MATRIX ALGORITHM FOR DIOPHANTINE EQUATIONS' ENUMERATION

by

Hubert Schaetzel

Abstract. — The purpose of this article is to give a method to compare the number of solutions of the Diophantine equations $R(z_1, z_2, \ldots, z_n) = c$, c being the parameter for which the comparison is made. Matrices with remarkable properties are produced which are the essential contribution of our study. Their usefulness is obvious as they characterize each independent constituent on the left hand side of the Diophantine equations and can therefore be reused in some other equations under specified conditions. The remarkable efficiency of the method allows us then to tackle the twin prime conjecture and Friedlander-Iwaniec theorem's generalization, these choices made among a lot of other practicable options.

Résumé. — *(Algorithme matriciel pour le dénombrement d'équations diophantines).* Le but ici est de donner une méthode pour comparer le nombre de solutions d'équations diophantines du type $R(z_1, z_2, \ldots, z_n) = c$, c étant le paramètre pour lequel la comparaison est faite. Des matrices aux propriétés remarquables sont produites qui sont la contribution essentielle de notre étude. Leur utilité est évidente car elles caractérisent chaque constituant indépendant du membre gauche de ces équations diophantines et peuvent donc être réutilisées dans d'autres équations sous des conditions spécifiques. La remarquable efficacité de la méthode nous permet ensuite d'aborder la conjecture des nombres premiers jumeaux et la généralisation du théorème de Friedlander Iwaniec, ces choix étant faits parmi bien d'autres options envisageables.

Contents

2000 ***Mathematics Subject Classification.*** — 11D45, 11D72, 11D25, 11Y50.
Key words and phrases. — Diophantine equations, algorithm, enumeration.

1. Introduction

David Hilbert's tenth problem titled "Of the possibility of solving a Diophantine equation" raised the question in 1900 of the existence of a general algorithmic method with a finite number of steps enabling to decide, for any Diophantine equation, whether this equation has integer solutions or not. This may seem a very low requirement as it doesn't ask for their precise values nor how many solutions exist. However, even for so small requirement, Yuri Matiyasevich's theorem [**12**] answered to Hilbert's question in 1970 by the negative, establishing that Diophantine sets, which are the sets of integer solutions of a Diophantine equation with parameters, are exactly all recursively enumerable sets, which means that such an algorithm cannot exist.

So what? Should we be discouraged for even a "yes or no" question cannot be answered? Will we always have to restart an exercise when going from one equation to another? Do only specifically adapted methods or use of brute force have any chance of being useful in this mathematical domain?

Of course not. Nothing indicates that there are not large domains where similar approaches can lead to prolific results. So what about beating some of the odds here? Our focus will be on decomposing Diophantine equations in independent pieces for which we can find enumerative properties reusable in other Diophantine equations where any one of these pieces occurs.

2. Frameworking

A Diophantine equation is a polynomial equation with one or more unknowns and integer coefficients. Let us have such an equation:

$$R(z_1, z_2, \dots, z_n) = 0 \tag{1}$$

In order to solve it, let us write a supposedly "equivalent" expression

$$R(z_1, z_2, \dots, z_n) \equiv 0 \mod m \text{ where } m \longrightarrow +\infty \tag{2}$$

It is indeed appropriate if a bijection emerges between the set of solutions $(z_1, z_2, \dots, z_n)$ of the equation and the set $(z_1 \mod m, z_2 \mod m, \dots, z_n \mod m)$ as m is given higher values. Let us observe that there is a surjection from the first set to the second set and the requirement for a bijection is the following:

- the equation has a finite number of solutions (z_1, z_2, $\dots$, z_n),
- the parameter m is given a sufficient high value,
- the domain of definition of each z_i is $]-m, m]$,
- if z_i is a solution then $z_i - m$, nor $z_i + m$ is one.

The last condition is met most of the time if the initial equation is not linear. Otherwise reducing the domain of definition of z_i to the appropriate choice of $[0, m[$ or $]-m, 0]$ will do the job.

Keeping the previous remarks in mind, we can refocus our attention towards equations with an infinite number of solutions. Of course, the search of the whole set of solutions is nonsense then. As m tends towards infinity, the asymptotic behaviour of the growth of the number of solutions is the new target. At this stage, we must be able to write $m \longrightarrow +\infty$ in a more practical way. Let us start with:

$$m = 2^{i_2} \cdot 3^{i_3} \dots p_k^{i_{p_k}} \dots p_r^{i_{p_r}}, \tag{3}$$

where p_k will eventually describe all prime numbers and i_{p_k} will be given, unsurprisingly for the reader, higher and higher values (supposedly up to $+\infty$). The solutions to the equation $R(z_1, z_2, \dots, z_n) \equiv 0 \mod 2^{i_2} \cdot 3^{i_3} \dots p_k^{i_{p_k}} \dots p_r^{i_{p_r}}$ will however still be out of reach unless there is some way to get them back from the composite equations:

$$R(z_1, z_2, \dots, z_n) \equiv 0 \mod p_k^{i_{p_k}} \tag{4}$$

To be fair, even this last equation may seem to be unsolvable when $i_{p_k} \longrightarrow +\infty$. We will nevertheless come up with a step by step method consisting on going up the previous path solving for the number of solutions of:

$$R(z_i) \equiv 0 \mod p_k$$
$$\downarrow$$

$$\begin{gathered}
R(z_i) \equiv 0 \mod p_k^{i_{p_k}} \\
\downarrow \\
R(z_1, z_2, \ldots, z_n) \equiv 0 \mod p_k^{i_{p_k}} \\
\downarrow \\
R(z_1, z_2, \ldots, z_n) \equiv 0 \mod 2^{i_2} \cdot 3^{i_3} \ldots p_k^{i_{p_k}} \ldots p_r^{i_{p_r}} \\
\downarrow \\
R(z_1, z_2, \ldots, z_n) \equiv 0 \mod +\infty \\
\downarrow \\
R(z_1, z_2, \ldots, z_n) = 0
\end{gathered}$$

This will be done by replacing first $R(z_1, z_2, \ldots, z_n) = 0$ by $R(z_1, z_2, \ldots, z_n) = c$ and solving for all c's in the same time. But prior to that, we give some indispensable writing conventions, vocabulary and definitions.

— *Target* c : We call c the target and use systematically this letter. One can look upon it as a fictive variable as it simply takes all the values taken by $R(z_1, z_2, \ldots, z_n) \mod 2^{i_2} \cdot 3^{i_3} \ldots p_k^{i_{p_k}} \ldots p_r^{i_{p_r}}$ when $z_1, z_2, \ldots, z_n$ described each of their chosen domain of definition (N, Z or P) in some m_environment.

— *N, Z, P* : Usual abbreviations of natural numbers, integers and prime numbers.

— *m_environment* : The choice of some finite ring Z/mZ as the domain of definition of $z_1, z_2, \ldots, z_n$ and $R(z_1, z_2, \ldots, z_n)$. The standard modulo m operation is implemented in this environment.

— $\#(c)$: Number of occurrences of some event c.

— *Variables* x_i, y_i, z_i : Variable z_i in $R(z_1, z_2, \ldots, z_n)$ represent either N, Z or P according to the following systematic writing conventions:

$$z_i = \begin{cases} x_i & : N \text{ or } Z\_\text{variable} \\ y_i & : P\_\text{variable} \\ z_i & : \text{Any kind of the previous variables} \end{cases}$$

— *Independent constituent* : Independent constituents are polynomials of one or more variables separated each other by a sum sign " + " in a given Diophantine equation and with no common variable on both side of the sign. To illustrate, for $R(x, y, z) = x^2 + y^2 - (xy)^2 - z^4$, variable z is an independent constituent (obviously $-z^4 = +(-z^4)$), variables x or y are not, but the expression $x^2 + y^2 - (xy)^2$ as a whole is an independent constituent.

— *Instance* : An instance is the choice of some prime number p_k in $m = 2^{i_2} 3^{i_3} \ldots p_k^{i_{p_k}} \ldots p_r^{i_{p_r}}$.

— *Cardinal matrix* : A finite or infinite rank matrix which eventually provides the relative proportions of solutions over all the targets c compared to target 0 (or some other target).

Some of the definitions need more explanation of course which will be taken care progressively underneath. Let us note that upcoming expressions $if(eq, a, b)$ mean if eq is true than a else b. Let us also note that whenever we will mention "solve the equation", we will generally mean "solve for the number of solutions of the equation".

3. Cardinal matrices

Theorem 1. — *Let us have two independent variables u and v and two Diophantine functions f and g. Let us consider the number of events $\#(u, v) = \#i$ such that $f(u) + g(v) = i$. Then*

$$\#(i) = \sum_{j=-\infty}^{+\infty} \#(i-j) \cdot \#(j) \tag{5}$$

where $\#(j)$ is the number of events u such that $f(u) = j$ and $\#(i-j)$ is the number of events v such that $g(v) = i - j$.

Proof. — This is trivial as we just cumulate the events such that $f(u)+g(v) = (i-j)+j = i$. □

Note. — The term "event" here, although reminiscent of it, has nothing to do with probabilities. It is related to an actual and straightforward enumeration.

Definition 1. — Let us suppose that i and j are defined in a finite set (like for example the *m_environment Z/mZ*). Let us consider the matrix $C_g(i, j) = [\#(i-j)]$ obtained above. The matrix $C_g(i, j)$ is named the circulant cardinal matrix of $g(v)$.

Note. — This matrix provides the contribution of $g(v)$ to get some final event $f(u) + g(v) = c$. If one provides the contribution $C_f(i', j')$ of $f(u)$ then the number $\#c$ of some event c is obtained by a simple matrix multiplication $C_f(i', j') \cdot C_g(i, j)$ and this process can be generalized to any number of independent variables or group of variables.

Theorem 2. — *The circulant cardinal matrix of an independent constituent, within the quotient ring Z/mZ environment, is a square (m, m) matrix.*

Proof. — Let us consider the matrix $C_g(i, j) = [\#(i-j)]$ of some function g. In the chosen m_environment, the quantities i and j take only integers values in $[0, m-1]$. We can then attribute the result to a matrix $C_g(r, s) = [\#(i-j)]$ with $r = 1$ to m and $s = 1$ to m. □

Theorem 3. — *Circulant cardinal matrices are commutative.*

Proof. — The number of events for $f(u)+g(v)=c$ is the same as for $g(v)+f(u)=c$. Hence the result. □

Theorem 4. — *Circulant cardinal matrices are (right) circulant matrices.*
Proof. — This is immediate as $[\#(i-j \mod m)] = [\#((i+r \mod m)-(j+r \mod m))]$. Hence, it follows the matrix's expression:

$$\begin{pmatrix} \#0 & \#(m-1) & \#(m-2) & \dots & \#1 \\ \#1 & \#0 & \#(m-1) & \dots & \#2 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ \#(m-2) & \#(m-3) & \#(m-4) & \dots & \#(m-1) \\ \#(m-1) & \#(m-2) & \#(m-3) & \dots & \#0 \end{pmatrix}$$

□

As a immediate consequence also, circulant cardinal matrices have all the properties of circulant matrices. Therefore:
Theorem 5. — *The eigenvectors matrix of the circulant cardinal matrices is an invariant in a given environment m.*
Proof. — The eigenvectors matrix $U(r,s)_{r=1\, to\, m,\, s=1\, to\, m}$ is equal to the m by m square matrix:

$$U(r,s) = \frac{1}{\sqrt{m}}[w^{(r-1)\cdot(s-1)}]$$

where $w = e^{\frac{2\pi i}{m}}$ is the m_root of 1. The reader can refer to [**1**] for example. Hence, for given m, the eigenvectors matrix is totally defined. □

Note. — In a given environment, the $\#c$ values of the targets are obtained essentially by eigenvalues multiplications.

Indeed, the reciprocal of the eigenvectors matrix is equal to its transconjugate $U^*(r,s)$ (and its conjugate $\overline{U}(r,s)$):

$$U^{-1}(r,s) = U^*(r,s) = \frac{1}{\sqrt{m}}[w^{-(r-1)\cdot(s-1)}] = \overline{U}(r,s)$$

Let us then have $\sigma_f(r,s)$ and $\sigma_g(r,s)$ the diagonal matrix of eigenvalues of the cardinal matrices $C_f(r,s)$ and $C_g(r,s)$ of f and g respectively. Leaving aside the (r,s) indexing we get:

$$\begin{aligned} C_f \cdot C_g &= U \cdot \sigma_f \cdot U^* \cdot U \cdot \sigma_g \cdot U^* \\ &= U \cdot \sigma_f \cdot \sigma_g \cdot U^*. \end{aligned}$$

This generalizes to as many independent constituents of the initially chosen Diophantine equation as long as the environment, that is the square matrix rank, is the same.

Theorem 6. — *Recalling that* $w = e^{\frac{2\pi i}{m}}$, *the eigenvalues in a* $m\_$ *environment are equal to:*

$$\sigma_j = \sum_{k=0}^{m-1} \#(m-k) \cdot w^{(j-1)\cdot k} = \sum_{k=0}^{m-1} \#k \cdot w^{-(j-1)\cdot k}$$

with $j = 1$ *to* m *and where* $\#k$ *are the projection's results of the currently studied function.*
Proof. — This is a standard result for circulant matrices. The reader can refer again to [**1**]. Here the indexing of the eigenvalues starts with $j = 1$ and goes up to $j = m$. □

Definition 2. — The projective cardinal image of $R(z_1, z_2, \dots, z_n)$ in the $m_$environment is defined as the set of numbers of occurrences of the value c, noted $\#c$, when variables $z_1, z_2, \dots, z_n$ described each the discrete domain of definition $[0, m-1]$. A projective cardinal image is the resulting m values of $\#c$: $[\#0,\ \#1,\ \dots,\ \#(m-1)]$.
Note. — Being in a $m_$environment, $\#(m+k) = \#k$. In particular $\#m = \#0$.
Definition 3. — The normalized cardinal image is the fractional values obtained by multiplying by the same ratio the previous cardinals of the cardinal image in order to get an average value over the m elements of the set equal to 1. Hence, writing normalized components as $\#\#c$, we get :

$$[\#\#0, \#\#1, \dots, \#\#(m-1)] = \frac{m}{\sum_{i=0}^{m-1} \#i}[\#0, \#1, \dots, \#(m-1)] \tag{6}$$

Theorem 7. — *The first column of the circulant cardinal matrices* $C_R(i,j)$ *of function* R *is the projective cardinal image and is therefore equal to the product* $C_R(i,j)$ *by the column vector*

$$K = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Proof. — Taking $j = 0$ in $C_R(i,j) = [\#(i-j)]$, we collect the column vector $[\#(i)]$ values which are the elements of the projective cardinal image, $i = 0$ to $m-1$. □

Definition 4. — Let us multiply all the components of the standard circulant cardinal matrix by the same constant such that its first column is equal to the normalized cardinal image. We call the resulting matrix, after dividing it by

$1/m$, the normalized circulant cardinal matrix $M(R(z_1,\ldots,z_n),m)$:

$$\frac{1}{m}\begin{pmatrix} \#\#0 & \#\#(m-1) & \#\#(m-2) & \ldots & \#\#1 \\ \#\#1 & \#\#0 & \#\#(m-1) & \ldots & \#\#2 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ \#\#(m-2) & \#\#(m-3) & \#\#(m-4) & \ldots & \#\#(m-1) \\ \#\#(m-1) & \#\#(m-2) & \#\#(m-3) & \ldots & \#\#0 \end{pmatrix}$$

In this section, we have taken care partially of the following step cited before:

$$\begin{gathered} R(z_i) \equiv 0 \mod p_k^{i_{p_k}} \\ \downarrow \\ R(z_1, z_2, \ldots, z_n) \equiv 0 \mod p_k^{i_{p_k}} \end{gathered}$$

In $p_k^{i_{p_k}}$, two terms may have large values, that is p_k and i_{p_k}, which therefore may be a messy challenge for the enumeration goal as the size of the matrix may rise to infinity. So let us address first the "i_{p_k}" challenge.

4. Degree of stability

We introduced in the previous section the cardinal image of some chosen function R, cardinal image which is giving the proportions of occurrences $\#\#c$ of $R(...) = c$, $c = 0, 1, ..., m-1$ in a m_environment:

$$[\#\#0, \#\#1, \ldots, \#\#(m-1)]$$

We propose now to observe what happens when we scale up from $m = p_k^{i_{p_k}}$ to $m = p_k^{i_{p_k}+1}$, $m = p_k^{i_{p_k}+2}$, $m = p_k^{i_{p_k}+3}$ and so on.

Definition 5. — We call i_{p_k} the degree of stability, of the p_k instance, when for any larger environment $m = p_k^{i_{p_k}+r}$, $r = 1, 2, ..., +\infty$, the new normalized values $\#\#c$ are obtained by simple $p_k^{i_{p_k}}$ translations of the original values in the $p_k^{i_{p_k}+r}$ environment:

$$\#\#c = \#\#(c + p_k^{i_{p_k}}) \tag{7}$$

Note. — According to the $R(\ldots)$ design encountered, one may have temporary stability from some r to $r+1$ and then a failure. Stability cannot be taken for granted for complex expressions too rapidly, but this is not the case for more standard functions (monomials, some symmetric expressions like $x_1^2 + a \cdot x_1 \cdot x_2 + x_2^2$) where there is no such potential mishap.

5. Enumeration in a product environment

We want to take care of the following step in our overall strategy:

$$R(z_1, z_2, \ldots, z_n) \equiv c \mod p_k^{i_{p_k}}$$
$$\downarrow$$
$$R(z_1, z_2, \ldots, z_n) \equiv c \mod 2^{i_2} \cdot 3^{i_3} \ldots p_k^{i_{p_k}} \ldots p_r^{i_{p_r}}$$

and therefore we have to start with the problem consisting in solving the scaling of two terms:

$$\{R(z_1, z_2, \ldots, z_n) \equiv c \mod p_1^{i_{p_1}}\} \; \{R(z_1, z_2, \ldots, z_n) \equiv c \mod p_2^{i_{p_2}}\}$$
$$\downarrow$$
$$R(z_1, z_2, \ldots, z_n) \equiv c \mod p_1^{i_{p_1}} \cdot p_2^{i_{p_2}}$$

Let us write respectively the pair of normalized cardinal images [##0, ##1, …, ##$(m_1 - 1)$], [##0, ##1, …, ##$(m_2 - 1)$] and besides [##0, ##1, …, ##$(m - 1)$] where $m_1 = p_1^{i_{p_1}}$, $m_2 = p_2^{i_{p_2}}$ and $m = p_1^{i_{p_1}} \cdot p_2^{i_{p_2}}$.

Theorem 8. — *The relative proportions of events in the product environment are given by the product of normalized events:*

$$\#\#c = \#\#(c \mod m_1) \cdot \#\#(c \mod m_2)$$

Proof. — The former expression simply express that the number of events of (u,v) is the product of the number of events u by the number of events v, which is a standard result. □

Now what about solving the "p_k" challenge?

6. Condensed cardinal matrices

6.1. General scope. — By now, the way to enumerate the number of solutions of some Diophantine equation $R(\ldots) = c$ has been described in almost all general aspects. In short, it consists, for each instance p_i, in matrices multiplications in a proper environment (where the degree of stability is reached), and the resulting normalized cardinal images, then undergo repetitive translations of values followed by an infinite product over all the instances 2, 3, …, p_i, …, $+\infty$. This finally gives the proportional ratio of solutions $\frac{\#\#c}{\#\#c_{ref}}$ of any target c to some chosen reference target c_{ref}.

A straightforward use of this general approach however would be still quite cumbersome to deal with. In particular, we mentioned the terms "each instance" and it would be quite beneficial to be able to level up to "analogous classes of instances". In the same way "any target" would be welcome to some "analogous classes of targets". Other lucky simplifications may also depend on the chosen Diophantine equation. Indeed, for functions like monomials for example, the normalized cardinal image [##0, ##1, ..., ##$(m-1)$] will contain multiple identical values and therefore cardinal matrices also.

In order to give a hint on the vast spectrum of the method's enhancements, we will take here two examples. The first one will be the Polignac conjecture and the second one the more complex Friendlander-Iwaniec equation generalization. This will be done after discussing the general monomial case.

6.2. Target permutations and primitive roots.

— Multiplication of cardinal matrices give the number of occurrences #c of some events c. The results are collected in the systematic order #0, #1, #2, and so on. It may be interesting, as we will see later on, to choose a different order. The most efficient way to deal with this is to use symmetrical permutation matrices (see reference [**15**]).

Property 1. — *Let us consider J a symmetrical permutation matrix. Then*

$$J^2 = I$$

where I is the identity matrix.

Proof. — The transpose matrix of J is the inverse matrix of J (see properties of permutation matrices at reference [**15**]). If J is symmetrical, the result follows. $J^2 = J.^tJ = I$. □

Property 2. — *The application of multiplications to the right and the left by the same symmetrical permutation matrix to each of eigenvectors matrix, eigenvalues matrix and inverse eigenvectors matrix of a cardinal matrix provides a permutation of cardinal images as long as the first component (first line) is excepted.*

Proof. — Let us remember that the cardinal image is obtained by multiplying the cardinal matrix by the specific column vector K (see K shape in theorem 7). Let us then have C some cardinal matrix, U and σ its eigenvectors and eigenvalues matrices. It follows $C.K = U.\sigma.U^*.K$ which is equivalent to $J.C.K = (J.U.J).(J.\sigma.J).(J.U^*.J).(J.K)$ Let us suppose that J does not swap the first component of K. Then $J.K = K$ as all the other components of K are equal to 0 and therefore $J.C.K = (J.U.J).(J.\sigma.J).(J.U^*.J).K$. □

The reader may refer to [**14**] for the definition of a primitive root modulo some integer. In particular, any odd prime p_i has at least one primitive root. In order to lighten notations, we will write the prime number p and choosing a primitive root of p, we note it systematically g. As a consequence there is a bijection, with equal elements in the source and the destination sets, between $\{0, 1, 2, \cdots, p-1\}$ and $\{0, g^0, g^1, g^2, \cdots, g^{p-2}\}$. This immediately shows that the target 0 will always be a particular case as it cannot be expressed as a power of g. This later remark combined with the above remark on the necessary exclusion of the permutation of the first component of K leads us precisely to do so. But other than this, we are free to swap the remaining components using the described procedure, if we need so, in order to transform the cardinal image $\{\#0, \#1, \#2, \cdots, \#(p-1)\}$ to $\{\#0, \#g^0, \#g^1, \#g^2, \cdots, \#(g^{p-2})\}$ or some other permutation. With the specified technique, it is easy to trace precisely the position of the components of the eigenvectors and eigenvalues matrices which individual values don't change in the process.

Note. — Switching the components of a matrix with the same symmetrical permutation matrix respectively on the right and on the left is to apply respectively the same permutations on the lines and on the columns.

Note. — After the permutations, the underneath circulant structure of the original matrix is no more visible.

The reader can refer to appendix A for a few examples of lines and columns switching. The chosen case is $p = 13$, $g = 2$ and $(\#(g^{2u} \mod p) \equiv 2, \#(g^{2u+1} \mod p) \equiv 0)$.

6.3. The monomial case. — Monomials are typically easier objects to handle with than polynomials in a practical sense. Indeed, the targets can be gathered in congruence classes allowing condensed matrix expressions. So, although reducing the global scope, these objects offer already a lot of study opportunities and are very interesting as they provide full literal expressions for enumeration.

In this subsection, we make a distinction of $p > 2$ and $p = 2$, the later case being taken care in another way. As we already mentioned, the target 0 plays a special role as it cannot be expressed as a function of g some primitive root of p. More insight reveals besides that formulas drawn for this case have usually simpler writing that those for $c \neq 0$. Nevertheless, it is not a specific case acknowledging that we will address it in the same time as all the targets. Also as previously mentioned, we have two types of variables x and y, and therefore two monomials to consider x^n and y^n, the first one where x takes integer values and the second where y addresses prime numbers.

The strategy of resolution remains the same, seeking cardinal images and cardinal matrices of x^n and y^n.

Theorem 9. — *The cardinal image of $-z^{2k+1}$ is the same as the cardinal matrix of z^{2k+1} where z is either a variable of integers or prime numbers and k is a natural number.*

Proof. — We have $-z^{2k+1} = (-z)^{2k+1}$. By Dirichlet's and Chebotarev's density theorem (see [**2**]), we have equiprobable events for z and $-z$, hence the result. □

Theorem 10. — *Let us have d the greater common divisor of n and $p-1$ where p is a prime number*

$$d = gcd(n, p-1).$$

The (original) cardinal matrix $CX(r,s)$ of x^n in the p_ environment is a circulant matrix with first column image components equal to:

$$\begin{array}{l} CX(1,1)=1 \\ CX(g^{u.d},1)=d,\ u=0 \text{ to } (p-1)/d-1 \\ CX(r,1)=0,\ r\neq 1 \text{ and } r\neq g^{u.d} \mod p \end{array}$$

Proof. — By "original" we mean here before normalization.
That said, we have the traditional result:

$$g^{p-1}\equiv 1 \mod p$$

The cardinal image of x^n is obtained thanks to the list $\{0^n,\ g^{0n},\ g^{1n},\ g^{2n},\ \cdots,\ g^{(p-2)n}\}$ mod p. It contains redundancies when $d\neq 1$ and the distinct elements reduce to $\{0,\underbrace{g^{0d},g^{1d},g^{2d},\cdots,g^{(\delta-1).d}}_{\text{d times}}\}$ mod p, where $\delta=\frac{p-1}{d}$ and the d antecedents of $g^{u.d}$ are $g^{u+v\cdot\frac{p-1}{d}}$, $v=0,\ 1,\ \cdots,\ d-1$. Therefore the set x^n, $x=0,1,2,\cdots,+\infty$ can be written as $\{0,\underbrace{g^{0d},g^{1d},g^{2d},\cdots,g^{(\delta-1).d}}_{\text{d times}}\}$ mod p, $p+\{0,\underbrace{g^{0d},g^{1d},g^{2d},\cdots,g^{(\delta-1).d}}_{\text{d times}}\}$ mod p, $2p+\{0,\underbrace{g^{0d},g^{1d},g^{2d},\cdots,g^{(\delta-1).d}}_{\text{d times}}\}$ mod p, $\cdots$, $+\infty$. The numbers of events of the congruence classes 0 and $g^kg^{u.d}$, $k\in\{0,1,2\}$ modulo p is therefore proportional to the value in the right member of the following equations

$$\begin{array}{l} \#(0 \mod p)=1 \\ \#(g^0g^{u.d} \mod p)=d \\ \#(g^1g^{u.d} \mod p)=0 \\ \#(g^2g^{u.d} \mod p)=0 \\ \cdots \\ \#(g^{d-1}g^{u.d} \mod p)=0 \end{array}$$

for any $u\in\{0,\ 1,\ \cdots,\ \delta-1\}$. □

Theorem 11. — *The cardinal image x^n in the p^k_ environment is identical to the case $k=1$ except for multiples of p.*
Proof. — A primitive root g modulo p is also a primitive root modulo p^k unless $g^{p-1}=1 \mod p^2$ in which case $p+g$ is a primitive root according to reference [**14**]. We therefore can always chose some primitive root for which we can represent the values x^n, $x=0$ to p^k-1 with the same d multiplicity of given previously except for multiples of p. For those there will be equal cardinality except for 0 (mod p). □

Theorem 12. — *The (original) cardinal matrix $CY(r,s)$ of y^n is equal to*

$$CY=CX-I$$

where I is the identity matrix of rank p.
Proof. — The set y^n, $y = 2, 3, 5, 7, 11, \cdots, +\infty$ modulo p gives equiprobable events $1^d, 2^d, \cdots, (p-2)^d \mod p$ by the Chebotarev's density theorem (see [**2**]). The only missing element compared to the case x^n is therefore 0. This means replacing $CX(1,1) = 1$ in the previous case by $CY(1,1) = 0$. The matrix being circulant, we get $CY(r,r) = 0$ for all integers $r = 1$ up to $r = p$. □

Theorem 13. — *The cardinal image y^n in the p^k_environment is identical to the case $k = 1$. The degree of stability of y^n is therefore equal to* 1.
Proof. — There are no multiples of p involved in this case and theorem 11 enable then to conclude. □

Theorem 14. — *For a Diophantine expression sum or difference of independent monomials containing at least one independent variable of prime numbers y^n, the global degree of stability is equal to* 1.
Proof. — This is an immediate result of theorem 8. Indeed, when the target c is a multiple of p the number of events $\#(u)$ contribution of y^n is 0 which cancels any combination of events $(u, v, \cdots)$. □

Note. — From now on, in all expressions involving exponentiation of g the mod p term is implied. By g^k, we systematically mean $g^k \mod p$ even if not expressly mentioned.
Definition 6. — Let us have d the greatest common divisor of n and $p-1$ where p is a prime number, $d = gcd(n, p-1)$. Let us have md a multiplier of d and a divisor of $p-1$ such that $d \leq md \leq p-1$. A (primitive root) ordered cardinal matrix $CX(r,s)$ of x^n versus md in the p_environment is a matrix obtained by switching lines and columns of the original cardinal matrix in the same way such than the first column (and therefore first line) of the new matrix corresponds to the order 0, $g^i.g^{u.md}$, $i = 0$ to md, $u = 0$ to $(p-1)/md-1$, that is, after 0, we take $i = 0$ and exhaust all the values $u = 0$ to $(p-1)/md - 1$, then we take $i = 1$ and exhaust again all the values $u = 0$ to $(p-1)/md - 1$ and so on.
Example 1. — *For p = 13, g = 2, n = 2, we have d = gcd(n,p-1) = gcd(2,12) = 2. Let us take md = 4. Then the original order of targets*

0	1	2	3	4	5	6	7	8	9	10	11	12
0	g^0	g^1	g^4	g^2	g^9	g^5	g^{11}	g^3	g^8	g^{10}	g^7	g^6

will be changed to

0	1	3	9	2	6	5	4	12	10	8	11	7
0	g^0	g^4	g^8	g^1	g^5	g^9	g^2	g^6	g^{10}	g^3	g^7	g^{11}

Property 3. — *Equal values transfer property : Let us consider C the cardinal matrix of x^n (or y^n). Let us have X, a column vector of rank p and suppose*

that its k^{th} components have same values for all line indices k such that $k \equiv g^i.g^{u.d} \mod p$, i a fixed value and u any integer. Then the l^{th} components of $C.X$ have same values for all line indices l such that $l \equiv g^j.g^{v.d} \mod p$, j a fixed value and v any integer.
Proof. — We consider respectively the $r+1^{th}$ component of the following objects: c_r of the first column of the cardinal matrix C, x_r of column vector X and y_r of column vector $Y = C.X$. We have $y_r = c_r.x_0 + c_{r-1}.x_1 + c_{r-2}.x_2 + ... + c_{r-p+1}.x_{p-1}$. We then re-index the members of the equality replacing r by g^j to get $y_{g^i} - c_{g^i}.x_0 = \sum_{j=0}^{p-1} c_{g^i - g^j}.x_{g^j}$. The hypothesis is $x_{k.g^{u.d}} = x_k$ and $c_{k.g^{u.d}} = c_k$. It results $y_{g^i} - c_{g^i.g^{u.d}}.x_0 = \sum_{j=0}^{p-1} c_{(g^i-g^j).g^{u.d}}.x_{g^j.g^{u.d}}$ so that trivially $y_{g^i} = c_{g^i.g^{u.d}}.x_0 + \sum_{j=0}^{p-1} c_{(g^i.g^{u.d}-g^j.g^{u.d})}.x_{g^j.g^{u.d}}$ which right member is the definition of $y_{g^i.g^{u.d}}$. □

Property 4. — *The equal values transfer property is true for any integer md multiple of d such that $d \leq md \leq p-1$.*
Proof. — This is a trivial consequence of property 3. □

Note. — Note also that the column vector K in theorem 7 has the previous property as all components except the first one are equal to 0.
Property 5. — *Let us consider a permutation of two columns (or two lines) of the cardinal matrix of x^n (or y^n). Then one recovers the said swapped matrix by the same permutation of the eigenvector matrix, eigenvalues matrix and inverse eigenvalues matrix.*
Proof. — This is a general property for any matrix. □

Property 6. — *The eigenvectors matrix of an ordered matrix versus md is composed of left circulant matrix blocks of rank $(p-1)/md$ except for the first column and line.*
Proof. — Using theorem 6 and property 5, let us consider the general term $\frac{1}{\sqrt{p}} w^{g^i.g^j}$ of the ordered matrix component in some matrix block. Then the equality $g^i.g^j = g^{-md+i}.g^{j+md}$ means conservation of value of the component on the secondary diagonal so long that we stay in the block. The rank $(p-1)/md$ is a direct consequence of the primitive root property $g^{p-1} \equiv 1 \mod p$. □

Property 7. — *The $(p-1)/md$ lines' sums of the blocks of the eigenvectors matrix are equal to each other. So also for columns' sums.*
Proof. — This is an immediate consequence of circulant matrices. □

Property 8. — *The $(p-1)/md$ lines' sums of the blocks of the conjugate eigenvectors matrix are equal to each other. So also for columns' sums.*
Proof. — This is again an immediate consequence of circulant matrices. □

Property 9. — *The eigenvalues of an ordered matrix versus md are equal to each other in the corresponding matrix blocks of rank $(p-1)/md$ facing the eigenvectors matrix except for the component on the first column and line.*
Proof. — This is an immediate result of the general value of the specific eigenvalues here (j $>$ 1)

$$\sigma_j = \sum_{k=0}^{m-1} \#k \cdot w^{-(j-1)\cdot k}.$$

Here $\#k = d$ for $k = g^{u \cdot d}$ and 0 otherwise, so that

$$\sigma_{g^k+1} = d \sum_{k=0}^{d-1} \cdot w^{-(j-1)\cdot g^k . g^{u.d}} = \sigma_{g^k . g^{u.d}+1}$$

where $u = 0$ to $(p-1)/d-1$. Being a property for d it is also for a multiple of d which is the case of md. Hence the same eigenvalues. □

Property 10. — *The multiplicity of the eigenvalues of a cardinal matrix, except the eigenvalue p, is $(p-1)/d$.*
Proof. — This is an immediate result of the previous property. □

Example 2. — $p = 13$, $g = 2$, $n = 2$, $d = 2$.
The three re-ordering cases are then:
Case versus $md = 2$.

0	g^0	g^2	g^4	g^6	g^8	g^{10}	g^1	g^3	g^5	g^7	g^9	g^{11}
0	1	4	3	12	9	10	2	8	6	11	5	7
13	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$

Case versus $md = 4$.

0	g^0	g^4	g^8	g^1	g^5	g^9	g^2	g^6	g^{10}	g^3	g^7	g^{11}
0	1	3	9	2	6	5	4	12	10	8	11	7
13	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$

Case versus $md = 6$.

0	g^0	g^6	g^1	g^7	g^2	g^8	g^3	g^9	g^4	g^{10}	g^5	g^{11}
0	1	12	2	11	4	9	8	5	3	10	6	7
13	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$

With these starting premises, we are now able to condensed the cardinal matrices reducing redundancies progressively from $(p-1)/d$ to 1 still keeping all the original information. We will follow track using numerical examples.
Theorem 15. — *Let us consider the components $c(r, s)$ of the ordered cardinal matrix versus md of x^n (or y^n) in the p_ environment where integer md is defined as multiplier of d and divider of $p-1$ as earlier. The following condensed matrix with components $cc(cr, cs)$ hold the same information in regard*

to the numbers of events for the targets $g^i.g^{u.md}$ as the original ordered cardinal matrix with reduced redundancies together with keeping property 3:

$cc(1,1) = c(1,1)$

$cc(1+j,1) = c(2+(j-1)\ \frac{p-1}{md},\ 1)$, $j = 1$ *to* md

$cc(1,1+k) = \sum_{i=1}^{\frac{p-1}{md}} c(1,1+i+(k-1)\ \frac{p-1}{md})$, $k = 1$ *to* md

$cc(1+j,1+k) = \sum_{i=1}^{\frac{p-1}{md}} c(2+(j-1).\frac{p-1}{md},1+i+(k-1)\ \frac{p-1}{md})$, $j = 1$ *to* md, $k = 1$ *to* md

Proof. — Thanks to property 7, it is a trivial redundancy progressive reduction from $(p-1)/d$ to 1, the parameter md, divider of $p-1$ and multiplier of d, being given some value in-between. Illustration is given by the examples in appendix A. □

Definition 7. — We call condensed matrix the result of a reduction process identical to the one described above which transforms a matrix of rank $1+(p-1)$ to a matrix of rank $1+md$.

Definition 8. — We call block and blocks' area the unit and the whole of components covering a range of size $((p-1)/md,(p-1)/md)$ of the ordered cardinal matrices before reduction (starting indexes $r \geq 2$, $s \geq 2$, indexes specified in theorem 15).

Definition 9. — By extension, we call blocks' area the resulting area of the condensed matrix, that is, the condensed matrix except first line and first column.

Theorem 16. — *The eigenvectors matrix of the condensed cardinal matrix versus md of x^n (or y^n) in the p_ environment is the condensed matrix of the eigenvectors matrix of the ordered cardinal matrix of x^{md} (or y^{md}) versus md. The eigenvalues matrix of the condensed cardinal matrix versus md of x^n (or y^n) in the p_ environment is the condensed matrix of the eigenvalues matrix of the ordered cardinal matrix of x^d (or y^d) versus md.*

Proof. — This is an immediate result of the equality of the sum in lines of the eigenvectors ordered matrix blocks (property 7), the equality of the eigenvalues in the eigenvalues matrix blocks facing it (property 9) and the equality of the sums in columns of the conjugate eigenvectors matrix blocks (property 8). □

Property 11. — *Eigenvalues multiplication property. The targets proportions for a Diophantine equation based on sums of monomials are carried out essentially by eigenvalues multiplications.*

Proof. — Let us have K as defined in theorem 7. Let us have M_i the contracted matrices of x^i to the common $1+md$ rank. The targets proportions $\#c$ are obtained by the matrix multiplication $M_1.M_2 \cdots M_k.K$. By the invariance property of the eigenvectors matrix of contracted matrix expressed by theorem 16, all M_i share the same eigenvectors matrix U. Therefore $M_1.M_2 \cdots M_k.K = (U.\sigma_1.U^{-1}).(U.\sigma_2.U^{-1}) \cdots (U.\sigma_k.U^{-1}).K = U.\sigma_1.\sigma_2 \cdots \sigma_k.U^{-1}.K$ □

Theorem 17. — *The condensed cardinal matrix of x^n and y^n, respectively equating $vi = 1$ for x^n and $vi = 0$ for y^n, is given by*

$$[C] = [U][\sigma][\overline{U}]$$

where

$$[U] = \frac{1}{\sqrt{p}} \begin{pmatrix} 1 & \lambda_0 & \lambda_0 & \cdots & \lambda_0 \\ 1 & \lambda_1 & \lambda_2 & \cdots & \lambda_{md} \\ 1 & \lambda_2 & \lambda_3 & \cdots & \lambda_1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \lambda_{md} & \lambda_1 & \cdots & \lambda_{md-1} \end{pmatrix}$$

$$[\overline{U}] = \frac{1}{\sqrt{p}} \begin{pmatrix} 1 & \lambda_0 & \lambda_0 & \cdots & \lambda_0 \\ 1 & \lambda_1^* & \lambda_2^* & \cdots & \lambda_{md}^* \\ 1 & \lambda_2^* & \lambda_3^* & \cdots & \lambda_1^* \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \lambda_{md}^* & \lambda_1^* & \cdots & \lambda_{md-1}^* \end{pmatrix}$$

$$[\sigma] = \begin{pmatrix} \sigma_0 & 0 & 0 & \cdots & 0 \\ 0 & \sigma_1 & 0 & \cdots & 0 \\ 0 & 0 & \sigma_2 & \cdots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \cdots & \sigma_{md} \end{pmatrix}$$

and where $[\overline{U}]$ is the conjugate matrix of $[U]$,
and for $u \geq 1$

$$\lambda_u = \sum_{r=0}^{\frac{p-1}{md}-1} w^{g^{u-1+r.md \ mod \ p-1}}$$

and

$$\lambda_0 = \frac{p-1}{md}.$$

and

$$\sigma_0 = p - 1 + vi$$

and

$$\sigma_u = vi + d. \sum_{r=0}^{\frac{p-1}{md}-1} w^{-g^{u-1+r.d \ mod \ p-1}}$$

Note. — If $md = d$ then

$$\sigma_u = vi + d.\lambda_u$$

Proof. — It is a straightforward calculation from the initial ordered cardinal matrix using $g^i.g^j = g^{i+j}$. □

Note. — The reader will find in appendix C a computer program enabling to calculate any example of the condensed cardinal matrices. It gives also the eigenvectors and eigenvalues matrices.

Property 12. — *As for the initial cardinal matrix, the difference between a condensed matrix CX of x^n and a condensed matrix CY of y^n of same rank (versus any admissible md) is the identity matrix.*

$$CX = CY + I \tag{8}$$

Proof. — According to theorem 17, the eigenvectors matrices are the same for the two cases and the eigenvalues differ by the identity. Hence the result. □

Note. — We cannot stress enough the importance of this relationship between the matrix of an integers' variable and its prime numbers' counterpart. Besides being a fundamental property, it is also utterly useful and will come up in no time.

Theorem 18. — *Let us have some condensed cardinal matrix $CY(a, b)$ versus md of a prime variable y^n. Here $a \geq 1$, $b \geq 1$. Let us re-index its components $c_y(a, b)$ using $r = a - 2$, $s = b - 2$. Then the components' values such that $r \geq 0$, $s \geq 0$ are given by the following expression*

$$c_y(r, s) = d \cdot \#(u, v) \ \setminus \ g^r \equiv g^{u.d} + g^s.g^{v.md} \mod p \tag{9}$$

where $\#(u, v)$ is the number of event (u, v) satisfying the equation for $u = 0$ to $\frac{p-1}{d} - 1$ and $v = 0$ to $\frac{p-1}{md} - 1$.

Proof. — It results from the initial definition of the cardinal matrix that $\#(i-j) = d$ when $i - j = g^{u.d}$ for some $u \in [0, \frac{p-1}{d}[$, hence the multiplying factor d. Within the blocks' area, we have $i = g^r.g^{w.md}$ and $j = g^s.g^{v.md}$ for some for some $(r, s, v, w) \in ([0, md-1], [0, md-1], [0, \frac{p-1}{md}[, [0, \frac{p-1}{md}[)$. Then equality $g^{u.d} = g^r.g^{w.md} - g^s.g^{v.md}$ is the same as $g^r.g^{w.md} = g^{u.d} + g^s.g^{v.md}$. We know by now that each target $g^r.g^{w.md}$ has same events' cardinality in front of a matrix' block as target g^r. The ordering to get a condensed matrix versus md means then to collect the events $(u, v) \in ([0, \frac{p-1}{d}[, [0, \frac{p-1}{md}[)$ with constant s. □

Note. — Again, for a second time but a different subject, we cannot stress enough the importance of equation 9 for any resolution of Diophantine equation based on monomials (but not only). Therefore, we purposely give here a specific denomination to such kind of expression, namely "the primitive roots' equation".

Property 13. — *Let us consider a condensed matrix of a prime variable y^n. Equalities between components $c(r, s)$ and $c(r', s')$, $r \geq 0$, $s \geq 0$, $r' \geq 0$, $s' \geq 0$, of such an object are defined by matrix involutions depending on two cases.*

Case 1 : $(p-1)/2 \equiv 0 \mod d$

$$\begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix}$$

Case 2 : $(p-1)/2 \equiv d/2 \mod d$

$$\begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix} + \begin{pmatrix} d/2 \\ d/2 \end{pmatrix}$$

Proof. — As g is a primitive root, we use the property $g^{\frac{p-1}{2}} \equiv -1 \mod p$. Then if $g^r \equiv g^{u.d} + g^s.g^{v.md} \mod p$, we can write $-g^r \equiv g^{u.d}.g^{\frac{p-1}{2}} - g^s.g^{v.md}$ mod p, that is $g^s \equiv g^{u.d-v.md+\frac{p-1}{2}} + g^r.g^{-v.md} \mod p$. As d divides md all values of $u.d - v.md$ are reached by $w.d$ for some integer w. Changing the dummy indexes (u, v) we get $g^s \equiv g^{u.d+\frac{p-1}{2}} + g^r.g^{v.md} \mod p$. The number of events $\#(u, v)$ is therefore the same if ($r' = s$, $s' = r$, $\frac{p-1}{2} \equiv 0 \mod d$) or ($r' = s + \frac{d}{2}$, $s' = r + \frac{d}{2}$, $(p-1)/2 \equiv d/2 \mod d$). Hence the result of each case. It is easy to check that these transformations are involutions (self-inverse functions). □

Property 14. — *For lesser condensed matrices of a prime variable y^n, where $d \neq md$, in the blocks 'area, the blocks of rank d form a right circulant pattern. That is, we have the following property for any components modulo md:*

$$\begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix} + \begin{pmatrix} d \\ d \end{pmatrix}$$

Proof. — If $g^r \equiv g^{u.d} + g^s.g^{v.md} \mod p$, we can write $g^{r+d} \equiv g^{d+u.d} + g^{s+d+v.md} \mod p$. The dummy parameter u being replaced by $u - 1$, we get $g^{r+d} \equiv g^{u.d} + g^{s+d+v.md} \mod p$. Hence simultaneously $r' = r + d \mod md$ and $r' \equiv r + d \mod md$. □

Note. — The property is true also in the case $md = d$ but useless.

Note. — This kind of "symmetry" extents to a variable of integers (therefore monomials x^n) as the addition of 1 to each of the components of the main diagonal preserves the previous relations.

Property 15. — *Let us consider the most condensed matrix of a prime variable y^n, that is $md = d$. We then get the additional matrix involutions depending on two cases.*

Case 1 : $(p-1)/2 \equiv 0 \mod d$

$$\begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix}$$

Case 2 : $(p-1)/2 \equiv d/2 \mod d$

$$\begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix} + \begin{pmatrix} 0 \\ d/2 \end{pmatrix}$$

Proof. — Using again the property $g^{\frac{p-1}{2}} \equiv -1 \mod p$, if $g^r \equiv g^{u.d} + g^s.g^{v.d}$ mod p, we can write $g^0 \equiv g^{-r}.g^{u.d} + g^{s-r}.g^{v.d} \mod p$, that is $g^{-r} \equiv g^{u.d} +$

$g^{s-r}.g^{v.d+\frac{p-1}{2}} \mod p$, changing the dummy indexes (u, v). The number of events $\#(u, v)$ is therefore the same if ($r' = -r$, $s' = -r + s$, $\frac{p-1}{2} = 0 \mod d$) or ($r' = -r$, $s' = -r + s + \frac{d}{2}$, $(p-1)/2 \equiv d/2 \mod d$). Hence the result of each case. Again, it is easy to check that these transformations are involutions (self-inverse functions). □

Note. — The three previous properties are very useful if the condensed matrix size is small as it allows quite shorter calculations.

Theorem 19. — *The minimal size of a condensed cardinal matrix for a Diophantine equation composed of monomials $z_1^{n_1}$ to $z_k^{n_k}$, z_i being either a variable of integers or of primes is equal to*

$$nr = 1 + lcm(d_1, \cdots, d_i, \cdots, d_k)$$

where $d_i = gcd(p-1, n_i)$, $i = 1$ to k.

Proof. — In order to multiply matrices, they ought to be of the same size. For each of the variable, the smallest size of the condensed matrix, excepting first line and row is d_i and necessary size is therefore a multiple of this value (plus one). Hence the lower common multiple when different powers are present in the equation. □

Note. — There are an infinity of condensed matrices of different sizes in some environment for a given Diophantine equation composed of monomials. But there is only one condensed matrix with minimal size within this environment and for this particular Diophantine equation. In order to simplify the upcoming overview, the most condensed matrix will be denominated without more detail as the condensed matrix.

6.4. The Polignac case.

— With the previous study on the monomial case, the Polignac case can be address quite rapidly. However, as it is our first example, we will repeat some of the previous arguments, with specific details, in order to make it easier on the reader. The Friedlander-Iwaniec will be treated without going in such details again. We ought to start here with the most trivial and seemingly useless case which of course is the monomial of degree one, namely x. Its cardinal image is $[1, 1, \ldots, 1]$ in any environment and therefore its degree of stability is 1. Its cardinal matrix is [1] which can be extended to any normalized cardinal matrix with components all equal to $1/m$ in a m_environment.

We can then turn our attention to the y variable, that is a prime numbers' variable case.

Theorem 20. — *The cardinal image and cardinal matrix of a P_variable in a p_i_environment, $p_i > 2$ are respectively equal to:*

$$\frac{p_i}{p_i - 1}\begin{pmatrix} 0 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix}$$

and

$$\frac{1}{p_i - 1}\begin{pmatrix} 0 & 1 & 1 & \ldots & 1 \\ 1 & 0 & 1 & \ldots & 1 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 1 & \ldots & 0 \end{pmatrix} \qquad (10)$$

Proof. — The projection, in a $m = p_i$ environment, consists in the proportions of values 0 to $m - 1$ obtained while y take all the values 2, 3, 5, 7, 11 up to $+\infty$. Referring to Dirichlet's and Chebotarev's theorem [**2**], we know that there is an equal asymptotic repartition of the prime numbers ending on the said values 0 to $p_i - 1$ for a modulo p_i process except for 0. In the latter case, the only prime (ending on 0) is p_i. This occurrence corresponds therefore to a proportion equal to $+1/\infty$. Asymptotically, we therefore get $\#\#0 = 0$ and $\#\#c = \frac{p_i}{p_i-1}$ if $c \neq 0$, the last fraction common to all $c \neq 0$ enabling to have an overall average equal to 1. In the normalized cardinal matrix each of the components are then multiplied by the inverse of the environment value, here $1/p_i$. □

Theorem 21. — *The degree of stability of the y variable is equal to* 1 *for any instance* $p_i > 0$*.*

Proof. — One can repeat the same argument as in theorem 20 changing the $m = p_i$ environment to an $m = p_i^r$ environment, $r > 1$, $r \in N$. The equiprobability for all instance not multiple of p_i is conserved. The only difference is that the previous projection from p_i onto 0 is just deviated onto p_i. We therefore get a proportion equal to 0 on all multiples of p_i. Going from $r = 1$ to $r > 1$ consist only for the cardinal image to translate p_i^{r-1} times the data by p_i steps. □

Note. — We write the matrix with only 1 as components [1] and the identity matrix as usually $[I]$. Then the cardinal matrix of theorem 10 is equal to

$$\frac{1}{m-1}([1] - [I]) \qquad (11)$$

Theorem 22. — *The circulant matrix* $([1] - [I])^n$ *first column components differ by a unit only.*

Proof. — Let us proceed by recurrence. The statement is true for $n = 1$ as there are only 0 and 1 in the column. Let us suppose $([1] - [I])^{n-1} = f(m) \cdot [1] \pm [I]$ for $n > 1$. This is also the initial form of $([1] - [I])^1$ as we just have to take $f(m) = 1$ and adjust the sign in front of $[I]$. Then using $[1][1] = m[1]$, we get $([1] - [I])^n = (f(m) \cdot [1] \pm [I]) \cdot ([1] - [I]) = f(m) \cdot [1][1] - f(m)[1] \pm [1] - \pm [I] = (mf(m) - f(m) \pm 1) \cdot [1] \mp [I] = g(m) \cdot [1] \mp [I]$. The first term has the same components and the second vary the result by 0 or 1. Hence the result. □

Theorem 23. — *When $m \longrightarrow +\infty$, the ratio of the value of a component of the first column of the matrix $([1] - [I])^n$ to the value of the first row and column tends towards* 1.
Proof. — Let us use the previous annotation : $g(m) = mf(m) - f(m) \pm 1 \sim mf(m) \longrightarrow +\infty$ when $m \longrightarrow +\infty$. As all components just differ by 0 or 1, the result follows. □

Theorem 24. — *The cardinal image and cardinal matrix of a P_variable in a $m = 2^{i2}$_environment, $i_2 \longrightarrow +\infty$ are respectively equal to:*

$$2\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

and

$$\frac{2}{m}\begin{pmatrix} 0 & 1 & 0 & 1 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0 & \dots & 1 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0 & \dots & 1 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & 1 & 0 & 1 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0 & \dots & 1 & 0 \end{pmatrix} \tag{12}$$

Proof. — The integer 2 doesn't have a primitive root which makes this case a very special one. The projection of the set P modulo 2, 4, 8, etc. gives equal repartition on odd numbers (again according to Chebotarev), but no even numbers are produced except when projecting 2. Hence a completely different pattern here. □

Note. — Let us take the writing convention for the former cardinal matrix $\frac{2}{m}[(0,1)]$

Theorem 25. — *When $m \longrightarrow +\infty$, the multiplication of $([1]-[I])^n$ by $\frac{2}{m}[(0,1)]$ is equivalent to a multiplication by the scalar* 1.
Proof. — According to theorem 23, the values of the components of $([1]-[I])^n$ are asymptotically equivalent as the maximum difference between components is 1 which becomes negligeable when $m \longrightarrow +\infty$. The multiplication by $[(0,1)]$ give components differing by 0 or $m/2$, thus the multiplication by $\frac{2}{m}[(0,1)]$ give components differing by 0 or 1 again. The ratios between matrix coefficients is therefore tending towards 1. The sole noticable effect on the initial matrix (remember that we are primarly interested in relative proportions) is therefore a multiplicative effect which is 1 for normalized items. □

Theorem 26. — *The eigenvalues of the cardinal matrix of a P_variable in a $m = 2^{i_2}$_environment, $i_2 \longrightarrow +\infty$ is equal to:*

$$\sigma_1 = \tfrac{1}{m}, \quad \sigma_{1+\frac{m}{2}} = -\tfrac{1}{m}, \quad \sigma_j = 0 \textit{ if } j \neq \{1, 1+\tfrac{m}{2}\}$$

Proof. — The eigenvectors matrix of the cardinal matrix is the same of course as given in theorem 5 as the matrix is still circulant and we use theorem 6 for the eigenvalues expression. Here m is even and therefore we get:

$$\sigma_j = \frac{1}{m}\sum_{k=0}^{m-1} \#(m-k)\cdot w^{(j-1)\cdot k} = \frac{w^{j-1}}{m}\sum_{k=0}^{\frac{m}{2}-1} w^{2k\cdot(j-1)}$$

Going back to the definition of w, we get:

$$\sigma_j = \frac{e^{\frac{2\pi(j-1)\cdot i}{m}}}{m}\sum_{k=0}^{\frac{m}{2}-1} e^{\frac{4\pi k\cdot(j-1)\cdot i}{m}}$$

The terms of the sum are roots of the unit. The sum is equal to 0 unless $e^{\frac{4\pi(j-1)\cdot i}{m}} = 1$ (case $k=1$), that is $j \equiv 1 \mod m/2$. Hence the result. □

Theorem 27. — *The relative proportion, c being the parameter, of solutions of equation*

$$y_1 + y_2 + \ldots + y_n = c$$

is given by:

$$\#\#(c) = 2\cdot \prod_{\substack{p_i \backslash c \\ p_i \geq 3}} (1 - (\frac{-1}{p_i - 1})^{n-1}) \cdot \prod_{\substack{p_i \nmid c \\ p_i \geq 3}} (1 - (\frac{-1}{p_i-1})^{n})$$

Proof. — The degree of stability of a variable y_k being 1 for any instance $p_i > 2$, we can use the theorems 10 and 12. Having the same result for all targets except 0, we can reduce the square matrix' rank to 2.

$$\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ \ddots & \ddots & \ddots & \ddots & 1 \\ 1 & 1 & 1 & \cdots & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & p_i - 1 \\ 1 & p_i - 2 \end{pmatrix}$$

Then, after normalization, the matrix being identical for each variable, we apply an exponent n to the said matrix and multiply by the column vector K of theorem 7:

$$\begin{pmatrix} \#\#(c=0) \\ \#\#(c \neq 0) \end{pmatrix} = p_i \begin{pmatrix} 0 & 1 \\ \frac{1}{p_i-1} & \frac{p_i-2}{p_i-1} \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Using eigenvalues and eigenvectors, we then get:

$$\begin{pmatrix} \#\#(c=0) \\ \#\#(c \neq 0) \end{pmatrix} = (p_i-1) \cdot \begin{pmatrix} 1 & 1 \\ 1 & \frac{-1}{p_i-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \frac{-1}{(p_i-1)} \end{pmatrix}^n \cdot \begin{pmatrix} \frac{1}{p_i-1} & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and therefore finally:

$$\begin{pmatrix} \#\#(c \equiv 0 \mod p_i) \\ \#\#(c \neq 0 \mod p_i) \end{pmatrix} = \begin{pmatrix} 1 - (\frac{-1}{p_i-1})^{n-1} \\ 1 - (\frac{-1}{p_i-1})^n \end{pmatrix}$$

We remind, in the last relations, the instance and environment in which we operate. The result in environment $p_k^{i_{p_k}}$ is the same as the degree of stability is 1. To upgrade the result to an environment $2^{i_2} \cdot 3^{i_3} \ldots p_k^{i_{p_k}} \ldots p_r^{i_{p_r}}$, according to theorem 8, we have to multiply together these results and, as $r \longrightarrow +\infty$, we get the infinite products of the theorem except for the factor 2. In theorem 25, we identified the contribution of the instance $p_i = 2$ as a mere multiplication by a scalar (with global normalized effect a unit multiplication). A direct look to the studied equation provides an immediate explanation. With even respectively odd quantity of variables in $y_1 + y_2 + ... + y_n = c$, the result gives overwhelmingly even respectively odd c values, in other words a factor 2 amplification to even numbers' class while a factor 0 to the odd numbers' class. The multiplicative factor 2 will provide this effect in both (odd and even number of variables) cases. □

This result opens a window for a more generalized case of the Polignac conjecture if we go further than the mere comparison of proportions. The reader can refer to [**18**] Fermat Sheet Exercises 5 and 18 for full enumeration resolution and more (Waring sums and so on).

But, let us now go back to our first objective here, the Polignac problem. The projection of the set $-P$ in the p_i environment gives the same Chebotarev distribution as for the set P. Going through all the previous step, we will end with the same cardinal image and cardinal matrix enabling us to settle the case of the following Diophantine equation.

Theorem 28. — *The asymptotic proportions of solutions $\#c$ of the equation $c = p_1 - p_2$ is given by:*

$$\#(c) = 2 \prod_{\substack{p_i \backslash c \\ p_i \geq 3}} \frac{p_i}{p_i - 1} \prod_{\substack{p_i \nmid c \\ p_i \geq 3}} \frac{p_i \cdot (p_i - 2)}{(p_i - 1)^2}$$

Proof. — We use the general result for n variables and take $n = 2$. Besides the relative proportions is the same notion for #c and ##c. □

Theorem 29. — *Polignac conjecture* [**11**].
The asymptotic number of solutions $\pi_c(x)$ of the equation $c = p_1 - p_2$, $c = 2n \neq 0$, $n \in N$, is given by

$$\lim_{x \longrightarrow +\infty} \pi_c(x) = 2 \cdot C_2 \cdot \prod_{\substack{p_i \backslash c \\ p_i \geq 3}} \frac{p_i - 1}{p_i - 2} \cdot \frac{x}{\ln^2(x)}$$

where $C_2 = \prod_{p_i \geq 3}(1 - \frac{1}{(p_i-1)^2}) = \prod_{p_i \geq 3} \frac{p_i(p_i-2)}{(p_i-1)^2} \approx 0,66016\ldots$ is the twin prime constant (see reference [**6**]*).*

Proof. — Any p_i is dividing 0, thus from theorem 28 we get:

$$\#(0) = 2 \prod_{p_i \geq 3} \frac{p_i}{p_i - 1}$$

It follows the ratio of asymptotic events for a target different from 0 and target 0:

$$\frac{\#(c \neq 0)}{\#0} = \frac{\prod_{\substack{p_i \nmid c \\ p_i \geq 3}} \frac{p_i(p_i-2)}{(p_i-1)^2}}{\prod_{\substack{p_i \nmid c \\ p_i \geq 3}} \frac{p_i}{p_i-1}} = \prod_{\substack{p_i \nmid c \\ p_i \geq 3}} \frac{p_i - 2}{p_i - 1}$$

This is equivalent to:

$$\lim_{x \longrightarrow +\infty} \pi_{c \neq 0}(x) = \prod_{\substack{p_i \nmid c \\ p_i \geq 3}} \frac{p_i - 2}{p_i - 1} \lim_{x \longrightarrow +\infty} \pi_0(x)$$

The asymptotic number of solutions $\pi(x)$ for $c = 0$, that is the number of events $p_1 = p_2$ is the number of primes up to x when $x \longrightarrow +\infty$ and is equal to $\pi_0(x) \backsim x/\ln(x)$ according to the prime numbers theorem (see reference [**3**]) and therefore

$$\lim_{x \longrightarrow +\infty} \pi_{c \neq 0}(x) = \prod_{\substack{p_i \nmid c \\ p_i \geq 3}} \frac{p_i - 2}{p_i - 1} \cdot \frac{x}{\ln(x)} = \prod_{\substack{p_i \backslash c \\ p_i \geq 3}} \frac{p_i - 1}{p_i - 2} \cdot \prod_{p_i \geq 3} \frac{p_i - 2}{p_i - 1} \cdot \frac{x}{\ln(x)}$$

Let us then evaluate

$$\prod_{p_i \geq 3} \frac{p_i - 2}{p_i - 1} = \prod_{p_i \geq 3} \frac{p_i(p_i - 2)}{(p_i - 1)^2} \cdot \prod_{p_i \geq 3} \frac{p_i - 1}{p_i} = C_2 \cdot \prod_{p_i \geq 3} \frac{p_i - 1}{p_i} = 2 \cdot C_2 \cdot \prod_{p_i} \frac{p_i - 1}{p_i}$$

Besides, the Euler product derived from the Riemann zeta function according to reference [**7**] is

$$\zeta(z) = \sum_{n \geqslant 1} \frac{1}{n^z} = \prod_{p_i} \frac{p_i^z}{p_i^z - 1}$$

Therefore using the harmonic series and reference [**6**]

$$\prod_{p_i} \frac{p_i}{p_i - 1} = \sum_{n \geqslant 1} \frac{1}{n} = lim_{n \longrightarrow +\infty} H_n \sim lim_{n \longrightarrow +\infty} \ln(n)$$

This gives us the ultimate $\frac{1}{\ln(n)}$ factor needed to confirm the Polignac formula.

□

6.5. A standard technique. — Dealing with the instance $p_i = 2$, as the reader may have noticed is quite cumbersome even for the simplest case exposed here. It is much more efficient to study this case without going back each time to the original premises in the following way which besides is an equivalent way to handle a Diophantine equation enumeration problem.

Solving $R(z_1, z_2, \ldots, z_n) \equiv c \mod p_k^{i_{p_k}}$ is simply to write the data processing loop:

```
for $z_1 = 0$ to $p_k^{i_{p_k}} - 1$
if $z_1$ is a $P$_variable skip events $z_1 \equiv 0 \mod p_k$
for $z_2 = 0$ to $p_k^{i_{p_k}} - 1$
if $z_2$ is a $P$_variable skip events $z_2 \equiv 0 \mod p_k$
...
for $z_n = 0$ to $p_k^{i_{p_k}} - 1$
if $z_n$ is a $P$_variable skip events $z_n \equiv 0 \mod p_k$
$c \equiv R(z_1, z_2, \ldots, z_n) \mod p_k^{i_{p_k}}$
$\#c = \#c + 1$
Next $z_n$
...
Next $z_2$
Next $z_1$
```

Skipping events of the type $z_j \equiv 0 \mod p_k$ is the process of transforming z_j into the proper cardinal image if z_j is a P_variable while there is no need of this operation otherwise.

For $p_k = 2$ the values are in general small enough for a direct calculation from which one can deduce the proportions between the different cardinals #c and thereafter pinpointing the degree of stability with adapted number of loops:

```
$\ldots$
for $y_j = 1$ to $2^k$ step 2
$\ldots$
$c = R(y_j, \ldots)$
$\#c = \#c + 1$
$\ldots$
Next $y_j$
$\ldots$
```

With the Polignac's equation, and $p = 2$, we get precisely:

```
for $y_1 = 1$ to $2^k$ step 2
for $y_2 = 1$ to $2^k$ step 2
$c = y_1 - y_2$
$\#c = \#c + 1$
Next $y_2$
Next $y_1$
```

This give the following table with increasing k, showing a degree of stability equal to 1:

	#0	#1	#2	#3	#4	#5	#6	#7	...
k = 1	1	0							
k = 2	2	0	2	0					
k = 3	4	0	4	0	4	0	4	0	
...	...	...	...	...	...	...	...	...	...

We can use section 3 definition 3 equation 6 or directly evaluate the normalizing ratio providing a unit average on targets' enumeration (confirming here the multiplicative factor 2):

#0	#1	#2	#3	#4	#5	#6	#7	...
2	0	2	0	2	0	2	0	...

This standard technique brings us also back to the previous section dealing with the degree of stability, section 4 definition 5 equation 7, the 2-period pattern extending up to infinity allowing us, after the instance $p = 2$, the successive multiplications with the results given for the instances $p = 3$, $p = 5$, and so on.

Appendix D provides an example of a computer program enabling to calculate the normalized cardinal factors for the Friedlander-Iwaniec equation which will be our next subject. A few adaptations would make it suitable for other types of equations with degree of stability equal to 1 according to the standard technique just given above (change of monomials' powers, number of loops, adaptation of normalizing factor). It can also be adapted of course to higher degrees of stability according to the same exposed technique, but with a risk of rapid time processing overflow. However, for any dubious result with alternative technique evaluation, going back for comparison to this standard procedure is essential.

6.6. The Friedlander-Iwaniec case. — Friedlander and Iwaniec proved in 1996 the infinite number of primes y of the type $x_1^2 + x_2^4$. We will generalize the research to an equation

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

where we want to compare the number of solutions $\#c$ of the target c to the number of solutions $\#0$ of the target 0, when $y \longrightarrow +\infty$, for which Friedlander and Iwaniec gave the additional formula:

$$\lim_{y \longrightarrow +\infty} \#\{y = x_1^2 + x_2^4\} = fan(0) \cdot \frac{w \cdot y^{3/4}}{\ln(y)} \tag{13}$$

where $fan(0) = 4/\pi$ and $w = \int_0^1 (1 - t^4)^{\frac{1}{2}} dt = \frac{\Gamma(1/2)\Gamma(5/4)}{2 \cdot \Gamma(7/4)}$.

Theorem 30. — *The degree of stability of the Friedlander-Iwaniec general equation is equal to* 1.

Proof. — The equation being composed of independent monomials including a variable of prime numbers, we use theorem 14. □

Theorem 31. — *The ranks of the condensed matrices for the Friedlander-Iwaniec equation are given by the following cases:*

$Matrices$	$M0$	$M1$	$M2$	$M0.M1.M2$	
$Instance$ p	$var\ -y$ $gcd(p-1,1)$	$var\ x_1^2$ $gcd(p-1,2)$	$var\ x_2^4$ $gcd(p-1,4)$	$rank$ $1 + lcm$	$lesser$ $cases$
2	1	1	1	2	
$1\ mod\ 4$	1	2	4	5	$p = 1\ mod\ 8$ $p = 5\ mod\ 8$
$3\ mod\ 4$	1	2	2	3	

Proof. — The case $p = 2$ is treated by a specific evaluation as described earlier. Otherwise, the size of the condensed matrix except first line and column is given for each monomial by $d = gcd(p-1, n)$ where n is the degree of the variable in a p_environment. Theorem 19 then enables to conclude. □

Theorem 32. — *Let us have* $M0$ *a condensed cardinal matrix of* $-y$*. Then: Case 1: Rank = 5.*

$$M0 = \begin{pmatrix} 0 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-5)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-5)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-5)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-5)/4 \end{pmatrix}$$

Case 2: Rank = 3.

$$M0 = \begin{pmatrix} 0 & (p-1)/2 & (p-1)/2 \\ 1 & (p-3)/2 & (p-1)/2 \\ 1 & (p-1)/2 & (p-3)/2 \end{pmatrix}$$

Proof. — The cardinal matrices of $-y$ and y are identical according to theorem 9. Besides, using theorem 15, the condensed cardinal matrix of x is

$$\begin{pmatrix} 1 & (p-1)/md & \cdots & (p-1)/md \\ 1 & (p-1)/md & \cdots & (p-1)/md \\ \cdots & \cdots & \cdots & \cdots \\ 1 & (p-1)/md & \cdots & (p-1)/md \end{pmatrix}$$

where md is any multiple of d and divider of $p-1$. Here we have $d = 1$, so the only condition is that md divides $p-1$. The condensed cardinal matrices of each case is then deduced by subtracting the identity matrix according to property 12. □

Theorem 33. — *Let us have* $M1$ *a condensed cardinal matrix of* x_1^2*. Then: Case 1: Rank = 5.*

$$M1 = \begin{pmatrix} 1 & (p-1)/2 & 0 & (p-1)/2 & 0 \\ 2 & x_1 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_3+1 & x_4 & x_1+1 \\ 2 & x_3 & x_4 & x_1 & x_2 \\ 0 & x_4 & x_1+1 & x_2 & x_3+1 \end{pmatrix}$$

where

$$x_4 = p - 2 - x_1 - x_2 - x_3$$

and where, for u *and* v *integers within the intervals* $[0,(p-1)/2[$ *and* $[0,(p-1)/4[$ *respectively,*

$$\begin{aligned} x_1 &= 1 + 2.\#(u,v) \ \backslash \ g^0 \equiv g^{2u} + g^{4v} \mod p \\ x_2 &= 2.\#(u,v) \ \backslash \ g^1 \equiv g^{2u} + g^{4v} \mod p \\ x_3 &= 2.\#(u,v) \ \backslash \ g^2 \equiv g^{2u} + g^{4v} \mod p \\ x_4 &= 2.\#(u,v) \ \backslash \ g^3 \equiv g^{2u} + g^{4v} \mod p \end{aligned}$$

Case 2: Rank = 3.

$$M1=\begin{pmatrix}1 & 0 & p-1\\ 2 & (p-1)/2 & (p-3)/2\\ 0 & (p+1)/2 & (p-1)/2\end{pmatrix}$$

Proof. — The values of the components for the first line and first column are obtained straightforwardly thanks to theorem 15.
For case 1, as shown in theorem 31, we have $p \equiv 1 \mod 4$, $d=2$ and $md=4$. We get $\frac{p-1}{2} \equiv 0 \mod 2$ and the symmetry versus the principal diagonal in the blocks' area is then deduced from property 13 case 1. Therefore $M1-I$ is equal to

$$M1-I=\begin{pmatrix}0 & (p-1)/2 & 0 & (p-1)/2 & 0\\ 2 & x_1-1 & x_2 & x_3 & x_4\\ 0 & x_2 & x_5 & x_6 & x_7\\ 2 & x_3 & x_6 & x_8 & x_9\\ 0 & x_4 & x_7 & x_9 & x_{10}\end{pmatrix}$$

for some integers x_i, $i=1$ to 10, to be defined. Then using property 14 case 1, the transformations $r' \equiv r+2 \mod 4$ and $s' \equiv s+2 \mod 4$ lead to the equivalence of positions starting with index $(0,0)$ on the second line and second column of the condensed matrix:

$$\begin{pmatrix}0\\0\end{pmatrix}\equiv\begin{pmatrix}2\\2\end{pmatrix},\ \begin{pmatrix}1\\0\end{pmatrix}\equiv\begin{pmatrix}3\\2\end{pmatrix},\ \begin{pmatrix}3\\0\end{pmatrix}\equiv\begin{pmatrix}1\\2\end{pmatrix},\ \begin{pmatrix}1\\1\end{pmatrix}\equiv\begin{pmatrix}3\\3\end{pmatrix}.$$

Therefore we get the following matrix:

$$M1-I=\begin{pmatrix}0 & (p-1)/2 & 0 & (p-1)/2 & 0\\ 2 & x_1-1 & x_2 & x_3 & x_4\\ 0 & x_2 & x_5 & x_4 & x_7\\ 2 & x_3 & x_4 & x_1-1 & x_2\\ 0 & x_4 & x_7 & x_2 & x_5\end{pmatrix}$$

The sum of the components of each line being the same provides the additional equality $2+x_1-1+x_3=x_5+x_7$ as x_2 and x_4 are common terms in the second and third lines of the matrix. Then using lemma 2, given later on in this article, we can write $x_5=x_3$ and therefore $x_7=x_1+1$. So that now:

$$M1-I=\begin{pmatrix}0 & (p-1)/2 & 0 & (p-1)/2 & 0\\ 2 & x_1-1 & x_2 & x_3 & x_4\\ 0 & x_2 & x_3 & x_4 & x_1+2\\ 2 & x_3 & x_4 & x_1-1 & x_2\\ 0 & x_4 & x_1+1 & x_2 & x_3\end{pmatrix}$$

The sum of a line being equal to $p-1$ by construction, we get $x_4=p-2-x_1-x_2-x_3$, reducing unknows to x_1, x_2 and x_3. Using theorem 18, we then can address the primitive roots' equations for the blocks' area.

For case 2, $p \equiv 3 \mod 4$, $d = 2$ and therefore $(p-1)/2 \equiv d/2 \mod d$, thus the value $p-1$ on the third position of the first line instead of the second. The initial matrix can then be written using property 13 case 2:

$$M1 = \begin{pmatrix} 1 & 0 & p-1 \\ 2 & x_1 & x_2 \\ 0 & x_3 & x_1 \end{pmatrix}$$

The sum of the components of each line is the same, we get:

$$M1 - I = \begin{pmatrix} 0 & 0 & p-1 \\ 2 & x_1-1 & x_2 \\ 0 & x_2+2 & x_1-1 \end{pmatrix}$$

Having $md = d$, we can use property 15 case 2 which gives $x_2 = x_1 + 1$. Thus we get the matrix

$$M1 = \begin{pmatrix} 1 & 0 & p-1 \\ 2 & x_1 & x_1-1 \\ 0 & x_1+1 & x_1 \end{pmatrix}$$

Because the sum of the components of each line of $M1$ is equal to p, we get the proposed result. □

Theorem 34. — *Let us have $M2$ the condensed cardinal matrix of x_2^4. Then: Case 1a: Rank = 5. Lesser case $p \equiv 1 \mod 8$.*

$$M2 = \begin{pmatrix} 1 & p-1 & 0 & 0 & 0 \\ 4 & x_1-3 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_4+1 & x_5 & x_5 \\ 0 & x_3 & x_5 & x_3+1 & x_5 \\ 0 & x_4 & x_5 & x_5 & x_2+1 \end{pmatrix}$$

where

$$\begin{aligned} x_3 &= \tfrac{p-1}{3} - \tfrac{x_1}{3} \\ x_4 &= \tfrac{2(p-1)}{3} - \tfrac{2x_1}{3} - x_2 \\ x_5 &= \tfrac{p-1}{6} + \tfrac{x_1}{3} \end{aligned}$$

and where, for u and v integers within the interval $[0, (p-1)/4[$,

$$\begin{array}{lll} x_1 = 4 + 4.\#(u,v) & \setminus\ g^0 \equiv g^{4u} + g^{4v} & \mod p \\ x_2 = 4.\#(u,v) & \setminus\ g^1 \equiv g^{4u} + g^{4v} & \mod p \\ x_3 = 4.\#(u,v) & \setminus\ g^2 \equiv g^{4u} + g^{4v} & \mod p \\ x_4 = 4.\#(u,v) & \setminus\ g^3 \equiv g^{4u} + g^{4v} & \mod p \end{array}$$

Case 1b: Rank = 5. Lesser case $p \equiv 5 \mod 8$.

$$M2 = \begin{pmatrix} 1 & 0 & 0 & p-1 & 0 \\ 4 & x_3+1 & x_5 & x_3 & x_5 \\ 0 & x_4 & x_5+1 & x_5 & x_2 \\ 0 & x_1 & x_2 & x_3+1 & x_4 \\ 0 & x_2 & x_4 & x_5 & x_5+1 \end{pmatrix}$$

where

$$\begin{gathered} x_3 = \tfrac{p-5}{3} - \tfrac{x_1}{3} \\ x_4 = \tfrac{2(p+1)}{3} - \tfrac{2x_1}{3} - x_2 \\ x_5 = \tfrac{p-5}{6} + \tfrac{x_1}{3} \end{gathered}$$

and where, for u and v integers within the interval $[0,(p-1)/4[$,

$$\begin{aligned} x_3 &= 4.\#(u,v) \ \backslash \ g^0 \equiv g^{4u} + g^{4v} \mod p \\ x_4 &= 4.\#(u,v) \ \backslash \ g^1 \equiv g^{4u} + g^{4v} \mod p \\ x_1 &= 4.\#(u,v) \ \backslash \ g^2 \equiv g^{4u} + g^{4v} \mod p \\ x_2 &= 4.\#(u,v) \ \backslash \ g^3 \equiv g^{4u} + g^{4v} \mod p \end{aligned}$$

Case 2: Rank = 3.

$$M2 = \begin{pmatrix} 1 & 0 & p-1 \\ 2 & (p-1)/2 & (p-3)/2 \\ 0 & (p+1)/2 & (p-1)/2 \end{pmatrix}$$

Proof. — The values of the components for the first line and first column are again obtained straightforwardly thanks to theorem 15.

For case 1, $d = md = 4$, so that the cardinal matrix is the most condensed possible. We can therefore use properties 13 and 15. Property 13 results in the transformations $r \equiv s \mod 4$ and $s \equiv r \mod 4$ as in this case $(p-1)/2 \equiv 0 \mod 4$. Therefore the blocks'area of the condensed matrix is symmetrical and we can write:

$$M2 - I = \begin{pmatrix} 0 & p-1 & 0 & 0 & 0 \\ 4 & x_1-4 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_5 & x_6 & x_7 \\ 0 & x_3 & x_6 & x_8 & x_9 \\ 0 & x_4 & x_7 & x_9 & x_{10} \end{pmatrix}$$

Then, using property 15, the transformations $r \equiv -r \mod 4$ and $s \equiv -r + s \mod 4$ lead to the equivalence of positions starting with index $(0,0)$ on the second line and column of the condensed matrix:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 3 \end{pmatrix}.$$

After reindexing x_5 to x_6, we get the following matrix:

$$M2 - I = \begin{pmatrix} 0 & p-1 & 0 & 0 & 0 \\ 4 & x_1 - 4 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_4 & x_5 & x_5 \\ 0 & x_3 & x_5 & x_3 & x_5 \\ 0 & x_4 & x_5 & x_5 & x_2 \end{pmatrix}$$

The sum of the components of each line being the same and equal to $p-1$ provides then the three additional equalities given above reducing the number of unknowns to x_1 and x_2. Using theorem 18, we then can address the primitive roots' equations for the blocks' area. Again, the exponent s in the theorem is equal to 2 which provides the proposed result.

For the lesser case $p \equiv 5 \mod 8$, $(p-1)/2 \equiv 2 \mod 4$ and, by property 13, equal components' positions in the blocks' area are now given by transformations $r \equiv s + 2 \mod 4$ and $s \equiv r + 2 \mod 4$.

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 3 \end{pmatrix}.$$

This gives the matrix

$$M2 - I = \begin{pmatrix} 0 & 0 & 0 & p-1 & 0 \\ 4 & x_3 & x_6 & x_8 & x_9 \\ 0 & x_4 & x_5 & x_9 & x_{10} \\ 0 & x_1 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_7 & x_6 & x_5 \end{pmatrix}$$

Then, using property 15, the transformations $r \equiv -r \mod 4$ and $s \equiv -r+s+2 \mod 4$ lead to the equivalence of positions:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

This provides the matrix:

$$M2 - I = \begin{pmatrix} 0 & 0 & 0 & p-1 & 0 \\ 4 & x_3 & x_5 & x_3 & x_5 \\ 0 & x_4 & x_5 & x_5 & x_2 \\ 0 & x_1 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_4 & x_5 & x_5 \end{pmatrix}$$

Again, the sum of the components of each line being the same and equal to p, we get the three former additional equalities reducing the number of unknowns

to two.
For case 2, $p \equiv 3 \mod 4$, $d = 2$ and therefore we get the same matrix of rank 3 as earlier for the monomial x_1^2. □

Now we can go back to theorem 31 and construct the matrices products to solve our general Friedlander-Iwaniec equation. We get the following cases:
Theorem 35. — *Let us name $M0$ the condensed matrix for variable $-p$, M1 the condensed matrix for variable x_1^2, M2 the condensed matrix for variable x_2^4 and the column vector K as defined earlier. Then:*
Case 1: $p = 2$.

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^u) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Case 2: $p \equiv 3 \mod 4$.

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{2u}) \\ \#\#(g.g^{2u}) \end{pmatrix} = \frac{1}{p.(p-1)} \begin{pmatrix} p^2-1 \\ p^2-p-1 \\ p^2-p-1 \end{pmatrix}$$

Case 3 : $p \equiv 1 \mod 4$.

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{4u}) \\ \#\#(g.g^{4u}) \\ \#\#(g^2.g^{4u}) \\ \#\#(g^3.g^{4u}) \end{pmatrix} = \frac{1}{p.(p-1)} \begin{pmatrix} (p-1)^2 \\ p^2-2-4x_1 \\ p^2-4x_2 \\ p^2-2-4x_3 \\ p^2-4x_4 \end{pmatrix}$$

where

$$x_4 = p - 2 - x_1 - x_2 - x_3$$

and where, for u and v integers within the intervals $[0,(p-1)/2[$ and $[0,(p-1)/4[$ respectively,

$$\begin{aligned} x_1 &= 1 + 2.\#(u,v) \ \backslash \ g^0 \equiv g^{2u} + g^{4v} \mod p \\ x_2 &= 2.\#(u,v) \ \backslash \ g^1 \equiv g^{2u} + g^{4v} \mod p \\ x_3 &= 2.\#(u,v) \ \backslash \ g^2 \equiv g^{2u} + g^{4v} \mod p \\ x_4 &= 2.\#(u,v) \ \backslash \ g^3 \equiv g^{2u} + g^{4v} \mod p \end{aligned}$$

Proof. — Let us name $M0$ the condensed matrix for variable $-p$, $M1$ the condensed matrix for variable x_1^2, $M2$ the condensed matrix for variable x_2^4, each one with appropriate rank. Let us consider also the column vector K as defined earlier.
Then case 1, $p = 2$ is obtained by direct calculation:

$$\begin{aligned} \begin{pmatrix} \#\#(0) \\ \#\#(g^u) \end{pmatrix} &= \tfrac{1}{p(p-1)} M0.M1.M2.K \\ &= \tfrac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

For case 2, $p \equiv 3 \mod 4$, we have $M1 = M2$ and the following calculations:

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{2u}) \\ \#\#(g.g^{2u}) \end{pmatrix} = \frac{1}{p.(p-1)} M0.M1.M2.K$$

$$= \frac{1}{p.(p-1)} M0.M1. \begin{pmatrix} 1 & 0 & p-1 \\ 2 & (p-1)/2 & (p-3)/2 \\ 0 & (p+1)/2 & (p-1)/2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$= \frac{1}{p.(p-1)} M0 \begin{pmatrix} 1 & 0 & p-1 \\ 2 & (p-1)/2 & (p-3)/2 \\ 0 & (p+1)/2 & (p-1)/2 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$$

$$= \frac{1}{p.(p-1)} \begin{pmatrix} 0 & (p-1)/2 & (p-1)/2 \\ 1 & (p-3)/2 & (p-1)/2 \\ 1 & (p-1)/2 & (p-3)/2 \end{pmatrix} \begin{pmatrix} 1 \\ p+1 \\ p+1 \end{pmatrix}$$

$$= \frac{1}{p.(p-1)} \begin{pmatrix} p^2-1 \\ p^2-p-1 \\ p^2-p-1 \end{pmatrix}$$

The reader is invited to remembered the distinctive respective definitions of x_i in different M_j matrices. Then, for case 3a, $p \equiv 1 \mod 8$, we get:

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{4u}) \\ \#\#(g.g^{4u}) \\ \#\#(g^2.g^{4u}) \\ \#\#(g^3.g^{4u}) \end{pmatrix} = \frac{1}{p.(p-1)} M0.M1.M2.K$$

$$= \frac{1}{p.(p-1)} M0.M1. \begin{pmatrix} 1 & p-1 & 0 & 0 & 0 \\ 4 & x_1-3 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_4+1 & x_5 & x_5 \\ 0 & x_3 & x_5 & x_3+1 & x_5 \\ 0 & x_4 & x_5 & x_5 & x_2+1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \frac{1}{p.(p-1)} M0 \begin{pmatrix} 1 & (p-1)/2 & 0 & (p-1)/2 & 0 \\ 2 & x_1 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_3+1 & x_5 & x_6 \\ 2 & x_3 & x_5 & x_1 & x_2 \\ 0 & x_4 & x_6 & x_2 & x_3+1 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \frac{1}{p.(p-1)} \begin{pmatrix} 0 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-5)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-5)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-5)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-5)/4 \end{pmatrix} \begin{pmatrix} 2p-1 \\ 2+4x_1 \\ 4x_2 \\ 2+4x_3 \\ 4x_4 \end{pmatrix}$$

$$= \frac{1}{p.(p-1)} \begin{pmatrix} (p-1)(x_1+x_2+x_3+x_4+1) \\ (p-1)(x_1+x_2+x_3+x_4+1)+2p-3-4x_1 \\ (p-1)(x_1+x_2+x_3+x_4+1)+2p-1-4x_2 \\ (p-1)(x_1+x_2+x_3+x_4+1)+2p-3-4x_3 \\ (p-1)(x_1+x_2+x_3+x_4+1)+2p-3-4x_4 \end{pmatrix}$$

$$= \frac{1}{p.(p-1)} \begin{pmatrix} (p-1)^2 \\ p^2-2-4x_1 \\ p^2-4x_2 \\ p^2-2-4x_3 \\ p^2-4x_4 \end{pmatrix}$$

Then we go back to theorem 33 case 1 for the primitive roots' equations. For case 3b, $p \equiv 5 \mod 8$, we get:

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{4u}) \\ \#\#(g.g^{4u}) \\ \#\#(g^2.g^{4u}) \\ \#\#(g^3.g^{4u}) \end{pmatrix} = \frac{1}{p.(p-1)} M0.M1.M2.K$$

The $M0$ and $M1$ matrices are the same as for case 3a. Matrix $M2$ is now different, but the product $M2.K$ is the same column vector:

$$\begin{pmatrix} 1 \\ 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Therefore the product will be the same as for case 3a. Besides the primitive roots' equation as also unchanged. Hence the result. □

Note. — Let us observe that there is no need here for the full expression of the cardinal matrix $M2$ to solve the Friedlander-Iwaniec equation. However, this matrix would be indispensable to compare asymptotically, for example, for different targets c, the number of solutions of the specific Waring type equation

$$p = x_1^4 + x_2^4 + ... + x_k^4 + c.$$

In this case, one would use the matrix product

$$M = M0.M2^k.$$

Theorem 36. — *Asymptotically, the ratio between the number of solutions of the Friedlander-Iwaniec equation with target c compared to the equation with target* 0 *is equal to:*

$$\prod_{\substack{p\equiv 1 \mod 4\\ i\backslash\{c\equiv g^{i \mod 4} \mod p\}}} \frac{1+\frac{p-4(x_{i+1}+\frac{(i+1) \mod 2}{2})}{p(p-1)}}{1-\frac{1}{p}} \prod_{p\equiv 3 \mod 4} \frac{1-\frac{1}{p(p-1)}}{1+\frac{1}{p}}$$

Proof. — According to theorem 8, the ratio between the number of solutions of the Diophantine equation with target c compared to the equation with target 0 is the ratio of the cardinal factors $fan(c)/fan(0)$. The multiplicative factors for $p=2$ is 1 as indicated in theorem 35 and therefore has no effect. Then using the other values obtained in theorem 35, the infinite product of the factors of $fan(0)$ and $fan(c\neq 0)$ are respectively

$$\prod_{p\equiv 1 \mod 4} 1-\frac{1}{p} \prod_{p\equiv 3 \mod 4} 1+\frac{1}{p}$$

and

$$\prod_{\substack{p\equiv 1 \mod 4\\ i\backslash\{c\equiv g^{i \mod 4} \mod p\}}} 1+\frac{p-4(x_{i+1}+\frac{(i+1) \mod 2}{2})}{p(p-1)} \prod_{p\equiv 3 \mod 4} 1-\frac{1}{p(p-1)}$$

In the second subscript, it is of course i which has to be deduced from c, p and g at each occurrence $p\equiv 1 \mod 4$. Regrouping the terms having modulo 4 in common, we get the result. □

Appendix E provides a computer program enabling to calculate the data resulting from theorem 35. It gets the data faster than the basic program given previously in appendix D.

The Friedlander-Iwaniec theorem was refined by Roger Heath-Brown and Li Xiannan in 2017 [**14**]. In particular, they proved that the polynomial x^2+p^4 represents infinitely many primes where the variable p is required to be prime numbers. With the premises of our study, we can immediately get the general enumeration's result for the Diophantine equation $p=x^2+y^4-c$ for some target c compared with the enumeration of target 0. All we have to do to get a literal formula is to replace the previous $M2$ matrices with $M2-I$ and to multiply the former normalizing factor $\frac{1}{p(p-1)}$ by $\frac{p}{p-1}$, thus getting $\frac{1}{(p-1)^2}$. This leads straightforward to:

Theorem 37. — *The enumeration of the Heath-Brown—Xiannan equation is pending on the three cases:*

Case 1: $p = 2$.

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^u) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Case 2: $p \equiv 3 \mod 4$.

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{2u}) \\ \#\#(g.g^{2u}) \end{pmatrix} = \frac{1}{(p-1)^2} \begin{pmatrix} p(p-1) \\ p^2-2p+1 \\ p^2-2p-1 \end{pmatrix}$$

Case 3 : $p \equiv 1 \mod 4$.

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{4u}) \\ \#\#(g.g^{4u}) \\ \#\#(g^2.g^{4u}) \\ \#\#(g^3.g^{4u}) \end{pmatrix} = \frac{1}{(p-1)^2} \begin{pmatrix} (p-1)(p-2) \\ p(p-1)-4x_1 \\ p(p-1)-4x_2 \\ p(p-1)-4x_3 \\ p(p-1)-4x_4 \end{pmatrix}$$

where

$$x_4 = p - 2 - x_1 - x_2 - x_3$$

and where, for u and v integers within the intervals $[0,(p-1)/2[$ *and* $[0,(p-1)/4[$ *respectively,*

$$\begin{aligned} x_1 &= 1 + 2.\#(u,v) \setminus g^0 \equiv g^{2u} + g^{4v} \mod p \\ x_2 &= 2.\#(u,v) \setminus g^1 \equiv g^{2u} + g^{4v} \mod p \\ x_3 &= 2.\#(u,v) \setminus g^2 \equiv g^{2u} + g^{4v} \mod p \\ x_4 &= 2.\#(u,v) \setminus g^3 \equiv g^{2u} + g^{4v} \mod p \end{aligned}$$

Proof. — We operate as with the previous example.
For case 1:

$$\begin{aligned} \begin{pmatrix} \#\#(0) \\ \#\#(g^u) \end{pmatrix} &= \tfrac{1}{(p-1)^2} M0.M1.(M2-I).K \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{aligned}$$

For case 2, $p \equiv 3 \mod 4$, we have $M1 = M2$ and the following calculations:

$$\begin{aligned} \begin{pmatrix} \#\#(0) \\ \#\#(g^{2u}) \\ \#\#(g.g^{2u}) \end{pmatrix} &= \tfrac{1}{(p-1)^2} M0.M1.(M2-I).K \\ &= \tfrac{1}{(p-1)^2} M0.M1. \begin{pmatrix} 0 & 0 & p-1 \\ 2 & (p-3)/2 & (p-3)/2 \\ 0 & (p+1)/2 & (p-3)/2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \end{aligned}$$

$$= \tfrac{1}{(p-1)^2} M0 \begin{pmatrix} 1 & 0 & p-1 \\ 2 & (p-1)/2 & (p-3)/2 \\ 0 & (p+1)/2 & (p-1)/2 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}$$

$$= \tfrac{1}{(p-1)^2} \begin{pmatrix} 0 & (p-1)/2 & (p-1)/2 \\ 1 & (p-3)/2 & (p-1)/2 \\ 1 & (p-1)/2 & (p-3)/2 \end{pmatrix} \begin{pmatrix} 0 \\ p-1 \\ p+1 \end{pmatrix}$$

$$= \tfrac{1}{(p-1)^2} \begin{pmatrix} p(p-1) \\ p^2-2p+1 \\ p^2-2p-1 \end{pmatrix}$$

For case 3, $p \equiv 1 \mod 8$, we get:

$$\begin{pmatrix} \#\#(0) \\ \#\#(g^{4u}) \\ \#\#(g.g^{4u}) \\ \#\#(g^2.g^{4u}) \\ \#\#(g^3.g^{4u}) \end{pmatrix} = \tfrac{1}{(p-1)^2} M0.M1.(M2-I).K$$

$$= \tfrac{1}{(p-1)^2} M0.M1. \begin{pmatrix} 0 & p-1 & 0 & 0 & 0 \\ 4 & x_1-4 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_4 & x_5 & x_5 \\ 0 & x_3 & x_5 & x_3 & x_5 \\ 0 & x_4 & x_5 & x_5 & x_2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \tfrac{1}{(p-1)^2} M0 \begin{pmatrix} 1 & (p-1)/2 & 0 & (p-1)/2 & 0 \\ 2 & x_1 & x_2 & x_3 & x_4 \\ 0 & x_2 & x_3+1 & x_5 & x_6 \\ 2 & x_3 & x_5 & x_1 & x_2 \\ 0 & x_4 & x_6 & x_2 & x_3+1 \end{pmatrix} \begin{pmatrix} 0 \\ 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \tfrac{1}{(p-1)^2} \begin{pmatrix} 0 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-5)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-5)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-5)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-5)/4 \end{pmatrix} \begin{pmatrix} 2(p-1) \\ 4x_1 \\ 4x_2 \\ 4x_3 \\ 4x_4 \end{pmatrix}$$

$$= \tfrac{1}{(p-1)^2} \begin{pmatrix} (p-1)(x_1+x_2+x_3+x_4) \\ (p-1)(x_1+x_2+x_3+x_4)+2p-2-4x_1 \\ (p-1)(x_1+x_2+x_3+x_4)+2p-2-4x_2 \\ (p-1)(x_1+x_2+x_3+x_4)+2p-2-4x_3 \\ (p-1)(x_1+x_2+x_3+x_4)+2p-2-4x_4 \end{pmatrix}$$

$$= \frac{1}{(p-1)^2}\begin{pmatrix} (p-1)(p-2) \\ p(p-1)-4x_1 \\ p(p-1)-4x_2 \\ p(p-1)-4x_3 \\ p(p-1)-4x_4 \end{pmatrix}$$

where x_1, x_2, x_3 and x_4 are the values extracted from the primitive roots' equation of theorem 35. □

Theorem 38. — *Asymptotically the ratio between the number of solutions of the Heath-Brown—Xiannan equation with target c compared to the equation with target* 0 *is equal to:*

$$\prod_{\substack{p\equiv 1 \mod 4\\ i\backslash\{c\equiv g^{i \mod 4} \mod p\}}} \frac{1+\frac{p-1-4x_{i+1}}{(p-1)^2}}{1-\frac{1}{p-1}} \prod_{\substack{p\equiv 3 \mod 4\\ i\backslash\{c\equiv g^{i \mod 2} \mod p\}}} \frac{1-\frac{1-(-1)^i}{(p-1)^2}}{1+\frac{1}{p-1}}$$

Proof. — According to 8 the ratio between the number of solutions of the Diophantine equation with target c compared to the equation with target 0 is the ratio of the cardinal factors $fan(c)/fan(0)$. The multiplicative factors for $p=2$ is 1 as indicated in theorem 35 and therefore has no effect. Then using the other values obtained in theorem 37, the infinite product of the factors of $fan(0)$ and $fan(c\neq 0)$ are respectively

$$\prod_{p\equiv 1 \mod 4} 1-\frac{1}{p-1}\prod_{p\equiv 3 \mod 4} 1+\frac{1}{p-1}$$

and

$$\prod_{\substack{p\equiv 1 \mod 4\\ i\backslash\{c\equiv g^{i \mod 4} \mod p\}}} 1+\frac{p-1-4x_{i+1}}{(p-1)^2} \prod_{\substack{p\equiv 3 \mod 4\\ i\backslash\{c\equiv g^{i \mod 2} \mod p\}}} 1-\frac{1-(-1)^i}{(p-1)^2}$$

In the second subscripts, it is of course i which has to be deduced from c, p and g. For the occurrences $p\equiv 3 \mod 4$ where $i=0$, we get $1-(-1)^i=0$ and therefore the local cardinal factor is simply 1. Regrouping the modulo 4 terms, we get the result. □

Proposition 1. — *The Friedlander-Iwaniec and the Heath-Brown—Xiannan generalized equations have an infinite number of solutions for any target c.*
Partial proof. — The Hardy-Littlewood twin prime constant is equal to

$$\prod_{p>2} 1-\frac{1}{(p-1)^2}\simeq 0.6601061$$

according to reference [8]. Therefore

$$\prod_{p>2} 1-\frac{1}{p(p-1)}$$

and

$$\prod_{p>2} 1+\frac{1}{p(p-1)}$$

converge as well as

$$\prod_{p\equiv 1 \mod 4} 1-\frac{1}{p(p-1)}$$

and

$$\prod_{p\equiv 3 \mod 4} 1+\frac{1}{p(p-1)}$$

The following Euler product converges and is equal to:

$$\prod_{p\equiv 1 \mod 4} 1-\frac{1}{p}\prod_{p\equiv 3 \mod 4} 1+\frac{1}{p}=\frac{4}{\pi}$$

according to reference [8] using the Leibniz formula.
Then:

$$\prod_{p\equiv 1 \mod 4} 1-\frac{1}{p-1}\prod_{p\equiv 3 \mod 4} 1+\frac{1}{p-1}=\frac{4}{\pi}\prod_{p\equiv 1 \mod 4}\frac{1-\frac{1}{p-1}}{1-\frac{1}{p}}\prod_{p\equiv 3 \mod 4}\frac{1+\frac{1}{p-1}}{1+\frac{1}{p}}$$

Asymptotically $\frac{1}{p}\longrightarrow 0$ and therefore:

$$\frac{1-\frac{1}{p-1}}{1-\frac{1}{p}}\simeq 1-\frac{1}{p-1}+\frac{1}{p}=1-\frac{1}{p(p-1)}$$

and similarly

$$\frac{1+\frac{1}{p-1}}{1+\frac{1}{p}}\simeq 1+\frac{1}{p(p-1)}$$

This gives a second order correction to the Leibniz formula and the infinite product with $p-1$ on the denominators, instead of p, will also converge (and the correction factor is about 1.0781). The same is true for the product

$$\prod_{\substack{p\equiv 3 \mod 4\\ i\backslash\{c\equiv g^{i \mod 2} \mod p\}}} 1-\frac{1-(-1)^i}{(p-1)^2}$$

leaving us with the last checks to be done on

$$\prod_{\substack{p=\equiv \mod 4 \\ i\backslash\{c\equiv g^{i \mod 4} \mod p\}}} 1+\frac{p-4(x_{i+1}+\frac{(i+1) \mod 2}{2})}{p(p-1)}$$

$$\prod_{\substack{p\equiv 1 \mod 4 \\ i\backslash\{c\equiv g^{i \mod 4} \mod p\}}} 1+\frac{p-1-4x_{i+1}}{(p-1)^2}$$

We have $x_1+x_2+x_3+x_4=p-2$, each x_i being a positive integer. Thus x_i is a fractional part of p, written underneath $frac(p)$. Therefore the two previous expressions are Euler infinite products looking like

$$\prod_{\substack{p\equiv 1 \mod 4 \\ i\backslash\{c\equiv g^{i \mod 4} \mod p\}}} 1\pm\frac{3.frac(p)}{(p-1)^2}$$

The multiplicative factor 3 in this expression will only multiply the constant value of the expression compared with the result of a factor 1 as in this Leibniz' type formula, therefore not changing the limit property (that is convergence or divergence). However, because the sum of the reciprocals of all prime numbers diverges, we need the same proportion of + and − signs (where we wrote ±) in order to get a convergent value here, which depends on the equal even and odd proportions of i resulting from $c\equiv g^{i \mod 2} \mod p$ equation. Even a slight difference will give a divergent result. In this case, if the Euler product diverges to $+\infty$, the number of solutions of the Diophantine equation will be infinite. If on the contrary it "diverges" to the 0 value, the number of solutions may still be infinite (it depends of the rate of convergence towards 0).

Although of no critical scope, the primitive roots' equation remains somewhat cumbersome to use. A "simpler" expression with faster data processing performance would be welcome. In order to do that, let us start with the following theorem before going further.

Theorem 39. — *Let us have g a primitive root of p. The numbers, respectively n_1 and n_2, of integer solutions $\#(u,v)$, $u\in[0,\frac{p-1}{2}[$, $v\in[0,\frac{p-1}{2}[$ to the equations*

$$\begin{array}{l} n_1=\#(u,v)\ \backslash\ g^0\equiv g^{2u}+g^{2v} \mod p \\ n_2=\#(u,v)\ \backslash\ g^1\equiv g^{2u}+g^{2v} \mod p \end{array}$$

is given by

$$\begin{pmatrix} n_1+1 \\ n_2 \end{pmatrix}=\begin{pmatrix} \frac{p-(-1)^{\frac{p-1}{2}}}{4} \\ \frac{p-(-1)^{\frac{p-1}{2}}}{4} \end{pmatrix}$$

Proof. — Let us use the cardinal matrix of the monomial y^2.
If $p \equiv 1 \mod 4$, we refer to the property 13 case 1 to get:

$$\begin{pmatrix} 0 & p-1 & 0 \\ 2 & x_1 & x_2 \\ 0 & x_2 & x_3 \end{pmatrix}$$

Therefore using property 15, the transformations $r \equiv -r \mod 2$ and $s \equiv -r + s \mod 2$ lead to the equivalence of positions in the block's area (the positions being referenced as previously):

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

so that we get the following matrix:

$$\begin{pmatrix} 0 & p-1 & 0 \\ 2 & x_1 & x_2 \\ 0 & x_2 & x_2 \end{pmatrix}$$

Using equalities to $p-1$ for each line, we end with the matrix:

$$\begin{pmatrix} 0 & p-1 & 0 \\ 2 & (p-5)/2 & (p-1)/2 \\ 0 & (p-1)/2 & (p-1)/2 \end{pmatrix}$$

According to theorem 18, the first column of the block's area gives the primitive roots' equations with a factor d correction and therefore:

$$x_1 = (p-5)/2$$
$$x_2 = (p-1)/2$$

where

$$x_1 = 2 \cdot \#(u,v) \setminus g^0 \equiv g^{2u} + g^{2v} \mod p$$
$$x_2 = 2 \cdot \#(u,v) \setminus g^1 \equiv g^{2u} + g^{2v} \mod p$$

and where $u \in [0, \frac{p-1}{2}[$, $v \in [0, \frac{p-1}{2}[$.
The case $p \equiv 3 \mod 4$, has already being solve earlier using the same tools. The matrix is equal to:

$$\begin{pmatrix} 0 & 0 & p-1 \\ 2 & (p-3)/2 & (p-3)/2 \\ 0 & (p+1)/2 & (p-3)/2 \end{pmatrix}$$

resulting in

$$x_1 = (p-3)/2$$
$$x_2 = (p+1)/2$$

The theorem follows then by taking $n_2 = \frac{1}{2}x_2$, the correction $1/2$ coming from the primitive roots' equation, and n_1 is deduced afterwards in a similar way. □

Lemma 1. — *Let us have* $p = 1 \mod 4$ *and* g *a primitive root of* p*. Then the numbers of integer solutions* $\#(u,v)$*,* $u \in [0, \frac{p-1}{2}[$*,* $v \in [0, \frac{p-1}{4}[$*, to the underneath primitive roots' equations are as follows*

$$\begin{array}{rcl} \frac{p-1}{4} & = & \#(u,v) \setminus 0 \equiv g^{2u} + g^{4v} \mod p, \\ 0 & = & \#(u,v) \setminus 0 \equiv g^{2u+1} + g^{4v+2} \mod p. \end{array}$$

Proof. — The first result is obtained by writing $g^{2u} \equiv -g^{4v} \equiv g^{4v+(p-1)/2} \mod p$, so that $2u \equiv 4v + (p-1)/2 \mod p-1$, which is equivalent to $u \equiv 2v + (p-1)/4 \mod (p-1)/2$, $(p-1)/4$ being an integer according to the hypothesis. The previous equation is linear with the coefficient of u equal to 1. Therefore, there is no constraint on this parameter to acquire any value provided by the second member if the equation. On that side (p-1)/4 is a constant and therefore can be ignored in numbering solutions. The coefficient in front of v being 2, the number of values taken by u is the cardinal of the domain of definition of v divided by 2. Hence the first result. The second result derives from $g^{2u+1} \equiv -g^{4v+2} \equiv g^{4v+2+(p-1)/2} \mod p$, so that $2u + 1 \equiv 4v + 2 + (p-1)/2 \mod p-1$, equivalent to $u + 1/2 = 2v + 1 + (p-1)/4 + k(p-1)/2$ for some integer k which is impossible as $1/2$ is not an integer while the rest of the terms are by the hypothesis. Hence the void set. □

Lemma 2. — *Let us have* $p = 1 \mod 4$ *and* g *a primitive root of* p*. The numbers of integer solutions* $\#(u,v)$*,* $u \in [0, \frac{p-1}{2}[$*,* $v \in [0, \frac{p-1}{4}[$*, to the equations*

$$\begin{array}{rcl} n_1 & = & \#(u,v) \setminus g^k \equiv g^{2u} + g^{4v} \mod p \\ n_2 & = & \#(u,v) \setminus g^k \equiv g^{2u+1} + g^{4v+2} \mod p \end{array}$$

are such that

$$\begin{array}{l} n_2 - n_1 = 0 \quad if \quad k \neq 0 \mod 4 \\ n_2 - n_1 = 1 \quad if \quad k = 0 \mod 4 \end{array}$$

Proof. — Let us consider A the set of integers $\{g^{2u}+g^{4v}\ mod\ p\} \cup \{g^{4w}\ mod\ p\}$ with (u,v) integers describing one time the cross product $([0,(p-1)/2[, [0,(p-1)/4[)$ and w integers describing one time $[0,(p-1)/4[$. In the same way, let us have the set B' of integers $\{g^{2u} + g^2.g^{4v}\ mod\ p\} \cup \{g^2.g^{4w}\ mod\ p\}$ with (u,v) in $([0,(p-1)/2[, [0,(p-1)/4[)$ and w in $[0,(p-1)/4[$ to which we remove the $(p-1)/4$ zero-value elements $\{0,...,0\}$ and let us then call the resulting set B. Lemma 1 proves that there are exactly $(p-1)/4$ zeroes in the sets A and B'. Therefore B contains no zeroes. Now B is the complementary set of A in the set T composed of $(p-1)/4$ times the integers $\{0,1,...,p-1\}$. Let us then have the set C' of integers $\{g.g^{2u} + g^2.g^{4v}\ mod\ p\}$ with (u,v) in $([0,(p-1)/2[, [0,(p-1)/4[)$ and $C = C' \cup \{0,...,0\}$ with $(p-1)/4$ zeroes in the second member of the union. By lemma 1, there are no zeroes in the set C' and therefore there are now exactly $(p-1)/4$ zeroes in C. The set C is the complementary set of B in T. Therefore A and C are the same sets submitted to some permutation of the elements keeping the equal cardinality property. The difference $n_2 - n_1$ is then again a consequence of lemma 1 and can be easily checked using either a numerical example or the above kind of arguments. □

Lemma 3. — *Let us have g a primitive root of p. The numbers, respectively n_1, n_2, n_3 and n_4, of integer solutions $\#(u,v)$, $u \in [0, \frac{p-1}{2}[$, $v \in [0, \frac{p-1}{2}[$, to the equations*

$$\begin{aligned} n_1 &= \#(u,v) \ \setminus \ g^0 \equiv g^{2u} + g^{4v} \mod p \\ n_2 &= \#(u,v) \ \setminus \ g^1 \equiv g^{2u} + g^{4v} \mod p \\ n_3 &= \#(u,v) \ \setminus \ g^2 \equiv g^{2u} + g^{4v} \mod p \\ n_4 &= \#(u,v) \ \setminus \ g^3 \equiv g^{2u} + g^{4v} \mod p \end{aligned}$$

is the numbers of solutions $\#(u,v)$ to the equation systems

$$\begin{aligned} n_1 &= \#(u,v) \ \setminus \ g^0 \equiv g^{2u} + g^{2v} \mod p \ \cap \ v = 0 \mod 2 \\ n_2 &= \#(u,v) \ \setminus \ g^1 \equiv g^{2u} + g^{2v} \mod p \ \cap \ v = 0 \mod 2 \\ n_3 &= \#(u,v) \ \setminus \ g^2 \equiv g^{2u} + g^{2v} \mod p \ \cap \ v = 0 \mod 2 \\ n_4 &= \#(u,v) \ \setminus \ g^3 \equiv g^{2u} + g^{2v} \mod p \ \cap \ v = 0 \mod 2 \end{aligned}$$

Proof. — This is a trivial result. □

Note. — We will soon see that the condition v *even* (and its opposite v odd condition) is of quite significant importance and the only purpose of this trivial lemma is to highlight that point.

Theorem 40. — *The equation*

$$p = (2\alpha)^2 + \beta^2$$

has a unique solution (α, β), $\alpha > 0$, $\beta > 0$, β odd, $p \equiv 1 \mod 4$.
There is no solution to the previous equation if $p \equiv 3 \mod 4$.

Proof. — This is Fermat's theorem on the sums of two squares. See reference [**15**]. A prime such that $p \equiv 1 \mod 4$ is called a Pythagorean prime. □

Theorem 41. — *The positive values of α and β are given by*

$$\begin{aligned} a \equiv{}& \frac{1}{4}\left(\frac{(\frac{p-1}{2})!}{(\frac{p-1}{4})!}\right)^2 \mod p \qquad & b \equiv{}& \frac{1}{2}\frac{(\frac{p-1}{2})!}{((\frac{p-1}{4})!)^2} \mod p \\ 2\alpha ={}& \min(2a, p-2a) & \beta ={}& \min(b, p-b) \end{aligned}$$

Proof. — This is a result by Friedrich Gauss. See reference [**16**]. □

Lemma 4. — *The integer α is always a square modulo p.*

Proof. — Theorem 41 shows obviously that a is a square. Moreover -1 is a square because $-1 \equiv g^{(p-1)/2} \mod p$ and $p \equiv 1 \mod 4$ implies $(p-1)/2 \equiv 0 \mod 2$. □

Lemma 5. — *The integer β is square modulo p if and only if $\frac{1}{2}\left(\frac{p-1}{2}\right)!$ is a square.*

Proof. — This is an immediate consequence of theorem 41 with the same argument applied on $-b$. □

Lemma 6. — *The integer* 2 *is a square modulo* p *if* $p \equiv or(1,7) \mod 8$ *and is not if* $p \equiv or(3,5) \mod 8$.
Proof. — Using the Legendre symbol [**9**], $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$ for any integer a, we apply the relationship, specific to 2, $2^{(p-1)/2} \mod p \equiv \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = if(p \equiv \pm 1 \mod 8, 1, -1)$. Let us have g a primitive root of p so that $g^i \equiv 2 \mod p$ for some integer i. Then $g^{i.(p-1)/2} = if(p \equiv \pm 1 \mod 8, 1, -1) \mod p$. Therefore i is even if $p \equiv \pm 1 \mod 8$ and i is odd if $p \equiv \pm 3 \mod 8$. Hence the result modulo 8. □

Lemma 7. — *The two integers* 2α *and* β *are linked by the relationship*

$$2\alpha \equiv g^{\frac{p-1}{4} + or(0, \frac{p-1}{2})}.\beta \mod p$$

where g *is a primitive root of* p.
Proof. — For some integers u and v, we have $2\alpha = g^u \mod p$ and $\beta = g^v \mod p$. Then $p = (2\alpha)^2 + \beta^2$ implies $g^{2u} + g^{2v} = g^{2u}.(1 + g^{2(v-u)}) = 0 \mod p$. As $g^{2u} \neq 0 \mod p$, we have necessarily $g^{2(v-u)} = -1 = g^{(p-1)/2} \mod p$ and therefore $v - u = \frac{p-1}{4} \mod \frac{p-1}{2}$. The interval $]-(p-1)/2, (p-1)/2]$ covering the whole domain of definition needed here to address values of u and v, we get $u - v = or(1,-1).\frac{p-1}{4}$ with one of the two terms u and v eventually negative. More simply, one can just write $(2\alpha)^2 + \beta^2 = 0 \mod p = 1 + (-1) \mod p = (1 + g^{2.(p-1)/4}) \mod p$ giving the result by straight identification of terms. Of course, similarly $\beta \equiv or(1,-1).g^{\frac{p-1}{4}}.(2\alpha) \mod p$. An alternative writing to $or(1,-1).g^{\frac{p-1}{4}}$ is then $g^{\frac{p-1}{4} + or(0, \frac{p-1}{2})}$. □

Note. — The $g^{\frac{p-1}{4}} \mod p$ value emerges here unsurprisingly. Another way to bring it forward is by writing:

$$\begin{aligned} p &= (2\alpha)^2 + \beta^2 \\ &\equiv -g^{\frac{p-1}{2}}(2\alpha)^2 + \beta^2 \mod p \\ &\equiv -(g^{\frac{p-1}{4}}2\alpha + \beta)(g^{\frac{p-1}{4}}2\alpha - \beta) \mod p \end{aligned}$$

or

$$\begin{aligned} p &= (2\alpha)^2 + \beta^2 \\ &\equiv (2\alpha)^2 - g^{\frac{p-1}{2}}\beta^2 \mod p \\ &\equiv -(g^{\frac{p-1}{4}}\beta + 2\alpha)(g^{\frac{p-1}{4}}\beta - 2\alpha) \mod p. \end{aligned}$$

Lemma 8. — *Let us have* $p \equiv 1 \mod 4$. *Then*

$$\left(\frac{p-1}{2}\right)! \equiv g^{\frac{p-1}{4} + or(0, \frac{p-1}{2})} \mod p$$

where g *is a primitive root of* p.

Proof. — By the Gauss formulas (theorem 41), the ratio $\frac{2\alpha}{\beta} \mod p$ is equal to $\left(\frac{p-1}{2}\right)! \mod p$. Then lemma 7 allows to conclude. Note that numerical verification shows that the previous result does not apply to the case $p \equiv 3 \mod 4$. □

Lemma 9. — *The integer β is always a square modulo p.*
Proof. — This is an immediate consequence of lemmas 5, 6 and 8. □

Lemma 10. — *Let us have $p \equiv 1 \mod 4$ and α, β the positive integer solutions of $p = (2\alpha)^2 + \beta^2$. Then*

$$\begin{array}{l} p = 1 \mod 8 \Leftrightarrow \alpha \equiv 0 \mod 2 \\ p = 5 \mod 8 \Leftrightarrow \alpha \equiv 1 \mod 2 \end{array}$$

Proof. — Let us consider the square of an odd integer : $(1+2r)^2 = 1+4r(1+r)$. The $r(1+r)$ factor is the product of an even term by an odd term and therefore, β being an odd number, $\beta^2 \equiv 1 \mod 8$. Then, using $(2\alpha)^2 = p - \beta^2$, if $p \equiv 1 \mod 8$ we get $(2\alpha)^2 \equiv 0 \mod 8$ and if $p \equiv 5 \mod 8$ we get $(2\alpha)^2 \equiv 4 \mod 8$, thus respectively $2\alpha \equiv 0 \mod 4$ and $2\alpha \equiv 2 \mod 4$. Hence the result after division by 2 to get α. □

Lemma 11. — *Let us have $p \equiv 1 \mod 4$ and $(\alpha,\ \beta)$ the positive integer solutions of $p = (2\alpha)^2 + \beta^2$. Then, for $I1 = [0, (p-1)/4[$ and $I2 = [0, (p-1)/2[$, and (u, v) integers, up to $p = 9973$,*

$$\begin{array}{ccllcl}
p \equiv 1 \; mod \; 16 & \Leftrightarrow & \exists \; (u,v) \in I1^2 & \backslash \;\; g^{4u} \equiv 2\alpha \; mod \; p & \bigcap & g^{4v} \equiv \beta \; mod \; p \\
p \equiv 9 \; mod \; 16 & \Leftrightarrow & \exists \; (u,v) \in I1^2 & \backslash \;\; g^{4u} \equiv 2\alpha \; mod \; p & \bigcap & g^{4v+2} \equiv \beta \; mod \; p \\
\{\emptyset\} & \Leftarrow & \exists \; u \in I1 & \backslash \;\; g^{4u+2} \equiv 2\alpha \; mod \; p & & \\
p \equiv 5 \; mod \; 8 & \Leftrightarrow & \exists \; (u,v) \in I2^2 & \backslash \;\; g^{2u-1} \equiv 2\alpha \; mod \; p & \bigcap & g^{2v} \equiv \beta \; mod \; p \\
\{\emptyset\} & \Leftarrow & \exists \; v \in I2 & \backslash \;\; g^{2v-1} \equiv \beta \; mod \; p & &
\end{array}$$

Proof. — For some $(r, s) \in N^2$, we can write $g^r \equiv 2\alpha \mod p$ and $g^s \equiv \beta \mod p$. Then $p = (2\alpha)^2 + \beta^2 \equiv g^{2r} + g^{2s} \equiv 0 \mod p$. Thus $g^{2r-2s} + 1 \equiv 0 \mod p$, that is $g^{2r-2s} \equiv g^{(p-1)/2} \mod p$, so that finally $r - s \equiv (p-1)/4 \mod (p-1)/2$. With the $I1$ and $I2$ domains of definition, we can ignore the $\mod (p-1)/2$ framework changing eventually simultaneously the sign of r and s if needed. We get then $p = 1 + 4(r - s)$. Hence the immediate cases: If $r \equiv 0 \mod 4$ and $s \equiv 0 \mod 4$ then $p \equiv 1 \mod 16$. If $r \equiv 0 \mod 4$ and $s \equiv 2 \mod 4$ then $p \equiv -7 \mod 16 \equiv 9 \mod 16$. If $r \equiv 1 \mod 2$ and $s \equiv 0 \mod 2$ then $p \equiv 5 \mod 8$. Now, in this two last cases, the symmetric pairs, respectively ($r \equiv 2 \mod 4$, $s \equiv 0 \mod 4$) and ($r \equiv 0 \mod 2, s \equiv 1 \mod 2$) are to be addressed. This is verified, as well as the first void case, numerically. Besides, the last void case is precisely lemma 9. □

Theorem 42. — *Let us have a prime number* p*, such that* $p \equiv 1 \mod 4$*, and its Pythagorean decomposition* $(2\alpha)^2 + \beta^2$ *and* g *a primitive root of* p*. Then, up to* $p = 9973$*,*

$$\begin{array}{rll} 2\alpha & = \mid \#v\ \ even\ \ - \#v\ \ odd & \mid \quad \backslash\ g^1 \equiv g^{2u} + g^{2v} \mod p \\ \beta & = \mid \#v\ \ even\ \ - \#v\ \ odd + 1 & \mid \quad \backslash\ g^0 \equiv g^{2u} + g^{2v} \mod p \end{array}$$

where $||$ *is the absolute value operator,* $u \in [0, \frac{p-1}{1}[$ *and* $v \in [0, \frac{p-1}{2}[$.
Proof. — The proof is obtained by direct numerical verification. □

Note. — The result is conjectured to be true for any prime number p such that $p \equiv 1 \mod 4$.
Note. — The same result is of course found with the choice of parameter u instead of v or a sampling $u \in [0, \frac{p-1}{1}[$ and $v \in [\frac{p-1}{2}, \frac{p-1}{1}[$.

In the first part of appendix G, the reader will find the example for $p = 89$, $g = 3$, $\alpha = 4$, $\beta = 5$ of the solutions of:

$$\begin{array}{llll} eq1: & g^0 \equiv g^{2u} + g^{2v} \mod p & \cap & v \equiv 0 \mod 2 \\ eq2: & g^0 \equiv g^{2u} + g^{2v} \mod p & \cap & v \equiv 1 \mod 2 \\ eq3: & g^1 \equiv g^{2u} + g^{2v} \mod p & \cap & v \equiv 0 \mod 2 \\ eq4: & g^1 \equiv g^{2u} + g^{2v} \mod p & \cap & v \equiv 1 \mod 2 \end{array}$$

As $g^{p-1} = 1 \mod p$, the second and fourth quarters of the data give redundant values of v and gaps $\frac{p-1}{2} = 44$ for the values of u.
Counting even and odd values for v provides:

	even	*odd*	$\Delta_{even-odd}$
eq1 | eq2	$12+6$	$12+12$	$-6 = -(\beta+1)$
eq3 | eq4	$10+16$	$10+8$	$8 = 2\alpha$

Theorem 43. — *Let us have* g *a primitive root of* p*. The number of integer solutions* $\#(u,v)$*,* $u \in [0, \frac{p-1}{2}[$*,* $v \in [0, \frac{p-1}{2}[$ *to the equations*

$$\begin{array}{l} n_1 = \#(u,v)\ \backslash\ g^0 \equiv g^{2u} + g^{4v} \mod p \\ n_2 = \#(u,v)\ \backslash\ g^1 \equiv g^{2u} + g^{4v} \mod p \\ n_3 = \#(u,v)\ \backslash\ g^2 \equiv g^{2u} + g^{4v} \mod p \\ n_4 = \#(u,v)\ \backslash\ g^3 \equiv g^{2u} + g^{4v} \mod p \end{array}$$

is given for $p \equiv 1 \mod 4$*, up to* $p = 9973$*, by*

$$\begin{pmatrix} n_1 + 1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} = \begin{pmatrix} (p-3)/4 + sign\beta \cdot \frac{\beta}{2} \\ (p-1)/4 + sign\alpha \cdot \alpha \\ (p-3)/4 - sign\beta \cdot \frac{\beta}{2} \\ (p-1)/4 - sign\alpha \cdot \alpha \end{pmatrix}$$

where

$$\begin{array}{ll} sign\alpha = sign(\#v\ \ even\ \ -\#v\ \ odd) & \backslash\ g^1 \equiv g^{2u} + g^{2v} \mod p \\ sign\beta' = sign(\#v\ \ even\ \ -\#v\ \ odd + 1) & \backslash\ g^0 \equiv g^{2u} + g^{2v} \mod p \\ sign\beta = if(sign(\beta') = 0, -1, sign(\beta')) & \end{array}$$

and where

$$u \in [0, \frac{p-1}{1}[, v \in [0, \frac{p-1}{2}[.$$

Proof. — This is an immediate result of theorem 42 as g^{2v} simply evolves to g^{4v} in the equations. Two implications provide the key to the process eq_i ⇒ eq_i+4 where

$$\begin{array}{lll} eq5: & g^0 \equiv g^{2u} + g^{4v} & \mod p \\ eq6: & g^2 \equiv g^{2u} + g^{4v} & \mod p \\ eq7: & g^1 \equiv g^{2u} + g^{4v} & \mod p \\ eq8: & g^3 \equiv g^{2u} + g^{4v} & \mod p \end{array}$$

and eq_i are the equations given here and in the former paragraph.
These implications are:

$$\begin{array}{llll} \text{If } v \equiv 0 \mod 2, & g^i \equiv g^{2u} + g^{2v} \mod p & \Rightarrow & g^i \equiv g^{2u} + g^{4\frac{v}{2}} \mod p \\ \text{If } v = 1 \mod 2, & g^i \equiv g^{2u} + g^{2v} \mod p & \Rightarrow & g^{i+2} \equiv g^{2(u+1)} + g^{4\frac{v+1}{2}} \mod p \end{array}$$

□

Note. — The result is conjectured to be true for any prime number p such that $p \equiv 1 \mod 4$ as it was for former theorem 42.

The second table in appendix G provides the solutions (u, v) to the equations $g^i \equiv g^{2u} + g^{4v} \mod p$ for $p = 89$, $i = 0$ to 3, and the sampling $u \in [0, \frac{p-1}{1}[$, $v \in [0, \frac{p-1}{2}[$. The reader can check the way the (u, v) data is modified from its original values, given in the first part of the appendix, to the values in the second part accordingly to the two previous implications.

Theorem 44. — *The previous signs in front of the positive α and β, up to $p = 9973$, are given by*

$$\begin{array}{rl} sign\alpha = & if(i = 0, (\#v\ even - \#v\ odd)/(2\alpha), 2 - i) \\ sign\beta = & (-1)^{\frac{-1+p \mod 8}{4} + \frac{\beta+1}{2}} \end{array}$$

where i is the solution of

$$g^{i\ mod\ 4} \equiv 2\alpha\ mod\ p$$

and where $\#v$ even and $\#v$ odd are evaluated by the number of solutions of $g^1 \equiv g^{2u} + g^{2v} \mod p$ within the domain of definition given in the previous theorem.

Proof. — The proof is obtained by direct numerical verification. The reader may refer to appendix H in that intent. □

Note. — Of course the theorem is conjectured to be true for any prime.
Note. — For parameter α, adding previous results on $p \bmod 8$ values, and reminding that the case $i = 2$ is an empty set, it is equivalent to the following table :

$p \bmod 8$	i	$\frac{\#v\ even - \#v\ odd}{2\alpha}$
1	0	$or(1, -1)$
1	2	$\{\emptyset\}$
5	1	1
5	3	-1

Here, within the case $p = 1 \mod 8$, up to $p = 9973$, we get $\frac{\#v\ even - \#v\ odd}{2\alpha} = -1$ when p is equal to either 97, 233, 281, 313, 401, 433, 521, 569, 593, 617, 673, 761, 769, 809, 857, 929, 977, 1009, 1033, 1097, 1153, 1193, 1217, 1289, 1433, 1553, 1657, 1697, 1753, 1777, 1889, 1993, 2017, 2089, 2137, 2161, 2273, 2393, 2441, 2473, 2609, 2617, 2633, 2689, 2713, 2729, 2753, 2801, 2857, 2953, 3041, 3121, 3137, 3169, 3257, 3449, 3593, 3761, 3881, 4177, 4241, 4273, 4337, 4409, 4441, 4457, 4481, 4729, 4793, 4801, 4937, 4969, 4993, 5009, 5113, 5273, 5393, 5417, 5441, 5641, 5657, 5689, 5801, 5849, 6089, 6121, 6217, 6257, 6337, 6353, 6481, 6521, 6553, 6569, 6673, 6737, 6793, 6833, 6857, 6961, 6977, 7121, 7193, 7297, 7321, 7369, 7457, 7529, 7561,7681, 7793, 7841, 7937, 8017, 8297, 8329, 8353, 8537, 8609, 8641, 8689, 8713, 9161, 9433, 9473, 9521, 9689, 9697, 9721, 9769, 9833, 9857.
Note. — For the sign in front of β, the simplicity of the rule is likely the result of the trivial equivalence $g^0 \equiv 1 \bmod p$ that provides a systematic well defined "anchor" $c = 1$ to the equation $g^0 \equiv g^{2u} + g^{4v} \mod p$ (and therefore indirectly to $g^2 \equiv g^{2u} + g^{4v} \mod p$). There is no possible confusion between the enumeration results to attribute to $g^0 \equiv g^{2u} + g^{4v} \mod p$ and those to his closely linked $g^2 \equiv g^{2u} + g^{4v} \mod p$ equation. It is not the case for $g^1 \equiv g^{2u} + g^{4v} \mod p$ equation, and directly linked $g^3 \equiv g^{2u} + g^{4v} \mod p$ equation. For some different choice of g, the former two enumeration results may be swapped. The two classes, among the $\varphi(\varphi(p))$ primitive roots of some prime p, are detected by verifying the $g^{(p-1)/4}$ values (resulting from the fact of one class for $g^{2.(p-1)/4} \equiv -1 \mod p$ with its systematic -1 result). For example, for $p = 17$, the two classes for g are $\{3, 5, 12, 14\}$ providing $g^{(p-1)/4} = 13 \bmod p$ and $\{6, 7, 10, 11\}$ providing $g^{(p-1)/4} = 4 \mod p$. This easy distinction however doesn't provide an attributing procedure for any literal formula. The researched "anchor" may then be provided by solving the equation $g^{i \bmod 4} \equiv 2\alpha \mod p$. This method is successful except for $g^{0 \bmod 4} \equiv 2\alpha \mod p$. It necessitated here a one-by-one sign adjustment missing so far some additional characteristic relationship.
Note. — Replacing $\frac{-1+p \mod 8}{4}$ with α within the literal expression of $sign\beta$ will provide the same result according to lemma 10.

Theorem 45. — *Let us have* $p \equiv 1 \mod 4$ *and* g *a primitive root of* p. *The number of integer solutions* $\#(u,v)$, $u \in [0, \frac{p-1}{2}[$, $v \in [0, \frac{p-1}{2}[$ *to the equations*

$$\begin{array}{l} n_1 = \#(u,v) \ \backslash \ g^0 \equiv g^{4u} + g^{4v} \mod p \\ n_2 = \#(u,v) \ \backslash \ g^1 \equiv g^{4u} + g^{4v} \mod p \\ n_3 = \#(u,v) \ \backslash \ g^2 \equiv g^{4u} + g^{4v} \mod p \\ n_4 = \#(u,v) \ \backslash \ g^3 \equiv g^{4u} + g^{4v} \mod p \end{array}$$

is given, up to $p = 9973$, *by*

$$\begin{pmatrix} n_1 + 1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} = \begin{pmatrix} (p-3)/4 + if(p \equiv 1 \ mod \ 8, \ sign\beta.\frac{3\beta}{2}, \ 1 + sign\beta.\frac{\beta}{2}) \\ (p+1)/4 + sign\alpha.2\alpha - sign\beta.\frac{\beta}{2} - if(p \equiv 1 \ mod \ 8, \ 1, \ 0) \\ (p-3)/4 + if(p \equiv 1 \ mod \ 8, \ - sign\beta.\frac{\beta}{2}, \ 1 - sign\beta.\frac{3\beta}{2}) \\ (p+1)/4 - sign\alpha.2\alpha - sign\beta.\frac{\beta}{2} - if(p \equiv 1 \ mod \ 8, \ 1, \ 0) \end{pmatrix}$$

where we still have the same definitions of α, β *and the signs in front of them.*
Proof. — The proof is obtained by direct numerical verification. □

Note. — Again, the result is conjectured to be true for any prime number p such that $p \equiv 1 \mod 4$.

Now, as mentioned earlier, the impact of missing very simple literal formulas for high values of p is totally minor for sufficiently precise numerical verifications. There is need for results on only a few instances of p to get good trending values as the reader can ascertain underneath.

Numeric verification. — *The Friedlander-Iwaniec equation.*

The following table gives the non-cumulative cardinal factors of the Friedlander-Iwaniec equation.

p	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
2	1	1	1	1	1	1	1	1	1	1
3	1.33333	0.83333	0.83333	1.33333	0.83333	0.83333	1.33333	0.83333	0.83333	1.33333
5	0.8	0.95	0.85	1.25	1.15	0.8	0.95	0.85	1.25	1.15
7	1.14286	0.97619	0.97619	0.97619	0.97619	0.97619	0.97619	1.14286	0.97619	0.97619
11	1.09091	0.99091	0.99091	0.99091	0.99091	0.99091	0.99091	0.99091	0.99091	0.99091
13	0.92308	1.04487	0.98077	1.04487	0.96795	0.98077	0.98077	1.03205	1.03205	1.04487
17	0.94118	1.01103	0.99632	0.97426	1.01103	0.97426	1.03309	1.03309	0.99632	0.99632
19	1.05263	0.99708	0.99708	0.99708	0.99708	0.99708	0.99708	0.99708	0.99708	0.99708
23	1.04348	0.99802	0.99802	0.99802	0.99802	0.99802	0.99802	0.99802	0.99802	0.99802
29	0.96552	0.98892	0.99631	0.99631	1.01355	1.01355	1.01355	0.98892	1.00616	1.01355
31	1.03226	0.99892	0.99892	0.99892	0.99892	0.99892	0.99892	0.99892	0.99892	0.99892
37	0.97297	0.99925	1.00976	1.00225	1.00225	0.99174	0.99174	0.99925	0.99174	0.99925
41	0.97561	1.00671	0.99451	1.00549	1.00671	0.99451	0.99573	1.00549	0.99451	0.99451
43	1.02326	0.99945	0.99945	0.99945	0.99945	0.99945	0.99945	0.99945	0.99945	0.99945
47	1.02128	0.99954	0.99954	0.99954	0.99954	0.99954	0.99954	0.99954	0.99954	0.99954
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
293	0.99659	0.99961	0.99996	0.99996	1.00041	0.99996	1.00041	0.99996	1.00006	1.00041

The cardinal factors tend towards 1 quite rapidly as the difference to 1 is typically plus or minus the order of magnitude of the inverse of the instance value p. The ten first instances give already a good prognosis of the cumulative cardinal factors infinite products as indicates the underneath table.

p	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
2	1	1	1	1	1	1	1	1	1	1
3	1.33333	0.83333	0.83333	1.33333	0.83333	0.83333	1.33333	0.83333	0.83333	1.33333
5	1.06667	0.79167	0.70833	1.66667	0.95833	0.66667	1.26667	0.70833	1.04167	1.53333
7	1.21905	0.77282	0.69147	1.62698	0.93552	0.65079	1.23651	0.80952	1.01687	1.49683
11	1.32987	0.76579	0.68518	1.61219	0.92701	0.64488	1.22527	0.80216	1.00762	1.48322
13	1.22757	0.80015	0.67201	1.68454	0.89730	0.63248	1.20170	0.82787	1.03992	1.54977
17	1.15536	0.80898	0.66953	1.64118	0.90720	0.61620	1.24147	0.85527	1.03609	1.54407
19	1.21617	0.80661	0.66758	1.63638	0.90454	0.61440	1.23784	0.85277	1.03306	1.53956
23	1.26905	0.80502	0.66626	1.63315	0.90276	0.61318	1.23539	0.85108	1.03102	1.53652
29	1.22529	0.79610	0.66380	1.62712	0.91499	0.62149	1.25213	0.84165	1.03737	1.55733
31	1.26481	0.79524	0.66308	1.62537	0.91400	0.62082	1.25078	0.84074	1.03626	1.55566
37	1.23063	0.79464	0.66955	1.62903	0.91606	0.61569	1.24045	0.84011	1.02770	1.55449
41	1.20061	0.79997	0.66588	1.63797	0.92220	0.61232	1.23516	0.84472	1.02206	1.54596
43	1.22853	0.79953	0.66551	1.63706	0.92169	0.61198	1.23447	0.84425	1.02149	1.54510
47	1.25467	0.79916	0.66520	1.63630	0.92127	0.61169	1.23390	0.84386	1.02102	1.54439
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
293	1.26320	0.80058	0.66351	1.62966	0.91868	0.61372	1.22177	0.83498	1.02317	1.53646
$fr_{c/0}$	1	$0,63377$	$0,52526$	$1,29010$	$0,72726$	$0,48585$	$0,96720$	$0,66100$	$0,80998$	$1,21632$

The ratio $fr_{c/0}$ at the last line of the table gives the ratio of the cardinal factors for the targets c compared to that of the target 0.

The effective numbers of solutions of the Friedlander-Iwaniec equation $x_1^2 + x_2^4 = p + c$, such that $p < p_i$, is indicated in the underneath table. These enumerations are available using appendix F. The ratio $r_{c/0}$ of numbers of solutions for the targets c compared to the number of solutions for the target 0, corresponding to the case $i = 3000000$, is given at the last line of the table:

i	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
100	21	10	20	37	19	16	28	21	27	33
1000	118	67	82	176	91	81	140	97	111	149
10000	623	382	386	866	464	335	675	433	561	782
100000	3348	2058	1910	4511	2510	1661	3320	2261	2783	4082
1000000	18101	11282	9936	23793	13256	9078	17463	12043	14867	22245
3000000	40381	25314	21522	52575	29223	20040	39282	26598	33223	49878
$r_{c/0}$	1	0.62688	0.53297	1.30197	0.72368	0.49627	0.97278	0.65868	0.82274	1.23518

Now we can compare the ratios $fr_{c/0}$ and $r_{c/0}$ which are supposedly equal asymptotically:

p	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
$fr_{c/0}$	1	$0,63377$	$0,52526$	$1,29010$	$0,72726$	$0,48585$	$0,96720$	$0,66100$	$0,80998$	$1,21632$
$r_{c/0}$	1	0.62688	0.53297	1.30197	0.72368	0.49627	0.97278	0.65868	0.82274	1.23518
		$-1,09\%$	$1,47\%$	$0,92\%$	$-0,49\%$	$2,14\%$	$0,58\%$	$-0,35\%$	$1,58\%$	$1,55\%$

Note. — The first comment that can be made here is that the proportions of the number of solutions from one target to another meet the expectations in a satisfactory way.

Note. — The asymptotic value of the cardinal factor $fan(0)$ is $4/\pi$ in the Friedlander-Iwaniec formula. The approximate value at stage $p = 293$ shows a $-0,79$ % offset to this value. It continues to oscillate between high and low offsets in the following way as p increases:

p	353	383	409	461	503	569	617	659
$offset$	-0.107%	-0.026%	-0.127%	-0.147%	$-0,002\%$	$-0,040\%$	$-0,056\%$	$-0,008\%$

Note. — Using equation 13, the literal formula for any value of c in Z of the Friedlander-Iwaniec equation is:

$$\lim_{y \longrightarrow +\infty} \#\{y = x_1^2 + x_2^4 - c\} = fan(c) \frac{\Gamma(1/2)\Gamma(5/4)}{2 \cdot \Gamma(7/4)} \cdot \frac{y^{3/4}}{\ln(y)}$$

where $fan(c)$ is the cardinal factor of c.

Numeric verification. — *The Heath-Brown−Xiannan equation.*

The following table gives the non-cumulative cardinal factors of the Heath-Brown−Xiannan equation.

p	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
2	1	1	1	1	1	1	1	1	1	1
3	1.5	1	0.5	1.5	1	0.5	1.5	1	0.5	1.5
5	0.75	1	0.75	1.25	1.25	0.75	1	0.75	1.25	1.25
7	1.16667	1	1	0.94444	1	0.94444	0.94444	1.16667	1	1
11	1.1	1	0.98	1	1	1	0.98	0.98	0.98	1
13	0.91667	1.05556	0.97222	1.05556	0.97222	0.97222	0.97222	1.02778	1.02778	1.05556
17	0.9375	1.01562	1	0.96875	1.01562	0.96875	1.03125	1.03125	1	1
19	1.05556	1	0.99383	0.99383	1	1	1	1	0.99383	1
23	1.04545	1	1	1	1	0.99587	1	0.99587	1	1
29	0.96429	0.98980	0.99490	0.99490	1.01531	1.01531	1.01531	0.98980	1.00510	1.01531
…	…	…	…	…	…	…	…	…	…	…
293	0.99658	0.99962	0.99995	0.99995	1.00042	0.99995	1.00042	0.99995	1.00005	1.00042

The cumulative cardinal factors follow:

p	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
2	1	1	1	1	1	1	1	1	1	1
3	1.5	1	0.5	1.5	1	0.5	1.5	1	0.5	1.5
5	1.12500	1.00000	0.37500	1.87500	1.25000	0.37500	1.50000	0.75000	0.62500	1.87500
7	1.31250	1.00000	0.37500	1.77083	1.25000	0.35417	1.41667	0.87500	0.62500	1.87500
11	1.44375	1.00000	0.36750	1.77083	1.25000	0.35417	1.38833	0.85750	0.61250	1.87500
13	1.32344	1.05556	0.35729	1.86921	1.21528	0.34433	1.34977	0.88132	0.62951	1.97917
17	1.24072	1.07205	0.35729	1.81080	1.23427	0.33357	1.39195	0.90886	0.62951	1.97917
19	1.30965	1.07205	0.35509	1.79962	1.23427	0.33357	1.39195	0.90886	0.62563	1.97917
23	1.36918	1.07205	0.35509	1.79962	1.23427	0.33219	1.39195	0.90511	0.62563	1.97917
29	1.32028	1.06111	0.35327	1.79044	1.25316	0.33727	1.41325	0.89587	0.62882	2.00946
…	…	…	…	…	…	…	…	…	…	…
293	1.36198	1.07474	0.35320	1.79168	1.26721	0.33289	1.37582	0.88937	0.62004	1.99581
$fr_{c/0}$	1	$0,78911$	$0,25933$	$1,31550$	$0,93042$	$0,24441$	$1,01017$	$0,65300$	$0,45525$	$1,46538$

The effective numbers of solutions of the Heath-Brown−Xiannan equation $x^2 + y^4 = p + c$ such that $p < p_i$ is indicated in the underneath table. These enumerations are available using appendix F pending on the suggested modifications of the program.

i	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
100	10	8	7	13	7	5	9	5	11	15
1000	62	43	34	73	39	30	54	43	48	73
10000	271	183	122	299	194	105	270	194	173	337
100000	1231	869	469	1493	958	402	1141	822	683	1590
1000000	5687	4235	1865	7239	4609	1777	5469	3617	2940	7843
3000000	12104	8883	3770	15554	9935	3550	11621	7651	6112	17093
6000000	18993	13987	5825	24246	15816	5469	18495	12139	9528	26725
$r_{c/0}$	1	$0,73643$	$0,30669$	$1,27658$	$0,83272$	$0,28795$	$0,97378$	$0,63913$	$0,50166$	$1,40710$

The ratio $r_{c/0}$ of numbers of solutions for the targets c compared to the number of solutions for the target 0, corresponding to the case $i = 6000000$ (i the index of p_i), is given at the last line of the table. Comparing the ratios $fr_{c/0}$ and $r_{c/0}$ which are supposedly equal asymptotically, we get:

p	$c=0$	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
$fr_{c/0}$	1	$0,78911$	$0,25933$	$1,31550$	$0,93042$	$0,24441$	$1,01017$	$0,65300$	$0,45525$	$1,46538$
$r_{c/0}$	1	$0,73643$	$0,30669$	$1,27658$	$0,83272$	$0,28795$	$0,97378$	$0,63913$	$0,50166$	$1,40710$
		$-6,68\%$	$18,26\%$	$-2,96\%$	$-10,50\%$	$17,81\%$	$-3,60\%$	$-2,12\%$	$10,19\%$	$-3,98\%$

The obvious comment that can be made here is that the comparison is much less satisfactory than in the Friedlander-Iwaniec case. The explanation is not in some hidden grounds making the cardinal factors method defective. Nor is the explanation in the lesser numbers of solutions (about 3.5 times) in comparison to the Friedlander-Iwaniec case, or at least, not exactly. The real cause is given by the following table. We check the evolution of the offset between the real numbers of solutions and the sample at a given step $p < p_i$:

i	$c=1$	$c=2$	$c=3$	$c=4$	$c=5$	$c=6$	$c=7$	$c=8$	$c=9$
1000	$-12,11\%$	$111,46\%$	$-10,50\%$	$-32,39\%$	$97,97\%$	$-13,78\%$	$6,21\%$	$70,06\%$	$-19,65\%$
10000	$-14,43\%$	$73,60\%$	$-16,13\%$	$-23,06\%$	$58,52\%$	$-1,37\%$	$9,63\%$	$40,22\%$	$-15,14\%$
100000	$-10,54\%$	$46,91\%$	$-7,80\%$	$-16,36\%$	$33,61\%$	$-8,24\%$	$2,26\%$	$21,87\%$	$-11,86\%$
1000000	$-5,63\%$	$26,46\%$	$-3,24\%$	$-12,89\%$	$27,84\%$	$-4,80\%$	$-2,60\%$	$13,56\%$	$-5,89\%$
6000000	$-6,68\%$	$18,26\%$	$-2,96\%$	$-10,50\%$	$17,81\%$	$-3,60\%$	$-2,12\%$	$10,19\%$	$-3,98\%$

The table shows a large discrepancy for low values of i. There are often many more or many less solutions near the origin than expected asymptotically. The situation is that, in order to reduce the offsets, we need a lot more enumeration of the solutions for the Heath-Brown−Xiannan type equations while we are limited on our laptop by memory overflows. For objection to the still far way to the expected results, let us just remember that this kind of enumeration evolution has likely a logarithmic trend and therefore, although rapid at the start, will prevail extremely slowly afterwards. The observed trends suggest an $i = 10^{12}$ range requirement, at least, to establish a less than 1% deviation for the above targets $c = 2$ or $c = 5$.

7. Broadening the picture

The focus of our study has been on the term that usually is called the "fudge factor" of the literal formula giving the number of solutions of a Diophantine equation. We lean on already known results (here those for c = 0) to proceed for other targets. Therefore it seems that the whole range of evaluations can be extracted only if we know at least one among them. This is true if we seek a mathematical proof of a literal formula. In case we don't dispose of an initial data, our approach remains however fully useful if we limit ourself to merely seeking what this formula should be. Indeed, the method here relies on the separation of two evaluations, the first one enabling to get the fudge factors, the second (not covered here) addressing the typical shape of the hyper-volumes in which the solutions to the proposed Diophantine problem spread. Normalization, as illustrated in this article, is the key to produce the relevant fudge factors. Using alternative methods to get the hyper-volumes may then give access to the general formula. Not being a proof then, it is nevertheless the "only possible literal result" one would expect after the problem c = 0 (for example) is properly solved. The unsaid premise (or axiom) here, of course, is that the space (or hyper-volume) in which the solutions develop for different targets isn't physical. Numbers are concepts, therefore without weight able to distort their environment as does for example mass in the universe. Speculating on such possibility seems to us more outlandish, or non-mathematical, than simply ignoring it.

A few theorems issued at the end of this article remain dependent on numerical verifications and are therefore limited to a finite number of prime numbers of the $p \equiv 1 \mod 4$ type. Although of no consequence to the enumeration results, a general literal answer would provide more than empty satisfaction. Further findings in that direction may well spread over the specific requirement for monomials z^2 and z^4 and be crucial in more general primitive roots' equations cases. One can cite for examples primitive roots' equations linked to z^3 and z^6. The decompositions of p, there again, has a prevailing role. Indeed decompositions like $p = r^2 + 3s^2$ or $p = ((t_1 + 2t_2)^2 + (t_1 - t_2)^2 + (-(2t_1 + t_2))^2)/6$ emerge on these occasions. Literal evaluations nevertheless are rapidly more complex when z^{12} or z^{24} cases are addressed and prioritizing the evaluation of the number of primes equal to $x^2 + xy + y^2$, or more generally $ux^2 + vxy + wy^2$ to start with, before meddling with $z_1^3 + z_1^2 z_2 + z_1 z_2^2 + z_2^3$, may be more captivating (if interested, refer to [**18**] Fermat Sheet Exercise 10) than the mere monomial cases.

Appendix A. Cardinal matrices samples

x^2

		0	g^0	g^1	g^4	g^2	g^9	g^5	g^{11}	g^3	g^8	g^{10}	g^7	g^6
		0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	0	2	2	0	0	0	0	2	2	0	2
g^0	1	2	1	2	0	2	2	0	0	0	0	2	2	0
g^1	2	0	2	1	2	0	2	2	0	0	0	0	2	2
g^4	3	2	0	2	1	2	0	2	2	0	0	0	0	2
g^2	4	2	2	0	2	1	2	0	2	2	0	0	0	0
g^9	5	0	2	2	0	2	1	2	0	2	2	0	0	0
g^5	6	0	0	2	2	0	2	1	2	0	2	2	0	0
g^{11}	7	0	0	0	2	2	0	2	1	2	0	2	2	0
g^3	8	0	0	0	0	2	2	0	2	1	2	0	2	2
g^8	9	2	0	0	0	0	2	2	0	2	1	2	0	2
g^{10}	10	2	2	0	0	0	0	2	2	0	2	1	2	0
g^7	11	0	2	2	0	0	0	0	2	2	0	2	1	2
g^6	12	2	0	2	2	0	0	0	0	2	2	0	2	1

x^2, $<< mp >>= 1$

		0	g^0	g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	g^{11}
		0	1	2	4	8	3	6	12	11	9	5	10	7
0	0	1	2	0	2	0	2	0	2	0	2	0	2	0
g^0	1	2	1	2	2	0	0	0	0	2	0	2	2	0
g^1	2	0	2	1	0	0	2	2	2	2	0	2	0	0
g^2	4	2	2	0	1	2	2	0	0	0	0	2	0	2
g^3	8	0	0	0	2	1	0	0	2	2	2	2	0	2
g^4	3	2	0	2	2	0	1	2	2	0	0	0	0	2
g^5	6	0	0	2	0	0	2	1	0	0	2	2	2	2
g^6	12	2	0	2	0	2	2	0	1	2	2	0	0	0
g^7	11	0	2	2	0	2	0	0	2	1	0	0	2	2
g^8	9	2	0	0	0	2	0	2	2	0	1	2	2	0
g^9	5	0	2	2	2	2	0	2	0	0	2	1	0	0
g^{10}	10	2	2	0	0	0	0	2	0	2	2	0	1	2
g^{11}	7	0	0	0	2	2	2	2	0	2	0	0	2	1

x^2, $mp = 6$

		0	g^0	g^6	g^1	g^7	g^2	g^8	g^3	g^9	g^4	g^{10}	g^5	g^{11}
		0	1	12	2	11	4	9	8	5	3	10	6	7
0	0	1	2	2	0	0	2	2	0	0	2	2	0	0
g^0	1	2	1	0	2	2	2	0	0	2	0	2	0	0
g^6	12	2	0	1	2	2	0	2	2	0	2	0	0	0
g^1	2	0	2	2	1	2	0	0	0	2	2	0	2	0
g^7	11	0	2	2	2	1	0	0	2	0	0	2	0	2
g^2	4	2	2	0	0	0	1	0	2	2	2	0	0	2
g^8	9	2	0	2	0	0	0	1	2	2	0	2	2	0
g^3	8	0	0	2	0	2	2	2	1	2	0	0	0	2
g^9	5	0	2	0	2	0	2	2	2	1	0	0	2	0
g^4	3	2	0	2	2	0	2	0	0	0	1	0	2	2
g^{10}	10	2	2	0	0	2	0	2	0	0	0	1	2	2
g^5	6	0	0	0	2	0	0	2	0	2	2	2	1	2
g^{11}	7	0	0	0	0	2	2	0	2	0	2	2	2	1

equivalent to

		0	g^0g^{6k}	g^1g^{6k}	g^2g^{6k}	g^3g^{6k}	g^4g^{6k}	g^5g^{6k}
		0	$1.g^{6k}$	$2.g^{6k}$	$4.g^{6k}$	$8.g^{6k}$	$3.g^{6k}$	$6.g^{6k}$
0	0	1	4	0	4	0	4	0
g^0g^{6k}	$1.g^{6k}$	2	1	4	2	2	2	0
g^1g^{6k}	$2.g^{6k}$	0	4	3	0	2	2	2
g^2g^{6k}	$4.g^{6k}$	2	2	0	1	4	2	2
g^3g^{6k}	$8.g^{6k}$	0	2	2	4	3	0	2
g^4g^{6k}	$3.g^{6k}$	2	2	2	2	0	1	4
g^5g^{6k}	$6.g^{6k}$	0	0	2	2	2	4	3

x^2, $mp = 4$

		0	g^0	g^4	g^8	g^1	g^5	g^9	g^2	g^6	g^{10}	g^3	g^7	g^{11}
		0	1	3	9	2	6	5	4	12	10	8	11	7
0	0	1	2	2	2	0	0	0	2	2	2	0	0	0
g^0	1	2	1	0	0	2	0	2	2	0	2	0	2	0
g^4	3	2	0	1	0	2	2	0	2	2	0	0	0	2
g^8	9	2	0	0	1	0	2	2	0	2	2	2	0	0
g^1	2	0	2	2	0	1	2	2	0	2	0	0	2	0
g^5	6	0	0	2	2	2	1	2	0	0	2	0	0	2
g^9	5	0	2	0	2	2	2	1	2	0	0	2	0	0
g^2	4	2	2	2	0	0	0	2	1	0	0	2	0	2
g^6	12	2	0	2	2	2	0	0	0	1	0	2	2	0
g^{10}	10	2	2	0	2	0	2	0	0	0	1	0	2	2
g^3	8	0	0	0	2	0	0	2	2	2	0	1	2	2
g^7	11	0	2	0	0	2	0	0	0	2	2	2	1	2
g^{11}	7	0	0	2	0	0	2	0	2	0	2	2	2	1

equivalent to

		0	g^0g^{4k}	g^2g^{4k}	g^1g^{4k}	g^3g^{4k}
		0	$1.g^{4k}$	$4.g^{4k}$	$2.g^{4k}$	$8.g^{4k}$
0	0	1	6	0	6	0
g^0g^{4k}	$1.g^{4k}$	2	1	4	4	2
g^1g^{4k}	$2.g^{4k}$	0	4	5	2	2
g^2g^{4k}	$4.g^{4k}$	2	4	2	1	4
g^3g^{4k}	$8.g^{4k}$	0	2	2	4	5

x^2, $mp = 2$

X		0	g^0	g^2	g^4	g^6	g^8	g^{10}	g^1	g^3	g^5	g^7	g^9	g^{11}
		0	1	4	3	12	9	10	2	8	6	11	5	7
0	0	1	2	2	2	2	2	2	0	0	0	0	0	0
g^0	1	2	1	2	0	0	0	2	2	0	0	2	2	0
g^2	4	2	2	1	2	0	0	0	0	2	0	0	2	2
g^4	3	2	0	2	1	2	0	0	2	0	2	0	0	2
g^6	12	2	0	0	2	1	2	0	2	2	0	2	0	0
g^8	9	2	0	0	0	2	1	2	0	2	2	0	2	0
g^{10}	10	2	2	0	0	0	2	1	0	0	2	2	0	2
g^1	2	0	2	0	2	2	0	0	1	0	2	2	2	0
g^3	8	0	0	2	0	2	2	0	0	1	0	2	2	2
g^5	6	0	0	0	2	0	2	2	2	0	1	0	2	2
g^7	11	0	2	0	0	2	0	2	2	2	0	1	0	2
g^9	5	0	2	2	0	0	2	0	2	2	2	0	1	0
g^{11}	7	0	0	2	2	0	0	2	0	2	2	2	0	1

equivalent to

		0	$g^0 g^{2k}$	$g^1 g^{2k}$
		0	$1.g^{2k}$	$2.g^{2k}$
0	0	1	12	0
$g^0 g^{2k}$	$1.g^{2k}$	2	5	6
$g^1 g^{2k}$	$2.g^{2k}$	0	6	7

Appendix B. Equal values transfer property

$p = 13$, 4_periodicity of r in g^r. $Y = MX$. Before re-ordering.

		0	g^0	g^1	g^4	g^2	g^9	g^5	g^{11}	g^3	g^8	g^{10}	g^7	g^6	X	Y
		0	1	2	3	4	5	6	7	8	9	10	11	12		
0	0	1	6	7	6	4	7	7	3	3	6	4	3	4	3	570
g^0	1	4	1	6	7	6	4	7	7	3	3	6	4	3	15	536
g^1	2	3	4	1	6	7	6	4	7	7	3	3	6	4	4	582
g^4	3	4	3	4	1	6	7	6	4	7	7	3	3	6	15	536
g^2	4	6	4	3	4	1	6	7	6	4	7	7	3	3	11	545
g^9	5	3	6	4	3	4	1	6	7	6	4	7	7	3	4	582
g^5	6	3	3	6	4	3	4	1	6	7	6	4	7	7	4	582
g^{11}	7	7	3	3	6	4	3	4	1	6	7	6	4	7	9	587
g^3	8	7	7	3	3	6	4	3	4	1	6	7	6	4	9	587
g^8	9	4	7	7	3	3	6	4	3	4	1	6	7	6	15	536
g^{10}	10	6	4	7	7	3	3	6	4	3	4	1	6	7	11	545
g^7	11	7	6	4	7	7	3	3	6	4	3	4	1	6	9	587
g^6	12	6	7	6	4	7	7	3	3	6	4	3	4	1	11	545

$p = 13$, 4_periodicity of r in g^r. $Y = MX$. After re-ordering.

		0	g^0	g^4	g^8	g^1	g^5	g^9	g^2	g^6	g^{10}	g^3	g^7	g^{11}	X	Y
		0	1	3	9	2	6	5	4	12	10	8	11	7		
0	0	1	6	6	6	7	7	7	4	4	4	3	3	3	3	570
g^0	1	4	1	7	3	6	7	4	6	3	6	3	4	7	15	536
g^4	3	4	3	1	7	4	6	7	6	6	3	7	3	4	15	536
g^8	9	4	7	3	1	7	4	6	3	6	6	4	7	3	15	536
g^1	2	3	4	6	3	1	4	6	7	4	3	7	6	7	4	582
g^5	6	3	3	4	6	6	1	4	3	7	4	7	7	6	4	582
g^9	5	3	6	3	4	4	6	1	4	3	7	6	7	7	4	582
g^2	4	6	4	4	7	3	7	6	1	3	7	4	3	6	11	545
g^6	12	6	7	4	4	6	3	7	7	1	3	6	4	3	11	545
g^{10}	10	6	4	7	4	7	6	3	3	7	1	3	6	4	11	545
g^3	8	7	7	3	6	3	3	4	6	4	7	1	6	4	9	587
g^7	11	7	6	7	3	4	3	3	7	6	4	4	1	6	9	587
g^{11}	7	7	3	6	7	3	4	3	4	7	6	6	4	1	9	587

Appendix C. Eigenvectors, eigenvalues matrices' program

This appendix gives the eigenvectors, eigenvalues matrices and expression of some condensed cardinal matrix. There are four parameters to be chosen by the reader. It suffices then to make a copy of the program on the Pari/gp online application (menu Main, GP in your browser).

Note that sometimes the exponentiation sign ˆ won't copy successfully and has to be retyped manually (lines 14 and 17 of program).

```
{vi = 1; /* choose type of variable (1 for integers, 0 for prime numbers) */
p = 13; /* choose the prime number instance */
n = 2; /* choose natural number power of variable z */
rmd = 3; /* choose integer for rank of cardinal matrix r = rmd*d+1 */
d = gcd(n,p-1); md = rmd*d; delta = (p-1)/md+0.0;
if(delta%1 <> 0, print("CAUTION : md must divide p-1"); md = p-1,
if(md > p-1, print("CAUTION : md must divide p-1"); md = p-1));
v = vector(md); g = vector(p-1); sigm = vector(md+1);
g[1] = 1; sigm[1] = p-1+vi; w = exp(2*I*Pi/p);
for(gg = 2,p-2, g[2] = gg;
for(i = 3, p-1, g[i]= (g[i-1]*gg)%p; if(g[i] == 1, break,ii = i));
if(ii == p-1, break));
for(i = 0, md-1,
sigm[i+2] = vi+d*sum(j = 0, (p-1)/d-1, w^(-g[1+(i+d*j)%(p-1)])));
SIG = matrix(md+1,md+1,i,j,if(j == i,sigm[i],0));
for(i = 0, md-1,
v[i+1] = sum(j = 0, (p-1)/md-1, w^(g[1+(i+j*md)%(p-1)])));
PL = matrix(md+1,md+1,i,j,if(j ==1,1,if(i ==
1,(p-1)/md,v[(i+j-4)%md+1])));
PC = conj(PL); MM = (1/p)*PL*SIG*PC;
print(); print("Eigenvector matrix real part of PL");
printf("%.3f",real(PL));
print(); print("Eigenvector matrix imaginary part of PL");
printf("%.3f",imag(PL));
print(); print("Eigenvalues matrix real part of SIG");
printf("%.3f",real(SIG));
print(); print("Eigenvalues matrix imaginary part of SIG");
printf("%.3f",imag(SIG));
print(); print("Condensed cardinal matrix MM");
printf("%.0f",real(MM))}
```

Appendix D. F-I-cardinal factors: Basic program

This appendix enables to get the normalized cardinal factors for the Friedlander-Iwaniec equation (F-I-equation) over a range of targets and instances (prime numbers) with the online PARI/GP platform. One can use it for other type of equations with degree of stability equal to 1. It suffices to make a copy of the program on the Pari/gp online application (menu Main, GP in your browser).

Note that sometimes the exponentiation sign ˆ won't copy successfully and has to be retyped manually (line 11 of program).

```
{cmax = 20; /* choose targets range */
pmax = 97; /* choose prime numbers range */
print("First vector : cardinal factor for p");
print("Second vector : product of cardinal factors from p = 2 to p");
fanc = vector(cmax+1);
for(j = 1, cmax+1, fanc[j] = 1);
forprime(p = 2, pmax, nc = vector(cmax+1);
for(y = 1, p-1,
for(x1 = 0, p-1,
for(x2 = 0, p-1,
c = (-y+x1^2+x2^4)%p+1;
if(c <= cmax+1, nc[c] = nc[c]+1.0))));
if(p <= cmax, for(j = 0, cmax-p, k = cmax-j; nc[k+1] = nc[k%p+1]));
nc = (1/(p*(p-1)))*nc;
print(""); print("p = " p" c = 0 to " cmax);
printf("%.7f", nc);
for(j = 1, cmax+1, fanc[j] = fanc[j]*nc[j]);
print(""); printf("%.7f", fanc))}
```

Appendix E. F-I-cardinal factors: Primitive roots' program

This appendix enables to get the normalized cardinal factors for the Friedlander-Iwaniec equation over a range of targets and instances (prime numbers). It suffices to make a copy of the program on the Pari/gp online application (menu Main, GP in your browser).

For equation: $p = x_1^2 + x_2^4 - c$, $(x_1, x_2) \in (N, N)$

```
{cmax = 13; /* choose targets' range */
pmax = 97; /* choose prime numbers' range */
print("Vector 1: None-cumulative cardinal factor for c = 0 to "cmax);
print("Vector 2: Cumulative cardinal factor for c = 0 to "cmax);
xa = vector(cmax+1); xc = vector(cmax+1);
print("p = 2");
for(c = 0, cmax, xa[c+1] = 1.0); printf("%.7f", xa);
print(""); xc = xa; printf("%.7f", xc);
forprime(p = 3, pmax, pmod4 = p%4; print(""); print("p = "p);
if(pmod4 == 3, for(c = 0, cmax, cmodp = c%p;
if(cmodp == 0, x = p*p-1, x = p*p-p-1); xa[c+1] = x/p/(p-1)+0.0),
g = lift(znprimroot(p));
g2 = (g*g)%p; g3 = (g2*g)%p; g4 = (g2*g2)%p;
nv = vector(4);
g2t = 1; for(u = 0, (p-1)/2-1,
g2t = g2*g2t; g4t = 1;
for(v = 0, (p-1)/2-1,
g4t = g4*g4t; t = g2t+g4t; t = t%p;
if((t-1)%p == 0, nv[1] = nv[1]+1,
if((t-g)%p == 0, nv[2] = nv[2]+1,
if((t-g2)%p == 0, nv[3] = nv[3]+1,
if((t-g3)%p == 0, nv[4] = nv[4]+1)))))); nv[1] = nv[1]+1;
for(c = 0, cmax, cmodp = c%p;
if(cmodp == 0, x = (p-1)*(p-1),
gj = 1; for(j = 1, p-1, gj = (gj*g)%p;
if(gj == cmodp, jg = j%(p-1); jg = jg%4;
jgpar = 2*frac(jg/2);
if(jgpar == 0, x = p*p-2-4*nv[jg+1]; break, x = p*p-4*nv[jg+1]; break))));
xa[c+1] = x/p/(p-1)+0.0));
printf("%.7f", xa); print("");
for(c = 0, cmax, xc[c+1] = xa[c+1]*xc[c+1]);
printf("%.7f", xc))}
```

For equation: $p = x^2 + y^4 - c$, $x \in N$, $y \in P$

```
{cmax = 13; /* choose targets' range */
pmax = 97; /* choose prime numbers' range */
print("Vector 1 : None-cumulative cardinal factor for c = 0 to "cmax);
print("Vector 2 : Cumulative cardinal factor for c = 0 to "cmax);
xa = vector(cmax+1); xc = vector(cmax+1);
print("p = 2");
for(c = 0, cmax, xa[c+1] = 1.0); printf("%.7f", xa);
print(""); xc = xa; printf("%.7f", xc);
forprime(p = 3, pmax, pmod4 = p%4; print(""); print("p = "p); g =
lift(znprimroot(p));
if(pmod4 == 3,
for(c = 0, cmax, cmodp = c%p;
if(cmodp == 0, x = p*(p-1),
gj = 1; for(j = 1, p-1, gj = (gj*g)%p;
if(gj == cmodp, jg = j%(p-1); jg = jg%2; break));
if(jg == 0, x = p*p-2*p+1, x = p*p-2*p-1));
xa[c+1] = x/(p-1)/(p-1)+0.0),
nv = vector(4);
g2 = (g*g)%p; g3 = (g2*g)%p; g4 = (g2*g2)%p; g2t = 1;
for(u = 0, (p-1)/2-1,
g2t = g2*g2t; g4t = 1;
for(v = 0, (p-1)/2-1,
g4t = g4*g4t; t = g2t+g4t; t = t%p;
if((t-1)%p == 0, nv[1] = nv[1]+1,
if((t-g)%p == 0, nv[2] = nv[2]+1,
if((t-g2)%p == 0, nv[3] = nv[3]+1,
if((t-g3)%p == 0, nv[4] = nv[4]+1))))));
nv[1] = nv[1]+1;
for(c = 0, cmax, cmodp = c%p;
if(cmodp == 0, x = (p-1)*(p-2),
gj = 1; for(j = 1, p-1, gj = (gj*g)%p;
if(gj == cmodp, jg = j%(p-1); jg = jg%4;
x = p*(p-1)-4*nv[jg+1])));
xa[c+1] = x/(p-1)/(p-1)+0.0));
printf("%.7f", xa); print("");
for(c = 0, cmax, xc[c+1] = xa[c+1]*xc[c+1]);
printf("%.7f", xc))}
```

Appendix F. F-I-equation's exact number of solutions

This appendix enables to get the number of solutions of the Friedlander-Iwaniec equation $x^2 + y^4 = p + c$ over a range of targets c with the condition $p < p_{max}$.
It suffices to make a copy of the program on the Pari/gp online application (menu Main, GP in your browser). Note that sometimes the exponentiation sign ˆ won't copy successfully and has to be retyped manually (lines 5 and 9 of program).

```
{ i= 100000; /* choose i such p_max = p_i */
pmax = primes(i)[i];
print("i = "i);
print("p_max = "pmax);
limit1 = floor(pmax^(1/2)); limit2 = floor(pmax^(1/4));
for(c = -5, 15, s = 0;
for(x = 0, limit1,
for(y = 0, limit2,
t = x^2+y^4-c; if(t < 0, t = -t);
if(isprime(t),
if(t < pmax, s++))));
print("c = "c" nbsol = "s))}
```

For the Heath-Brown−Xiannan equation, the only thing to do is to replace "for(y" with "forprime(y" in line 8.

Appendix G. Primitive roots' solutions

Case 1: $p = 89$, $g = 3$, $\alpha = 4$, $\beta = 5$.
Solutions of:

$$\begin{array}{lllllll} eq1: & g^0 \equiv g^{2u} + g^{2v} & \bmod p & \cap & v \equiv 0 & \bmod 2 \\ eq2: & g^0 \equiv g^{2u} + g^{2v} & \bmod p & \cap & v \equiv 1 & \bmod 2 \\ eq3: & g^1 \equiv g^{2u} + g^{2v} & \bmod p & \cap & v \equiv 0 & \bmod 2 \\ eq4: & g^1 \equiv g^{2u} + g^{2v} & \bmod p & \cap & v \equiv 1 & \bmod 2 \end{array}$$

where $u \in [0, \frac{p-1}{1}[$, $v \in [0, \frac{p-1}{2}[$, $w = 2u + 2v$.

$eq1$				$eq2$				$eq3$				$eq4$		
u	v	w		u	v	w		u	v	w		u	v	w
1	2	6		2	1	6		13	24	74		24	13	74
3	10	26		10	3	26		5	34	78		34	5	78
19	6	50		6	19	50		39	12	102		12	39	102
15	34	98		34	15	98		27	36	126		36	27	126
21	42	126		42	21	126		35	30	130		30	35	130
35	38	146		38	35	146								
45	2	94		46	1	94		57	24	162		68	13	162
47	10	114		54	3	114		49	34	166		78	5	166
63	6	138		50	19	138		83	12	190		56	39	190
59	34	186		78	15	186		71	36	214		80	27	214
65	42	214		86	21	214		79	30	218		74	35	218
79	38	234		82	35	234								
8	22	60		9	25	68		16	22	76		7	25	64
22	8	60		25	9	68		22	16	76		25	7	64
				23	43	132		2	42	88		31	41	144
				43	23	132		42	2	88		41	31	144
36	36	144		29	41	140		8	44	104				
				41	29	140		44	8	104				
								26	28	108				
								28	26	108				
52	22	148		53	25	156		60	22	164		51	25	152
66	8	148		69	9	156		66	16	164		69	7	152
				67	43	220		46	42	176		75	41	232
				87	23	220		86	2	176		85	31	232
80	36	232		73	41	228		52	44	192				
				85	29	228		88	8	192				
								70	28	196				
								72	26	196				

Case 2: $p = 89$, $g = 3$, $a = 4$, $b = 5$.
Solutions of:

$$\begin{aligned} eq5: &\quad g^0 \equiv g^{2u} + g^{4v} \mod p \\ eq6: &\quad g^2 \equiv g^{2u} + g^{4v} \mod p \\ eq7: &\quad g^1 \equiv g^{2u} + g^{4v} \mod p \\ eq8: &\quad g^3 \equiv g^{2u} + g^{4v} \mod p \end{aligned}$$

where $u \in [0, \frac{p-1}{1}[$, $v \in [0, \frac{p-1}{2}[$, $w = 2u + 4v$.

$eq5$				$eq6$				$eq7$				$eq8$		
u	v	w		u	v	w		u	v	w		u	v	w
1	1	6		3	1	10		13	12	74		25	7	78
3	5	26		11	2	30		5	17	78		35	3	82
19	3	50		7	10	54		39	6	102		13	20	106
15	17	98		35	8	102		27	18	126		37	14	130
21	21	126		43	11	130		35	15	130		31	18	134
35	19	146		39	18	150								
45	1	94		47	1	98		57	12	162		69	7	166
47	5	114		55	2	118		49	17	166		79	3	170
63	3	138		51	10	142		83	6	190		57	20	194
59	17	186		79	8	190		71	18	214		81	14	218
65	21	214		87	11	218		79	15	218		75	18	222
79	19	234		83	18	238								
8	11	60		10	13	72		16	11	76		8	13	68
22	4	60		26	5	72		22	8	76		26	4	68
				24	22	136		2	21	88		32	21	148
				44	12	136		42	1	88		42	16	148
36	18	144		30	21	144		8	22	104				
				42	15	144		44	4	104				
								26	14	108				
								28	13	108				
52	11	148		54	13	160		60	11	164		52	13	156
66	4	148		70	5	160		66	8	164		70	4	156
				68	22	224		46	21	176		76	21	236
				88	12	224		86	1	176		86	16	236
80	18	232		74	21	232		52	22	192				
				86	15	232		88	4	192				
								70	14	196				
								72	13	196				

Appendix H. Sign rectifications of α and β

This appendix enables to get the signs of the ratios |#v even − #v odd|/2α and |#v even − #v odd+1|/*beta* as defined more precisely in the main text (taking specific power of g in each case in account).
It suffices to make a copy of the program on the Pari/gp online application (menu Main, GP in your browser).

```
{pmax = 1000;
forprime(p = 3, pmax, g = lift(znprimroot(p));
g2 = (g*g)%p; g3 = (g*g2)%p; g4 = (g2*g2)%p;
if(p%4 == 1,for(j = 1, p, b = sqrt(p-4*j*j);
if(b-truncate(b) == 0, a = j; b = truncate(b); break));
rgg2 = 0;
w3 =1; for(u = 1, (p-1), w3 = (w3*g)%p;
if(w3 == 2*a, rga = u; break));
bb = (b+1)/2+(-1+p%8)/4; bb = 1-2*(bb%2);
pp = ((p-1)/4)%2; if(pp == 0, pp = "even", pp = "odd");
rga4 = rga%4; if(rga4 ==3, aa = -1, aa = 1);
rgb4 = rgb%4;
g2 = (g*g)%p; aeven = 0; aodd = 0; beven = 0; bodd = 0;
w1 =1; for(u = 1, (p-1)/1, w1 = (w1*g2)%p;
w2 =1; for(v = 1, (p-1)/2, w2 = (w2*g2)%p;
t = w1+w2; tt = t%p; pv = v%2;
if(tt == g, if(pv == 0, aeven = aeven+1, aodd = aodd+1));
if(tt == 1, if(pv == 0, beven = beven+1, bodd = bodd+1))));
r1 = (aeven -aodd)/(2*a)*aa;
r2 = (beven -bodd+1)/(b)*bb;
print("p = "p" (p-1)/4 is "pp" g = "g" a = "a" b = "b
" r1 = "r1" r2 = "r2" rga4 = "rga4)))}
```

Literature and sources

[1] https://en.wikipedia.org/wiki/Circulant_matrix

[2] https://en.wikipedia.org/wiki/Chebotarev's_density_theorem
https://en.wikipedia.org/wiki/Dirichlet's_theorem_on_arithmetic_progressions

[3] https://en.wikipedia.org/wiki/Prime_number_theorem

[4] https://en.wikipedia.org/wiki/Primitive_root_modulo_n

[5] https://en.wikipedia.org/wiki/Permutation_matrix

[6] https://en.wikipedia.org/wiki/Twin_prime

[7] https://en.wikipedia.org/wiki/Infinite_product

[8] https://en.wikipedia.org/wiki/Euler_product

[9] https://en.wikipedia.org/wiki/Legendre_symbol

[10] https://mathworld.wolfram.com/HarmonicSeries.html

[11] Alphonse de Polignac. Recherches nouvelles sur les nombres premiers. Comptes rendus des séances de l'Académie 1849, v29, p397–401. https://en.wikipedia.org/wiki/Polignac's_conjecture

[12] Yuri V. Matiyasevich (1970). Enumerable sets are Diophantine. Doklady Akademii Nauk SSSR. 191: 279–282.

[13] John Friedlander, Henryk Iwaniec (Feb 1997). Using a parity sensitive sieve to count prime values of a polynomial. PNAS Vol 94, p1054-1058. https://en.wikipedia.org/wiki/Friedlander-Iwaniec_theorem

[14] Roger Heath-Brown, Li Xiannan (2017). Prime values of $a^2 + p^4$. Inventiones Mathematicae, V208: p441–499

[15] Leonard Eugene Dickson. History of the Theory of Numbers. https://en.wikipedia.org/wiki/Fermat's_theorem_on_sums_of_two_squares.

[16] Stan Wagon (1990). Editor's Corner: The Euclidean Algorithm Strikes Again. American Mathematical Monthly, 97 (2): 125, doi:10.2307/2323912.

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

[18] https://hubertschaetzel.wixsite.com/website.

September 26, 2022

Hubert Schaetzel, INPG Grenoble • *E-mail :* hubert.schaetzel@wanadoo.fr
Url : https://hubertschaetzel.wixsite.com/website