

OWARDS THE PROOF OF TWIN PRIMES CONJECTURE: A MODULAR CHARACTERIZATION

Ibrahima GUEYE¹, Cheikh Ahmadou Bamba DIENG²,
Papa Ousmane NIASS²

¹ Mathématicien amateur résident à Ouakam - Dakar – Sénégal

² Mathématicien amateur élève de l'Ecole Polytechnique de Thiès – Sénégal

Keywords Twin primes conjecture; Fermat's little theorem; Bachet-Bézout Theorem

Abstract

In this paper we reduce the twin prime conjecture to a simple Euclidean division problem using the Fermat's little theorem and Bachet-Bezout theorem.

Introduction

Twin primes are two primes that differ by only 2. The twin prime conjecture states that there are infinitely many twin primes, the numerical observations and heuristic reasoning justifies the conjecture, but no demonstration has yet been made [4].

Some properties

Any pair of twin primes (with the exception of the couple (3, 5)) is of the form $(6m - 1, 6m + 1)$ for an integer m . Indeed, any set of three consecutive natural numbers has at least a multiple of 2 (possibly two) and one multiple of 3, the integer that lies between the two twin primes is both the multiple of 2 and this multiple of 3, because it cannot be one of the primes.

It can be shown that for any integer m greater than 2, the pair $\{m(m - 1), m(m + 1)\}$ is a pair of twin primes if only if: $4[(m - 1)! + 1] + m \equiv 0 \pmod{m(m + 1)}$. This characterization factorial and modular OF twin primes was discovered by P. A. Clement in 1949 [2].

While the series of reciprocals of primes diverges, the series of reciprocals of twin primes converges (to a constant number called Brown, whose decimal expansion begins 1.90216 ...). This property was demonstrated by Viggo Brun in 1919 [3].

Record

January 15, 2007, two distributed computing projects, Twin Prime Search and PrimeGrid, discovered the largest pair of twin primes currently known (that is to say in January 2007). The discoverer was Eric Vautier the French [1].

Twin primes conjecture

The twin prime conjecture states that there are infinitely many twin primes. Although most researchers in number theory believe that this conjecture is true, it has never been demonstrated. They are based on numerical observations and heuristic reasoning using probabilistic distribution of prime numbers. In 1849, Alphonse de Polignac issued a more general conjecture: De Polignac's conjecture that the case $n = 2$ is the twin prime conjecture. There is also a stronger version of this conjecture: the Hardy-Littlewood conjecture, which provides a probability distribution of twin primes and inspired by the prime number theorem.

The twin prime conjecture is a special case of the conjecture of Schinzel.

Partial results

In 1940, Paul Erdős proved the existence of a constant $c < 1$ and infinitely many primes p such that: $p' - p < c \ln(p)$ where p' is the number immediately following the first page

This result was improved several times, in 1986, Helmut Maier showed a constant $c < 0.25$ could be reached.

In 2003, Daniel Goldston and Cem Yildirim have shown that for any $c > 0$, there are infinitely many primes p such that $p' - p < c \ln(p)$. In 1966, Chen Jingrun demonstrated the existence of infinitely many primes p such that $p + 2$ is the product of at most two prime factors (so many, the product of at most two prime factors, is said to be 2 -almost-first). His approach was that of the theory of the screen, he used to treat similarly the twin prime conjecture and Goldbach's conjecture.

Conjecture 1 Twin primes conjecture [4]

Given (p, q) a pair of integers such that p and q are both prime numbers p lower than q . We say that (p, q) form a pair of twin primes if $q = p + 2$.

Theorem 1 Fermat's little theorem

Given two integers a and d not all zero, if f is the GCD of a and d then there exist two integers x and y such that $ax + dy = f$

If a and d are coprime, a particular solution can be found by multiplying c by a particular solution of the equation $ax + by = 1$. A particular solution (x_1, y_1) knowned, all the solutions are $(x_1 + dk, y_1 - k)$ where k is an integer [6].

Theorem 3: DIENG-NIASS-GUEYE's theorem

Given two integers $p = 6m - 1$ and $q = 6m + 1$ such that m nonzero integer. $\{p, q\}$ is a pair of twin primes if we can find b (non-zero integer), c (non-zero integer) and h (integer) such that:

$$b = 3((h + 1)q + 1)/8 ; c = 3((h + 1)p + 1)/2 \text{ and } m = (4b + c - 3)/6(4b - c)$$

Proof:

p and q are twin primes, $p = 6m - 1$ and $q = 6m + 1$ with m nonzero integer.

With Fermat's little theorem:

$$e^p \equiv e [p]$$

With the corollary of the Fermat's little theorem:

$$e^{p-1} \equiv 1 [p]$$

If $e = 2$ we have:

$$0 = 64^m - 24bm + 4b - 4$$

b is a nonzero integer

Doing the same with q we will have:

$$0 = 64^m - 6cm - c - 1$$

c is a nonzero integer

After calculations: $m = (4b + c - 3)/6(4b - c)$

$$(4b + c) - 6m(4b - c) = 3$$

Examples:

For $m=1$; $b = 3$; $c = 9$; $p = 5$ and $q = 7$

For $m=2$; $b = 93$; $c = 315$; $p = 11$ and $q = 13$

Now use the Bachet-Bézout theorem

Given a ; d ; x and y nonzero integers so that :

$$ax + dy = 3$$

Given $a = 1$; $d = 6m$; $x = (4b + c)$ et $y = -(4b - c)$

1 and $6m$ are coprime

$$(4b + c) - 6m(4b - c) = 3 \tag{1}$$

According to a particular case of Bachet-Bézout theorem, all the solutions are of the form: $(x' + dk ; y' - ak)$; k is an integer multiple of 3 [6].

$$(4b + c) = (18m + 3) + 6mk \text{ and } -(4b - c) = -3 - k$$

$$(4b + c) = 18m + 6mk + 3 \text{ and } (4b - c) = k + 3$$

This system of equations in b and c , have for a general solution the pair $\{b, c\}$ with: $b = (18m + 6mk + k + 3)/8$ and $c = (18m + 6mk - k)/2$

$$p = (6m - 1) \text{ and } q = (6m + 1)$$

Then : $b = ((k + 3)q + 3)/8$ and $c = ((k + 3)p + 3)/2$

Examples For $m = 1$; $k = 0$; $b = 3$ and $c = 9$

For $m = 2$; $k = 54$; $b = 93$ and $c = 315$

k is multiple of 3; $k = 3h$ (with h an integer)

$$b = 3((h + 1)q + 1)/8 \text{ and } c = 3((h + 1)p + 1)/2$$

Hence a simple modular characterization of twin primes.

Thus we transform the problem of twin primes conjecture into a simple exercise of Euclidean division.

Now back to the equality: $m = (4b + c - 3)/6(4b - c)$ (1)

$$m = (4b + c - 3)/6(4b - c)$$

Given: $4b + c = r$; $4b - c = s$

So : $b = (r + s)/8$ et $c = (r - s)/2$

$$m = (r - 3)/6s$$

$$r = 3 \text{ modulo } 6s$$

$$r = -s \text{ modulo } 4$$

$$r = s \text{ modulo } 2$$

A is all m such that $m = (r - 3)/6s$, $r = -s \text{ modulo } 8$ and $r = s \text{ modulo } 2$.

A is not empty because, for $m = 1$, $r = 21$ and $s = 3$

Suppose that A is bounded by $M = \max(A)$

Given R and S such that: $M = (R - 3)/6S$ and $R = -S \text{ modulo } 8$ and $R = S \text{ modulo } 2$

Given $M' = M + 132$; therefore $M' = (R' - 3)/6S'$ with $R' = R + 792S$ and $S' = S$

$$R' + S' = R + S + 792S = R + S + 8*99S$$

$$R' - S' = R - S + 792S = R - S + 2*396S$$

M' is element of A and M' less than M . This is absurd. Hence A is unbounded.

Cardinal of A is infinite. Hence the existence of infinitely many m .

Hence the infinitude of twin primes.

References

- [1]- Twin Prime Search, Communiqué officiel de la découverte du 15 janvier 2007
- [2]- P.A. Clement, Congruences for sets of primes, American Mathematical Monthly n° 56 (1949), pp. 23-25
- [3]- Viggo Brun, La série $1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/29 + 1/31 + 1/41 + 1/43 + 1/59 + 1/61 + \dots$ où les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie, Bulletin des Sciences Mathématiques n°43 (1919), pp. 100-104 et 124-128
- [4]- http://fr.wikipedia.org/wiki/Nombres_premiers_jumeaux
- [5]- http://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_de_Bachet-B%C3%A9zout
- [6]- http://fr.wikipedia.org/wiki/%C3%89quation_diophantienne_ax%2Bby_%3D_c