SMOOTH VALUES OF SOME QUADRATIC POLYNOMIALS

Filip Najman

University of Zagreb, Croatia

Abstract. In this paper, using a method of Luca and the author, we find all values x such that the quadratic forms $x^2 + 1$, $x^2 + 4$, $x^2 + 2$ and $x^2 - 2$ are 200-smooth and all values x such that the quadratic form $x^2 - 4$ is 100-smooth.

1. Introduction

For any integer n we let $P(n)$ be the largest prime factor of n with the convention $P(0) = P(\pm 1) = 1$. We say that a integer s is m-smooth if $P(s) < m$. In 1964, Lehmer ([8]) found all positive integer solutions x to the inequality $P(x(x + 1)) \leq 41$. Notice that this amounts to finding all odd positive integers $y = 2x + 1$ such that $P(y^2 - 1) \leq 41$. There are 869 such solutions. In [9], Luca found all positive integer solutions of the similar looking inequality $P(x^2 + 1) < 100$. There are 156 of them. In [6], Guzmán Sánchez found the largest solutions of $P(x^2 + 2) < 100$ and $P(x^2 - 2) < 100$. Recently, Luca and the author, in [10] extended Lehmer's results, finding all the solutions to $P(x^2 - 1) < 100$. There are 16167 solutions of this inequality.

In this paper, we find all the positive integer x that are a solution to the inequalities

$$(1.1) \qquad\qquad P(x^2 + 1) < 200,$$

extending Luca's results,

$$(1.2) \qquad\qquad P(x^2 + 4) < 200,$$

$$(1.3) \qquad\qquad P(x^2 - 4) < 100,$$

$$(1.4) \qquad\qquad P(x^2 + 2) < 200,$$

and

(1.5)
$$P(x^2 - 2) < 200.$$

By solving (1.4) and (1.5) we will extend the results of Guzmán Sánchez (see [6]).

When considering the inequality (1.3), we have to consider all the primes in the factorization of $x^2 - 4$ (except 2, as we will later see), while when considering (1.1) and (1.2) we can disregard the primes congruent to 3 modulo 4 and when considering (1.4) and (1.5) we need only consider the prime 2 and the primes congruent to 1 or 3 modulo 8 for (1.4) and the primes congruent to 1 or 7 modulo 8 for (1.5). This is the reason we can only find 100-smooth values of $x^2 - 4$, compared to 200-smooth values of all the other quadratic forms.

In [8], [9] and [10] the following approach was taken. Assume that x is a positive integer such that $P(x^2 \pm 1) \leq K$ for the appropriate K. Then we can write

(1.6)
$$x^2 \pm 1 = dy^2,$$

where d is squarefree, and $P(dy) \leq K$. This implies that only a small number n of primes participates in the factorization of d. For example, $n = 13$ for $P(x^2 - 1) \leq 41$ (as in [8]), $n = 12$ for $P(x^2 + 1) < 100$ (as in [9]) and $n = 25$ for $P(x^2 - 1) < 100$ (as in [10]). In all the cases, we can write equation (1.6) in the form
$$x^2 - dy^2 = \mp 1.$$

Thus, our possible values for x appear as the first coordinate of one of the solutions of at most $2^n - 1$ Pell equations. For a given Pell equation, the sequence $(y_n/y_1)_{n \geq 1}$ forms a Lucas sequence with real roots. The *Primitive Divisor Theorem* for Lucas sequences with real roots (see, for example, [4], or the more general result from [1] which applies to all Lucas sequences) says that if $n > 6$, then y_n has a prime factor which is at least as large as $n - 1$. In the mentioned papers it suffices to check the first 42, 98 and 98 values respectively of the component x of the Pell equations involved and among these one finds all possible solutions of the equations considered.

It is easy to see that in these calculations the number of equations becomes huge. An even bigger problem are the coefficients of the Pell equations, as the size of the solutions grows exponentially in respect to d. This means that just *writing down* the solution takes exponential time. This is why in [10] *compact representations* of the solutions to the Pell equations were used. A compact representation of an algebraic number $\beta \in \mathbb{Q}(\sqrt{d})$ is a representation of β of the form

(1.7)
$$\beta = \prod_{j=1}^{k} \left(\frac{\alpha_j}{d_j} \right)^{2^{k-j}},$$

where $d_j \in \mathbb{Z}$, $\alpha_j = (a_j + b_j\sqrt{d})/2 \in \mathbb{Q}(\sqrt{d})$, $a_j, b_j \in \mathbb{Z}$, $j = 1, \ldots, k$, and k, α and d_j have $O(\log d)$ digits. A detailed description of compact representations and their use can be found in [7]. Using compact representation cuts down the space needed from exponential to polynomial in respect to d and the time needed to compute the regulator of the appropriate real quadratic field from exponential to subexponential. Without the use of compact representations, the results of [10] would be hopelessly unattainable. For comparison, in [8] 8191 equations were considered, the largest of them having $d = 304250263527210$ and the largest solution having less than 8600 digits, while in [10] 33554431 equations were considered, the largest of them having $d = 230556796394551842475310214733175070$, and many of the solutions having billions of digits.

In this paper, we will use the same strategy to improve on the results of [9] concerning the inequality (1.1), using compact representations where standard representations were previously used. In examining the inequalities (1.2) and (1.3) we will consider fundamental units η_d of the quadratic fields $\mathbb{Q}(\sqrt{d})$ satisfying the condition that the cube of η_d is the fundamental solution of the Pell equation $x^2 - dy^2 = -1$ for the case (1.2) and $x^2 - dy^2 = 1$ for the case (1.3). When considering the inequalities (1.4) and (1.5), we will use the fact that if ν is the smallest solution of the equation $x^2 - dy^2 = \pm 2$, then $\nu^2/2 = \eta_d$. This means that all the solutions of $x^2 - dy^2 = \pm 2$ are of the form $\nu^{2n+1}/2^n$. One can show that the solutions form a *Lehmer sequence* with real roots, and by a result of Ward (see [14], and [1] for a more general result), we again have control over the prime factors of the members of the sequence. Again, it is necessary to use compact representations when representing the solutions of all these equations.

Note that $k = \pm 1, \pm 2, \pm 4$ are the only values of k such that the integer solutions x to the inequality $P(x^2 + k) < M$, for some bound M, can be determined in this manner. This is because only for these cases do the solutions of the corresponding equations form either a Lucas or Lehmer sequence. Buchmann, Győry, Mignotte and Tzanakis found all solutions of $P(x^3 + 1) < 31$, which leads to $P(x^2 + 3) < 31$ in [3]. They did this by a case by case study and considered each of the Pellian equations (there are 16 of them) separately.

2. THE INEQUALITY $P(x^2 + 1) < 200$

Let x be a integer such that $x^2 + 1$ is 200-smooth. By a classical result of Fermat, a number can be represented as a sum of to squares only if it has no prime divisors congruent to 3 modulo 4. This means that $x^2 + 1$ can be divisible only by 2 and the 21 primes congruent to 1 modulo 4 up to 200. We can now write $x^2 + 1 = dy^2$, i.e., $x^2 - dy^2 = -1$, where

$$d = 2^{a_1} \cdot 5^{a_2} \cdots 197^{a_{22}}, \ a_i \in \{0, 1\} \text{ for } i = 1, \ldots 22.$$

This is a negative Pell equation, so $(x, y) = (X_n, Y_n)$, where $X_n + Y_n\sqrt{d} = (X_1 + Y_1\sqrt{d})^{2n+1}$, for some positive integer n and $X_1 + Y_1\sqrt{d}$ being the fundamental solution of the negative Pell equation. We have $2^{22} - 1 = 4194303$ equations that we need to consider. The largest d appearing is $d = 9402582969259446086628952212335664431210$. Note that this d is more than 400 times larger than any d appearing in [10].

One can easily check that Y_1 divides Y_n. We define $u_n = \frac{Y_n}{Y_1}$. The sequence (u_n) is a Lucas sequence of the first kind with real roots η and ζ. By a result of Carmichael (see [4]), the Primitive Divisor Theorem, this implies that for every $n > 12$, u_n has a *primitive divisor* p, a prime satisfying, among other properties, $p \equiv \pm 1 \pmod{n}$. This implies that for $n > 200$, there exists a prime $p \geq 200$ dividing u_n. Thus, only the first 200 values of (Y_n) can possibly be 200-smooth. This means that we only need to consider the first 200 solutions of each negative Pell equation.

We will follow the methods of [10] very closely, so we will give only an outline of the algorithm (for a detailed explanation of each step see [10]). The algorithm that finds all the solutions goes through all the possible values d and for each, does the following: First it computes the regulator of the quadratic field $\mathbb{Q}(\sqrt{d})$ using Buchmann's subexponential algorithm (see [2]). The results of this algorithm are dependent on the Generalized Riemann hypothesis. Next, using the computed regulator, we construct a compact representation of the fundamental solution $X_1 + Y_1\sqrt{d}$ of the negative Pell equation $x^2 - dy^2 = -1$, using the methods from [11]. Now, using the algorithm for modular arithmetic described in [12], we check whether Y_1 is 200-smooth. If it is, then we check which of the Y_n, $2 \leq n \leq 200$ is 200-smooth. Each 200-smooth value of Y_n gives us a solution X_n of our problem. If Y_1 is not 200-smooth, then no Y_n will be. There is one last check that needs to be done: compute all the convergents $\frac{p_n}{q_n}$ of the continued fraction expansion of $\sqrt{d}$ such that $q_n < z$, where z is the 200-smooth part of Y_1, and check whether there exists a convergent $\frac{p_n}{q_n}$ such that $p_n^2 - q_n^2 = -1$. This test removes the dependence of our results on the Generalized Riemann hypothesis. In all tested cases it failed, as if a convergent $\frac{p_n}{q_n}$ satisfying the test were to be found, it would imply that the Generalized Riemann hypothesis is false.

We obtain the following results:

THEOREM 2.1.   a) *The largest three solutions of the equation $P(x^2 + 1) < 200$ are $x = 69971515635443, 120563046313$ and 104279454193.*

  b) *The largest solution of $P(x^4 + 1) < 200$ is $x = 10$.*

  c) *The largest solution of $P(x^6 + 1) < 200$ is $x = 8$.*

  d) *The largest n such that $P(x^{2n} + 1) < 200$ has a solution is $n = 9$, the solution being $x = 2$.*

  e) *The inequality $P(x^2 + 1) < 200$ has 811 solutions.*

f) *The greatest power n of the fundamental solution of the negative Pell equation $(X_1 + Y_1\sqrt{d})^n$ which leads to a solution of our problem is $n = 9$ for $d = 5$. The case $d = 5$ also gives us most solutions, namely 4 of them.*

PROOF. Part b) is proved by finding the largest square of all the x, c) by finding the largest a cube, etc.   □

3. THE INEQUALITY $P(x^2 + 4) < 200$

Obviously, $P(x^2+1) < 200$ iff $P((2x)^2+4) < 200$. Thus, we have already obtained all the even solutions to the inequality (1.2). It remains to find the odd solutions. Let $\eta_d = \frac{u+v\sqrt{d}}{2}$ be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$ and $x_1 + y_1\sqrt{d}$ the fundamental solution of the Pell equation $x^2 - dy^2 = 1$. Then $x_1 + y_1\sqrt{d} = \eta_d^n$, where $n = 1, 2, 3$ or 6, and the exact value can be found by examining u and v modulo 8, from the Table 1. It is

d	v	u	n
$d \equiv 1 \pmod 4$	$v \equiv 0 \pmod 4$	$-$	1
	$v \equiv 2 \pmod 4$	$-$	2
$d \equiv 5 \pmod{16}$	$v \equiv 1 \pmod 2$	$u \equiv \pm 3v \pmod 8$	3
		$u \equiv \pm v \pmod 8$	6
$d \equiv 13 \pmod{16}$	$v \equiv 1 \pmod 2$	$u \equiv \pm v \pmod 8$	3
		$u \equiv \pm 3v \pmod 8$	6
$d \equiv 2 \pmod 4$	$v \equiv 0 \pmod 2$	$-$	1
	$v \equiv 1 \pmod 2$	$-$	2
$d \equiv 3 \pmod 4$	$-$	$-$	1

TABLE 1.

easy to see that $x^2 - dy^2 = -4$ will have a solution iff $n = 6$ in Table 1, and then the solutions will be of the form

$$X_m + Y_m\sqrt{d} = 2\eta_d^k,$$

where $k \equiv \pm 1 \pmod 6$. Also, one can see that $n = 6$ only if $d \equiv 5 \pmod 8$. This also means that we do not have to consider 2 in the factorization of d, leaving only the 21 primes congruent to 1 modulo 4.

Using the same algorithm from Section 2, with the appropriate minor changes, we obtain the following results.

THEOREM 3.1.   a) *The largest three odd solutions of the equation $P(x^2+4) < 200$ are $x = 191686681859, 112899039159$ and 28608252345.*
b) *The largest odd solution of $P(x^4 + 4) < 200$ is $x = 923$.*
c) *There are no odd solutions to $P(x^{2n} + 4) < 200$ for $n \geq 3$.*

d) *The inequality $P(x^2 + 4) < 200$ has 344 odd solutions.*

f) *The greatest power n of the smallest solution of our problem $(X_1 + Y_1\sqrt{d})^n$ which leads to a solution is $n = 19$ for $d = 5$. The case $d = 5$ also gives the most solutions, namely 5 of them.*

4. The inequality $P(x^2 - 4) < 100$

Obviously, $P(x^2 - 1) < 100$ iff $P((2x)^2 - 4) < 100$. Thus, we have already obtained in [10] all the even solutions to the inequality (1.2). It remains to find the odd solutions. Again, let $\eta_d = \frac{u + v\sqrt{d}}{2}$ be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$ and $x_1 + y_1\sqrt{d}$ the fundamental solution of the Pell equation $x^2 - dy^2 = 1$, and $x_1 + y_1\sqrt{d} = \eta_d^n$, where n can be found in Table 1. It is easy to see that $x^2 - dy^2 = 4$ will have a solution iff $n = 3$ in Table 1, and then the solutions will be of the form

$$X_m + Y_m\sqrt{d} = 2\eta_d^k,$$

where $k \not\equiv 0 \pmod 3$. Again, one can see that $n = 3$ only if $d \equiv 5 \pmod 8$, so once again we can disregard the prime 2 in the factorization of d

Using the same algorithm from Section 2, with the appropriate minor changes, we obtain the following results.

Theorem 4.1.   a) *The largest three odd solutions of the equation $P(x^2 - 4) < 100$ are $x = 407479035814853$, 335682488669673 and 250734674482437.*

b) *The largest odd solution of $P(x^4 - 4) < 100$ is $x = 59$.*

c) *The largest odd solution of $P(x^6 - 4) < 100$ is $x = 7$.*

d) *The largest n such that $P(x^{2n} - 4) < 100$ has a solution is $n = 7$, the solution being $x = 3$.*

e) *The inequality $P(x^2 - 4) < 100$ has 2846 odd solutions.*

f) *The greatest power n of the smallest solution of our problem $(X_1 + Y_1\sqrt{d})^n$ which leads to a solution of our problem is $n = 10$ for $d = 5$. The case $d = 5$ also gives the most solutions, namely 7 of them.*

5. The inequality $P(x^2 + 2) < 200$

Consider the equation $x^2 - dy^2 = \pm 2$, where d is square free, and let $x_1 + y_1\sqrt{d} = \nu$ be the least solution. Obiviously, $d \equiv 2, 3 \pmod 4$ has to hold. One can see that, using the notation from Table 1, this implies $n = 1$ or 2. From a result of Perron (see [13, p. 126-129]), if $d \neq 2$, at most one of the equations $x^2 - dy^2 = -1$, $x^2 - dy^2 = 2$ and $x^2 - dy^2 = -2$ is solvable. This implies that $n = 2$ is impossible. By a elementary argument (see for example [7, p. 420]), one can also show that $\nu^2/2 = \eta_d$ holds. This can be reformulated in terms of the infrastructure of a real quadratic field by saying the ideal with norm ± 2 appears half way through the cycle of the principal class, or in terms of continued fractions by saying that the $p_{l/2}^2 - dq_{l/2}^2 = \pm 2$,

where l is the length of the continued fraction expansion of $\sqrt{d}$. Thus all the solutions of $x^2 - dy^2 = \pm 2$ are of the form

$$x_k + y_k\sqrt{d} = \nu\eta_d^k = \frac{\nu^{2k+1}}{2^k}, \quad \text{for } k \leq 0.$$

Now let

$$\alpha = \frac{x_1 + y_1\sqrt{d}}{\sqrt{2}} \text{ and } \beta = \frac{x_1 - y_1\sqrt{d}}{\sqrt{2}}.$$

Then

$$y_k = \frac{\alpha^k - \beta^k}{\sqrt{2d}},$$

and

$$u_k = \begin{cases} \frac{y_k}{y_1} & \text{if } k \text{ is odd} \\ \frac{y_k}{y_2} & \text{if } k \text{ is even} \end{cases}$$

is a Lehmer sequence. Note that only the odd members of this sequence yield a solution to our equation. Thus, by the Primitive divisor theorem for Lehmer sequences (see [14] and [1]), only the first 100 odd members of the sequence $(u_k)_{k\geq 0}$ can possibly be 200-smooth.

To narrow down our search we will use the following results of Yokoi:

THEOREM 5.1 ([15, Theorems 1 and 2])). *Let* $t + u\sqrt{d}$, *where* d *is a squarefree positive integer congruent to* 2 *or* 3 *modulo* 4, *be the fundamental unit of the real quadratic field* $\mathbb{Q}(\sqrt{d})$.

    a) *The Diophantine equation* $x^2 - dy^2 = 2$ *is solvable if and only if* $t \equiv 1$ (mod d).

    b) *The Diophantine equation* $x^2 - dy^2 = -2$ *is solvable if and only if* $t \equiv -1$ (mod d).

PROPOSITION 5.2 ([15, Proposition 2]).   a) *If the Diophantine equation* $x^2 - dy^2 = 2$ *is solvable then* $p \equiv \pm 1$ (mod 8) *for any odd prime factor* p *of* d.

    b) *If the Diophantine equation* $x^2 - dy^2 = -2$ *is solvable then* $p \equiv 1$ *or* 3 (mod 8) *for any odd prime factor* p *of* d.

Using Theorem 5.1 and Proposition 5.2 to narrow down our search, we proceed in the same manner as for (1.1), (1.2) and (1.3). We obtain the following results:

THEOREM 5.3.   a) *The largest three odd solutions of the equation* $P(x^2+2) < 200$ *are* $x = 9575480365630,\ 14629598023$ *and* 8850900308.

    b) *The largest odd solution of* $P(x^4 + 2) < 200$ *is* $x = 171$.

    c) *The largest solution of* $P(x^6 + 2) < 200$ *is* $x = 3$.

    d) *The largest* n *such that* $P(x^{2n} + 2) < 200$ *has a solution is* $n = 5$, *the solution being* $x = 2$.

e) *The inequality $P(x^2 + 2) < 200$ has 914 solutions, of which 516 are odd and 398 are even.*

f) *The greatest power n such that*

$$\frac{(X_1 + Y_1\sqrt{d})^{2n+1}}{2^n}$$

leads to a solution of our problem is $n = 8$ for $d = 2$. The case $d = 3$ gives the most solutions, namely 6 of them.

6. The inequality $P(x^2 - 2) < 200$

We search for the solutions of this inequality as explained in the previous section, again using Theorem 5.1 and Proposition 5.2 to narrow down our search. We obtain the following results:

THEOREM 6.1.   a) *The largest three solutions of the equation $P(x^2 - 2) < 200$ are $x = 324850200677887, 1600947755823$ and 494400410248.*

b) *The largest solution of $P(x^4 - 2) < 200$ is $x = 47$.*

c) *The largest odd solution of $P(x^6 - 2) < 200$ is $x = 10$.*

d) *The largest n such that $P(x^{2n} - 2) < 200$ has a solution is $n = 5$, the solution being $x = 2$.*

e) *The inequality $P(x^2 - 2) < 200$ has 537 solutions, of which 313 are even and 224 are odd.*

f) *The greatest power n such that*

$$\frac{(X_1 + Y_1\sqrt{d})^{2n+1}}{2^n}$$

leads to a solution of our problem is $n = 7$ for $d = 2$. The case $d = 2$ also gives the most solutions, namely 5 of them.

Problem number 4 on the list [5] of open problems concerning Diophantine equations is to find all the solutions (x, y, p) to

$$x^2 - 2 = y^p,$$

where p is a odd prime. By searching through our solutions we prove the following proposition.

PROPOSITION 6.2. *If the Diophantine equation $x^2 - 2 = y^p$, where p is an odd prime, then $P(y) > 200$.*

REMARK 6.3. The tables produced by our computations can be found on the web page `http://web.math.hr/~fnajman`.

References

[1] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte*, J. Reine Angew. Math. **539** (2001), 75–122.

[2] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, in Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math. **91** Birkhäuser, Boston, 1990, 27–41.

[3] J. Buchmann, K. Győry, M. Mignotte and N. Tzanakis, *Lower bounds for $P(x^3 + k)$, an elementary approach*, Publ. Math. Debrecen **38** (1991), 145–163.

[4] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of. Math. (2) **15** (1913/1914), 30–70.

[5] J. H. Evertse and R. Tijdeman, *Some open problems about Diophantione equations* from a workshop in Leiden in May 2007, see `http://www.math.leidenuniv.nl/~evertse/07-workshop-problems.pdf`.

[6] S. Guzmán Sánchez, Factores primos de $x^2 \pm 2$, Bachelor Thesis, Universidad de Guanajuato, Guanajuato, México, 2008.

[7] M. J. Jacobson Jr. and H. C .Williams, Solving the Pell equation, Springer, New York, 2009.

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

[9] F. Luca, *Primitive divisors of Lucas sequences and prime factors of $x^2 + 1$ and $x^4 + 1$*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **31** (2004), 19–24.

[10] F. Luca and F. Najman, *On the largest prime factor of $x^2 - 1$*, Math. Comp. **80** (2011), 429–435.

[11] M. Maurer, Regulator approximation and fundamental unit computation for real quadratic orders, PhD thesis, Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt, Germany, 2000.

[12] F. Najman, *Compact representation of quadratic integers and integer points on some elliptic curves*, Rocky Mountain J. Math., to appear.

[13] O. Perron, Die Lehre von den Kettenbruchen, Chelsea Publ. Comp., 1929.

[14] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) **62** (1955), 230–236.

[15] H. Yokoi, *Solvability of the Diophantine equation $x^2 - Dy^2 = \pm 2$ and new invariants for real quadratic fields*, Nagoya Math. J. **134** (1994), 137–149.

F. Najman
Department of Mathematics
University of Zagreb
Bijenička cesta 30, 10000 Zagreb
Croatia
E-mail: `fnajman@math.hr`