ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

MARINA MUREDDU

A lower bound for $P(x^4 + 1)$

Annales de la faculté des sciences de Toulouse 5^e série, tome 8, n° 2 (1986-1987), p. 109-119

<http://www.numdam.org/item?id=AFST_1986-1987_5_8_2_109_0>

Annales Faculté des Sciences de Toulouse Vol.VIII, n°2, 1986-1987

A lower bound for $P(x^4+1)$

MARINA MUREDDU [1]

RÉSUMÉ. — On démontre que, pour tout $x > 3$, le plus grand facteur de x^4+1 est plus grand que 113. On donne aussi un algorithme pour déterminer toutes les solutions $x, \alpha_1, \alpha_2, ..., \alpha_n$ de l'équation $x^2+1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$, où $p_1, p_2, ..., p_n$ sont des nombres premiers donnés.

ABSTRACT. — In this paper it is shown that the greatest prime factor of the integer of the form x^4+1 is greater than 113 for $x > 3$. Moreover, the author describes an algorithm leading to all solution $x, \alpha_1, \alpha_2, ..., \alpha_n$ of equation $x^2+1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$, where the p_i are given primes.

Introduction

The search for prime factors of polynomials such as $x^n + 1$ has a long history beginning with Gauss and Legendre, cf. Dickson's "History of Theory of Numbers".

In this paper we are concerned with the problem of finding a lower bound for the greatest prime factor of integers of the form $x^4 + 1$. In the sequel, we shall denote this factor by $P(x^4+1)$.

Specifically, we shall prove in detail that $P(x^4+1) > 73$ for every integer $x > 3$. By following the same pattern and using a personal computer, however, it is possible to improve on this result.

Actually we know that $P(x^4+1) > 113$ for every $x > 3$ and $P(x^4+1) = 137$ for $x = 10$.

It is to be observed that, as shown in section 3, theorem in section 2 enable us to solve completely equations of the form $x^2+1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$ (where the p_i are given primes), in a way different from those followed by

[1] Dipartimento di Matematica, Università di Cagliari, Via Ospedale,72 - 09100 Cagliari Italia

mathematicians such as STØRMER [8], WEGER [7], MIGNOTTE [4] and others, who studied problems of this kind.

§ I. Preliminary

We shall begin by reducing our problem to that of solving a number of Pell's equations.

Legendre proved that every prime divisor of x^4+1 is either 2 or of the form $8h+1$. Hence

$$x^4+1 = 2^{\alpha}17^{\beta}41^{\gamma}73^{\delta}... \tag{1.1}$$

Suppose now $P(x^4+1) < 73$. In such a case, (1.1) becomes :

$$x^4+1 = 2^{\alpha}17^{\beta}41^{\gamma} \tag{1.2}$$

that is,

$$z^2+1 = 2^{\alpha}17^{\beta}41^{\gamma} \quad , \quad z = x^2. \tag{1.3}$$

Since 4 does not divide z^2+1, we rewrite (1.3) in the forme

$$z^2 - 2^{a}17^{b}41^{c}y^2 = -1 \tag{1.4}$$

where $a,b,c \in \{0,1\}$ and $y = 17^m41^n$, $m,n \in \mathbf{N}$.

Therefore, we have to study the following Pell equations :

$$\begin{aligned}
&z^2 - y^2 = -1\\
&z^2 - (2\times 17\times 41)y^2 = -1\\
&z^2 - (2\times 17)y^2 = -1\\
&z^2 - (17\times 41)y^2 = -1\\
&z^2 - 41y^2 = -1\\
&z^2 - 2y^2 = -1\\
&z^2 - (2\times 41)y^2 = -1\\
&z^2 - 17y^2 = -1
\end{aligned} \tag{1.5}$$

where $y = 17^m41^n$, $m,n \in \mathbf{N}$.

Without going into detail about Pell's equations, it is nevertheless usefull to state the following :

THEOREM A.— *If (x,y) is a positive solution of Pell's equation*

$$x^2 - dy^2 = -1, \tag{A}$$

then x/y is a convergent $p_n/q_n = [a_o, a_1, ..., a_n]$ of the periodic expansion of $\sqrt{d}$ as a continued fraction :

$$\sqrt{d} = [a_o, \overline{a_1, ..., a_{r-1}, 2a_o}].$$

Equation (A) has no solution if period r of that expansion is even; otherwise, if r is odd, all positive solutions of (A) are given by :

$$x_n = p_{nr-1} \qquad \text{and} \qquad y_n = q_{nr-1}$$

or, equivalently, by $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, where n is an odd positive integer and (x_1, y_1) is the smallest positive solution of (A).

We refer to [6] for the proof.

§ 2.

In this section we shall present a few theorems in order to study Pell's equation by use of linearly recursive sequences (for short l.r.s.). For a survey of this subject see [2].

THEOREM 1.— *Let $u = (u_n)_{n\in\mathbb{N}}$ be the second order l.r.s.*

$$u_o = 0 \quad , \quad u_1 = 1 \quad , \quad u_{n+2} = au_{n+1} + bu_n \tag{2.1}$$

(where a, b, c are integers) and let Δ be the discriminant $a^2 + 4b$ of its characteristic polynomial. For any given prime p, numbers u_n have the following properties :

i) if $p|\Delta$ then $(p|n \iff p|u_n)$

ii) if $\left(\frac{\Delta}{p}\right) = 1$ then $\big((p-1)|n \Rightarrow p|u_n\big)$

iii) if $\left(\frac{\Delta}{p}\right) = -1$ then $\big((p+1)|n \Rightarrow p|u_n\big)$.

Proof.— Consider the l.r.s. (2.1) modulo p

$$v_o = 0 \quad , \quad v_1 = 1 \quad , \quad v_{n+2} \equiv av_{n+1} + bv_n \pmod{p} \tag{2.2}$$

and let $f(x)$ be the characteristic polynomial of (2.2) :

$$f(x) = x^2 - ax - b. \tag{2.3}$$

L denotes the extension of $\mathbf{F}_p$, which contains the roots ρ_1, ρ_2 of $f(x)$. In particular, in cases i) and ii) we have $L = \mathbf{F}_p$ and in case iii) $L = \mathbf{F}_{p^2}$. It is known that any term of a second order l.r.s. is given by :

$$v_n = (A + Bn)\rho^n \quad \text{if } \Delta \equiv 0 \ (mod.p) \quad \text{and hence } \rho_1 = \rho_2 \qquad (2.4)$$

$$v_n = A\rho_1^n + B\rho_2^n \quad \text{if } \Delta \not\equiv 0 \ (mod.p) \quad \text{and hence } \rho_1 \neq \rho_2 \qquad (2.5)$$

where constants $A, B \in L$ depend on the values of v_o and v_1. In this case, since $v_o = 0$ and $v_1 = 1$ a straightforward calculation gives :

$$v_n = n\ \rho_1^{n-1} \qquad (2.4)'$$

$$v_n = \frac{\rho_1^n - \rho_2^n}{\rho_1 - \rho_2} \qquad (2.5)'$$

Case i) of the theorem is a direct consequence of (2.4)'.

In the hypothesis of case iii), we have $L = \mathbf{F}_p$, and then $\rho_i \in \mathbf{F}_p$. Because of Fermat's Theorem we have $\rho_1^{p-1} \equiv \rho_2^{p-1} \equiv 1$ (mod. p) and the statement follows from (2.5.)'.

Suppose now $\left(\frac{\Delta}{p}\right) = -1$, then $L = \mathbf{F}_{p^2}$. Let σ be the Froebenius automorphism :

$$\rho : \mathbf{F}_{p^2} \longrightarrow \mathbf{F}_{p^2}$$
$$x \longmapsto x^p$$

an easy computation shows that

$$0 = \sigma(f(\rho_i)) = f(\sigma(\rho_i)) = 0.$$

Since $\sigma(\rho_i)$ is not ρ_i (for, if it was, σ would be the identity), then

$$\rho_1^p = \rho_2 \quad \text{and} \quad \rho_2^p = \rho_1;$$

and from this and (2.5.)' :

$$v_{(p+1)k} = \frac{(\rho_1^{p+1})^k - (\rho_2^{p+1})^k}{\rho_1 - \rho_2} \equiv \frac{(\rho_1\rho_2)^k - (\rho_1\rho_2)^k}{\rho_1 - \rho_2} \equiv 0 \ (mod.p)$$

We note that in cases ii) and iii) the terms $u_{k(p-1)}$ and $u_{k(p+1)}$, respectively, are not necessarily the only ones divisible by p. In particular $u_{(p-1)}$ (resp. $u_{(p+1)}$) is not always the first one.

The following theorem will state something more about divisibility of the terms in the second order l.r.s. which have characteristic polynomial $f(x) = x^2 - ax - 1,\ a \in \mathbf{Z}$.

THEOREM 2.— *Let* $(u_n)_{n\in\mathbf{N}}$ *be the second order l.r.s. :*

$$u_o = 0 \quad , \quad u_1 = 1 \quad , \quad u_{n+2} = au_{n+1} + u_n \tag{2.6}$$

then,

i) $n|m \iff u_n|u_m$

ii) $(u_n, u_m) = u_{(n,m)}$

where the symbol (n,m) *denotes the greatest common divisor of* m *and* n.

Proof.— We shall begin by proving

i') $n|m \Longrightarrow u_n|u_m$.

It is known that the sub-sequence

$$u_o = 0 \quad , \quad u_n \quad , \quad u_{2n} \quad , \ \dots \ , \quad u_{kn} \quad , \ \dots \tag{2.7}$$

is a l.r.s. It follows that all the terms (2.7) are divisible by $(u_o, u_n) = u_n$.

ii) One can easily prove, by induction on k, that the relation

$$u_{m+k} = u_{m-1}u_k + u_m u_{k+1} \tag{2.8}$$

holds for the l.r.s. (2.6). We shall use (2.8) to prove

$$(u_n, u_m) = (u_{n-m}, u_m) \qquad (n > m) \tag{2.9}$$

which is equivalent to ii) :

$$(u_n, u_m) = (u_{m+(n-m)}, u_m) = (u_{m-1}u_{n-m} + u_m u_{n-m+1}, u_m)$$
$$= (u_{m-1}u_{n-m}, u_m)$$

but $(u_{m-1}, u_m) = 1$ so

$$(u_{m-1}u_{n-m}, u_m) = (u_{n-m}, u_m).$$

We have now to prove the converse of i'). Suppose $u_n|u_m$ then after ii) :

$$u_n = (u_n, u_m) = u_{(n,m)}$$

It is easy to prove that $k \mapsto u_k$ is one to one. So, $n = (n, m)$ and $n|m$.

COROLLARY .— *Let k be the smallest positive integer such that $u_k \equiv 0$ (mod.p). If $u_\ell \equiv 0$ (mod.p) then $k|\ell$.*

THEOREM 3.— *Let (x_1, y_1) be the fundamental solution of*

$$x^2 + 1 = dy^2. \tag{2.10}$$

If $(U, V) \in \mathbf{N} \times \mathbf{N}$ is a different solution of (2.10), then the following statements hold :

i) $y_1|V$

ii) there exists a prime q such that $q|V$ and $q \times dy$.

Proof.— Because of Theorem A, the general solution (U, V) is given by

$$U_n + V_n\sqrt{d} = (x_1 + y_1\sqrt{d})^{2n+1} = \rho_1^{2n+1} \tag{2.11}$$

or, equivalently by

$$U_n - V_n\sqrt{d} = (x_1 - y_1\sqrt{d})^{2n+1} = \rho_2^{2n+1}. \tag{2.11}'$$

Hence

$$2V_n\sqrt{d} = \rho_1^{2n+1} - \rho_2^{2n+1}$$

and so

$$V_n = \frac{1}{2\sqrt{d}}\left(\rho_1^{2n+1} - \rho_2^{2n+1}\right). \tag{2.12}$$

Consider the second order l.r.s (y_n), associated with the characteristic polynomial $g(z) = z^2 - 2x_1z - 1 = (z - \rho_1)(z - \rho_2)$, whose first terms are $y_o = 0$ and y_1. (2.12) ensures that values V_n are exactly the terms in odd places of this l.r.s. :

$$V_n = y_{2n+1}$$

This proves part i) of the Theorem; in fact all the terms of (y_n) are divisible by $(y_o, y_1) = y_1 = V_o$.

ii) Since $y_1 < V$, we can put $V = y_1V'$, with $V' > 1$. If $(y_1d, V') = 1$ the Theorem is proved. Otherwise let $p > 3$ be a divisor of (y_1d, V') (without loss of generality we suppose $p > 3$, in fact 2^2 and 3 do not divide $x^2 + 1$). We shall prove that there exists a prime q which divides V but not y_1d.

For that, consider the new l.r.s. $y'_n = y_n/y_1$:

$$y'_o = 0 \quad , \quad y'_1 \quad , \quad y'_{n+2} = 2xy'_{n+1} + y'_n \tag{2.13}$$

whose scale is still $g(z)$. Obviously, $V' = y'_m$ for a suitable odd m, moreower p divides both y'_m and $y_1 d$.

Since the discriminant of $g(z)$ is $\Delta = 4y^2 d$, applying Theorem 1.i) to the l.r.s. (y'_n) we obtain $m \equiv 0 \pmod{p}$ and so -because of Theorem 2.i- $y'_p | y'_m$. It is therefore sufficient to prove that there exists a prime q such that $q | y'_p$ but $q \times y_1 d$.

From (2.11) we obtain

$$y'_p = px^{p-1} + d^{[\frac{p}{2}]} y_1^{p-1} + py_1^2 dA = pB, \tag{2.14}$$

where A and $B > 1$ are suitable integers. Notice that $p \times B$: in fact $p|B$ implies $p|x^{p-1}$ and hence $x \equiv 0 \pmod{p}$, a contradiction. Let q be any prime factor of B, then $q \neq p$ cannot divide $\Delta = 4y_1^2 d$: by Theorem 1.i) q would divide p, a contradiction. This completes the proof.

§ 3

In this section we shall present an algorithm to solve completely the equation

$$x^2 + 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \tag{3.1}$$

where p_i are given different primes (the unknows are $x, \alpha_1, \alpha_2, \dots, \alpha_n$).

We have to find all solutions (x, y), with

$$y = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} \tag{3.2}$$

of each equation

$$x^2 - dy^2 = -1 \qquad \left(d = p_1^{\varsigma_1} p_2^{\varsigma_2} \dots p_n^{\varsigma_n},\ \varsigma_i \in \{0,1\}\right). \tag{3.3}$$

Theorems in section 2 imply that we can effectively find all the solutions of equation (3.3) which satisfy the condition (3.2). In fact, let us consider one of the equations (3.3) and let us put :

$P := \{p_1, p_2, \dots, p_n\}$,

$E_o := \{p_i \mid p_i \mid d\}$,

$Y := \{y \mid (y = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n})$ and (there exists x such that (x, y) is a solution of (3.3))$\}$.

Let (3.3) be solvable and let (x_1, y_1) be its fundamental solution. If y_1 is not of the form (3.2) then -because of Theorem 3.i)- there is no solution of that form : $Y = \emptyset$.

Suppose this false, and let us consider the subset of P, say E_1, which contains all the prime factors of y_1 :

$$E_1 := \{p_i \mid p_i \,|y_1\} \subset P,$$

and let us put

$$E_2 := P \setminus (E_o \cup E_1).$$

If $E_2 = \emptyset$, then -because of Theorem 3- $Y = \{y_1\}$. If not, let $p_s \in E_2$. Bearing in mind that all solutions of (3.3) are the terms with odd indices of the l.r.s.

$$y_o = 0 \quad , \quad y_1 \quad , \quad y_{n+2} = 2x_1 y_{n+1} + y_n, \tag{3.4}$$

we can find the smallest solution, say y_s, divisible by p_s. If $y_s \notin Y$, then no solution divisible by p_s belongs to Y, since -by Corollary- it is a multiple of y_s. Otherwise, if $y_s \in Y$, we consider, together with (3.2) :

$$x^2 - Dy^2 = -1 \qquad (D = dy_s/y_1) \tag{3.5}$$

(whose fundamental solution is $(\overline{x}, \overline{y} = y_1)$),

$$E_{o,s} := \{p_i \mid p_i \mid D\}$$
$$E_{2,s} := P \setminus (E_{o,s} \cup E_1)$$

and argue as under (3.3) above.

It is plain that such an iteration terminates.

Remark. — It is useful, in the search for the smallest solution divisible by p_s, to consider the l.r.s. (3.4) modulo p. In fact, generally, -by Theorem 2.i)- actually it is not necessary to find y_s, but only its index in the l.r.s. Moreover, it is to be noted that the l.r.s. associated to (3.5) is the sequence

$$z_o = 0 \ , \ z_1 = y_s/y'_s = y_1 \ , \ z_k = y_{ks}/y'_s \quad (\text{where } y'_s = y_s/y_1).$$

An easy computation shows that the bound for the number of odd solutions of (3.1) is

$$\sum_{h=1}^{n} \binom{n}{h} 2^{n-h} + 1 = 3^n - 2^n.$$

§ 4

We are now in a position to study equations (1.5).

$$x^2 = y^2 = -1$$

has only the trivial solution $(x,y) = (0,1)$.

* * *

$$z^2 - (2 \times 17 \times 41)y^2 = -1 \quad \text{and} \quad z^2 - (2 \times 17)y^2 = -1$$

have no solutions. In fact, the period of expansion in continued fraction of both $\sqrt{1394}$ and $\sqrt{34}$ is even (see Theorem A).

* * *

The fundamental solutions of

$$z^2 - (17 \times 41)y^2 = -1 \quad \text{and} \quad z^2 - 41y^2 = -1$$

are $(z_1, y_1) = (132,5)$ and $(z_1, y_1) = (32,5)$ respectively. Hence, after Theorem 3.i) all solutions are multiples of 5 and not of the form $y = 17^m 41^n$.

* * *

The fundamental solution of

$$z^2 - 2y^2 = -1 \tag{4.1}$$

is $(z_1, y_1) = (1,1)$. Therefore, all solutions y are the terms in odd places of the l.r.s. :

$$y_o = 0 \quad , \quad y_1 = 1 \quad , \quad y_{n+2} = 2y_{n+1} + y_n.$$

After Theorem 1 and Corollary, we obtain :

a) all terms divisible by 17 are with even index and so are not solutions of (4.1);

b) for the terms divisible by 41, since $\left(\frac{\Delta}{41}\right) = 1$ and we are interested in terms with odd index, it is sufficient to examine y_5. A little calculation shows that $y_5 = 29$.

Hence, the only solution of (4.1) satisfying the condition $y = 17^m 41^n$ is $(z_1, y_1) = (1, 1)$.

* * *

The fundamental solution of

$$z^2 - (2 \times 41)y^2 = -1 \tag{4.2}$$

is $(z_1, y_1) = (9, 1)$, so, the solutions y are the terms in odd places of the l.r.s. :

$$y_o = 0 \quad , \quad y_1 = 1 \quad , \quad y_{n+2} = 18y_{n+1} + y_n .$$

After Theorem 3, $\Delta = 82$ ensures that no solution of (4.2) can be of the form 41^n.

On the other hand, $\left(\frac{\Delta}{17}\right) = \left(\frac{82}{17}\right) = -1$; let i be such that $17 | y_i$. In such a case a suitable divisor of $18 = p + 1$ divides i (see Theorem 3.iii and Corollary). Arguing as in (4.2), it is enough to observe that $17 \times y_3 = 325$ to be sure that the only solution is the fundamental one $(z_1, y_1) = (9, 1)$.

* * *

The fundamental solution of

$$z^2 - 17y^2 = -1 \tag{4.3}$$

is $(z_1, y_1) = (4, 1)$. The values y_n are now the terms in odd places of the l.r.s. :

$$y_o = 0 \quad , \quad y_1 = 1 \quad , \quad y_{n+2} = 8y_{n+1} + y_n .$$

As in (4.2), apply Theorem 1 and Corollary. We need only consider y_3 and y_7. Since $y_3 = 65 = 13 \times 5$ and $y_7 = 28009$ (prime), the only solution is $(z_1, y_1) = (4, 1)$.

* * *

In conclusion, we get $z \in \{0, 1, 4, 9\}$ so that $P(x^4 + 1) < 73$ only for $x \in \{0, 1, 2, 3\}$ and the proof is accomplished.

Références

[1] BOREVITCH (S.I.) and SCHAFAREVITCH (I.R.). — *Théorie des Nombres.* — Paris, Gauthier-Villars, 1967.

[2] CERLIENCO (L.), MIGNOTTE (M.) and PIRAS (F.). — *Suites Récurrentes Linéaires.* Strasbourg, Publication de l'I.R.M.A., 1984.

[3] HARDY (G.H.) and WRIGHT (B.M.). — *An Introduction of the Theory of Numbers.* Oxford, Claredon Press, 1979.

[4] MIGNOTTE (M.). — $P(x^2 + 1) \geq 17$ *si* $x \geq 240$. — C.R. Acad. Sc. t.301, series I, n°13, 1985.

[5] LUCAS (E.). — *Théorie des Nombres.* — Paris, Gauthier-Villars, 1891.

[6] NIVEN (I.) and ZUCKERMAN (H.S.). — *An Introduction to the Theory of Numbers.* New York, John Wiley & Sons, 1960.

[7] PETHÖ (A.) and DE WEGER (B.M.M.). — *Products of prime Powers in Binary Recurrences Sequences*, Mathematical Institute University of Leiden. The Netherlands, Report n.24, September 1985; Report n.29, November 1985.

[8] STØRMER (C.). — *Quelques Théorèmes sur l'équation de Pell* $x^2 - Dy^2 = \pm 1$ *et leurs applications,*. — Vid.-Selsk. Skrifter. Math. Naturv. K1, 1897.

(Manuscrit reçu le 15 septembre 1986)