for ln(t) in the interval of integration. In particular, the replacement of the indefinite boundary by a definite boundary c_0 should not involve a divergence (hence $c_0 = 2$ in general).

9. Applications to enumerations

9.1. Monomial with unit coefficients, in a limited volume

We will first discuss the problem of diophantine equation solutions enumeration in the case of variables of positive integers for a given target c :

$$x_1^{(1)} + x_2^{(2)} + \ldots + x_k^{(k)} = c \qquad (56)$$

Here the exponent of x_i is not equal to i but a positive integer noted (i). The above equation has asymptotic character when c tends towards infinity. We do write first

$$x_1^{(1)} + x_2^{(2)} + \ldots + x_k^{(k)} \leq c \qquad (57)$$

whose enumeration is given by:

$$V(c) = \int_0^{x_1 = c^{(1/(1))}} \int_0^{x_2 = (c-x_1^{(1)})^{(1/(2))}} \int_0^{x_3 = (c-x_1^{(1)}-x_2^{(2)})^{(1/(3))}} \ldots\ldots \int_0^{x_k = (c-x_1^{(1)}-x_2^{(2)}-\ldots-x_{k-1}^{(k-1)})^{(1/(k))}} 1.dx_k dx_{k-1}\ldots dx_1$$

This integral is with separable variables and can be solved into a product of simple integrals. To get the expression of this integral, we study first the following one :

$$I = \int_0^{x_i = (c+r(x)-x_{i-1}^{(i-1)})^{(1/(i))}} (c+r(x)-x_{i-1}^{(i-1)}-x_i^{(i)})^{(m)}\, dx_i \qquad (58)$$

The variable of this expression is x_i and r(x) do not depend on this variable (all x_i's are independent variables) and can be seen briefly as a constant. Adopting the change of variable $z = x_i/(c+r(x)-x_{i-1}^{(i-1)})^{(1/(i))}$, we get $dz = dx_i/(c+r(x)-x_{i-1}^{(i-1)})^{(1/(i))}$, so that $dx_i = (x_i/z)dz$. Moreover $(c+r(x)-x_{i-1}^{(i-1)}-x_i^{(i)})^{(m)} = ((x_i/z)^{(i)}-x_i^{(i)})^{(m)} = ((x_i/z)^{(i)(m)}(1-z^{(i)})^{(m)}$.
Then

$$I = \int_{z=0}^{z=1} (x_i/z)\,((x_i/z)^{(i)(m)}(1-z^{(i)})^{(m)}\, dz = (x_i/z)^{((i)(m)+1)} \int_{z=0}^{z=1} (1-z^{(i)})^{(m)}\, dz = (c+r(x)-x_{i-1}^{(i-1)})^{((m)+1/(i))} \int_{z=0}^{z=1} (1-z^{(i)})^{(m)}\, dz$$

It is clear that the successive use of this relationship in the multiple integral will give, step by step, a product of simple integrals as follows :

Step	1	2	3	…	k
(i)	(k)	(k-1)	(k-2)		(1)
(m)	0	1/(k)	1/(k) + 1/(k-1)		1/(k) + 1/(k-1) +…+1/(2)

Thus :

$$V(c) = c^{(1/(k)+1/(k-1)+\ldots+1/(2)+1/(1))} \int_0^1 (1-t^{(1)})^{(1/(k)+1/(k-1)+\ldots+1/(2))}\, dt \quad \ldots \quad \int_0^1 (1-t^{(k-2)})^{(1/(k)+1/(k-1))}\, dt \int_0^1 (1-t^{(k-1)})^{(1/(k))}\, dt \int_0^1 (1-t^{(k)})^{(0/(k))}\, dt \qquad (59)$$

The derivative results easily :

$$V'(c) = (1/(k)+\ldots+1/(2)+1/(1))c^{1/(k)+\ldots+1/(2)+1/(1)-1} \int_0^1 (1-t^{(1)})^{(1/(k)+\ldots+1/(2))}dt \ldots \int_0^1 (1-t^{(k-2)})^{(1/(k)+1/(k-1))}dt \int_0^1 (1-t^{(k-1)})^{(1/(k))}dt \qquad (60)$$

The divergence condition for V'(c) is :

$$1/(k)+1/(k-1)+\ldots+1/(2)+1/(1) > 1 \qquad (61)$$

The preceding expressions can be also written as Γ functions. For that, let us proceed first to the change of variable $z = t^{(i)}$, so that $dz = (i).t^{(i)-1}dt$, then :

$$\int_0^1 (1-t^{(i)})^{(1/(k)+1/(k-1)+\ldots+1/(i+1))}dt = 1/(i) \int_0^1 z^{(1/(i)-1)}.(1-z)^{(1/(k)+1/(k-1)+\ldots+1/(i+1))}\, dz$$

Let us recall the identities for beta and gamma functions :

$$\int_0^1 (z)^{b-1}.(1-z)^{a-1}\,dz = B(a,b) = \Gamma(a).\Gamma(b)/\Gamma(a+b) \qquad (62)$$

Identification of couples (a, b) gives :

$$(a,b) = (1/(k)+1/(k-1)+\ldots+1/(i+1)+1,1/(i))$$

Then

$$\prod_{i=1}^{k} I(n,i) = \prod_{i=1}^{k} (1/(i)).B(1/(k)+1/(k-1)+\ldots+1/(i+1)+1,1/(i)) \qquad (63)$$

After mutual elimination of Γ expressions in numerator and denominator, we will get :

$$\prod_{i=1}^{k} I(n,i) = (\prod_{i=1}^{k} (1/(i))).(\prod_{i=1}^{k} \Gamma(1/(i))) / \Gamma(1/(k)+1/(k-1)+\ldots+1/(1)+1) \qquad (64)$$

Thus using gamma function factorisation property $\Gamma(x+1) = x.\Gamma(x)$, we get (here (i) describes all the values (1) to (k)) :

$$V(c) = \frac{\prod_{(i)} \Gamma(1+\frac{1}{(i)})}{\Gamma(1+\sum_{(i)} \frac{1}{(i)})} c^{\sum_{(i)}(\frac{1}{(i)})} \qquad (65)$$

and :

$$V'(c) = \sum_{(i)}(\frac{1}{(i)}).\frac{\prod_{(i)} \Gamma(1+\frac{1}{(i)})}{\Gamma(\sum_{(i)} \frac{1}{(i)})} c^{-1+\sum_{(i)}(\frac{1}{(i)})} \qquad (66)$$

In the interest of simplification of entries, we write down :

$$cti = \frac{\prod_{(i)} \Gamma(1+\frac{1}{(i)})}{\Gamma(1+\sum_{(i)} \frac{1}{(i)})} \qquad (67)$$

and

$$sti = \sum_{(i)}(\frac{1}{(i)}) \qquad (68)$$

9.2. Monomial with unit coefficients, in an unlimited volume

We now address the problem of diophantine equations solutions enumeration (x_i positive integers) of

$$x_1^{(1)} + x_2^{(2)} +\ldots+ x_k^{(k)} = c + x_{k+1}^{(k+1)} \qquad (69)$$

and of

$$x_1^{(1)} + x_2^{(2)} +\ldots+ x_k^{(k)} \leq c + x_{k+1}^{(k+1)} \qquad (70)$$

The enumeration of the inequality satisfies to the integral :

$$V(c) = \int_0^{x_{k+1}} V_k(c).dx_{k+1} \qquad (71)$$

where according with previous study

$$V_k(c) = (c+x_{k+1}^{(k+1)})^{(1/(k)+1/(k-1)+\ldots+1/(2)+1/(1))} \int_0^1 (1-t^{(1)})^{(1/(k)+1/(k-1)+\ldots+1/(2))}\,dt \quad \ldots \int_0^1 (1-t^{(k-2)})^{(1/(k)+1/(k-1))}\,dt \int_0^1 (1-t^{(k-1)})^{(1/(k))}\,dt \int_0^1 (1-t^{(k)})^{(0/(k))}\,dt$$

So that simply :

$$V_k(c) = cti.(c+x_{k+1}^{(k+1)})^{sti}$$

Then :

$$V(c) = cti. \int_0^{x_{k+1}} (c+x_{k+1}^{(k+1)})^{sti}\,.dx_{k+1}$$

and deriving inside the integral with respect of c :

$$V'(c) = cti.sti. \int_0^{x_{k+1}} (c+ x_{k+1}^{(k+1)})^{sti-1}.dx_{k+1}$$

Asymptotically, c is negligible, thus:

$$V(c) = cti. \int_0^{x_{k+1}} x_{k+1}^{(k+1).sti} .dx_{k+1}$$

and :

$$V'(c) = cti.sti. \int_0^{x_{k+1}} x_{k+1}^{(k+1).(sti-1)}.dx_{k+1}$$

Then :

$$V(c) = (cti/((k+1).sti+1)).x_{k+1}^{(k+1).sti+1}$$

and

$(k+1).(sti-1) \neq -1$	$V'(c) = (cti.sti/((k+1).(sti-1)+1)).x_{k+1}^{(k+1).(sti-1)+1}$
$(k+1).(sti-1) = -1$	$V'(c) = cti.sti.\ln(x_{k+1})$

9.3. Affine monomials

We focus now on the enumeration of relatively general diophantine equation, namely :

$$a_{x1}.x_1^{(x1)} + a_{x2}.x_2^{(x2)} +\ldots+ a_{xk}.x_k^{(xk)} + a_{y1}.y_1^{(y1)} + a_{y2}.y_2^{(y2)} +\ldots+ a_{ym}.y_m^{(ym)} = c + a_{zr}.z_r^{(zr)} \qquad (72)$$

We simply use the following techniques :
- We divide by a_{zr} the two members of the equation.
- We make the changes of variables $X_k^{(xk)} = (a_{xk}/a_{zr}).x_k^{(xk)}$, so that $x_k = (a_{xk}/a_{zr})^{(1/(xk))}.X_k$ for each variable except z_r.
- We pose :

$$a^{k+m} = \prod_i \left(\frac{a_{zr}}{a_{xi}}\right)^{1/(xi)}. \prod_j \left(\frac{a_{zr}}{a_{yj}}\right)^{1/(yj)} \qquad (73)$$

and

$$ctxy = \frac{\prod_{i \text{ describes (xi) et (yj)}} \Gamma(1+\frac{1}{i})}{\Gamma(1+\sum_{i \text{ describes (xi) et (yj)}} \frac{1}{i})} \qquad (74)$$

and

$$stxy = \sum_{i \text{ describes (xi) et (yj)}} \frac{1}{i} \qquad (75)$$

In addition, for variables of prime numbers, we must handle integral of the type

$$I = \int_2^{Y_i = (c/a_{zr}+z_r^{(zr)}-r(X,Y))^{(1/(yi))}} ((c/a_{zr}+z_r^{(zr)}-r(X,Y)-Y_i^{(yi)})^{(m)})/Ln((c/a_{zr}+z_r^{(zr)}-r(X,Y))^{(1/(yi))}).dY_i \qquad (76)$$

The logarithm extraction, when Y_i tends towards infinite, give using the wall-trough remark :

$$I \equiv (1/Ln(e.(c/a_{zr}+z_r^{(zr)})^{(1/(yi))})) \int_2^{Y_i = (c+a_{zr}.z_r^{(zr)}-r(X,Y))^{(1/(yi))}} (c/a_{zr}+z_r^{(zr)}-r(X,Y)-Y_i^{(yi)})^{(m)}\, dY_i \qquad (77)$$

with

$$(1/Ln(e.(c/a_{zr}+z_r^{(zr)})^{(1/(yi))}) = <a>/Ln((c/a_{zr}+z_r^{(zr)})^{(1/(yi))}) \approx <a>/Ln((z_r^{(zr)})^{(1/(yi))}) = <a>/(((zr)/(yi)).Ln(z_r))$$

where e is comprised in interval]0,1[, <a> tends towards 1 when z_r tends towards infinite (c finite and (zr) and (yi) are the exponents of the variables z_r and y_i).
We pose thus in addition :

$$clny = \prod_i \left(\frac{(zr)}{(yi)}\right) = (zr)^m.\prod_i \left(\frac{1}{(yi)}\right) \qquad (78)$$

and it follows two cases.

Case z_r is a variable of integers

$$V(c) = (a^{k+m}.ctxy/(clny.\ln^m(z_r))).\int_0^{z_r}(c/a_{zr}+z_r^{(zr)})^{stxy}.dz_r$$

So that (by neglecting c in front of z_r which tends to ∞) :

$$V(c) = \frac{a^{k+m}.ctxy.}{((zr).stxy+1)).clny}.\frac{z_r^{((zr).stxy+1)}}{\ln^m(z_r)} \qquad (79)$$

Moreover, by derivation inside the integral:

$$V'(c) = (a^{k+m}.ctxy/(clny.\ln^m(z_r))).\int_0^{z_r}((c/a_{zr}+z_r^{(zr)})^{stxy})'.dz_r$$

So that :

$$V'(c) = (a^{k+m}/a_{zr}).(stxy.ctxy/(clny.\ln^m(z_r))).\int_0^{z_r}(c/a_{zr}+z_r^{(zr)})^{stxy-1}.dz_r$$

Then by neglecting c asymptotically :

$$V'(c) = (a^{k+m}/a_{zr}).(stxy.ctxy/\ln^m(z_r)).\int_0^{z_r}z_r^{(zr).(stxy-1)}.dz_r$$

So that :

$if(zr).(stxy-1) \neq -1$	$V'(c) = \frac{a^{k+m}.stxy.ctxy}{a_{zr}.((zr).(stxy-1)+1).clny}.\frac{z_r^{(zr).(stxy-1)+1}}{\ln^m(z_r)}$

(80)

$if(zr).(stxy-1) = -1$	$V'(c) = \frac{a^{k+m}.stxy.ctxy}{a_{zr}.clny}.\frac{1}{\ln^{m-1}(z_r)}$

(81)

The divergence condition is here :

$$\begin{array}{ll} \text{if } m \geq 1 & (zr).(stxy-1) > -1 \\ \text{if } m = 0 & (zr).(stxy-1) \geq -1 \end{array} \qquad (82)$$

Case z_r is a variable of prime numbers

$$V(c) = (a^{k+m}.ctxy/(clny.\ln^m(z_r))).\int_2^{z_r}(c/a_{zr}+z_r^{(zr)})^{stxy}/\ln(z_r).dz_r$$

Extracting the logarithm and neglecting c :

$$V(c) = \frac{a^{k+m}.ctxy.}{((zr).stxy+1)).clny}.\frac{z_r^{((zr).stxy+1)}}{\ln^{m+1}(z_r)} \qquad (83)$$

In addition, by derivation inside the integral :

$$V'(c) = (a^{k+m}.ctxy/(clny.\ln^m(z_r))).\int_2^{z_r}(((c/a_{zr}+z_r^{(zr)})^{stxy})/\ln(z_r))'.dz_r$$

So that, after asymptotic extraction of the logarithm and other elementary operations :

$$V'(c) = (a^{k+m}/a_{zr}).(stxy.ctxy/(clny.\ln^{m+1}(z_r))).\int_2^{z_r}(c/a_{zr}+z_r^{(zr)})^{stxy-1}.dz_r$$

Then by neglecting c asymptotically :

$$V'(c) = (a^{k+m}/a_{zr}).(stxy.ctxy/(clny.\ln^{m+1}(z_r))).\int_2^{z_r}z_r^{(zr).(stxy-1)}.dz_r$$

So that :

$if(zr).(stxy-1) \neq -1$	$V'(c) = \frac{a^{k+m}.stxy.ctxy}{a_{zr}.((zr).(stxy-1)+1).clny}.\frac{z_r^{(zr).(stxy-1)+1}}{\ln^{m+1}(z_r)}$

(84)

if(zr).(stxy-1) = -1	$V'(c) = \frac{a^{k+m}.stxy.ctxy}{a_{zr}.clny} \cdot \frac{1}{\ln^m(z_r)}$ (85)

The divergence condition is here

$$(zr).(stxy-1) > -1 \qquad (86)$$

Application : Iwaniec and Friedlander equation

We have k = 2, m = 0, $a_{x1} = 1$, $(x_1) = 2$, $a_{x2} = 1$, $(x_2) = 4$, $a^{k+m} = 1$, $a_{zr} = 1$, clny = 1, stxy = 1/2+1/4 = 3/4, (zr).(stxy-1)+1 = stxy = 3/4 ≠ 0. We use $\Gamma(1+x) = x.\Gamma(x)$, $\Gamma(1/2) = \pi^{1/2}$ and duplication formula $\Gamma(s).\Gamma(s+1/2) = 2^{1-2s}.\pi^{1/2}.\Gamma(2s)$ giving $\Gamma(3/4) = 2^{1/2}\pi/\Gamma(1/4)$, hence $ctxy = \Gamma(1+1/2).\Gamma(1+1/4)/\Gamma(1+1/2+1/4) = (1/6).\Gamma(1/2).\Gamma(1/4)/\Gamma(3/4) = (1/(6.2^{1/2}\pi^{1/2})).(\Gamma(1/4))^2$.
Then :

$$\lim_{p\to\infty} \#\{ x_1^2+x_2^4 = p+c\} = (1/(6.2^{1/2}\pi^{1/2})).(\Gamma(1/4))^2.Fan(c).p^{3/4}/\ln(p)$$

The theory of the numbers of classes of quadratic forms implies :

$$\prod_{p = 1 \bmod 4} 1-1/p \;.\; \prod_{p = 3 \bmod 4} 1+1/p = 4/\pi$$

which here is also Fan(0).
Thus :

$$\lim_{p\to\infty} \#\{x_1^2+x_2^4 = p\} = 2^{1/2}.(\Gamma(1/4))^2/(3.\pi^{3/2}).p^{3/4}/Ln(p) \approx 0{,}874.p^{3/4}/Ln(p)$$

The method of Bombieri asymptotic sieve [1] implemented by Iwaniec and Friedlander gives the same result. We get, in addition, the enumeration for any relative integer c provided we go back to our earlier paragraph on #(c) and fan(c) for equation $x_1^2+x_2^4 = p+c$. Euler products for c ≠ 0 are quite more complex than for c = 0 and certainly difficult to get with some other method.

9.4. Generation of prime numbers by a polynomial

Let us have k and a respectively the degree and the dominant coefficient of P. Then asymptotically $P(x) \to a.x^k$ and $P^{-1}(x) \to (x/a)^{(1/k)}$. Thus :

$$\lim_{p\to\infty} \#\{(n,p) / P(n) - p = c\} = \lim_{p\to\infty} Fan(c).\,(p/a)^{(1/k)}/Ln(p) \qquad (87)$$

9.5. Quadratic forms

9.5.1. Discriminant et equations of volume

We focus first on equation

$$u.x_1^2+v.x_1.x_2+w.x_2^2 = c \quad (88)$$

whose discriminant is

$$\Delta = v^2-4u.w \quad (89)$$

Let us write

$$[X] = \begin{vmatrix} x_1 \\ x_2 \end{vmatrix}$$

Let us write in matrix form :

$$u.x_1^2+v.x_1.x_2+w.x_2^2 = [x_1\ x_2]\,[U]\begin{vmatrix} x_1 \\ x_2 \end{vmatrix} = [x_1\ x_2]\begin{vmatrix} u & v/2 \\ v/2 & w \end{vmatrix}\begin{vmatrix} x_1 \\ x_2 \end{vmatrix}$$

For symmetrical [U], the theorem of the principal axis [3] applies. Let us have λ_1 and λ_2 the eigenvalues of [U]. The orthogonal matrix [Q] which diagonalizes [U] allows the change of co-ordinates :

$$\begin{vmatrix} y_1 \\ y_2 \end{vmatrix} = [{}^tQ]\begin{vmatrix} x_1 \\ x_2 \end{vmatrix}$$

Hence we have :

$$[\lambda] = \begin{vmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{vmatrix} = [{}^tQ].[U].[Q] \quad (90)$$

and

$$u.x_1^2+v.x_1.x_2+w.x_2^2 = \lambda_1.y_1^2+\lambda_2.y_2^2$$

Let us write

$$[Q] = \begin{vmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{vmatrix}$$

Then :

$$\lambda_1 = \cos^2(\theta).u-\sin(\theta).\cos(\theta).v+\sin^2(\theta).w$$
$$\lambda_2 = \sin^2(\theta).u+\sin(\theta).\cos(\theta).v+\cos^2(\theta).w$$
$$0 = \sin(\theta).\cos(\theta).(u-w)+(\cos^2(\theta)-\sin^2(\theta)).v/2$$

Hence for last equation :

$$\tan(2\theta) = -v/(u-w)$$

So that

$$\theta = -(1/2).\text{atan}(v/(u-w))+k.\pi/2 \qquad (91)$$

Using some elementary trigonometric identities and by choosing k = 0, it follows :

$$\cos(\theta) = ((1+1/(1+(v/(u-w))^2)^{1/2})/2)^{1/2}$$
$$\sin(\theta) = ((1-1/(1+(v/(u-w))^2)^{1/2})/2)^{1/2}$$

Then :

$$\lambda_1 = (1/2).((1+1/(1+(v/(u-w))^2)^{1/2}).u-1/(1+(v/(u-w))^2)^{1/2}.v+(1-1/(1+(v/(u-w))^2)^{1/2}).w)$$
$$\lambda_2 = (1/2).((1-1/(1+(v/(u-w))^2)^{1/2}).u+1/(1+(v/(u-w))^2)^{1/2}.v+(1+1/(1+(v/(u-w))^2)^{1/2}).w) \qquad (92)$$

and

$$y_1 = ((1+1/(1+(v/(u-w))^2)^{1/2})/2)^{1/2}.x_1+((1-1/(1+(v/(u-w))^2)^{1/2})/2)^{1/2}.x_2$$
$$y_2 = -((1-1/(1+(v/(u-w))^2)^{1/2})/2)^{1/2}.x_1+((1+1/(1+(v/(u-w))^2)^{1/2})/2)^{1/2}.x_2 \qquad (93)$$

These last equations give the conics principal axis.
As $[\lambda] = [{}^tQ].[U].[Q]$ and $\det([{}^tQ]) = \det([Q]) = 1$, we get $\det([\lambda]) = \det([U])$, thus :

$$\lambda_1.\lambda_2 = -\Delta/4 \qquad (94)$$

Equation $\lambda_1.y_1^2+\lambda_2.y_2^2 = c$, c a constant, is of elliptic type when λ_1 and λ_2 are of same sign ($\Delta < 0$) and of hyperbolic type when λ_1 and λ_2 are opposite signs ($\Delta > 0$). Thus, $\Delta = 0$ is the borderline between these two types of curves. The conditions $v = 0$ and $u.w = 0$ form other borderlines involving on principal axis orientation.
To limit the complexity of further integral evaluation, we are interested only in cases $\Delta \neq 0$, $u \geq 0$, $v \geq 0$ and $w \geq 0$. We begin with the evaluation of "volume" V(c) delimited by the target c such us :

$$u.x_1^2+v.x_1.x_2+w.x_2^2 \leq c \qquad (95)$$

Here x_1 and x_2 are variables, u, v and w parameters.
The domain of definition of the variables is the first quadrant $x_1 \geq 0$ and $x_2 \geq 0$.

$$V(c) = \int_{x_1=0}^{x_1=(c/u)^{1/2}} \int_{x_2=0}^{x_2=(-v.x_1+(4w.c+\Delta.x_1^2)^{1/2})/2w} dx_2.dx_1 \qquad (96)$$

Thus :

$$V(c) = \int_{x_1=0}^{x_1=(c/u)^{1/2}} (-v.x_1+(4w.c+\Delta.x_1^2)^{1/2})/2w.dx_1$$

The integration of this expression requires distinguishing positive and negative cases for Δ.

<u>Case $\Delta < 0$</u>

The change of variable $x_1 = (4w.c/(4u.w-v^2))^{1/2}.\sin(\theta)$ gives after some elementary transformations :

$$V(c) = \frac{\arcsin((-\Delta/(4u.w))^{1/2})}{(-\Delta)^{1/2}}.c \qquad (97)$$

<u>Case $\Delta > 0$</u>

In the same way, the change of variables $x_1 = (4w.c/(4u.w-v^2))^{1/2}.\text{sh}(\theta)$ leads to :

$$V(c) = \frac{\text{arcsh}((\Delta/(4u.w))^{1/2})}{(\Delta)^{1/2}}.c \qquad (98)$$

Let us pose (with $\Delta \neq 0$) :

$$f = \text{if}(\Delta < 0, \frac{\arcsin((-\Delta/(4u.w))^{1/2})}{(-\Delta)^{1/2}}, \frac{\text{arcsh}((\Delta/(4u.w))^{1/2})}{(\Delta)^{1/2}}) \qquad (99)$$

In the case u = 1, v = 0, w = 1 ($v^2-4u.w < 0$), we have $V(c) = (\text{Arcsine}(1)/2).c = (\pi/4).c$.

9.5.2. Generation of prime numbers

A quadratic equation of the preceding type (positive u, v and w) has only a finite number of solutions. This type of problem does not interest us (except if $c \to \infty$). However, using V(c) expression, we can tackle with an equation of the following type where x and y are integers variables and p a prime number variable :

$$u.x_1^2+v.x.x_2+w.x_2^2 \leq p+c \quad (100)$$

Then, boundless volume is given thanks to integral :

$$V(c) = \int_{p=2}^{p} \int_{x_1=0}^{x_1=((c+p)/u)^{1/2}} \int_{x_2=0}^{x_2=(-v.x_1+(4w.(c+p)+(v^2-4u.w).x_1^2)^{1/2})/2w} dx_2.dx_1.dp/\ln(p) \quad (101)$$

Thus :

$$V(c) = f.\int_{p=2}^{p} ((p+c)/\ln(p)).dp \quad (102)$$

At this step, c being negligible in front of p, asymptotic evaluation gives :

$$V(c) = (f/2).(p^2/\ln(p))$$

and (by deriving first p+c inside the integral) :

$$V'(c) = f.p/\ln(p)$$

So that :

$$\lim_{p\to\infty} \#\{u.x_1^2+v.x_1.x_2+w.x_2^2 \leq p+c\} = (f/2).p^2/Ln(p) \quad (103)$$

and

$$\lim_{p\to\infty} \#\{u.x_1^2+v.x_1.x_2+w.x_2^2 = p+c\} = f.Fan(c).p/Ln(p) \quad (104)$$

In the same way, we can get the enumeration with y_1 et y_2 variables of prime numbers :

$$u.y_1^2+v.y_1.y_2+w.y_2^2 \leq p+c \quad (105)$$

Then, with the same conditions on Δ, u, v and w that previously, the volume is given by the triple integral :

$$V(c) = \int_{p=2}^{p} \int_{y_1=2}^{y_1=((c+p)/u)^{1/2}} \int_{y_2=2}^{y_2=(-v.y_1+(4w.(c+p)+\Delta.y_1^2)^{1/2})/2w} (dy_2/Ln(y_2)).(dy_1/Ln(y_1)).(dp/\ln(p)) \quad (106)$$

Logarithms can be extracted from integrals when the upper boundary diverges. By $u.y_1^2+v.y_1.y_2+w.y_2^2 < p+c$, y_1 is bounded to $y_1 < (p/u)^{1/2}$, that is $\ln(y_1) \approx< (1/2).\ln(p)$. In the same way, $\ln(y_2) \approx< (1/2).\ln(p)$.
Hence :

$$V(c) \equiv (1/\ln(p)).((1/2)/\ln(p)).((1/2)/\ln(p)).f \int_{p=2}^{p} (p+c).dp \quad (107)$$

It follows simply :

$$\lim_{p\to\infty} \#\{u.y_1^2+v.y_1.y_2+w.y_2^2 \leq p+c\} = 2.f.p^2/Ln^3(p)$$

and

$$\lim_{p\to\infty} \#\{u.y_1^2+v.y_1.y_2+w.y_2^2 = p+c\} = 4.f.Fan(c).p/Ln^3(p)$$

Numerical application

For u = 1, v = 1, w = 1, we get $f = \pi/(3\sqrt{3})$. Thus (the values of a are distinct in each equation, but all tend asymptotically towards 1) :

$$\lim_{p\leq q} \#\{x_1^2+x_1.x_2+x_2^2 \leq p+c\} = (a.\pi/(6\sqrt{3})).q^2/Ln(q)$$

and

$$\lim_{p \le q} \#\{x_1^2+x_1.x_2+x_2^2 = p+c\} = (a.\pi/(3\sqrt{3})).Fan(c).q/Ln(q)$$

and

$$\lim_{p \le q} \#\{y_1^2+y_1.y_2+y_2^2 \le p+c\} = (2a^3.\pi/(3\sqrt{3})).q^2/Ln^3(q)$$

and

$$\lim_{p \le q} \#\{y_1^2+y_1.y_2+y_2^2 = p+c\} = (4a^3.\pi/(3\sqrt{3})).Fan(c).q/Ln^3(q)$$

The discriminant of the quadratic groups is here -3 and is a square for the 1 modulo 6 sequences and a non-square for the 5 modulo 6 sequences (the modulo 6 distinction results from a more thorough study that the reader will find on the author website).
The degree of stability of the proposed equations is $\delta s = 1$ or 2. One will use relevant cardinal matrices accordingly to these degrees of stability. We gave the cardinal matrix for $x_1^2+x_1.x_2+x_2^2$ for a non-square discriminant previously (page 18) and gave also the cardinal matrix corresponding to the variable –p (page 11), thus for $x_1^2+x_1.x_2+x_2^2 = p+c$ and sequences 1 modulo 6 :

$$\begin{vmatrix} \#(0) \\ \#(g^i) \end{vmatrix} = \begin{vmatrix} 1 & (p-1).(p+1) \\ (p+1) & (p^2-p-1) \end{vmatrix} \begin{Vmatrix} 0 & p-1 \\ 1 & p-2 \end{Vmatrix} \begin{Vmatrix} 1 \\ 0 \end{Vmatrix} = \begin{vmatrix} (p-1).(p+1) \\ (p^2-p-1) \end{vmatrix}$$

Normalisation results by a division by $p^{2-1}.(p-1)$.
The other abundance factors are drawn in the same way, thus the table :

Variables (x,y) of integer integers	c = 0 mod p	$c = g^0.g^{2u} \bmod p$	$c = g^1.g^{2u} \bmod p$
p = 2	3/2	1/2	
p = 3	1	1/2	3/2
p = 1 mod 6	(p-1)/p	$(p^2-p+1)/((p-1).p)$	$(p^2-p+1)/((p-1).p)$
p = 5 mod 6	(p+1)/p	$(p^2-p-1)/((p-1).p)$	$(p^2-p-1)/((p-1).p)$

Variables (x,y) of prime numbers	c = 0 mod p	$c = g^0.g^{2u} \bmod p$	$c = g^1.g^{2u} \bmod p$
p = 2	2	0	
p = 3	3/4	3/4	3/2
p = 1 mod 6	$p.(p-3)/(p-1)^2$	$p.(p^2-3p+6)/(p-1)^3$	$p.(p^2-3p+2)/(p-1)^3$
p = 5 mod 6	p/(p-1)	$p.(p^2-3p+4)/(p-1)^3$	$p^2.(p-3)/(p-1)^3$

The numerical application then gives for variables of integers :

		Exact number of solutions						Calculated number of solutions						Variation					
c	Fan(c)	p < 100	p < 1000	p < 10000	p < 100000	p < 1000000	p < 10000000	p < 100 a = 1,39556	p < 1000 a = 1,19388	p < 10000 a = 1,16128	p < 100000 a = 1,11339	p < 1000000 a = 1,08694	p < 10000000 a = 1,07236	p < 100	p < 1000	p < 10000	p < 100000	p < 1000000	p < 10000000
0	1,65328	23	161	1223	9569	78463	664389	30,29	172,76	1260,30	9666,66	78641,81	665027,66	31,70%	7,30%	3,05%	1,02%	0,23%	0,10%
1	0,24178	7	28	183	1412	11511	96763	4,43	25,26	184,31	1413,68	11500,78	97255,39	-36,72%	-9,77%	0,72%	0,12%	-0,09%	0,51%
2	2,17601	37	239	1631	12638	103612	874283	39,87	227,38	1658,78	12723,04	103506,59	875294,47	7,75%	-4,86%	1,70%	0,67%	-0,10%	0,12%
3	0,48356	8	34	354	2800	22816	194082	8,86	50,53	368,62	2827,35	23001,57	194510,78	10,75%	48,62%	4,13%	0,98%	0,81%	0,22%
4	0,72534	14	76	542	4211	34744	291816	13,29	75,79	552,93	4241,03	34502,35	291766,16	-5,07%	-0,27%	2,02%	0,71%	-0,70%	-0,02%
5	0,91621	18	104	709	5362	43753	368739	16,79	95,74	698,43	5357,04	43581,50	368543,13	-6,74%	-7,94%	-1,49%	-0,09%	-0,39%	-0,05%
6	1,45067	22	150	1074	8538	68960	584132	26,58	151,59	1105,85	8482,00	69004,23	583528,31	20,81%	1,06%	2,97%	-0,66%	0,06%	-0,10%
7	0,20242	6	29	167	1203	9609	81672	3,71	21,15	154,31	1183,54	9628,54	81422,93	-38,19%	-27,06%	-7,60%	-1,62%	0,20%	-0,30%
8	2,17601	34	225	1647	12718	103749	875896	39,87	227,38	1658,78	12723,04	103506,59	875294,47	17,26%	1,06%	0,72%	0,04%	-0,23%	-0,07%
9	0,48356	9	55	393	2861	22955	195281	8,86	50,53	368,62	2827,35	23001,57	194510,78	-1,56%	-8,13%	-6,20%	-1,18%	0,20%	-0,39%
10	0,91621	16	102	689	5419	43536	369315	16,79	95,74	698,43	5357,04	43581,50	368543,13	4,92%	-6,14%	1,37%	-1,14%	0,10%	-0,21%
Mean value														0%	0%	0%	0%	0%	0%
Standard deviation														21,94%	18,53%	3,79%	0,93%	0,39%	0,25%

We have adjusted here arbitrarily the parameter “a” such that the average value of mean values for selected the targets will equal 0. This setting does gradually converge to 1. At the same time, the standard deviation of the variations gradually run towards 0 also.

The numerical application then gives for variables of integers :

		Exact number of solutions						Calculated number of solutions						Variation					
c	Fan(c)	p < 1 000	p < 10 000	p < 100 000	p < 1 000 000	p < 10 000 000	p < 100 000 000	p < 1 000 a = 1,21519	p < 10 000 a = 1,23971	p < 100 000 a = 1,21153	p < 1 000 000 a = 1,18934	p < 10 000 000 a = 1,16599	p < 100 000 000 a = 1,1456	p < 1 000	p < 10 000	p < 100 000	p < 1 000 000	p < 10 000 000	p < 100 000 000
0	1,51898	28	104	468	2454	14262	89072	20,00	89,58	428,09	2343,68	13906,53	88361,03	-28,58%	-13,87%	-8,53%	-4,50%	-2,49%	-0,80%
2	2,4854	35	146	701	3835	22378	142833	32,72	146,57	700,45	3834,81	22754,27	144578,93	-6,51%	0,39%	-0,08%	-0,01%	1,68%	1,22%
4	1,93725	11	75	468	2790	17302	110952	25,51	114,25	545,96	2989,05	17735,86	112692,34	131,87%	52,33%	16,66%	7,13%	2,51%	1,57%
6	1,53172	32	112	424	2398	14188	89748	20,17	90,33	431,68	2363,34	14023,16	89102,13	-36,98%	-19,35%	1,81%	-1,45%	-1,16%	-0,72%
8	2,4855	43	179	773	4042	23161	146147	32,72	146,58	700,47	3834,96	22755,19	144584,75	-23,90%	-18,11%	-9,38%	-5,12%	-1,75%	-1,07%
10	1,77095	21	103	531	2708	16132	102567	23,32	104,44	499,10	2732,46	16213,36	103018,45	11,03%	1,40%	-6,01%	0,90%	0,50%	0,44%
12	1,1589	16	66	322	1760	10212	66858	15,26	68,34	326,61	1788,11	10609,93	67414,71	-4,64%	3,55%	1,43%	1,60%	3,90%	0,83%
14	2,57835	30	156	695	3930	23470	149722	33,95	152,06	726,64	3978,22	23605,24	149985,95	13,15%	-2,53%	4,55%	1,23%	0,58%	0,18%
16	1,93725	27	94	480	2850	17533	112448	25,51	114,25	545,96	2989,05	17735,86	112692,34	-5,53%	21,54%	13,74%	4,88%	1,16%	0,22%
18	1,24275	26	88	398	2040	11726	73122	16,36	73,29	350,24	1917,48	11377,59	72292,37	-37,07%	-16,72%	-12,00%	-6,01%	-2,97%	-1,13%
20	3,64042	55	235	1049	5543	33990	213338	47,93	214,69	1025,96	5616,92	33328,68	211767,94	-12,86%	-8,64%	-2,20%	1,33%	-1,95%	-0,74%
Mena value														0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Standard deviation														44,80%	21,15%	9,16%	4,07%	2,22%	0,95%

Le même principe que précédemment a été retenu ici pour valoriser le paramètre « a ».
Nous observons dans ce tableau que le nombre de solutions près de l'origine peut être très éloigné de la tendance asymptotique. Pour autant, le nombre de solutions attendu s'affiche progressivement sans écart notable par rapport aux autres cibles (remarquable pour c = 4 notamment).
The same principle that previously was held here to evaluate the parameter "a". We see in this table that the number of solutions near the origin can be very distant from the asymptotic tendency. However, the expected number of solutions finds his way gradually without significant deviation from other targets (especially remarkable for c = 4).

We get what we expect : the reduction of standard deviation when q increases and adjustment coefficients a tending slowly towards 1.

10. Singularities

The study of the quadratic equation $u.x^2+v.x.y+w.y^2$ shows the existence of several conditions relative to variables coefficients and discriminant of the expression giving domains where abundance factors have same literal formulas (same literal functions of parameter "sequence"). The limits between these domains are called boundaries.
These boundaries, where the studied equations are not irreducible (modulo p), are likely sources of trouble and can break down a beautiful construction with results not complying with expectations. Target 0 is often involved within a boundary.

11. A conclusion that is not one

The expression of the eigenvalues of cardinal matrices is given in this text in a fully literal way. Thus, in principle, we can compute Euler products (and the abundance factors) within any accuracy. In fact, the calculation should be conducted for each sequence and this until a high enough ranking. Thus things are not always so practical. However, properties deriving from the primitive roots equations give a simpler framework for 1, 2, 3 and 4 environments. The comprehensive study of the eigenvalues of non prime environments gives also rise to interesting constructions based on prime environments and highlights some matrix decompositions of the said primes. These points are the subject of an upcoming article.

SIGNS ET ABBREVIATIONS

$\#\{(x_1, \ldots, x_n)\}$:	Cardinal (number of, multiplicity…) of n-uplets $(x_1, \ldots, x_n)$, also noted $\#(x_1, \ldots, x_n)$.
(,) :	Greatest common divisor of (,)
lcm :	Lowest common multiple
Fan(c, p) :	Normalized abundance factor of target c for sequence p
Fan(c) :	Normalized abundance factor of target c (Euler product)
If(x, y, z) :	If x true then y if not z. The condition can be overlapping : if (x, if (y, z, t)…)
^ :	Sign of exponentiation (x^n = x^n)

PROGRAM CODE PARI/GP

Findinng of the exact number of solutions of $x_1^2+x_1.x_2+x_2^2 = p+c$ with parameter q = 100 (to change).

```
{q = 100; limit = floor(q^(1/2));
for(c = 0 , 10,
s = 0 ;
for(x = 0 , limit,
for(y = 0, limit, t = x^2+x*y+y^2-c;
if(isprime(t),
if(t < q,
s++))));
print(s))}
```

Findinng of the exact number of solutions of $y_1^2+y_1.y_2+y_2^2 = p+c$ with parameter q = 1000 (to change).

```
{q = 1000; limit = floor(q^(1/2));
for(i = 1,10^1000,
if(primes(i)[i] >= limit, ii = i;break));
for(c = 0 , 10, cc = 2*c;
s = 0 ;
for(x = 1 , ii,
for(y = 1, ii,  t = (primes(ii)[x])^2+(primes(ii)[x])* (primes(ii)[y])+ (primes(ii)[y])^2-cc;
if(isprime(t),
if(t < q,
s++))));
print(s))}
```

Finding the abundance factors of equation with integers' variables $x_1^2+x_1.x_2+x_2^2 = p+c$.

```
{limit = 500;
for(c = 0,10,
if(Mod(c,2) == 0, x = 1.5, x = 0.5);
if(Mod(c,3) == 1, x = 1/2*x);
if(Mod(c,3) == 2, x = 3/2*x);
for(i = 3, limit-1, p = primes(limit)[i]; g = znprimroot(p); gg = g*g;
if(Mod(c,p) == 0,
if(Mod(p,6)== 1, x = x*(p-1)/p, x = x*(p+1)/p),
if(Mod(p,6)== 1, x = x*(p*p-p+1)/((p-1)*p), x = x*(p*p-p-1)/((p-1)*p))));
print(x))}
```

Finding the abundance factors of equation with primes' variables $y_1^2+y_1.y_2+y_2^2 = p+c$.

```
{limit = 500;
for(cc = 0,10,c =2*cc;
x = 2.0;
if(Mod(c,3) == 2, x = 3/2*x, x = 3/4*x);
for(i = 3, limit-1, p = primes(limit)[i]; g = znprimroot(p); gg = g*g;
if(Mod(c,p) == 0,
if(Mod(p,6)== 1, x = x*p*(p-3)/((p-1)^2), x = x*p/(p-1)),
for(j = 1, (p-1)/2, if(Mod(c,p) == gg^j, if(Mod(p,6)== 1, x = x*p*(p*p-3*p+6)/((p-1)^3), x = x*p*(p*p-3*p+4)/((p-1)^3));
break, if(Mod(c,p) == g*gg^j, if(Mod(p,6)== 1, x = x*p*(p*p-3*p+2)/((p-1)^3), x = x*p^2*(p-3)/((p-1)^3)); break)))));
print(x))}
```

REFERENCES

[1] John Friedlander, Henryk Iwaniec. Using a parity-sensitive sieve to count prime values of a polynomial. PNAS Vol 94, p1054-1058, feb 1997

[2] Melvyn B. Nathanson. Additive Number Theory. Springer.

[3] Peter V. O'Neil. Advanced Engineering Mathematics. Third Edition. Wadsworth Publishing Company.

[4] Nikolaï S. Piskounov. Calcul différentiel et intégral. Editions Mir. Moscou.