

DIOPHANTINE EQUATIONS
 $\mathbf{x}^4 + \mathbf{y}^4 = \mathbf{z}^n, \mathbf{n} \geq 0$
APPLICATION IN CRYPTOGRAPHY
René-Louis Clerc (june 2026) (*)

- ABSTRACT

We provide an overview of the known and expressible solutions in the family of Diophantine quartic equations

$$x^4 + y^4 = z^n, xyz \neq 0, n \geq 0.$$

We will determine the values of n that lead to non-trivial solutions and describe families of solutions that are not necessarily primitive and belong essentially to \mathbf{Z} .

For the case $x = y$ with odd exponents n greater than 1, we will express all possible solutions parametrically.

Finally, we will describe an application to asymmetric cryptography by considering the finite field \mathbf{Z}/\mathbf{pZ} , where p is a large prime number satisfying two conditions, and by defining a one-way function associated with these equations.

-EQUATIONS DIOPHANTIENNES $\mathbf{x}^4 + \mathbf{y}^4 = \mathbf{z}^n$

APPLICATION EN CRYPTOGRAPHIE

Nous proposons un aperçu des solutions connues et exprimables de la famille des équations quartiques diophantiennes

$$x^4 + y^4 = z^n, xyz \neq 0, n \geq 0.$$

Nous déterminerons les valeurs de n qui conduisent à des solutions non triviales et expliciterons des familles de solutions non nécessairement primitives appartenant essentiellement à \mathbf{Z} .

Pour le cas $x = y$ avec des exposants n impairs supérieurs à 1, nous exprimerons paramétriquement toutes les solutions possibles.

Nous décrirons enfin un schéma d'application à la cryptographie asymétrique

en nous plaçant dans le corps fini $\mathbf{Z}/p\mathbf{Z}$, p étant un grand nombre premier vérifiant deux conditions, en définissant une fonction à sens unique associée à ces dernières équations.

- Mathematics Subject Classification-MSC2020: 11D41, 11D45, 11J25.
- Keywords: Diophantine equations, Fermat's equation, solutions of Diophantine equations, modular arithmetic.

- INTRODUCTION

Many Diophantine equations have been studied ([2], [3], [4], [5], [6], [7], [8], [10], [11], [12], [13], [14], [15], [16], [17], [18], ...) connected with the one in the title. For example, K. Gyory studied in ([1],[2]) the Diophantine equation $x^p + y^p = cz^p$ and in [5] B. J. Powell proved that this equation has no integer solutions for special values of p .

Here we will consider the equations given in the title for various values of the positive integer exponent n . For our quartic equations (of the Fermat-Catalan type)

$$x^4 + y^4 = z^n,$$

we recall that their primitive solutions are defined by the conditions

$$xyz \neq 0 \text{ and } \gcd(x, y, z) = 1.$$

However, we will consider examining and listing all possible non-trivial solutions for a given n , especially since, as soon as $n > 2$, we know that Beal's conjecture ([11]), which remains neither proven nor disproven, states that these equations have no non-trivial primitive integer solutions.

It should be noted that the parity of the exponent 4 of the variables x and y allows us to immediately extend the set of solutions from \mathbf{N} to \mathbf{Z} : if the pair (x, y) is a solution, then the combinations $(\pm x, \pm y)$ are also solutions.

-1- Case $n = 0; x^4 + y^4 = 1$

There is no non-trivial solution.

In \mathbf{R}^2 , the set of solutions forms a closed curve that is symmetric about the axes and the origin and resembles a square with rounded corners. If we replace the exponent 4 with an even number $m > 1$, our curve is one of the intermediate superellipses between the circle for $m = 2$ and the square for $m \rightarrow \infty$.

-2- Case $n = 0; x^4 + y^4 = z$

This is the classic Waring's problem (1770): there are infinitely many integers z that can be expressed as a sum of two powers of four (see [2quatre](#), [A003336](#): 2, 17, 32, 82, 97, 162, 257, 272, 337, 512, 626, 641, 706, 881, 1250, 1297, 1312, 1377, 1552, 1921, 2402, 2417, 2482, 2592, 2657, 3026, 3697, 4097, 4112, 4177, 4352, 4721, 4802, 5392, 6497, 6562, 6577, 6642, 6817, 7186, 7857, 8192, 8962, 10001, 10016, 10081, 10256, 10625 ...

For example, $1312 = 2^4 + 6^4$, $10081 = 3^4 + 10^4$, $71769617 = 19^4 + 92^4$.

The smallest number with two solutions is $635318657 = 59^4 + 158^4 = 133^4 + 134^4$ ([A018786](#)), the next is $3262811042 = 7^4 + 239^4 = 157^4 + 227^4$ ([A003824](#)).

(59, 158) is a so-called primitive solution ($\gcd(59, 158, 635318657) = 1$), whereas (118, 316) is not primitive because: $118^4 + 316^4 = 16^4 (59^4 + 158^4)$.

Note that there are no cases with 3 solutions (see [Bill Butler](#): there are 1413 integers corresponding to two primitive solutions).

-3- Case $n = 2; x^4 + y^4 = z^2$

There is no non-trivial integer solution according to Fermat and Kummer.

On the other hand, there are infinitely many non-integer solutions, such as $(2, 2, 4\sqrt{2})$, $(2, 3, \sqrt{97})$, $(1, 4, \sqrt{257})$ or $(X, Y, \sqrt{X^4 + Y^4})$ for all X, Y .

-4- Case $n = 4; x^4 + y^4 = z^4$

According to Fermat-Wiles' theorem [9], there are no non-trivial integer solutions.

Here, too, there are infinitely many non-integer solutions.

-5- Case $n = 2p; x^4 + y^4 = z^{2p}$, p positif

These equations reduce to Fermat equations

$$(x^2)^2 + (y^2)^2 = (z^p)^2$$

It can be shown quite easily that there is no non-trivial integer solution for all $p \geq 1$.

For any p , there will always be an infinite number of non-integer solutions.

Following Fermat and Euler, assume a minimal solution, transform the equation with another smaller solution to arrive at a contradiction (method of infinite descent).

-6- Case $n = 2p + 1; x^4 + y^4 = z^{2p+1}, p > 0$

Interesting cases ([1], [8]) corresponding to odd n greater than 1 : there are non-trivial integer solutions for every p , at least in the case where $x = y$.

-Property 1

For any $p > 0$, all integer solutions of $2x^4 = z^{2p+1}$ will necessarily be of the general form $x = A^n 2^{k(n)}, n = 2p + 1$, where the expression for k depends on n and A is an integer, which may be relative; z will then be of the form $z = A^{4m(n)}$.

Let's first look for solutions where $x = y = 2^k$.

This gives $1 + 4k \equiv 0 \pmod{n}$, so we obtain $k(n)$, which will allow us to express the general form of all integer solutions $x = y$ for the case $n = 2p + 1$ under consideration.

Since $k(n)$ is a solution to $1 + 4k = mn$ for m an integer, the minimum values of k and m can be easily calculated in terms of n (see the following paragraphs):

$$\begin{aligned} n = 3, k = 2, m = 3 \\ n = 5, k = 1, m = 1 \\ \dots \\ n = 15, k = 11, m = 3 \end{aligned}$$

This will yield all non-trivial solutions where $x = y$. Indeed, given a solution (x, z) , for any prime number p that divides x :

1. • If $p > 2$, the exponent of p in $2x^4$ is $4v_p(x)$ and in z it is $nv_p(z)$. The equality $4v_p(x) = nv_p(z)$ and $\gcd(4, n) = 1$ implies that $v_p(x)$ must be a multiple of n , hence the factor A^n .
2. • If $p = 2$, the exponent of 2 in $2x^4$ is $4v_2(x) + 1$; it must be equal to $nv_2(z)$, so it is exactly $k(n)$.

In both of these cases, we can easily deduce the exponent $m(n)$ in z (see Property 2 of paragraph 14 for the explicit form of the solutions (x, z) for all p).

We thus parameterize the infinite set of all non-trivial solutions with $x = y$.

We will now examine in detail some of these odd cases where $n \geq 3$, by expanding the expressions for the exponents $k(n)$ and $m(n)$ for each n .

-7- Case $n = 3; x^4 + y^4 = z^3$

This case defines elliptic curves which may have a positive rank, and thus an infinite number of rational points and consequently an infinite number of integer solutions ([1]).

There are an infinite number of solutions $x = y$ and none with x and y not proportional.

For any odd $n > 1$, integer solutions of the form $x = y$ will necessarily be of the general form $A^n 2^{k(n)}$ where the expression for k depends on n .

The search for solutions of the form $x = y = 2^k$ leads to

$$1 + 4k \equiv 0 \pmod{3}, \text{ so } k = 2 + 3t.$$

Thus all integer solutions $x = y$ are of the form

$$\begin{aligned} x = y &= 2^{2+3t} \prod_{i=1}^r p_i^{3u_i} \\ z &= 2^{3+4t} \prod_{i=1}^r p_i^{4u_i} \end{aligned}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

Examples:

$$\begin{aligned} t = 0, r = 0, x = y = 4, z = 8 \\ t = 0, r = 1, p_1 = 3, u_1 = 1, x = y = 108, z = 648 \\ t = 1, r = 0, x = y = 32, z = 128 \\ t = 0, r = 1, p_1 = 5, u_1 = 1, x = y = 500, z = 5000 \end{aligned}$$

We can find solutions where x and y are different but satisfy $y = kx$:

$$x = (1 + k^4)^2 t^3, y = k (1 + k^4)^2 t^3, \quad z = (1 + k^4)^3 t^4$$

Examples:

$$\begin{aligned} k = 2, t = 1, x = 289, y = 578, z = 4913; \\ k = 2, t = 2, x = 2312, y = 4624, z = 78608; \\ x^4 + y^4 = 485735942131712; \\ k = 3, t = 1, x = 6724, y = 20172, z = 551368; \\ x^4 + y^4 = 167619550409708032; \\ k = 5, t = 1, x = 391876, y = 1959380, z = 245314376; \\ x^4 + y^4 = 14762808930988484877349376. \end{aligned}$$

Are there any others?

Probably not of a different type from kx (conjecture).

-8- Case $n = 5; x^4 + y^4 = z^5$

This is a rather unusual and interesting case, as there are solutions x and y that are NOT proportional.

The associated curve is an elliptic curve of positive rank, hence there are infinitely many rational points and therefore infinitely many families of integer solutions.

As mentioned above, if we look for solutions of the form $x = y = 2^k$, we obtain $k = 1 + 5t$ and thus all integer solutions $x = y$ are of the form

$$\begin{aligned} x &= y = 2^{1+5t} \prod_{i=1}^r p_i^{5u_i} \\ z &= 2^{1+4t} \prod_{i=1}^r p_i^{4u_i} \end{aligned}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

Examples:

$$\begin{aligned} t &= 0, r = 0, x = y = 2, z = 2; \\ t &= 1, r = 0, x = y = 64, z = 32; \\ t &= 0, r = 1, p_1 = 3, u_1 = 1, x = y = 486, z = 162; \\ t &= 0, r = 1, p_1 = 7, u_1 = 1, x = y = 33614, z = 4802; \\ t &= 2, r = 1, p_1 = 5, u_1 = 1, x = y = 6400000, z = 320000. \end{aligned}$$

It is also fairly easy to find solutions where $x \neq y$ but $y = kx$ (where k is a positive integer > 1):

$$\begin{aligned} x &= (1 + k^4) t^5, y = k (1 + k^4) t^5 \\ z &= (1 + k^4) t^4 \end{aligned}$$

$k(> 1)$ and t are positive integers.

Examples with $k = 2$:

$$\begin{aligned} t &= 1 : 17, 34, 17; \\ t &= 2 : 544, 1088, 272; \\ t &= 3 : 4131, 8262, 1377; \\ t &= 4 : 17408, 34816, 4352; \\ t &= 5 : 53125, 106250, 10625. \end{aligned}$$

Let us now try to construct solutions $x \neq y$ where y/x is rational. If we let $\gcd(x, y) = d$, we can write

$$x = dm, y = dn, \gcd(m, n) = 1, \text{ } m \text{ and } n \text{ positive integers;}$$

by setting $S = m^4 + n^4$, our equation becomes $d^4 S = z^5$.

By factoring S and d into prime factors, we can fairly easily express d and z in the form

$$d = S^{1+5v} w^{5u}, z = S^{1+4v} w^{4u}, \text{ where } u, v, \text{ and } w \text{ are integers } (w \neq 0),$$

and derive the expressions for x and y .

Since attempts to find alternative solutions have failed, we can reasonably propose the following conjecture.

- Conjecture

All distinct integer solutions ($y/x = n/m$ any rational number) of $x^4 + y^4 = z^5$ are of the form

$$x = m (m^4 + n^4)^{1+5v} w^{5u}, y = n (m^4 + n^4)^{1+5v} w^{5u}$$

$$z = (m^4 + n^4)^{1+4v} w^{4u}$$

$m \neq n, n, w$ non-negative integers, u and v integers.

Examples:

$$m = 4, n = 7, v = 0, w = 1, u = 0$$

$$x = 10628, y = 18599, z = 2657$$

$$x^4 + y^4 = z^5 = 132421277116505057$$

$$m = 2, n = 3, v = 1, w = 2, u = 1$$

$$x = 53310208315456, y = 79965312473184, z = 137397444112$$

$$x^4 + y^4 = z^5 = 48965846853680836650881544765598622770576250993961336832.$$

We have shown here an infinite family of non-trivial solutions, where y/x is any rational number, but these are not primitive, since $\gcd(x, y, z) \geq m^4 + n^4 > 1$.

At present, no non-trivial primitive solution is known.

It should be noted that this case is particularly interesting, even exceptional, primarily because the associated curve is elliptic of strictly positive rank.

-9- Case $n = 7; x^4 + y^4 = z^7$

In this hyperbolic case, the absence of non-proportionnal non-trivial solution follows from the incompatibility between the Galois representation attached to the Frey curve and the space of modular forms of the corresponding level ([9]). As in the cases where $n = 3$ and 5 , we can express all integer solutions $x = y$ in the form

$$x = y = 2^{5+7t} \prod_{i=1}^r p_i^{7u_i}$$

$$z = 2^{3+4t} \prod_{i=1}^r p_i^{4u_i}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

Examples:

$$t = 0, r = 0, x = y = 32, z = 8$$

$$t = 1, r = 0, x = y = 4096, z = 128$$

$$t = 2, r = 0, x = y = 2^{19}, z = 2^{11}$$

$$t = 0, r = 1, p_1 = 3, u_1 = 1, x = y = 69984, z = 648$$

$$t = 1, r = 1, p_1 = 5, u_1 = 2, x = y = 25000000000000, z = 50000000$$

There is no solution where x is different from y .

-10- Case $n = 9; x^4 + y^4 = z^9$

The case $n = 9$ can be reduced to the cubic case by setting $Z = z^3$ (any solution for $n = 9$ yields a solution for $n = 3$).

The latter defines an elliptic curve of rank 0 , implying that only trivial non-proportionnal solutions exist. Although no non-trivial non-proportional integer solutions are known, it is possible to obtain non-trivial proportional solutions. There are only two "small" solutions less than 10^3 :

$$x = y = 4, z = 2 \text{ and } x = 289, y = 578, z = 17;$$

corresponding solutions for $n = 3$: (4, 4, 8) and (289, 578, 4 913).

Note that the second solution is such that $x = 2 * y$.

We can also obtain a solution such as $y = 4x/3$

$$x = 340707, y = 454276, z = 337$$

Trivial rational solutions can be expressed

$$x = 0, y = t^9, z = t^4 \text{ ou } x = t^9, y = 0, z = t^4 \text{ for any } t \in \mathbf{Q}.$$

As mentioned above, all non-trivial integer solutions $x = y$ are of the form

$$\begin{aligned} x = y &= 2^{2+9t} \prod_{i=1}^r p_i^{9u_i} \\ z &= 2^{1+4t} \prod_{i=1}^r p_i^{4u_i} \end{aligned}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

Here (since $n = 3^2$) there are solutions where x is different from y .

-11- Case $n = 11; x^4 + y^4 = z^{11}$

In this hyperbolic case since 11 is prime, there is no reduction to a lower possible case (unlike in the case of $n = 9$).

All integer solutions where $x = y$ are of the form

$$\begin{aligned} x = y &= 2^{8+11t} \prod_{i=1}^r p_i^{11u_i} \\ z &= 2^{3+4t} \prod_{i=1}^r p_i^{4u_i} \end{aligned}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

The small solution with $m = 0$ is (256, 256, 8).

There is no solution where x is different from y .

-12- Case $n = 13; x^4 + y^4 = z^{13}$

With the prime 13 as the exponent, we see the same behaviour here as in the case where $n = 11$.

All integer solutions where $x = y$ are of the form

$$\begin{aligned} x = y &= 2^{3+13t} \prod_{i=1}^r p_i^{13u_i} \\ z &= 2^{1+4t} \prod_{i=1}^r p_i^{4u_i} \end{aligned}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

The small solution with $m = 0$ is $(8, 8, 2)$.

There is no solution where x is different from y .

-13- Case $n = 15; x^4 + y^4 = z^{15}$

This case is not unusual, even though $15 = 3 \times 5$: no reduction is possible.

All integer solutions where $x = y$ are of the form

$$\begin{aligned} x = y &= 2^{11+15t} \prod_{i=1}^r p_i^{15u_i} \\ z &= 2^{3+4t} \prod_{i=1}^r p_i^{4u_i} \end{aligned}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

The small solution with $m = 0$ is $(2048, 2048, 8)$.

There is no solution where x is different from y .

-14- General case: $2x^4 = z^{2p+1}$

In contrast to the preceding paragraphs, we will use more symmetric notation for x and z here (k will become a and m will become b).

For any positive p , you can always find solutions such as $x = 2^\alpha, z = 2^\beta$; they must check $4\alpha + 1 = 2\beta p + \beta$.

Since, for any positive p , there are always an infinite number of solutions (α, β) , by calling (a, b) the smallest ones, we can denote them as

$$\alpha = a + (2p + 1)t, \beta = b + 4t, \text{ for any } t \geq 0.$$

-Property 2

For any $p > 0$, all integer solutions of $2x^4 = z^{2p+1}$ are of the form

$$\begin{aligned} x = y &= 2^{a+(2p+1)t} \prod_{i=1}^r p_i^{(2p+1)u_i} \\ z &= 2^{b+4t} \prod_{i=1}^r p_i^{4u_i} \end{aligned}$$

t, r, u_i integers ≥ 0 , p_i odd primes.

For any $n = 2p + 1$, we can easily find the pair (a, b) and thus the general form of the solutions (for example, for $n = 17$ we obtain $a = 4$ and $b = 1$, for $n = 19$, $a = 14$ and $b = 3, \dots$).

-15- General case: $x^p + y^p = z^n$

Let us consider the general problem of the type
 $x^p + y^p = z^n$, $\gcd(x, y) = 1$, $xy \neq 0$, n and p positive integers > 2 .
 Let's consider the characteristic

$$q = 1/p + 1/p + 1/n = 2/p + 1/n;$$

the fundamental classification of pairs (p, n) will lead to
 $q > 1$, elliptic cases, of which there are relatively few, such as $(2, 2)$ or $(2, 3)$, with many possible solutions;
 $q = 1$, parabolic cases, such as $(3, 3)$, which behave in a tricky way;
 $q < 1$, hyperbolic cases, which are by far the most common and usually have a finite number of primitive solutions ([7], [8]).

This exceptional case corresponds to the prime 5 (the first pentagonal number greater than 1) with its many and varied symbolic interpretations, such as the number of Aphrodite, the number of life, the number of material existence or the number of the five senses (see "The Symbolism of Numbers" by R. Berteaux, 2016).

We could have considered certain mixed equations of the form $x^p + y^r = z^n$, where p and r are different, in particular, the case of three exponents greater than 2 and the famous Beal conjecture ([11]) (if there are positive integer solutions, then x, y , and z have a common prime factor). As a reminder, the next Beal Prize will be awarded in 2028 ...

-16- Application in cryptography

The structure of the solutions to our quartic Diophantine equations for the symmetric case $x = y$ with odd exponents n greater than 1 exhibits remarkable arithmetic properties that can be exploited in asymmetric cryptography.

This will lead us to the design of a one-way function.

We can use the previous results to create functions that are easy to compute in one direction but difficult to reverse. This is the technology behind zero-knowledge proofs, which are booming with the rise of cryptocurrency blockchains. The idea is to prove that we know the solution to a complex equation (one of our equations) without ever revealing the solution itself, but by indicating that it possesses a certain arithmetic property (see Paillier's asymmetric encryption or the Diffie-Hellman symmetric protocol involving Alice and Bob).

Using the canonical projection

$$\pi : \mathbf{Z} \longrightarrow \mathbf{Z}/p\mathbf{Z},$$

where p is a prime number (which will be chosen to be very large, on the order of 2048 bits, i.e., with more than 600 digits), we transpose our equations $2x^4 = z^n$ from \mathbf{Z} into the finite field $\mathbf{Z}/p\mathbf{Z}$; thus we will define a transformation function f such that

$$f(x) \equiv 2x^4(\text{mod } p).$$

Any exact solution to the equation in \mathbf{Z} automatically translates into a modular solution in $\mathbf{Z}/p\mathbf{Z}$, although the reverse is not true, of course, which provides cryptographic security.

To ensure the robustness and injectivity of the system, the following conditions must hold:

- n odd > 1 , to obtain the solutions $x = A^n 2^{k(n)}$ explained above;
- p such that $\gcd(n, p-1) = 1$, to ensure that for every image $C = f(x)$, there exists a unique z satisfying the relation

$$z^n \equiv C(\text{mod } p),$$

that is, n is invertible modulo $p - 1$.

The notation C is inspired by the classic RSA asymmetric encryption (algorithm defined in 1977).

Given $p - 1$, we can compute the inverse of n modulo $p - 1$, denoted by $d \equiv 1/n(\text{mod } p - 1)$, and thus obtain, using Fermat's Little Theorem, z from C (see proof (+))

$$z \equiv C^d(\text{mod } p).$$

Note that $z \in (0, 1, \dots, p - 1)$.

The security of this function relies on the asymmetry of the computation: while evaluating $f(x)$ is simple and fast using the binary exponentiation algorithm (for our odd n , we will write $x^n = x * x^{n-1}$ to speed up the calculation), its inversion requires the very difficult and tedious calculation (which is an understatement for very large p) of modular quartic roots to obtain x or modular n th roots to obtain z .

To ensure the uniqueness of the result, we prefer to find z .

Public data: x , a very large prime number p and C .

Problem: Find z such that $2x^4 \equiv z^n(\text{mod } p)$.

We consider $C \equiv 2x^4(\text{mod } p)$ to be the encrypted message (from the secret x), d to be the private key, and z to be the result (or proof value).

For a solution (x, z) , the chosen value of p must be (at least) strictly greater than z to ensure the injectivity of the modular process.

Finding z without knowing d would correspond to the difficult problem of n th roots or discrete logarithms.

The holder of the secret x can generate a proof z (such that $z^n \equiv 2x^4 \pmod{p}$). Using the key d , this z can be computed in polynomial time and is protected by the difficulty of n th root extraction for someone who does not know the factorization of $p-1$.

Note that in our approach, where starting from $C = 2x^4$ we aim to ensure that $C \equiv z^n \pmod{p}$, C can be unlocked in two ways: either via the fourth root or via the n th root.

We thus have a two-input system, where x can be considered the key of user A, z the key of user B, and C the shared secret (meeting point).

- Example 1:

$n = 3$ with the solution ($x = 4, z = 8$) and $p = 107$,

$C = 2x^4 = 512$, so $C \equiv 84 \pmod{107}$,

$\gcd(n, p-1) = \gcd(3, 106) = 1$; we obtain $d \equiv 1/3 \pmod{106} \equiv 71$,

$z = 84^{71} \equiv 8 \pmod{107}$.

We will give n, p, C ; find z modulo 107.

- Example 2:

$n = 5$ with the solution ($x = 33614, z = 4802$) and $p = 20147$,

$C = 2x^4 = 2553352521523584032$, so $C \equiv 14257 \pmod{20147}$,

$\gcd(n, p-1) = \gcd(5, 20146) = 1$; we obtain $d \equiv 1/5 \pmod{20146} \equiv 16117$,

$z = 14257^{16117} \equiv 4802 \pmod{20147}$.

We will give n, p, C ; find z modulo 20147.

With numbers of 600 digits or more, these calculations are currently impossible.

Let's take an example with larger numbers and perform the coding and calculations using Pari/Gp, a free software package specialized in number theory.

- Example 3

$n = 5, x = 6400000, z = 320000, p = 100000000019, \gcd(5, 100000000018) = 1$.

As mentioned above, we must perform the following calculations ($\text{Mod}(C, p)$ is a function from Pari/Gp that uses a fast exponentiation algorithm; note that here this function will perform only about sixty multiplications instead of 60 billion, because at each step of the calculation the result is reduced modulo p , hence the extreme speed):

$$C = \text{Mod}(2^*x^4, p); d = \text{Mod}(1/5, p-1); \text{Mod}(C, p)^d = \text{Mod}(z, p).$$

We obtain, respectively:

$\text{Mod}(2^*6400000^4, 100000000019) = \text{Mod}(92121131517, 100000000019)$,

$\text{Mod}(1/5, 100000000018) = \text{Mod}(60000000011, 100000000018)$,

$\text{Mod}(92121131517, 100000000019)^{60000000011} = \text{Mod}(320000, 100000000019)$.

For the secret number x , with the public identifier $C = 92121131517$, the prime $p = 100000000019$, and the encryption key $d = 60000000011$, the result obtained

is indeed $z = 320000$ modulo p .

Using the same solution, we can perform these calculations with the prime having 77 digits:

$p = 28948022309329048855892746252171976963317496166410141009864396001978$

282410063 (such as $\gcd(5, p - 1) = 1$);

we will obtain, respectively (and almost instantly)

$C = 335544320000000000000000000000$,

$d = 11579208923731619542357098500868790785326998466564056403945758400791312964025$,

the resulting z is indeed 320000 modulo p .

-REMARK: On the need to exclude primes congruent to 1 modulo 4.

It should be noted that we have chosen all the previous values of p to be equal to 3(mod4), which ensures that p is not the sum of two squares and that there are no roots of -1 modulo p ; the polynomial $2x^4$ thus becomes completely irreducible in \mathbf{Z}/\mathbf{pZ} (no extraneous factorisation or complex roots in the modulus), unlike the case where p is congruent to 1 modulo 4, where we know (Euler-Fermat's twosquares theorem) that p is the unique sum of two squares. We would then have, on the one hand, four valid solutions ($x, -x, ix, -ix$) associated with the same C and leading to the same z ; on the other hand, we could write, modulo p , $2x^4 = (x^2 + ix^2)(x^2 - ix^2)$, this reducibility weakening the protection of our 'secret'. Therefore, to avoid these problems, we shall exclude primes of the form $4k + 1$.

-Modular computation scheme

Given n and selecting an initial p (sufficiently large, congruent to 3 modulo 4 and such as $\gcd(n, p - 1) = 1$), the process begins with the secret number x , which is converted into a public identifier C ; then, using the encryption key d , the resulting z is derived.

Let's summarize the three elements of the proposed implementation.

- The theoretical structure of solutions of the form $x = A^n 2^{k(n)}$,
- The encryption function $f(x) \equiv 2x^4 \pmod{p}$,
- The encryption mechanism, derived from Fermat's Little Theorem, $z \equiv C^d \pmod{p}$.

Problem: Given n, p and C (public data), find the unique value of z modulo p .

We will have, successively,

$(x, p) \rightarrow C \equiv 2x^4 \pmod{p}$,

$(n, p) \rightarrow d \equiv 1/n \pmod{p - 1}$,

$(C, d) \rightarrow z \equiv C^d \pmod{p}$.

For an observer who knows only n, p , and C , finding z without knowing the factorization of $p - 1$ would be practically impossible (how would one calculate

d?), whereas the designer, who chose and constructed p "on demand" and knows the factorization of $p - 1$, can easily obtain d and thus z .

We could have found x given z , but extracting the fourth modular root

$$x \equiv (z^n/2)^{1/4} \pmod{p}$$

is more delicate and would not allow for uniqueness as mentioned above. We could also define a symmetric Diffie-Hellman-type protocol for our equations:

- Alice chooses a secret x , calculates $C \equiv 2x^4 \pmod{p}$, and sends it to Bob.
- Bob chooses a secret z , calculates $C' \equiv z^n \pmod{p}$ and sends it to Alice.

If Alice and Bob manage to agree on a configuration where $C = C'$, without revealing their secrets (x and z , respectively), they will have created a secure communication channel of the shared secret type.

- CONCLUSION

For any odd number n greater than 1, there always exist, at least for $x = y$, an infinite number of nontrivial solutions in \mathbf{Z} ; for even numbers n , there are no non-trivial solutions.

These solutions, that we have explained, which are most often proportional to powers of 2, are indeed infinite in number, but they are not primitive solutions since $\gcd(x, y, z) > 1$, which is consistent with Beal's conjecture ([11]).

The exceptional and most interesting case, $n = 5$, also has solutions where x and y are not proportional; this is the only known case with an infinite number of non-proportional solutions.

For the case $x = y$ with odd exponents n greater than 1, we have shown that all non-trivial solutions are necessarily of the general form $x = y = A^n 2^{k(n)}$, $z = A^4 2^{m(n)}$, where we have specified the various elements.

By transposing these equations into the finite field \mathbf{Z}/\mathbf{pZ} , where p is a prime number (to be chosen large, congruent to 3 modulo 4 and such that $\gcd(n, p - 1) = 1$), we propose an application to asymmetric cryptography by constructing a one-way function and describe the modular computation scheme that allows us, given n, p and $C \equiv 2x^4 \pmod{p}$, the encrypted message from the secret x , to obtain the unique solution z modulo p .

(+) Proof of $z \equiv C^d \pmod{p}$.

Recall that Fermat's Little Theorem states that if p is a prime number and z is an integer that is not a multiple of p , then

$$z^{p-1} \equiv 1 \pmod{p}.$$

Since $\gcd(n, p - 1) = 1$, there exists an integer d (the inverse of n) such that

$$nd = 1 + k(p - 1), \text{ where } k \text{ is any integer,}$$

which can also be written as

$$nd \equiv 1 \pmod{p-1}, \text{ or } d \equiv 1/n \pmod{p-1}.$$

We can raise $z^n \equiv C \pmod{p}$ to the power of d

$$(z^n)^d \equiv C^d \pmod{p},$$

hence

$$z^{1+k(p-1)} = z(z^{p-1})^k \equiv C^d \pmod{p},$$

and by Fermat's Little Theorem, we indeed have

$$z \equiv C^d \pmod{p}.$$

(*)Honorary professor Paul Sabatier University, Toulouse, France, Webmaster of the site [SAYRAC](#) , Email: renelouis.clerc@free.fr.

- REFERENCES

- [1] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Cam. Phil. Soc., vol. 21, p. 179-192, 1922.
- [2] K. Gyory, Über die diophantische Gleichung $x^p + y^p = cz^p$, Publ. Math. Debrecen, 13, 301-306, 1966.
- [3] K. Gyory, On the diophantine equation, Mat. Lapok, 18, 93-96, 1967.
- [4] G. Kümmer, OEuvres complètes, Tome 1, éditées par A. Weil, Springer Verlag, 1975.
- [5] B. J. Powell, Sur l'équation diophantienne $x^4 + -y^4 = z^p$, Bull. Sc. Math., 107, 219-223, 1983.
- [6] B. J. Powell, Proof of the Impossibility of the Fermat Equation $X^p + Y^p = Z^p$ for Special Values of p and of the More General Equation $bX^n + cY^n = cE^n$, J. Number Theory 18, pp. 34-40, 1984.
- [7] H. Darmon, The equation $x^4 - y^4 = cz^p$, C.R. Math. Rep. Acad. Sci. Canada. XV, No. 6, 286-290, 1993.
- [8] H. Darmon, A. Granville, Sur les équations $zm = f(x, y)$ et $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. , 27 , pp. 513-543, 1995.
- [9] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. Math., Princeton University, vol. 141, p. 443-551 (DOI 10.2307/2118559), 1995.
- [10] H. Darmon, L. Merel, Winding quotients and some variants of Fermat's Last Theorem, Journal für die reine angew. Math. 490, 1997.
- [11] R. Daniel Mauldin. A Generalization of Fermat's Last Theorem: The Beal Conjecture et Prize Problem. Notice of AMS, Vol 44, n 11, pp 1436-1437, 1997.
- [12] K. Gyory, A. Petho and V. T. Sos, Number Theory, Diophantine, Computational and Algebraic Aspects, Walter de Gruyter, Berlin-New York, 1998.
- [13] D. Hilbert, The theory of algebraic number fields, Springer-Verlag, 1998.

- [14] F. Beukers, The Diophantine equations $x^p + y^p = z^q$, Duke Mathematical Journal, Vol. 91, No. 1, 1998.
- [15] N. Bruin, On powers as sums of two cubes, in Algorithmic Number Theory, ANTS-IV, Springer, 2000.
- [16] B. G. Sloss, A Note on a Diophantine Equation Considered by Powell, The Fibonacci quarterly, vol. 40 (3), pp. 255-258, 2002.
- [17] L. V. Dieulefait, Modular congruences, Q-curves, and the Diophantine equation $x^4 + y^4 = z^p$, Bull. Belg. Math. Soc. Simon Stevin, 12(3), pp. 363-369, 2005.
- [18] Diana Savin, About the diophantine equation $x^4 - y^4 = pz^r$, arXiv:0907.0777[math.NT.], 2009.