Number Theory / *Théorie des Nombres*

Asymptotic Diophantine counting with John Friedlander and Henryk Iwaniec equation common thread.

Hubert Schaetzel

Abstract John Friedlander and Henryk Iwaniec showed in 1997 the infinity of primes being written as $x_1^2+x_2^4$, where x_1 and x_2 are integers. Their results included an asymptotic expression of the enumeration of solutions. Here we give a method to find such result jointly to its generalization.

Dénombrements asymptotiques d'équations diophantines avec le fil conducteur de l'équation de John Friedlander et Henryk Iwaniec.

Résumé John Friedlander et Henryk Iwaniec ont démontré en 1997 l'infinité des nombres premiers s'écrivant $x_1^2+x_2^4$, les variables x_1 et x_2 étant des entiers. Leur résultat incluait une expression asymptotique du dénombrement des solutions. Nous donnons ici une méthode pour trouver un tel résultat conjointement à sa généralisation.

Statute Preprint
Date November 06 2017

Summary

1. Preamble

This article includes many shortcuts.
For the courageous reader, another article online enables one to have a much more complete overview (some 400 pages to this day). [2]

In order to get asymptotically the number of solutions for a given Diophantine equation, the idea here is to form an asymptotic equivalent of each variable within the proposed equation and then assemble emerging results. This presupposes the independence of each brick of this construction (in the spirit of the operations one wishes to execute here). This is the case, for example, but another example could have been chosen aswell, for the Friedlander and Iwaniec equation $y = x_1^2+x_2^4$, where we can distinguish y, x_1^2 and x_2^4. In that Diophantine equation, y is a variable that takes values in the set of prime numbers P and x_1 and x_2 are variables that take values in the set of the nonnegative integers N.

We adopt in this text the following writing convention :

- x_i (or x) for a variable of integers,
- y_i (or y) for a variable of prime numbers,
- z_i (or z) for a variable one or the other type.

The initial idea here is not new, but further use is innovative technique in our view, having not found such thing in other texts. We start by saying that the assessment of the number of solutions of $y = x_1^2+x_2^4$ should be accessible in one way or another by evaluating first

$$y = x_1^2+x_2^4 \text{ modulo } 2^{m2}.3^{m3}.5^{m5}.7^{m7}.11^{m11}\ldots p_i^{mpi} \qquad (1)$$

while m_i and p_i will tend towards infinity.

Our method is then to analyse the "potential to provide solutions" of each part of the chosen equation through their local contribution, that is modulo p_i, and then modulo p_i^{ki} where we extend k_i to infinity. The following will show how to assemble these experiments to provide modulo $2^{m2}.3^{m3}.5^{m5}.7^{m7}.11^{m11}\ldots p_i^{mp}$ results. Of course, there is a basis to this building saga, which lies in particular in the Chinese theorem (if m_1, m_2, …, m_i are coprime integers, $m = m_1.m_2\ldots m_i$, then the ring Z/m_1Z x Z/m_2Z x … x Z/m_iZ is isomorphic to the ring Z/mZ), point which is not developed here.

We will deduce, at the same time for our example (but this can be achieved in a similar way with any other example), the number of asymptotic solutions of $y+c = x_1^2+x_2^4$, c being a given constant. More specifically, c will be used as a parameter.

We want to solve $y+c = x_1^2+x_2^4$. To do this, it is appropriate to write primarily in a quite trivial way :

$$c = x_1^2+x_2^4-y \qquad (2)$$

Although trivial, this is not innocuous. Indeed, the goal here is to register onto c, entity which we will call the target, the result of some local operations, namely a number of occurrences corresponding to the event “I got the value c”.

This approach gives way to the constitution of two new entries that are equivalent for the counting purpose of the proposed equation.
The first is:

$$c \equiv \{\{x_1^2\}\}+\{\{x_2^4\}\}+\{\{-y\}\} \qquad (3)$$

The second is :

$$c \equiv [x_1^2].[x_2^4].[-y] \qquad (4)$$

In fact, the first step will be processed here in a direct way as $c \equiv \{\{x_1^2+x_2^4-y\}\}$ without recourse to basic bricks, but the second, which is based on matrix manipulations, is always built brick by brick. It enables asymptotical enumeration of a whole range of other Diophantine equations, namely those containing y_i, x_j^2 and x_k^4 blocks, and is conceptually much more important.
It turns out that the manipulation of matrices’ product is possible whenever blocks of variables within these matrices are independent from each other.

The way one is writing c to the left of the previous equalities has no importance. Place hooks such as {{c}} and [c], or not, doesn't change anything. The reality of the calculation is not an immediate conversion. It is not a gradual transformation of one equation into another, but rather a way to rethink the problem. The writing is symbolic.

2. Asymptotic representatives

Our investigations are of asymptotic nature. We can then assume that it suffices to get a probabilistic representation of a variable to identify its potential to create solutions.

Entities created on this occasion will be called asymptotic representatives and indicated within brackets {{}}. We will describe below how they are formed distinguishing the case of variables of integers from the case of variables of prime numbers.

2.1. Case of variables of prime numbers

Let us start with a variable of prime numbers {{y}} and observe its local potential :
We project, to do this, the whole set P of prime numbers y on the congruence classes modulo p_i.

$$\begin{array}{lcl} & \text{mod } p_i & \\ P & \rightarrow & \{0, 1, 2, \ldots, p_i-1\} \\ y & & y \text{ mod } p_i \end{array}$$

This application sends a unique number y on 0. This is p_i. Other classes are images in same density (equidensity) of all other primes, which is a well-known result. By assigning a probability density to the quantities of numbers projected on each of the congruence 0, 1, 2,..., p_i-1 and arbitrarily summing all densities to p_i (i.e. getting an average density of 1 per class), we get the correspondence :

Congruencies	0	1	2	…	p_i-1
Normalized densities of probability	→ 0	→ $p_i/(p_i-1)$	→ $p_i/(p_i-1)$	…	→ $p_i/(p_i-1)$

This means that locally, that is modulo p_i, (or at the sequence p_i), omitting equiprobable weighting, the set of prime numbers is equivalent to the following classes :

$$\{1, 2, \ldots, p_i-1\} \approx \{\{P\}\} \equiv \{\{y\}\} \qquad (5)$$

Indeed, the density of probability of 0 being 0, we can ignore this value 0 and we can then ignore weightings since weights are of equal values.

However we used the sign ≈ instead of ≡ because we have neglected temporarily $p_i/(p_i\text{-}1)$ weighting which is essential elsewhere and to which we will return at the chapter "normalization". Variable of type y_i (or y) and P are otherwise the same in our use and need (thus the sign ≡).

The set $\{1, 2,..., p_i\text{-}1\}$ is the Galois Group $(Z/p_iZ)^*$. This group is generated by some root primitive g_i of p_i :

$$\{g_i^0, g_i^1, \ldots, g_i^{pi-2}\} \qquad (6)$$

We can make similar projections on any set of congruencies modulo p_i^{ki}.

$$\begin{array}{ccc} & \text{mod} & \\ P & \rightarrow & \{0, 1, 2, \ldots, p_i^{ki}\text{-}1\} \\ y & & y \bmod p_i^{ki} \end{array}$$

Then, the table will be (with always an average weighting value of 1 per class) :

Congruencies	0 mod p_i	≠ 0 mod p_i
Densities	→ 0	→ $p_i/(p_i\text{-}1)$

(7)

Let us have $\varphi(p_i) = p_i^{(ki-1)}(p_i\text{-}1)$, φ the Euler totient.
The corresponding group will be :

$$\{g_i^0, g_i^1, \ldots, g_i^{\varphi(pi)-1}\} \qquad (8)$$

Of course, for $p_i = 2$, there is no unique primitive g_i and the case is more complex, but the spirit of the approach remains exactly the same. The detail is not included in this article which is intended to be synthetic.

2.2. Case of variables of integers

The set of nonnegative integers N will project in an equiprobable way modulo p_i^{ki} :

$$\begin{array}{ccc} & \text{mod} & \\ N & \rightarrow & \{0, 1, 2, \ldots, p_i^{ki}\text{-}1\} \\ x & & x \bmod p_i^{ki} \end{array}$$

We have the following congruencies mapping table densities with trivial average density of 1 per class :

Congruencies	0 mod p_i	≠ 0 mod p_i
Densities	→ 1	→ 1

(9)

For $p_i = 2$, there is no unique primitive root, but there is still equiprobability.

The following remark is important. We mentioned probabilities. It is wise to do so when we consider a sufficiently large part of P. But when all of P is on the line, the concept is more than a simple probability : there is rather identity (or equivalence) strictly speaking.

The case of the previous variable of integers x is trivial, but that of x^2 or more generally those like x^m would not (we will see that for x^2 and x^4 below). Similarly, buildings are more developed for a variable of prime numbers y^2 and more generally y^m.
But the projection method is the same for these examples as for all Diophantine equations.

2.3. Case of a multifaceted expression

Let us see this with the equation of Iwaniec and Friedlander.
We can simply write (instead of $c \equiv \{\{x_1^2\}\}+\{\{x_2^4\}\}+\{\{-y\}\}$) the expression :

$$c \equiv \{\{x_1^2+x_2^4-y\}\} \qquad (10)$$

Locally, that is modulo p_i^{ki}, looking for occurrences of the target c, means just to write a set of nested loops where the three variables y, x_1 and x_2 are incremented on a discrete domain (thus integers) :
The previous equation (10), applied locally, is to be simply the following sequence of operations :

```
From y = 0 to $p_i^{ki}$-1
If y = 0 mod $p_i$ goto next y otherwise
From $x_1$ = 0 to $p_i^{ki}$-1
From $x_2$ = 0 to $p_i^{ki}$-1
c = $x_1^2+x_2^4-y \bmod p_i^{ki}$                              (11)
#(c) = #(c)+1
Next $x_2$
Next $x_1$
Next y
```

Let us give a few details fur these operations.
- What interests us here is the evaluation of the expression #(c).
- The order of the loops has no impact on results #(c). He is indifferent to start with y, x_1 or x_2 and continue in any order.
- A local exploration is, for a given variable to test modulo p_i^{ki} all values of the variable from 0 to p_i^{ki}-1. Of course an exploration from 1 to p_i^{ki} would be a quite equivalent choice and giving the same result.
- We find a conditional line after variable y that we do not find after variables x_1 and x_2. Indeed, y is a variable representing the set of prime numbers P. Thus, we have seen in paragraph 2.1 that the probability of a number of P to reach a value that is a multiple of p_i is 0. We endorse this fact by jumping this instance each time that we face a multiple of p_i. On the other hand, in paragraph 2.2, we have seen that a variable of integers x_i is trivially equiprobable. There are therefore no additional conditions to be provided after such variables in nested loops.
- As we look at a problem of enumeration of solutions, when the result of the operation $x_1^2+x_2^4-y \bmod p_i^{ki}$ provides a given value c, we store the number of occurrences in the counting variable #(c), thus the incremental operation #(c) = #(c)+1.

The comparison of all values #(c), in reviewing c from 0 to p_i^{ki}-1, gives access to a local “probability” (here $\#(c)/(p_i^{3ki}.(p_i-1))$ with two variables x_i and one variable y_j) of events.
We will call #(c) = Fa(c) the factors of abundance of the target c.

Performing the calculations for our example gives the following table limiting results to range p_i between 2 and 29 and for k_i = 1.

p_i	k_i	c															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		#(c) = Fa(c)															
2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	1	8	5	5	8	5	5	8	5	5	8	5	5	8	5	5	8
5	1	16	19	17	25	23	16	19	17	25	23	16	19	17	25	23	16
7	1	48	41	41	41	41	41	41	48	41	41	41	41	41	41	48	41
11	1	120	109	109	109	109	109	109	109	109	109	109	120	109	109	109	109
13	1	144	163	153	163	151	153	153	161	161	163	151	161	151	144	163	153
17	1	256	275	271	265	275	265	281	281	271	271	281	281	265	275	265	271
19	1	360	341	341	341	341	341	341	341	341	341	341	341	341	341	341	341
23	1	528	505	505	505	505	505	505	505	505	505	505	505	505	505	505	505
29	1	784	803	809	809	823	823	823	803	817	823	817	809	817	823	809	817

It should be noted that during the execution of calculation, numbers in red font are not displayed. They must be added modulo p_i^{ki} (so modulo p_i here).

It is useful, at this stage, to highlight a key point from the practical (and theoretical) point of view.

3. Degree of stability

Let us suppose that we evaluate from k_i = 1 up to k, the local “probabilities” modulo p_i^{ki} (mentioned above), and that the said relative probabilities are stabilizing from k on. We will then call k the local degree of stability (at the sequence p_i). For some given problem, the degree of stability may vary from one sequence p_i to another. We will call its maximum the degree of stability of the Diophantine equation. This degree may be finite or infinite, locally and/or for the maximum.

If the degree is finite, the asymptotic enumeration is easier to achieve.
If it is infinite, there may be still some way to identify a convergence of the different probabilities when k_i tends towards infinity by a careful study.

The degree of stability is finite (and equal to 1) for the monomials y_1^m, i.e. variables of prime numbers, but also for sufficiently symmetrical expressions like for example $y_1^4+y_1^3.y_2+y_1^2.y_2^2+y_1.y_2^3+y_2^4$ placed inside Diophantine equations (in this case equal to 1 locally except for p_i = 2 and p_i = 5 which degree is 2).

This is not the case for monomials of variables of integers or for polynomials (therefore generating likely difficult problems for elliptic equations and more complex equations) for which sole remedy is to understand how relative occurrences evolve at infinity (of k_i) and this for each p_i as there is no formal reason for families (modulo some values) with similar behaviours to exist.

In the example chosen for this article, it turns out that the degree of stability is equal to 1 for all p_i (thus the systematic selection of $k_i = 1$ made in the table of the previous paragraph). The presence of monomials of variables of integers is not an obstacle here because there is also a monomial of prime numbers which imposes its stability to the whole.

4. Normalization of occurrences

With the nested loops such as those numbered (11), we get occurrences of the target c. According to the number of variables, it is necessary to submit quantities to the right “probability”. The goal is to get an average per class, after calculation, weighted at 1. We call this normalization.

Modulo p, we have for the variables of integers x and for a variable of prime numbers y :

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

0	1	2	…	p-1
1	1	1	…	1

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

1	2	3	…	p-1
1	1	1	…	1

Note that c = 0 is absent in the second expression.

For an additional variable :

$\{\{x_i\}\}_p \equiv$

0	1	2	…	p-1
1/p	1/p	1/p	1/p	1/p

(i.e. $\sum = 1$)

$\{\{y_i\}\}_p \equiv$

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

(i.e. $\sum = 1$)

This operation is prolonged modulo p^δ.

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

These ratios apply to each new entry of variables : k variable of integers → ratio $1/(p^\delta)^k$, m variables of prime numbers → ratio $1/(p^\delta.(p-1))^m$.
To bring back the sum to p^δ, we then perform a multiplication of the coefficients by p^δ.
Hence the rules :

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

This normalization results for our example in the following table :

p_i	k_i	c															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		#(c)															
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1,333	0,833	0,833	1,333	0,833	0,833	1,333	0,833	0,833	1,333	0,833	0,833	1,333	0,833	0,833	1,333
5	1	0,8	0,95	0,85	1,25	1,15	0,8	0,95	0,85	1,25	1,15	0,8	0,95	0,85	1,25	1,15	0,8
7	1	1,143	0,976	0,976	0,976	0,976	0,976	0,976	1,143	0,976	0,976	0,976	0,976	0,976	0,976	1,143	0,976
11	1	1,091	0,991	0,991	0,991	0,991	0,991	0,991	0,991	0,991	0,991	0,991	1,091	0,991	0,991	0,991	0,991
13	1	0,923	1,045	0,981	1,045	0,968	0,981	0,981	1,032	1,032	1,045	0,968	1,032	0,968	0,923	1,045	0,981
17	1	0,941	1,011	0,996	0,974	1,011	0,974	1,033	1,033	0,996	0,996	1,033	1,033	0,974	1,011	0,974	0,996
19	1	1,053	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997
23	1	1,043	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998	0,998
29	1	0,966	0,989	0,996	0,996	1,014	1,014	1,014	0,989	1,006	1,014	1,006	0,996	1,006	1,014	0,996	1,006
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
Fan(c)		1,225	0,796	0,664	1,627	0,915	0,621	1,252	0,842	1,037	1,557	0,646	0,891	1,035	0,948	1,095	1,009

We have here k = 2 variables of integers and m = 1 variable of prime numbers, with $\delta = k_i = 1$, i.e. a ratio $r_i = 1/(p_i^{\delta})^{(k-1)}/((p_i^{\delta-1}(p_i-1))^m) = 1/(p_i.(p_i-1))$ that was used for each of the lines.
As the average of the values is adjusted to 1 on each line (modulo p_i^{ki}), the product by column Fan(c) indicates, depending on whether it is higher or lower than 1, the potential of the target c to give an excess or lack of solutions from the average. Here the solutions corresponding to c = 3 (Fan(3) = 1,627) are a priori 2,5 times more abundant than those of c = 2 (Fan(2) = 0.621).
Of course, to get a more precise result the product must be realized for p_i describing all of the set P.
Let us notice that having big gaps of populations between targets will be welcome when we test our method numerically.

It should be noted also that if all of the lines were adjusted to an average strictly greater than 1, respectively strictly lower than 1, infinite products would generally diverge (if not null), respectively would tend towards 0. This would be unusable in an asymptotic formula for counting. If such a formula exists, it can be derived with our method only after normalization. We will find these infinite products further. We call them normalized abundances factors. They have also in the literature the names of singular series or Euler products. However, to our knowledge, they are not obtained by a systematic method, such as the one proposed here.

We now do much better.

5. Construction of cardinal matrices

We have shown so far how to get numerically what we called the factors of abundance. However, this is so far experimental work and we want a comprehensive calculation of these items. In the example, the pattern of the occurrences looks very simple for p_i equal to 3, 7, 11, 19 or 23, but is more complicated for other values.

In addition, when the degree of stability is not 1 and with a greater number of variables, the amount of calculations increases exponentially. So, it is essential to find a parry to the digital explosion.

The solution is then, since the variables are independent from each other, to use the calculation loops of the elementary building blocks :

```
From $y = 0$ to $p_i^{ki}-1$
If $y = 0 \bmod p_i$ goto next y otherwise
$c = (-y) \bmod p_i^{ki}$                              (12)
$\#(c) = \#(c)+1$
Next y
```

```
From $x_1 = 0$ to $p_i^{ki}-1$
$c = x_1^2 \bmod p_i^{ki}$                             (13)
$\#(c) = \#(c)+1$
Next $x_1$
```

```
From $x_2 = 0$ to $p_i^{ki}-1$
$c = x_2^4 \bmod p_i^{ki}$                             (14)
$\#(c) = \#(c)+1$
Next $x_2$
```

There is no degree of stability for variables of integers due to one exception, namely c = 0 (but not for p_i and multiples). Thus, we propose an alternative to this peculiar obstacle by avoiding it : we first calculate simulating a variable of prime numbers (which does not contain 0), which then allows effectively to establish a degree of stability, then we return to the case of the integers' variable by using an extremely precious property which is given further :

```
From $x_1 = 0$ to $p_i^{ki}-1$
If $x_1 = 0 \bmod p_i$ goto next $x_1$ otherwise
$c = x_1^2 \bmod p_i^{ki}$                             (15)
$\#(c) = \#(c)+1$
Next $x_1$
```

```
From $x_2 = 0$ to $p_i^{ki}-1$
If $x_2 = 0 \bmod p_i$ goto next $x_2$ otherwise
$c = x_2^4 \bmod p_i^{ki}$                             (16)
$\#(c) = \#(c)+1$
Next $x_2$
```

The degree of stability of each loop is then 1 (and for each p_i) in our case.

In fact, the proposed methodology requires, to make it the most effective possible, an essential and absolute rule of work : Always start considering all variables as variables of prime numbers.

Solving the proper problem is done in a second time.

For each of the variables, one can build a square matrix that is representative of its individual action within a Waring sum, i.e. a sum of monomials of identical degree j (y^j or x^j). A problem of counting involving t nested loops and thus t variables then translates in a result deriving from a matrix to the power t. This matrix, which we call cardinal matrix, (because it is used to count) is obtained through what we call a primitive root equation.
It is, in general terms, the following expression :

$$m(r,s) = \{\#(r,s) \,/\, or(0,g_i^{r-1}) = or(0,g_i^{u.d})+ or(0,g_i^{s-1}.g_i^{v.d}) \bmod p_i^{ki}\} \qquad (17)$$

Indeed, we seek the effect of the introduction of a new monomial $z_{n+1}^{\ j}$ in a Waring sum $c = z_1^{\ j}+ z_2^{\ j}+\ldots+ z_n^{\ j}$ on #(c). This research is done by crossing classes of equal size, if they exist, which is the case when a primitive root is used to create these classes. Of course, integer 0 is to be taken into account also as it cannot be generated by a root primitive g_i.

Here m(r, s) is the component of the matrix on the r line and s column, and $d = \gcd(j,\varphi(p_i^{ki}))$. The parameters u and v are integers and are incremented from 0 to p_i^{ki}-1. During this incrementing, for each occurrence of $g_i^{r-1} = g_i^{u.d}+g_i^{s-1}.g_i^{v.d} \bmod p_i^{ki}$, and taking also into account 0, the operation #(r,s) = #(r,s)+1 is performed and m(r, s) are the end results of all the #(r,s) thus obtained.

Initially, cardinal matrices have rank p_i^{ki}, but due to targets with identical number of occurrences (the patterns mentioned at the beginning of this paragraph), they can contract into smaller entities. Expression (17) already takes account of these associations with factor $d = \gcd(j,\varphi(p_i^{ki}))$ playing a central role.

The collection of occurrences $\#(c = g_i^{w}.g_i^{u.d})$ is done by considering the classes of equal occurrences (u is generic in a class, and in our case we have either d = env = 1, d = 2, or d = 4). These classes present generic form based on a primitive root g_i of p_i (for $p_i > 2$), any choice of primitive root providing the same classes within eventually a permutation. Matric results are collected in a column vector :

$$\begin{vmatrix} \#\{0\} \\ \#\{g_i^{\,0}.g_i^{u.d}\} \\ \#\{g_i^{\,1}.g_i^{u.d}\} \\ \ldots \\ \#\{g_i^{\,d-1}.g_i^{u.d}\} \end{vmatrix}$$

where $\#\{g_i^{\,j}.g_i^{u.d}\} \equiv \#\{g_i^{\,j}\}$ for any u (as one can verify).

Let us return to the case of the Iwaniec and Friedlander equation, with basic bricks -y, $x_1^{\,2}$ et $x_2^{\,4}$ already mentioned, whose representative matrices are noted [M0], [M1] and [M2] respectively.

For a variable of integers x, the original square matrix [MI0] is rank p_i (the degree of stability is 1) with all components equal to 1.

The passage of a variable of integers to a variable of primes always results in the withdrawal of identity [I] to the initial matrix (the precious property referred to above).

$$[M0] = [MI0]-[I] \qquad (18)$$

To simplify writings, we refrain from indexing i within p_i and g_i.
According to the degree of potential contraction (linked directly to d), matrices for x (variable of integers) and y (variable of prime numbers) are as follows :

$$\begin{array}{c}\text{Var x}\\ \text{or –x}\end{array} \qquad [A] \qquad\qquad \begin{array}{c}\text{Var y}\\ \text{or -y}\end{array} \qquad [B] = [A]-[I]$$

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{u}\} \end{vmatrix} : [MI0] = \begin{vmatrix} 1 & p-1 \\ 1 & p-1 \end{vmatrix} \qquad \begin{vmatrix} \#\{0\} \\ \#\{g^{u}\} \end{vmatrix} : [M0] = \begin{vmatrix} 0 & p-1 \\ 1 & p-2 \end{vmatrix}$$

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{2u}\} \\ \#\{g.g^{2u}\} \end{vmatrix} : [MI0] = \begin{vmatrix} 1 & (p-1)/2 & (p-1)/2 \\ 1 & (p-1)/2 & (p-1)/2 \\ 1 & (p-1)/2 & (p-1)/2 \end{vmatrix} \qquad \begin{vmatrix} \#\{0\} \\ \#\{g^{2u}\} \\ \#\{g.g^{2u}\} \end{vmatrix} : [M0] = \begin{vmatrix} 0 & (p-1)/2 & (p-1)/2 \\ 1 & (p-3)/2 & (p-1)/2 \\ 1 & (p-1)/2 & (p-3)/2 \end{vmatrix}$$

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^{2}.g^{4u}\} \\ \#\{g^{3}.g^{4u}\} \end{vmatrix} : [MI0] =: \begin{vmatrix} 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \end{vmatrix} \qquad \begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^{2}.g^{4u}\} \\ \#\{g^{3}.g^{4u}\} \end{vmatrix} : [M0] = \begin{vmatrix} 0 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-5)/4 & (p-1)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-5)/4 & (p-1)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-5)/4 & (p-1)/4 \\ 1 & (p-1)/4 & (p-1)/4 & (p-1)/4 & (p-5)/4 \end{vmatrix}$$

For [M1] corresponding to x^2, we have four useful formulations :

For d = 1

$$[M1] = \begin{vmatrix} 1 & p-1 \\ 1 & p-1 \end{vmatrix}$$

For d = 2 and p = 3 mod 4 :

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

For env = 4 (d = 2) and p = 1 mod 8 :

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

where

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

For env = 4 (d = 2) and p = 5 mod 8 :

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

where

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

We will come back on the “env” later on.

For [M2] corresponding to x^4, we have again four other useful formulations:

For d = 1

$$[M2] = \begin{vmatrix} 1 & p-1 \\ 1 & p-1 \end{vmatrix}$$

For d = 2 and p = 3 mod 4, the matrix is identical to the case x^2 :

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

For p = 1 mod 8, we have d = 4 and :

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

where

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

with integers’ decomposition of p

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

For p = 5 mod 8, we have also d = 4 and :

$$[M2] = \left| \begin{array}{ccccc} 1 & 0 & 0 & p-1 & 0 \\ 4 & x_3+1 & x_5 & x_3 & x_5 \\ 0 & x_4 & x_5+1 & x_5 & x_2 \\ 0 & x_1 & x_2 & x_3+1 & x_4 \\ 0 & x_2 & x_4 & x_5 & x_5+1 \end{array} \right|$$

where

$$\left| \begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{array} \right| = \left| \begin{array}{l} (p+1)/4+(-1)^{(\beta+1)/2}.(3/2).\beta \\ (p+1)/4+2\alpha.\text{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-7)/4-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p+1)/4-2\alpha.\text{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4+(-1)^{(\beta+1)/2}.(1/2).\beta \end{array} \right|$$

with still same integers' decomposition of p

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

Each of these results here derives from a primitive root equation and its comprehensive study. In appendix 1, we provide some examples of numerical calculations using some general constructive rules of cardinal matrices. Each of these matrices displays by construction a sum equal to respectively p or p-1 per line depending on whether it represents a variable respectively of integers or of prime numbers (when the degree of stability is 1).

The reader can see here the complexity of the literal formulas for simple monomials. To get an expression directly, without decomposition in independent terms, is hence quite illusory (and thus probably inaccessible to another approach than the one proposed here).

We have three main situations (and two lower cases) to examine when the nested loops given in (11) are decrypted. Each of the variables, with assigned power, gives rise to a particular "environment" (9 environments here by the crossing of cases, plus 3 environments due to the subcase p_i = 5 mod 8, which is in addition to p_i = 1 mod 8).

p_i	variable x^2	variable x^4	variable -p	Common multiple	lower case
2	1	1	1	1	/
1 mod 4	2	4	1	4	p_i = or(1,5) mod 8
3 mod 4	2	2	1	2	/

What we call environment is linked to the size (rank) of the matrix which gives an account of occurrences for a given basic brick rated generically {{z}}. The environment is equal to the rank of the matrix minus one unit.
Thus :

$$\text{env}\{\{z\}\} = \text{rang}\{\{z\}\}-1 \qquad (19)$$

It turns out that any assembly of basic bricks can be treated by adopting a common environment which is the lowest common multiple (lcm) of the environments of each brick.

The difference of 1 between rank and environment stems from the specific and systematic behaviour of target c = 0 in the assessment of occurrences, behaviour that we mentioned above and which extends into the matrix treatment.
Any matrix of environment "env" can be transformed into a matrix of multiple environment k.env. These matrices can be multiplied after adjustment to the same environment (being of identical rank). The object is not to show in a short text the mechanism to get multiple environment matrix from another, nor to expand on the many properties of these matrices ("semi-hermicity", common basis change matrices, formal writing as p functions of eigenvalues and eigenvectors, moving to a multiple environment by the rules attached to the eigenvalues, relationship with the Gauss sums, etc.).
We just give away them.

It should be noted that the asymptotic representatives (and the matrices) of y and y are identical as {1, 2, ..., p_i-1} and {-1, -2, ..., -p_i+1} are the same modulo p_i.

Then, we get :

For p = 2

The case p = 2 resolves directly immediately showing the equality of occurrences :

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

For p = 3 mod 4

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

For p = 1 mod 8

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} = [M0].[M1].[M2]. \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ 4x_1+6 \\ 4x_2 \\ 4x_3+2 \\ 4x_4 \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ p-1+2.(-1)^{(\beta+1)/2}.\beta \\ p-1+4\alpha.\text{if}(x_4>x_2,-1,1) \\ p-1-2.(-1)^{(\beta+1)/2}.\beta \\ p-1-4\alpha.\text{if}(x_4>x_2,-1,1) \end{vmatrix} = \begin{vmatrix} (p-1)^2 \\ p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1-4\alpha.\text{if}(x_4>x_2,-1,1) \\ p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1+4\alpha.\text{if}(x_4>x_2,-1,1) \end{vmatrix}$$

For p = 5 mod 8

$$\begin{vmatrix} \#\{0\} \\ \#\{g^{4u}\} \\ \#\{g.g^{4u}\} \\ \#\{g^2.g^{4u}\} \\ \#\{g^3.g^{4u}\} \end{vmatrix} = [M0].[M1].[M2]. \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ 4x_3+6 \\ 4x_4 \\ 4x_1+2 \\ 4x_2 \end{vmatrix} = [M0] \begin{vmatrix} 2p-1 \\ p-1-2.(-1)^{(\beta+1)/2}.\beta \\ p-1-4\alpha.\text{if}(x_4>x_2,-1,1) \\ p-1+2.(-1)^{(\beta+1)/2}.\beta \\ p-1+4\alpha.\text{if}(x_4>x_2,-1,1) \end{vmatrix} = \begin{vmatrix} (p-1)^2 \\ p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1+4\alpha.\text{if}(x_4>x_2,-1,1) \\ p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1-4\alpha.\text{if}(x_4>x_2,-1,1) \end{vmatrix}$$

Normalization consists in dividing cardinals by $p^{2-1}(p-1)^1 = p(p-1)$.

For p = 2

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

For p = 3 mod 4

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

For p = 1 mod 8

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

Pour p = 5 mod 8

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

In these entries, please do not forget that all the results are identical modulo p^{ki}, hence modulo p here. In particular, we have Fan{c\p, p} = Fan {0, p}.

Let us go back to our example and take a sample of each type (the choice of primitive roots g is that of the smallest value, the results being identical for any other choice).

	p	g	α	β	x_2	x_4
3 mod 4	23	5	/	/	/	/
1 mod 8	17	3	2	1	8	0
5 mod 8	29	2	1	5	8	12

For p = 23

$$\begin{vmatrix} \text{Fa}\{0, p\} \\ \text{Fa}\{g^u, p\} \end{vmatrix} = \begin{vmatrix} (p+1).(p-1) \\ p^2-p-1 \end{vmatrix} = \begin{vmatrix} 528 \\ 505 \end{vmatrix}$$

For p = 17

$$\begin{vmatrix} Fa\{0, p\} \\ Fa\{g^{4u}, p\} \\ Fa\{g.g^{4u}, p\} \\ Fa\{g^2.g^{4u}, p\} \\ Fa\{g^3.g^{4u}, p\} \end{vmatrix} = \begin{vmatrix} (p-1)^2 \\ p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1-4\alpha.\mathrm{if}(x_4>x_2,-1,1) \\ p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1+4\alpha.\mathrm{if}(x_4>x_2,-1,1) \end{vmatrix} = \begin{vmatrix} 256 \\ 275 \\ 265 \\ 271 \\ 281 \end{vmatrix}$$

For p = 29

$$\begin{vmatrix} Fa\{0,p\} \\ Fa\{g^{4u}, p\} \\ Fa\{g.g^{4u}, p\} \\ Fa\{g^2.g^{4u}, p\} \\ Fa\{g^3.g^{4u}, p\} \end{vmatrix} = \begin{vmatrix} (p-1)^2 \\ p^2-p+1+2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1+4\alpha.\mathrm{if}(x_4>x_2,-1,1) \\ p^2-p+1-2.(-1)^{(\beta+1)/2}.\beta \\ p^2-p+1-4\alpha.\mathrm{if}(x_4>x_2,-1,1) \end{vmatrix} = \begin{vmatrix} 784 \\ 803 \\ 809 \\ 823 \\ 817 \end{vmatrix}$$

and it is necessary to check the relative values of x_2 and x_4, which depends on the initial choice of g.

$$\begin{vmatrix} x_2 \\ x_4 \end{vmatrix} = \begin{vmatrix} (p-3)/4+2\alpha.\mathrm{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4-2\alpha.\mathrm{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \end{vmatrix} \qquad \text{For p = 17 = 1 mod 8}$$

et

$$\begin{vmatrix} x_2 \\ x_4 \end{vmatrix} = \begin{vmatrix} (p+1)/4+2\alpha.\mathrm{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p+1)/4-2\alpha.\mathrm{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \end{vmatrix} \qquad \text{For p = 29 = 5 mod 8}$$

For p = 17, iterated powers of g = 3 are :

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
g^r	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

The targets c from 1 to 15 are thus in the following families' classification :

	g^{4u}	$g^{4u}.g$	$g^{4u}.g^2$	$g^{4u}.g^3$
c	1, 4, 13	3, 5, 12, 14	2, 8, 9, 15	6, 7, 10, 11
Fa(c)	275	265	271	281

and x_2 = 8 and x_4 = 0 (with this choice of g).

For p = 29, iterated powers of g = 2 are :

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
g^r	2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25	21	13	26	23	17	5	10	20	11	22	15	1

The targets c from 1 to 15 are thus in the following families' classification :

	g^{4u}	$g^{4u}.g$	$g^{4u}.g^2$	$g^{4u}.g^3$
c	1, 7	2, 3, 11, 14	4, 5, 6, 9, 13	8, 10, 12, 15
Fa(c)	803	809	823	817

and x_2 = 8 and x_4 = 12 (with this choice of g).

The reader may refer to the table at paragraph 2.3 to check the consistency of the results.

Thus, we get after normalization :

$$Fan(0) = \prod_{p\,=\,1 \bmod 4} (1-1/p) \prod_{p\,=\,3 \bmod 4} (1+1/p) \qquad (20)$$

and

$$\mathrm{Fan}(c \neq 0) = \prod_{p \backslash c} 1-((-1)^{(p-1)/2})/p \;.\; \prod_{\substack{p \nmid c \\ p = 3 \bmod 4}} \left(1-\frac{1}{p.(p-1)}\right). \prod_{\substack{p \nmid c \\ p = 1 \bmod 4 \\ c \;=\; g^i.g^{4u}}} \left(1+\frac{1+2a}{p.(p-1)}\right) \qquad (21)$$

where

$$\begin{gathered} a = (-1)^{(p+3)/4+\mathrm{int}(i/2)}.\mathrm{if}(i \bmod 2 = 0, (-1)^{(\beta+1)/2}.\beta, 2\alpha.\mathrm{if}(x_4>x_2,-1,1)) \\ \text{and} \\ p = (2\alpha)^2+\beta^2 \quad \alpha > 0, \beta > 0 \end{gathered} \qquad (22)$$

From previous matrices [M0], [M1] and [M2], we are able to evaluate the (normalized) factors of abundance of a Diophantine equation such as :

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

Previously (for the enumeration of $x_1^2+x_2^4 = y+c$), the complete knowledge of the components of the matrices [M2] was not useful (the first quasi-trivial column knowledge was sufficient). For the general count however, it becomes indispensable.

6. Asymptotic formula

So far, our results allow us to compare the number of solution between targets. If we have an asymptotic formula counting solutions for c = 0, we can deduce a general formula for any target c by simply using the ratio Fan(c)/Fan(0).
Friedlander and Iwaniec study [1] settled the following formula for c = 0 (here Γ is the Gamma function) :

$$\lim_{y \to \infty} \#\{x_1^2+x_2^4 = y\} = 2^{1/2}.(\Gamma(1/4))^2/(3.\pi^{3/2}).y^{3/4}/\mathrm{Ln}(y) \qquad (23)$$

We get straightforward :

$$\lim_{y \to \infty} \#\{ x_1^2+x_2^4 = y+c\} = \mathrm{Fan}(c).(1/(6.2^{1/2}\pi^{1/2})).(\Gamma(1/4))^2.y^{3/4}/\mathrm{Ln}(y) \qquad (24)$$

using :

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

7. Numerical application

We have $(1/(6.2^{1/2}\pi^{1/2})).(\Gamma(1/4))^2 \approx 0.8740191847640399368216131966$ and then according to formula (24) :

$$\lim_{y \to \infty} \#\{x_1^2+x_2^4 = y+c\} \approx \mathrm{Fan}(c).0,874019184764.y^{3/4}/\mathrm{Ln}(y) \qquad (25)$$

This formula cannot be used directly without taking a few precautions as the distribution of the prime numbers near the origin shows a surplus compared to the formula :

$$\lim_{y \to \infty} \#\{y\} = y/\mathrm{Ln}(y) \qquad (26)$$

Then let us write the count of prime numbers near the origin in the form :

$$\#\{y\} \approx \mathrm{coef}(y).y/\mathrm{Ln}(y) \qquad (27)$$

Let us have y(i) = y the i-th prime number. We have the following values :

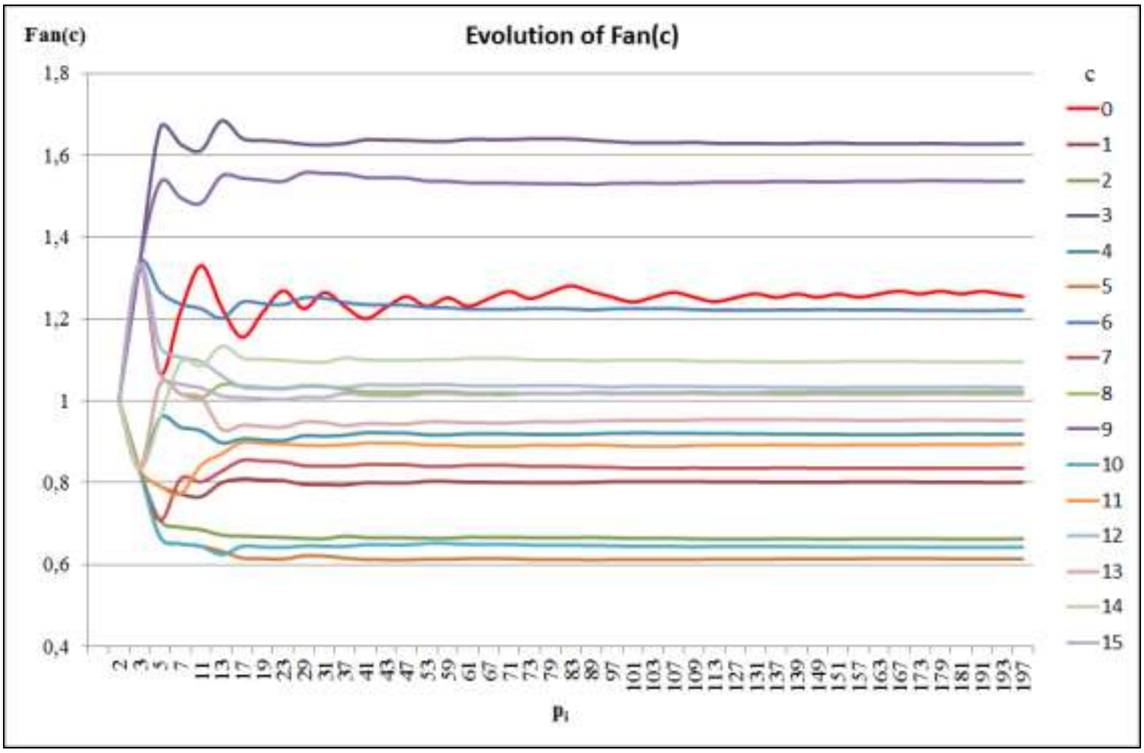
i	50	100	200	500	1000	2500	5000	10000	20000	30000	40000	50000
$y(i) = p_i$	229	541	1223	3571	7919	22307	48611	104729	224737	350381	479909	611953
$\mathrm{coef}(y_i)$	1,1864	1,1633	1,1626	1,1454	1,1336	1,1221	1,1100	1,1037	1,0966	1,0931	1,0903	1,0887

We will use these values to correct the initial counting formula of Friedlander and Iwaniec equation by writing :

$$\lim_{y \to \infty} \#\{x_1^2+x_2^4 = y+c\} \approx \mathrm{Fan}(c).0,874019184764.\mathrm{coef}(y).y^{3/4}/\mathrm{Ln}(y) \qquad (28)$$

In addition, we do an approximate calculation of the normalized factors of abundance Fan(c) taking the column products up to $p_i = 197$, products given by the following table :

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Fan(c)	1,2548	0,8009	0,6628	1,6285	0,9182	0,6138	1,2209	0,8356	1,0220	1,5366	0,6424	0,8945	1,0326	0,9528	1,0948	1,0159



The evolution of the curves Fan(c), when values of p_i are increasing, stabilizes very early as shown in the previous graphic. One target shows as an exception, namely c = 0, for which undulations of the curve remain important throughout the area presented here, but however a trend exists. All factors expressed at the p_i = 197 sequence are less than 2.5 percent of their values at the sequence p_i = 29.

We will now be able to test the formula Fan(c).0,874019184764.coef(y).$y^{3/4}$/Ln(y) by comparing it to the effective number of solutions of the equation when y is increasing. The distribution of the solutions in a given volume, here delimited by the value y, is not necessarily homogeneous. The road to infinity is very long. We do not know a priori whether there may be concentration or scarcity of the solutions on this or that part of the volume.

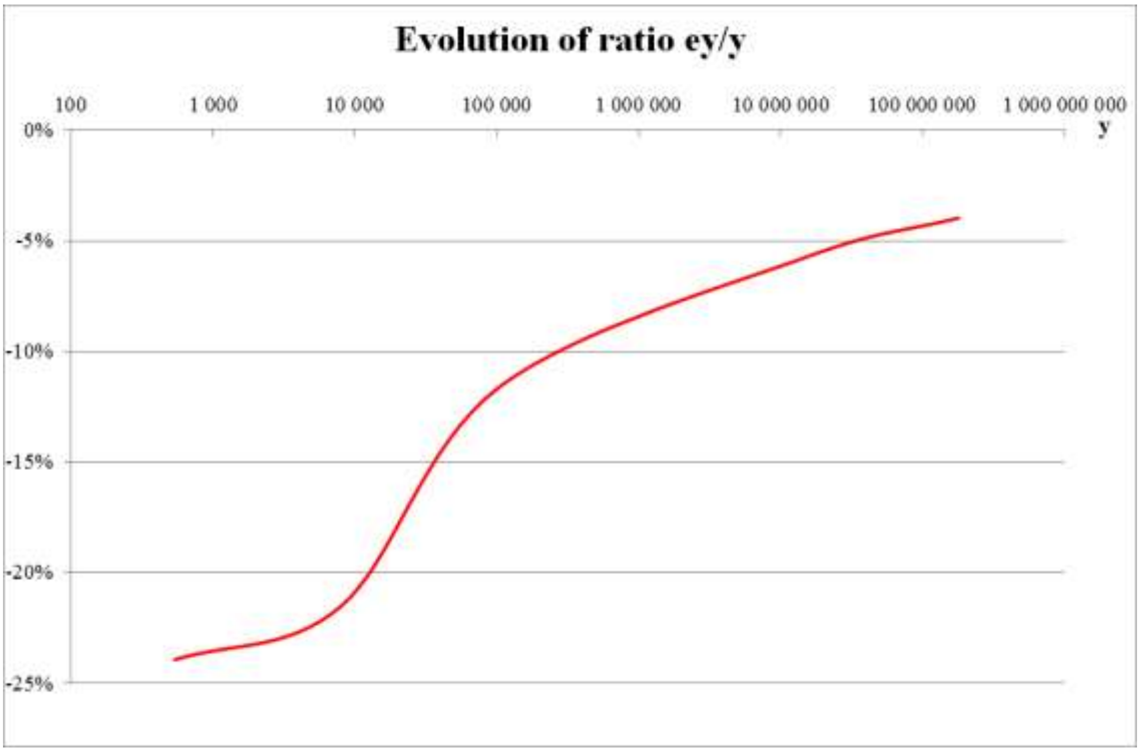
Let us consider the case of the 16 targets selected in a natural way (without skipping some that would be annoying) and for this we will check deviations from an average value. Thus, we will use the following equality :

$$\Sigma(\#\{x_1^2+x_2^4 = y+c\} - \mathrm{Fan}(c).0{,}874019184764.\ \mathrm{coef}(y).(y-ey)^{3/4}/\mathrm{Ln}(y-ey)) = 0 \qquad (29)$$

The unknown here is parameter ey and we evaluate the relative gap ey/y obtained when y increases. In practice, this gap should tend towards 0 when y is increasing (with coef(y) tending towards 1 at the same time). This gap being settled for an given y, we then check the target by target gaps.

The results are :

i	100	1000	10000	100000	1000000	10000000
y(i) = p_i	541	7919	104729	1299709	15485863	179424673
ey_i/y_i	-25,3%	-21,6%	-11,6%	-6,8%	-5,7%	-4,0%



The ripple of ey/y actually takes a direction towards 0 % when y is increasing.

For the number of solutions target by target and for given y, we get the following table :

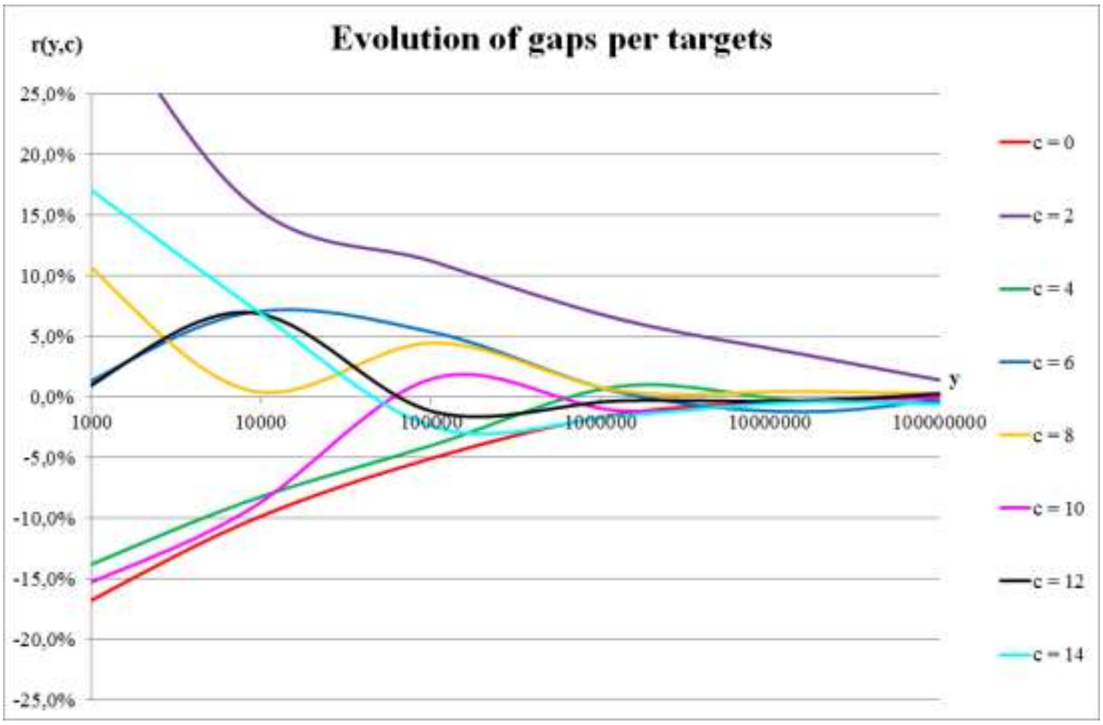
i	y(i)	c = 0	c = 1	c = 2	c = 3	c = 4	c = 5	c = 6	c = 7	c = 8	c = 9	c = 10	c = 11	c = 12	c = 13	c = 14	c = 15
100	541	21	10	19	34	16	14	25	17	24	31	11	19	21	23	27	20
1000	7919	118	67	81	173	88	79	137	93	108	147	61	99	116	99	124	103
10000	104729	623	382	385	863	461	333	672	429	558	780	341	466	533	510	558	534
100000	1299709	3348	2058	1909	4508	2507	1659	3317	2257	2780	4080	1719	2450	2786	2606	2917	2744
1000000	15485863	18101	11282	9935	23790	13253	9076	17460	12039	14864	22243	9274	12909	14901	13743	15782	14827
10000000	179424673	97682	61200	51813	126733	70928	48005	94937	64465	79482	119508	49846	69138	80521	73767	84364	79028

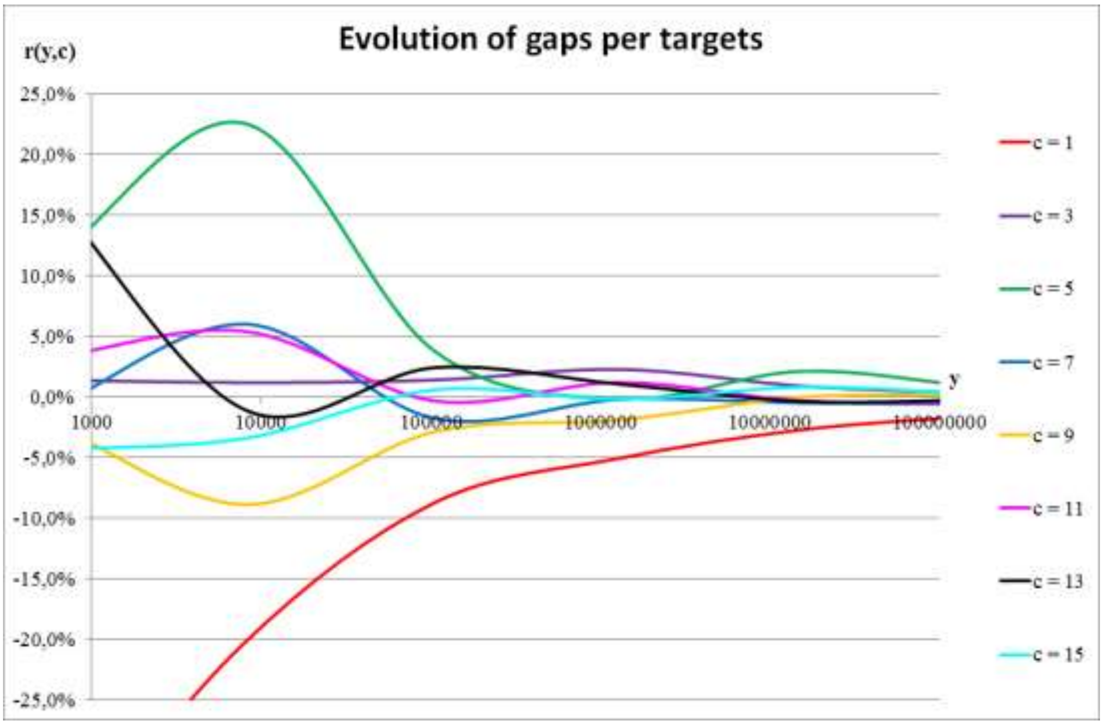
For the gaps of each of the targets, the ratios

$$r(y,c) = (\#\{x_1^2+x_2^4 = y+c\} - Fan(c).0,874.\ coef(y).(y-ey)^{3/4}/Ln(y-ey))/\ (\#\{x_1^2+x_2^4 = y+c\}) \qquad (30)$$

are given by the table :

i	y = y(i)	c = 0	c = 1	c = 2	c = 3	c = 4	c = 5	c = 6	c = 7	c = 8	c = 9	c = 10	c = 11	c = 12	c = 13	c = 14	c = 15
100	541	-18,7%	-39,3%	39,3%	1,4%	-15,4%	10,8%	-0,5%	-1,2%	14,1%	-2,0%	-16,8%	3,2%	-1,2%	17,3%	19,8%	-4,4%
1000	7919	-10,4%	-20,3%	16,4%	1,2%	-8,7%	22,6%	6,9%	6,0%	0,7%	-8,9%	-9,6%	5,4%	7,0%	-1,0%	7,9%	-3,4%
10000	104729	-5,0%	-8,7%	11,2%	1,4%	-3,9%	3,8%	5,3%	-1,8%	4,5%	-2,9%	1,6%	-0,3%	-1,2%	2,4%	-2,5%	0,6%
100000	1299709	-1,4%	-5,0%	6,4%	2,3%	0,9%	-0,1%	0,4%	-0,2%	0,5%	-1,9%	-1,1%	1,2%	-0,3%	1,1%	-1,6%	-0,2%
1000000	15485863	-0,4%	-2,7%	3,5%	0,9%	-0,3%	2,1%	-1,2%	-0,5%	0,5%	0,0%	-0,3%	-0,3%	-0,3%	-0,4%	-0,4%	0,8%
10000000	179424673	0,3%	-1,5%	0,7%	0,3%	-0,5%	0,8%	0,2%	-0,6%	0,2%	0,2%	0,0%	-0,4%	0,5%	-0,2%	-0,7%	0,3%





The population densities corresponding to any particular target vary along the “volume” y : the curves are undulating. Targets that follow less the expected approximate formula are here c = 1, c = 2 and c = 9. However, the trend toward 0 % is underway for all targets.

8. Fugue et prelude

This article is a case study, which gives general terms for the asymptotic enumeration of Diophantine equations. Many aspects of the method are not covered here including :

- The constitution of global asymptotic formulas (i.e. the assessment of r and s in asymptotic formulas $\alpha.z^r/Ln^s(z)$),
- The type of completely solvable equations,
- The genesis and properties of cardinal matrices,
- The construction of the cardinal matrices of a given environment,
- The classic examples (De Polignac, Hua, Catalan, Pillai, Waring, quadratic equations $u.z_1^2+v.z_1.z_2+w.z_2^2$) and more complex examples (z_1^6, $z_1^3z_1^3+z_1^2.z_2+z_1.z_2^2+z_2^3$, $z_1^4+z_1^3.z_2+z_1^2.z_2^2+z_1.z_2^3+z_2^4$),
- Etc.

REFERENCES

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

[2] https://sites.google.com/site/schaetzelhubertdiophantien/.
https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzY2hhZXR6ZWxodWJlcnRkaW9waGFudGllbnxneDozNmNmYzhlODNkYjMwN2Nm

APPENDIX 1

This appendix provides two examples of calculation of cardinal matrices related to the Friedlander and Iwaniec equation. The calculation is based on a general formulation for a cardinal matrix corresponding to the monomial x^n where d = gcd(n,p-1) and with a degree of stability that is equal to 1 (for the complete equation) :

$$[M] \;= (1/p) \begin{vmatrix} 1 & \lambda_0{*}/d & \lambda_0{*}/d & \dots & \lambda_0{*}/d \\ 1 & \lambda_1{*}/d & \lambda_2{*}/d & \dots & \lambda_d{*}/d \\ 1 & \lambda_2{*}/d & \lambda_3{*}/d & \dots & \lambda_1{*}/d \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \lambda_d{*}/d & \lambda_1{*}/d & \dots & \lambda_{d-1}{*}/d \end{vmatrix} \begin{vmatrix} \sigma_0 & 0 & 0 & \dots & 0 \\ 0 & \sigma_1 & 0 & \dots & 0 \\ 0 & 0 & \sigma_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \sigma_d \end{vmatrix} \begin{vmatrix} 1 & \lambda_0/d & \lambda_0/d & \dots & \lambda_0/d \\ 1 & \lambda_1/d & \lambda_2/d & \dots & \lambda_d/d \\ 1 & \lambda_2/d & \lambda_3/d & \dots & \lambda_1/d \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \lambda_d/d & \lambda_1/d & \dots & \lambda_{d-1}/d \end{vmatrix}$$

where

$$\lambda_0 = p\text{-}1$$

and for u > 0 :

$$\lambda_k = d.\sum_{r = 0 \text{ à } (p-1)/d-1} e^{(-2\pi i/p).g\hat{}(k-1+r.d)}$$

and

$$\sigma_k = \text{if(variable of integers,1,0)} + \lambda_k$$

In this entry, the complex number $\lambda_k{*}$ is the complex conjugate of λ_k.
If p = 1 mod 2d, then eigenvalues σ_k (and the λ_k) are real, as $g^{(u+(p-1)/(2d)).d} = g^{(p-1)/2}.g^{u.d} = -g^{u.d}$ mod p and the terms $\sin((2\pi/p).g^{k-1+(u+(p-1)/(2d)).d}) + \sin((2\pi/p).g^{k-1+u.d}) = 0$ offset each other in pairs.
If p = 1 + d mod 2d, on the contrary eigenvalues σ_k (and the λ_k) have an imaginary part.

We write the product of previous matrices as :

$$[M] = (1/p).[\lambda_d{*}].[\sigma_d].[\lambda_d]$$

The matrices $[\sigma_d]$ and $[\lambda_d]$ are complex according to the cases and $[\lambda_d{*}]$ is, except for the first row and the first column, the transconjugate matrix of $[\lambda_d]$. In fact, matrices $[\lambda_d]$ and $[\lambda_d{*}]$ are contracted expressions of transconjugate (and unitary) basis change matrices of circular matrices. The eigenvalues of these basis change matrices are typically consisting of $\sum c_t.e^{-2\pi i.t.r/n}$, hence the previous form of the λ_k. By the way, $[I_d]$ being the identity matrix of rank d, we have also :

$$[\lambda_d{*}].[\lambda_d] = p.[I_d]$$

For what interests us here, we have d = 4, and we consider two cases.

Case p = 1 mod 8.
We take the example p = 17 and g = 3

Calculation of λ_k/d

$$\lambda_k/d = \sum\cos(2\pi/17.3^{k-1+4r}) + i.\sum\text{-}\sin(2\pi/17.3^{k-1+4r})$$

cos

k \ r	0	1	2	3
1	0,445738	-0,273663	0,445738	-0,273663
2	-0,982973	0,739009	-0,982973	0,739009
3	-0,850217	-0,602635	-0,850217	-0,602635
4	0,092268	0,932472	0,092268	0,932472

-sin

k \ r	0	1	2	3
1	0,895163	0,961826	-0,895163	-0,961826
2	-0,183750	-0,673696	0,183750	0,673696
3	-0,526432	-0,798017	0,526432	0,798017
4	-0,995734	-0,361242	0,995734	0,361242

Calculation of $[\lambda_d]$ et $[\lambda_d{*}]$

$$[\lambda_d] = \begin{vmatrix} 1 & 4 & 4 & 4 & 4 \\ 1 & 0{,}344151 & -0{,}487928 & -2{,}905704 & 2{,}049481 \\ 1 & -0{,}487928 & -2{,}905704 & 2{,}049481 & 0{,}344151 \\ 1 & -2{,}905704 & 2{,}049481 & 0{,}344151 & -0{,}487928 \\ 1 & 2{,}049481 & 0{,}344151 & -0{,}487928 & -2{,}905704 \end{vmatrix}$$

$$[\lambda_d{*}] = \begin{vmatrix} 1 & 4 & 4 & 4 & 4 \\ 1 & 0{,}344151 & -0{,}487928 & -2{,}905704 & 2{,}049481 \\ 1 & -0{,}487928 & -2{,}905704 & 2{,}049481 & 0{,}344151 \\ 1 & -2{,}905704 & 2{,}049481 & 0{,}344151 & -0{,}487928 \\ 1 & 2{,}049481 & 0{,}344151 & -0{,}487928 & -2{,}905704 \end{vmatrix}$$

It is easy to check here that $[\lambda_d{*}].[\lambda_d] = 17.[I_d]$.

Calculation of $[\sigma_d]$

$$[\sigma_d] = \begin{vmatrix} 17 & 0 & 0 & 0 & 0 \\ 0 & 2{,}376603 & 0 & 0 & 0 \\ 0 & 0 & -0{,}951713 & 0 & 0 \\ 0 & 0 & 0 & -10{,}622814 & 0 \\ 0 & 0 & 0 & 0 & 9{,}197925 \end{vmatrix}$$

Calculation of [M]

$$[M] = \begin{vmatrix} 1 & 16 & 0 & 0 & 0 \\ 4 & 1 & 8 & 4 & 0 \\ 0 & 8 & 1 & 4 & 4 \\ 0 & 4 & 4 & 5 & 4 \\ 0 & 0 & 4 & 4 & 9 \end{vmatrix}$$

This compares to

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

where

$$\begin{vmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{vmatrix} = \begin{vmatrix} (p+5)/4+(-1)^{(\beta+1)/2}.(3/2).\beta \\ (p-3)/4+2\alpha.\mathrm{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4-2\alpha.\mathrm{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p+1)/4+(-1)^{(\beta+1)/2}.(1/2).\beta \end{vmatrix} = \begin{vmatrix} 4 \\ 8 \\ 4 \\ 0 \\ 4 \end{vmatrix}$$

with integers' decomposition of p

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

thus also $\alpha = 2$ and $\beta = 1$.

Case p = 5 mod 8.
We take the example p = 29 and g = 2

Calculation of λ_u/d

$$\lambda_k/d = \sum\cos(2\pi/29.2^{k-1+4r}) + i.\sum-\sin(2\pi/29.2^{k-1+4r})$$

cos

k r	0	1	2	3	4	5	6
1	0,907575	0,796093	-0,561187	-0,994138	-0,161782	-0,856857	-0,725995
2	0,647386	0,267528	-0,370138	0,976621	-0,947653	0,468408	0,054139
3	-0,161782	-0,856857	-0,725995	0,907575	0,796093	-0,561187	-0,994138
4	-0,947653	0,468408	0,054139	0,647386	0,267528	-0,370138	0,976621

-sin

k r	0	1	2	3	4	5	6
1	0,419889	0,605174	-0,827689	0,108119	-0,986827	-0,515554	0,687699
2	0,762162	0,963550	0,928977	-0,214970	0,319302	0,883512	-0,998533
3	0,986827	0,515554	-0,687699	-0,419889	-0,605174	0,827689	-0,108119
4	-0,319302	-0,883512	0,998533	-0,762162	-0,963550	-0,928977	0,214970

Calculation of $[\lambda_d]$ et $[\lambda_d{*}]$

$$\mathcal{Re}[\lambda_d] = \begin{vmatrix} 1 & 7 & 7 & 7 & 7 \\ 1 & -1{,}596291 & 1{,}096291 & -1{,}596291 & 1{,}096291 \\ 1 & 1{,}096291 & -1{,}596291 & 1{,}096291 & -1{,}596291 \\ 1 & -1{,}596291 & 1{,}096291 & -1{,}596291 & 1{,}096291 \\ 1 & 1{,}096291 & -1{,}596291 & 1{,}096291 & -1{,}596291 \end{vmatrix}$$

and

$$\mathcal{Im}[\lambda_d] = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0,509188 & -2,643998 & -0,509188 & 2,643998 \\ 0 & -2,643998 & -0,509188 & 2,643998 & 0,509188 \\ 0 & -0,509188 & 2,643998 & 0,509188 & -2,643998 \\ 0 & 2,643998 & 0,509188 & -2,643998 & -0,509188 \end{vmatrix}$$

$$\mathcal{Re}[\lambda_d{}^*] = \begin{vmatrix} 1 & 7 & 7 & 7 & 7 \\ 1 & -1,596291 & 1,096291 & -1,596291 & 1,096291 \\ 1 & 1,096291 & -1,596291 & 1,096291 & -1,596291 \\ 1 & -1,596291 & 1,096291 & -1,596291 & 1,096291 \\ 1 & 1,096291 & -1,596291 & 1,096291 & -1,596291 \end{vmatrix}$$

and

$$\mathcal{Im}[\lambda_d{}^*] = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -0,509188 & 2,643998 & 0,509188 & -2,643998 \\ 0 & 2,643998 & 0,509188 & -2,643998 & -0,509188 \\ 0 & 0,509188 & -2,643998 & -0,509188 & 2,643998 \\ 0 & -2,643998 & -0,509188 & 2,643998 & 0,509188 \end{vmatrix}$$

It is easy to verify here that $[\lambda_d{}^*].[\lambda_d] = 29.[I]$

Calculation of $[\sigma_d]$

$$\mathcal{Re}[\sigma_d] = \begin{vmatrix} 29 & 0 & 0 & 0 & 0 \\ 0 & -5,385165 & 0 & 0 & 0 \\ 0 & 0 & 5,385165 & 0 & 0 \\ 0 & 0 & 0 & -5,385165 & 0 \\ 0 & 0 & 0 & 0 & 5,385165 \end{vmatrix}$$

and

$$\mathcal{Im}[\sigma_d] = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2,036750 & 0 & 0 & 0 \\ 0 & 0 & -10,575994 & 0 & 0 \\ 0 & 0 & 0 & -2,036750 & 0 \\ 0 & 0 & 0 & 0 & 10,575994 \end{vmatrix}$$

Calculation of [M]

$$[M] = \begin{vmatrix} 1 & 0 & 0 & 28 & 0 \\ 4 & 9 & 4 & 8 & 4 \\ 0 & 12 & 5 & 4 & 8 \\ 0 & 0 & 8 & 9 & 12 \\ 0 & 8 & 12 & 4 & 5 \end{vmatrix}$$

This compares to

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

where

$$\begin{vmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{vmatrix} = \begin{vmatrix} (p+1)/4+(-1)^{(\beta+1)/2}.(3/2).\beta \\ (p+1)/4+2\alpha.\text{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-7)/4-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p+1)/4-2\alpha.\text{if}(x_4>x_2,-1,1)-(-1)^{(\beta+1)/2}.(1/2).\beta \\ (p-3)/4+(-1)^{(\beta+1)/2}.(1/2).\beta \end{vmatrix} = \begin{vmatrix} 0 \\ 8 \\ 8 \\ 12 \\ 4 \end{vmatrix}$$

with integers' decomposition of p

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

so that $\alpha = 1$ and $\beta = 5$.

APPENDIX 2

CODE FOR PARI/GP

Getting the exact number of solutions to $x^2+y^4 = p+c$ with parameter $q = p_i$ (to be chosen).

```
{i= 100000;
q = primes(i)[i]; print(i); print(q);limit1 = floor(q^(1/2)); limit2 = floor(q^(1/4));
for(c = 0 , 15,
s = 0 ;
for(x = 0 , limit1,
for(y = 0, limit2, t = x^2+y^4-c;
if(isprime(t),
if(t < q,
s++))));
print(s))}
```