PRIMITIVE DIVISORS OF LUCAS SEQUENCES AND PRIME FACTORS OF x^2+1 AND x^4+1

Florian Luca (Michoacán, México)

Abstract. In this paper, we show that $24208144^2+1=29^3\cdot 37^2\cdot 53\cdot 61^2\cdot 89$ is the largest instance in which n^2+1 does not have any prime factor >100.

1. Introduction

For any integer n let $P(n)$ be the largest prime factor of n with the convention that $P(0)=P(\pm 1)=1$. In [8], it is shown that if x is an integer, then $P(x^2+1)\geq 17$ once $|x|\geq 240$. The method presented in [8] is elementary, and the computations were done using congruences with respect to small moduli.

The purpose of this note is two fold. First of all, we improve the lower bound from [8] by showing that $P(x^2+1)\geq 101$ once $|x|\geq 24208145$. Secondly, our method is entirely different from the one presented in [8] in the sense that it uses the existence of primitive prime divisors for the Lucas sequences associated to certain Pell equations. This method has been used previously by Lehmer in [6] to compute all the positive integer solutions x of the inequality $P(x(x+1))\leq 41$. The method is completely general and, in practice, armed with a good computer, one can employ it to find all the integer solutions x of the inequality $P(x^2+1)<K$, where K is any given reasonable constant. We also use the same method to show that $P(x^4+1)\geq 233$ for $x\geq 11$, which extends the range of computations described in [7] and [9] where it was shown that $P(x^4+1)\geq 73$ if $x\geq 3$. We recall that explicit lower bounds for $P(x^3+1)$ appear in [1].

This note is organized as follows. In the second section, we present our algorithm and computational findings. In the third section, we make an analysis of the running time of our algorithm for computing all positive integer solutions x of the inequality $P(x^2+1)<K$ in terms of K.

2. Computational Results

Theorem 2.1.

(i) The largest positive integer solution x of the inequality

$$P(x^2+1)<101 \tag{1}$$

is $x = 24208144$.

(ii) The largest positive integer solution x of the inequality

$$P(x^4+1) < 233 \tag{2}$$

is $x = 10$.

Proof. We start with the first question. Assume that x is a positive integer such that $P(x^2+1) < 101$. The only prime numbers p that can divide a number of the form x^2+1 are either $p = 2$, or $p \equiv 1 \pmod 4$. There are only 12 such primes p less than 101 and they are

$$p \in \mathcal{P} = \{2,\ 5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97\}.$$

In particular, the number x has the property that

$$x^2+1 = dy^2, \tag{3}$$

where $d > 1$ and $y \geq 1$ are integers whose factors belong to $\mathcal{P}$, and d is squarefree. If we rewrite equation (3) as

$$x^2 - dy^2 = -1, \tag{4}$$

it follows that the pair $(x,\ y)$ is a positive integer solution of a Pell equation of the form (4) for some squarefree $d > 1$ whose prime factors are in the set $\mathcal{P}$. Let $\mathcal{A}$ be the set of all the squarefree positive integers $d > 1$ whose prime factors are in the set $\mathcal{P}$. Clearly, $\mathcal{A}$ contains precisely $2^{|\mathcal{P}|} - 1 = 2^{12} - 1 = 4095$ elements. For each $d \in \mathcal{A}$ let $(X_1(d), Y_1(d))$ be the first positive integer solution of the Pell equation

$$X^2 - dY^2 = \pm 1. \tag{5}$$

It is wellknown that if we denote by m_d the length of the continued fraction of $\sqrt{d}$, then $(X_1(d),\ Y_1(d)) = (P_{m_d-1},\ Q_{m_d-1})$, where for a nonnegative integer k we have denoted by P_k/Q_k the kth convergent to $\sqrt{d}$. Moreover, if m_d is even, then equation (5) has no integer solution $(X,\ Y)$ with the sign -1 appearing on the right hand side. Of the totality of 4095 elements d of $\mathcal{A}$, only 2672 of them have the property that the period m_d is odd. Let us denote by $\mathcal{B}$ the subset of $\mathcal{A}$ consisting of only these elements. We used Mathematica to compute $(X_1(d),\ Y_1(d))$ for all $d \in \mathcal{B}$. These computations took about 7 hours.

Assume now that $(x,\ y)$ is a solution of equation (4) for some $d \in \mathcal{B}$. It then follows that $(x,\ y) = (X_n(d),\ Y_n(d))$ for some odd value of $n \geq 1$, where $X_n(d)$ and $Y_n(d)$ can be computed using the formulae

$$X_n(d) = \frac{(\alpha(d))^n + (\beta(d))^n}{2} \qquad \text{and} \qquad Y_n(d) = \frac{(\alpha(d))^n - (\beta(d))^n}{2\sqrt{d}}$$

for all $n \geq 1$, where

$$\alpha(d) = X_1(d) + \sqrt{d}Y_1(d), \qquad \beta(d) = X_1(d) - \sqrt{d}Y_1(d).$$

It is wellknown that $Y_1(d) \mid Y_n(d)$ for all $n \geq 1$. Thus, since in equation (4) the number y has $P(y) < 101$, it follows that $P(Y_1(d)) < 101$ must hold. Of the totality of 2672 pairs $(X_1(d),\ Y_1(d))$ with $d \in \mathcal{B}$, only 143 of them satisfy this condition. Testing this took a few minutes with Mathematica. Of course, we did not factor the numbers $Y_1(d)$ because some of them are quite large. Instead, we computed, for each given d, the largest divisor M_d of $Y_1(d)$ having $P(M_d) < 101$, and we tested if $Y_1(d)$ is equal to M_d.

Let now $\mathcal{C}$ be the set consisting of these 143 elements $d \in \mathcal{B}$ for which $P(Y_1(d)) < 101$, and assume that $y = Y_n(d)$ for some odd $n \geq 1$ and some $d \in \mathcal{C}$. Since

$$Y_n(d)Y_1(d) = \frac{\alpha(d)^n - \beta(d)^n}{\alpha(d) - \beta(d)}, \qquad \text{for all } n \geq 1,$$

it follows that the sequence $\left\{\frac{Y_n(d)}{Y_1(d)}\right\}_{n\geq 1}$ is a *Lucas sequence* of the first kind with roots $\alpha(d)$ and $\beta(d)$. Since $\alpha(d)$ and $\beta(d)$ are real, it follows, by a result of Carmichael (see [2]), that the nth term of this sequence has a *primitive divisor* for all $n > 12$. We recall that a primitive divisor of the nth term of a Lucas sequence is a prime divisor p of it which, among other properties, it also fulfills the condition that $p \equiv \pm 1 \pmod{n}$. In particular, if $n > 12$ is odd, then there exists a prime number $p \mid Y_n(d)$ such that $p \geq 2n - 1$. Since we are searching for values of n and d such that $P(Y_n(d)) \leq 97$, it follows that n is an odd number such that $2n - 1 \leq 97$, hence, $n \leq 49$. Thus, we used Mathematica to compute, for every one of the 143 values of $d \in \mathcal{C}$, the numbers $Y_n(d)$ for all odd values of $n \leq 49$, resulting in a totality of $143 \cdot 25 = 3575$ such numbers. For each one of these numbers, we applied the procedure described above to eliminate the ones for which $P(Y_n(d)) > 97$. The computation took a few minutes, and a totality of 156 numbers $Y_n(d)$ survived (that is, only 13 new numbers $Y_n(d)$ for $n > 1$ odd and $d \in \mathcal{C}$ were found). For each of these numbers we computed $x = X_n(d)$. The conclusion of these computations is that there are precisely 156 positive integer values of x for which $P(x^2 + 1) < 101$. Of these 156 positive integers, 140 of them are less than 10^5, 10 more of them are between 10^5 and 10^6, and the largest 6 of them are 1984933, 2343692, 3449051, 6225244, 22709274, and 24208144. Thus, the largest positive integer solution x of the inequality $P(x^2 + 1) < 101$ is

$$24208144^2 + 1 = 29^3 \cdot 37^2 \cdot 53 \cdot 61^2 \cdot 89.$$

We now turn our attention to $P(x^4 + 1)$. Suppose that x is a positive integer such that $P(x^4 + 1) < 233$. If p is a prime number dividing $x^4 + 1$, then either $p = 2$, or

p is congruent to 1 modulo 8. There are only 9 such primes which are smaller than 233, namely

$$\mathcal{P}_1 = \{2,\ 17,\ 41,\ 73,\ 89,\ 97,\ 113,\ 137,\ 193\}.$$

So, with $z = x^2$, we need to find all the solutions of the equation

$$z^2 - dy^2 = -1, \tag{6}$$

where $d > 1$ and $y \geq 1$ are integers whose factors belong to $\mathcal{P}_1$, and d is squarefree. There are precisely $2^{|\mathcal{P}_1|} - 1 = 2^9 - 1 = 511$ possible values for d. We used Mathematica to find, for every such d, the smallest solution $(X_1(d),\ Y_1(d))$ of the Pell equation (5). Only 255 values of d have the property that equation (5) has a solution with the sign -1 in the right hand side. Out of these values of d, only 13 have the property that all prime factors of $Y_1(d)$ are in $\mathcal{P}_1$. Now suppose that $(z,\ y) = (X_n(d),\ Y_n(d))$ is a solution of equation (6) for some odd value of n and one of these 13 values of d. Since $P(Y_n(d)) \leq 197$, it follows, by the primitive divisor theorem, that $2n - 1 \leq 197$, i.e. $n \leq 99$. Thus, we have computed all the $50 \cdot 13 = 650$ values of $Y_n(d)$ (i.e., for each one of the 13 values of d, and for each odd n with $n \leq 99$), and we tested each one of these numbers to see if their prime factors are in $\mathcal{P}_1$. No new number was found, so $n = 1$. Thus, $z = X_1(d)$ for one of the 13 values of d. Since $z = x^2$, we tested if $X_1(d)$ is a perfect square. Five values of x were found, namely $x = 1,\ 2,\ 3,\ 9,\ 10$. So, the largest solution of the inequality $P(x^4 + 1) < 233$ is

$$10^4 + 1 = 73 \cdot 137,$$

and $P(x^4 + 1) \geq 233$ holds for all integers $x \geq 11$.

We conclude this section by remarking that we could have done the final testing for $P(x^4 + 1) < 233$ by combining the primitive divisor technique with a result of J. H. E. Cohn from [3]. Namely, in [3], the following result is proved: Assume that $d > 1$ is a squarefree number. Then the equation $X^4 - dY^2 = -1$ can have at most one solution in positive integers $(X,\ Y)$. Moreover, let $(X_1(d),\ Y_1(d))$ denote the smallest positive solution of $X^2 - dY^2 = -1$, and write $X_1(d) = AB^2$, where A is squarefree. Then the only possible value of the odd integer k for which $X_k(d)$ can be a square is $k = A$.

3. The running time of the algorithm

Given $K > 1$, an algorithm to compute all positive integer solutions x of the inequality $P(x^2+1) \leq K$ was presented in section 1, together with its findings when $K = 100$. Let $f(X) \in \mathbf{Z}[X]$ be a polynomial having at least two distinct roots. In his PhD thesis, Haristoy (see [4]) improved upon earlier estimates of Shorey and Tijdeman (see chapter 7 of [10]) and showed that the inequality $P(f(x)) \gg \log_2 x \log_3 x / \log_4 x$ holds if x is a sufficiently large positive integer. Here and in what follows, for a positive real number y we use $\log y$ for the maximum between the natural logarithm of y and 1, and for a positive integer k we use $\log_k y$ for the kth fold iterate of the function $\log y$. From this result, if follows that if $P(x^2+1) < K$, then $x < \exp\left(\exp\left(O(K \log_2 K / \log K)\right)\right)$, so if one wants to find all the positive integer solutions x of the inequality $P(x^2+1) < K$ by simply factoring x^2+1 for all positive integers x up to the above upper bound, then the running time of such a naive algorithm will be almost doubly exponential in K. In this section, we present the following result.

Theorem 3.1. *The algorithm presented in section 2 finds all positive integer solutions x of the inequality $P(x^2+1) \leq K$ after at most* $\exp(O(K))$ *elementary bit operations.*

Proof. Here, we keep the notations from section 2. First, to generate $\mathcal{A}$, one first generates the $2^{\pi(K;4,1)+1} = \exp(O(K))$ squarefree numbers d all whose prime factors are 2 or congruent to $1 \pmod 4$ and having $P(d) \leq K$. Secondly, to find $\mathcal{B}$, for each one of the numbers $d \in \mathcal{A}$ one computes the minimal solution $(X_1(d),\ Y_1(d))$ of the Pell equation $X^2 - dY^2 = \pm 1$. Then $\mathcal{B}$ is the subset of those $d \in \mathcal{A}$ such that $(X_1(d),\ Y_1(d))$ is a solution of the equation $X^2 - dY^2 = -1$. The continued fraction algorithm for quadratic irrationalities shows that this is computable in $O(d^{1/2}) = \exp(O(K))$ steps and since $d < 4^K$, it follows that at each step only numbers of the form $\exp(O(K))$ are being handled. Now with each one of these numbers $Y_1(d)$, we test if $P(d) < K$. This step requires $\exp(O(K))$ elementary operations. Indeed, let $p \leq K$ be a fixed prime and assume that $p^\alpha || Y_1(d)$. Then $\alpha I\!\!L \log Y_1(d) = \exp(O(K))$. Moreover, since $a \pmod b$ requires $O\left(\log^2(a+b)\right)$ elementary bit operations (using naive arithmetic, and even less using Fast Fourier Transform), it follows that this part of the computation requires $\exp(O(K))$ elementary bit operations. Thus, the subset $\mathcal{C}$ of $\mathcal{B}$ consisting of those $d \in \mathcal{B}$ such that $P(d) \leq K$ can be generated after at most $\exp(O(K))$ elementary bit operations. Finally, one now generates $Y_k(d)$ for $k \leq K$ and tests again if $P(Y_k(d)) \leq K$. As previously, this requires again at most $\exp(O(K))$ elementary bit operations after which the set consisting of all the positive integers x such that $x^2+1 = dY_k(d)^2$ has the largest prime factor $\leq K$ is obtained.

Acknowledgments. The computations were carried out on the machines at the Tata Institute for Fundamental Research in Mumbai, India, on June 25 and June 26, 2001. I would like to thank the Tata Institute for its hospitality, Professors Yann Bugeaud, Maurice Mignotte, Igor Shparlinski and Tarlok Shorey for useful advice, and the Third World Academy of Sciences for financial support.

References

[1] Buchmann, J., Győry, K., Mignotte, M., Tzanakis, N., Lower bounds for $P(x \supset 3 + k)$, an elementary approach, *Publ. Math. Debrecen* **38** (1991), no. 1–2, 145–163.

[2] Carmichael, R. D., On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913), 30–70.

[3] Cohn, J. H. E., The Diophantine equation $x^4 + 1 = Dy^2$, *Math. Comp.* **66** no. 219 (1997), 1347–1351.

[4] Haristoy, J., Equations diophantiennes exponentielles, *Prépublications de IRMA* **029**, 2003.

[5] Hua, L.-K., On the least solution to Pell equation, *Bull. Amer. Math. Soc.* **48** (1942), 731–735; *Selected papers*, Springer, New York, 1983, 119–123.

[6] Lehmer, D. H., On a problem of Störmer, *Illinois J. Math.* **8** (1964), 57–79.

[7] Mabkhout, M., Minoration de $P(x^4+1)$, *Rend. Sem. Fac. Sci. Univ. Cagliari* **63** no. 2 (1993), 135–148.

[8] Mignotte, M., $P(x^2+1) \geq 17$ si $x \geq 240$, *C.R. Acad. Sci. Paris Sér. I Math.* **301** no. 13 (1985), 661–664.

[9] Mureddu, M., A lower bound for $P(x^4+1)$, *Ann. Fac. Sci. Toulouse Math.* (5) **8** no. 2 (1986/1987), 109–119.

[10] Shorey, T. N., Tijdeman, R., *Exponential diophantine equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press, Cambridge, 1986.

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán,
México
E-mail: fluca@matmor.unam.mx