Publ. Math. Debrecen
38 / 1–2 (1991), 145–163

Lower bounds for $P(x^3+k)$, an elementary approach

By J. BUCHMANN, K. GYŐRY, M. MIGNOTTE and N. TZANAKIS

As usual, for a non-zero integer $n, P(n)$ denotes the largest prime factor of n.

This paper continues some work of the third author who considered $P(x^2+1)$ and of MARINA MUREDDU about $P(x^4+1)$, [Mi 1] and [Mu]. The method used goes back to STÖRMER [S] and has been applied to some other exponential diophantine equations, for example to Ramanujan–Nagell equation in [Mi 2], see also [Mi 3]. In those papers the key step is to use some suitable Pell–Fermat equations and to study some linear recursive sequences coming from this equation. But this method can be extended to more general cases: we don't really need a reduction to Pell–Fermat equation, but only linear recursive sequences. Such sequences appear in the study of norm form equations when the group of units of the number field K associated with this form has rank one.

This allows us to get lower bounds for $P(x^3+k)$. There are two cases:

(i) k is a perfect cube in $\mathbf{Z}$; then K is a real quadratic field;

(ii) k is not a perfect cube in $\mathbf{Z}$; then K is cubic field with a non-real embedding in the complex field.

Here, we consider an example of each case : $k=1$ for case (i), $k=2$ for case (ii). In practice these two cases lead to quite different difficulties: for case (i) the main question is to find all the values of a linear recursive sequence which are only composed of some fixed prime numbers, for case (ii) most of the work consists in the resolution of some norm form equations.

This paper is also related to several works of A. PETHŐ and B. de WEGER: [Pe], [Pe–W] and [W1].

Other methods can be used for finding effective lower bounds of $P(x^3+k)$. They are based on estimates on linear forms of logarithms, see [W2] for example.

1. Solution of $P(x^3+1) \leq 19$

Since

$$x^3+1 = (x+1)(x^2-x+1),$$

we have

$$P(x^3+1) \geq P(x^2-x+1),$$

and we shall only consider the right hand side expression.

Suppose that p is a prime number which divides x^2-x+1 for some integer x, then this number p is odd and -3 is a square mod p; so that $p=3$ or $p \equiv 1 \bmod 6$. Thus

$$P(x^2-x+1) \geq 31$$

or

$$x^2-x+1 = 3^{k'}7^{l'}13^{m'}19^{n'}; \quad k',l',m',n' \in \mathbf{N}.$$

Since 9 never divides x^2-x+1, this equation is equivalent to the 16 systems of equations

$$x^2-x+1 = 3^{\alpha}7^{\beta}13^{\gamma}19^{\delta}y^2, \quad y = 7^{m}13^{m'}19^{m''},$$

for $(\alpha,\beta,\gamma,\delta) \in \{0,1\}^4$.

The first equation of this system is of the type

$$(E_a) \qquad x^2-x+1 = ay^2,$$

where $a = 3^{\alpha}7^{\beta}13^{\gamma}19^{\delta}$. By the change of variables $X = 2x-1$, $Y = 2y$, this equation is transformed in

$$(E'_a) \qquad X^2 - aY^2 = -3, \quad Y > 0.$$

In the field $\mathbf{Q}(\sqrt{a})$, for all values of $a > 1$ that we study in this section, we have one of the following two types of prime ideal factorization:

$$(3) = \wp^2; \quad (3) = \wp \cdot \wp', \ \wp \neq \wp',$$

depending on whether 3 divides a or not. From this, it becomes obvious that in the order $\mathbf{Z}[\sqrt{a}]$, a complete set of non-associated elements of norm -3, if non-empty, is of the form

$\{X_0 + Y_0\sqrt{a}, X_0 - Y_0\sqrt{a}\}$ (in case that 3 does not divide a),

or $\{X_0 + Y_0\sqrt{a}\}$ (in case that 3 divides a),

where, in both cases, we may suppose $Y_0 > 0$.

Let $\eta > 0$ be a fundamental unit in $\mathbf{Z}[\sqrt{a}]$. In both cases, equation (E'_a) implies

$$X + Y\sqrt{a} = \pm(X_0 + Y_0\sqrt{a}) \cdot \eta^n, \quad n \in \mathbf{Z} \tag{1}$$

or

$$X + Y\sqrt{a} = \pm(X_0 - Y_0\sqrt{a}) \cdot \eta^n, \quad n \in \mathbf{Z}. \tag{2}$$

We claim now that every value of Y obtained from (2), can be obtained from (1) as well. Indeed, suppose first that $\mathrm{Norm}(\eta) = +1$. Since $(X+Y\sqrt{a})(X-Y\sqrt{a}) = -3$ and $Y > 0$, it follows that $X+Y\sqrt{a} > 0$ and $X-Y\sqrt{a} < 0$; in the same way, $X_0+Y_0\sqrt{a} > 0$ and $X_0-Y_0\sqrt{a} < 0$. Therefore (1) must hold with the plus sign and (2) with the minus sign. Then, on taking the conjugate relation of (2) we get $-X+Y\sqrt{a} = (X_0+Y_0\sqrt{a})\eta^{-n}$, from which we see that Y can also be obtained from relation (1) if we replace n by $-n$. If $\mathrm{Norm}(\eta) = -1$ (in this section this is the case only when $a = 13$) then, by taking norms in (1) and (2), we see that n must be even. Therefore, we replace η by η^2 in (1) and (2) ; and since $\mathrm{Norm}(\eta^2) = 1$, the previous argument applies.

Thus, we conclude that we have only to consider a relation of the form

$$X + Y\sqrt{a} = (X_0 + Y_0\sqrt{a})\varepsilon^n, \ n \in \mathbf{Z} \tag{3}$$

where $X_0 + Y_0\sqrt{a}$ is any element in $\mathbf{Z}[\sqrt{a}]$ of norm -3 with $Y_0 > 0$ and $\varepsilon = u + v\sqrt{a}$ is either a positive fundamental unit or the square of such a unit. The second alternative is forced either by the fact that $\mathrm{Norm}(\eta) = -1$ $(a = 13)$ or by the fact that an odd exponent in (1) or (2) furnishes an odd Y $(a = 3, 7, 19, 21)$ which is not compatible with $Y = 2y$. Note that, in view of the above discussion, one has always $\mathrm{Norm}\,(\varepsilon) = +1$.

For the computation of the integers (X_0, Y_0) and (u, v) the following result is very useful (see [Lev], v. 1, Theorem 9.8).

Lemma 1. – *If a and b are rational integers, $a > 0$ and $|b| < \sqrt{a}$, a not a perfect square, all the positive solutions of the Pell–Fermat equation*

$$x^2 - ay^2 = b$$

are such that x/y is a convergent of the continued fraction expansion of $\sqrt{a}$.

Now, from (3) and its conjugate we get

$$Y = \frac{X_0 + Y_0\sqrt{a}}{2\sqrt{a}}\varepsilon^n - \frac{X_0 - Y_0\sqrt{a}}{2\sqrt{a}}\varepsilon^{-n} =: Y_n$$

(notice that for $n = 0$ our definition is compatible with the up to now used notation Y_0). Thus, Y must be searched among the values of a linear second-order recurrence sequence $(Y_n)_{n\in\mathbf{Z}}$, defined as follows:

$$Y_0 \text{ as already defined, } Y_1 = uY_0 + vX_0 \text{ and } Y_n = 2uY_{n-1} - Y_{n-2}$$

(as it is well-known, the recursive relation comes from the equation of $\varepsilon : \ \varepsilon^2 = 2u\varepsilon - 1$). Therefore, y must be equal to some y_n $(n \in \mathbf{Z})$, where

$$y_0 = Y_0/2, \ y_1 = (uY_0 + vX_0)/2, \text{ and } y_n = 2uy_{n-1} - y_{n-2}.$$

We have reduced our problem to the following: find all the elements of a given binary recursive sequence which are only composed of some fixed primes. To solve this problem, we consider this recursive sequence modulo "well-chosen" numbers M. Modulo any integer M, this recursive sequence is periodical and the set of its values can be easily computed. To conclude, we gather the information obtained for suitable moduli M.

1. The case $(0,0,0,0)$: $a = 1$.

The quadratic equation is $x^2 - x + 1 = y^2$, and it is easy to prove that the only solutions are $x = 0, 1, \ y = 1$ (recall that we always suppose $y > 0$), so that

$$x^3 + 1 = 1 \text{ or } 2.$$

2. The case $(1,0,0,0)$: $a = 3$.

We have $X_0 = 3$, $Y_0 = 2$, $u = 7$, $v = 4$,
and, therefore, the recursive sequence is defined by

$$y_0 = 1, \ y_1 = 13, \ y_n = 14y_{n-1} - y_{n-2}.$$

One verifies immediately that 7 and 19 never divide y_n and that

$$13|y_n \Rightarrow n \equiv 1 \pmod 3, \quad 13^2|y_n \Rightarrow n \equiv 19 \pmod{39}.$$

Modulo 17 we have

$$13^m \in \{1, 13, 16, 4\} \text{ and } y_n = 13^m \Rightarrow n \equiv 1, 7 \pmod 9 \text{ and } m \equiv 1 \pmod 4.$$

Modulo 233 : $n \equiv 19 \pmod{39} \Rightarrow y_n \equiv 13 \times 121, 13 \times 224$, but $m \equiv 1 \pmod 4 \Rightarrow 13^m \bmod 233 \notin \{13 \times 121, 13 \times 224\}$.

This proves that there is no solution with $m > 1$. The only solutions are

$$y = 1 \text{ and } y = 13,$$

which correspond to $x = -1, 2, 23, -22$ and

$$x^3 + 1 = 0, 9, 12168 (= 2^3 \cdot 3^2 \cdot 13^2), -10647 (= -3^2 \cdot 7 \cdot 13^2).$$

3. The case $(0,1,0,0)$: $a = 7$.

We have $X_0 = 37$, $Y_0 = 14$, $u = 127$, $v = 48$,
and the recursive sequence is defined by

$$y_0 = 7,\ y_1 = 1777,\ y_n = 254y_{n-1} - y_{n-2}.$$

One verifies that $7|y_n \Rightarrow n \equiv 0 \pmod 7$ and $13|y_n \Rightarrow n \equiv 5 \pmod 7$; this shows that the study splits into two cases:

$$\text{(i)}\quad y = 7^m \cdot 19^{m''}, \qquad \text{(ii)}\quad y = 13^{m'} \cdot 19^{m''}.$$

Consider first the case when $m'' = 0$, that is to say:

$$\text{(i.0)}\quad y = 7^m, \qquad \text{(ii.0)}\quad y = 13^{m'}.$$

In the case (i.0) the scheme is the following,

$M = 127 \Rightarrow n \equiv 0,3 \pmod 4$ and $m \equiv 1,0 \pmod 6$,
$M = 49$ and $m > 1 \Rightarrow n \equiv 7 \pmod{49}$,
$M = 97$ and $n \equiv 7 \pmod{49} \Rightarrow y \equiv 39 \pmod{97}$ and
$m \equiv 65 \pmod{96}$,

so that the only solution is $m = 1$, which corresponds to $y = 7$ and $x = -18, 19$ and

$$x^3 + 1 = -5831 = -7^3 \cdot 17 \quad \text{or} \quad = 6860 = 2 \cdot 5 \cdot 7^3.$$

In the case (ii.0), we argue as follows,

$M = 8 \Rightarrow n \equiv 1 \pmod 2$ and $m' \equiv 0 \pmod 2$,
$M = 127$ and $n \equiv 1 \pmod 2 \Rightarrow n \equiv 3 \pmod 4$ and $m' \equiv 0 \pmod 3$,
$M = 7$ and $m' \equiv 0 \pmod 6 \Rightarrow n \equiv 6 \pmod 7 \Rightarrow y_n = 1 \pmod{13}$,

so that $m' = 0$, $y = 1$, $x = -2$ and $x = 3$, $x^3 + 1 = -7$ and $x^3 + 1 = 28$.
Now suppose $m'' > 0$. Taking $M = 19$, we see that $n \equiv 1 \pmod 3$ so that

$$y \equiv 2 \pmod 5 \text{ and } m \text{ or } m' \text{ is odd.}$$

The choice $M = 17$ shows that there is no solution in case (i), since

$$n \equiv 1 \pmod 3 \Rightarrow y \equiv 9 \pmod{17} \text{ and } m \equiv 0 \pmod 2.$$

In case (ii), we argue as follows:

$M = 19$ and $m'' > 0 \Rightarrow n \equiv 1 \pmod 3$,
$M = 5$ and $n \equiv 1 \pmod 3 \Rightarrow y_n \equiv 2 \pmod 5 \Rightarrow m' \equiv 1 \pmod 2$,
$M = 17$ and $n \equiv 1 \pmod 3 \Rightarrow y_n \equiv 9 \pmod{17} \Rightarrow m'' \equiv 1 \pmod 2$,
$M = 13^2$ and $m' \geq 2 \Rightarrow n \equiv 40 \pmod{91}$,
$M = 19^2$ and $m'' \geq 2 \Rightarrow n \equiv 34 \pmod{171} \Rightarrow n \equiv 15 \pmod{19}$,
$M = 4$ and $m'' \equiv 1 \pmod 2 \Rightarrow y_n \equiv -1 \pmod 4 \Rightarrow n \equiv 0 \pmod 2$,
$M = 53$, $n \equiv 15 \pmod{19}$ and $n \equiv 0 \pmod 2 \Rightarrow y_n \equiv 25 \pmod{53}$
$\Rightarrow m'' \equiv 0 \pmod 2$: contradiction. Therefore $m' \in \{0, 1\}$.
$M = 151$, $n \equiv 40 \pmod{91}$ and $n \equiv 0 \pmod 2 \Rightarrow y_n \equiv 72 \pmod{151}$
$\Rightarrow m' \equiv 0 \pmod 2$: contradiction. Therefore $m'' \in \{0, 1\}$.

Now, one verifies that the only solution is $y_{-2} = 13 \cdot 19$, which gives $x = 654, -653$ and

$$x^3 + 1 = 5 \cdot 7 \cdot 13^2 \cdot 19^2 \cdot 131, \ -2^2 \cdot 7 \cdot 13^2 \cdot 19^2 \cdot 163 \text{ respectively .}$$

4. The case $(0, 0, 1, 0)$: $a = 13$.

Then $X_0 = 7$, $Y_0 = 2$, $u = 649$, $v = 180$,
and the recursive sequence is defined by

$$y_0 = 1, \ y_1 = 1279, \ y_n = 1298 y_{n-1} - y_{n-2}.$$

If 7 divides y_n then $n \equiv 2 \pmod 4$ but if 19 divides y_n then $n \equiv 9 \pmod{10}$, so that there are two cases

$$\text{(i)} \ y_n = 7^m \cdot 13^{m'} \quad \text{and} \quad \text{(ii)} \ y_n = 13^{m'} \cdot 19^{m''} \text{ with } m'' > 0.$$

In the first case the argument is the following,

$M = 5 \Rightarrow m \equiv m' \pmod 2$,
$M = 8$ and $m \equiv m' \pmod 2 \Rightarrow n \equiv 0, 3 \pmod 4$,
$M = 7$ and $n \equiv 0, 3 \pmod 4 \Rightarrow m = 0$,
$M = 9$ and $m = 0 \Rightarrow m' \equiv 0 \pmod 3$,
$M = 13$ and $m' > 0 \Rightarrow n \equiv 11 \pmod{13}$,
$M = 79$ and $n \equiv 11 \pmod{13} \Rightarrow y_n \equiv 13 \pmod{79}$ and
$m' \equiv 1 \pmod 3$,

so that the only solution is $m = m' = 0$, which gives $y = 1$, $x = -3$ and $x = 4$,

$$x^3 + 1 = -26 \text{ and } x^3 + 1 = 65.$$

In the second case, we have $n \equiv 9 \pmod{10}$, so that $M = 5$ implies that m' is even. Then, a glance at $M = 59$ shows that $n \equiv 3 \pmod 4$. On the other hand,

$M = 11$ and $n \equiv 3 \pmod 4 \Rightarrow m'' \equiv 1 \pmod 2$,
$M = 13$ and $m' > 0 \Rightarrow y_n \equiv 0 \pmod{13} \Rightarrow n \equiv 11 \pmod{13}$,
$M = 53$ and $n \equiv 11 \pmod{13} \Rightarrow y_n \equiv 16 \pmod{53} \Rightarrow m''$ even,

a contradiction. Thus, $m' = 0$.

$$M = 109 \text{ and } n \equiv 9 \pmod{10} \text{ and } m' = 0 \Rightarrow m'' \equiv 1 \pmod{36},$$
$$M = 19^2 \text{ and } m'' \geq 2 \Rightarrow y_n \equiv 0 \pmod{19^2} \Rightarrow n \equiv 11 \pmod{38}$$
$$\Rightarrow y_n \equiv 13 \pmod{37} \Rightarrow m'' \equiv 25 \pmod{36}, \text{ a contradiction.}$$

This shows that the only possibilities are $m' = 0$ and $m'' = 1$, so that $y = 19$, $x = -68$ and $x = 69$, which gives

$$x^3 + 1 = -314431 = -13 \cdot 19^2 \cdot 67 \text{ and } x^3 + 1 = 328510 = 2 \cdot 5 \cdot 7 \cdot 13 \cdot 19^2.$$

5. The case $(0,0,0,1)$: $a = 19$.

In this case $X_0 = 61$, $Y_0 = 14$, $u = 57799$, $v = -13260$ and the recursive sequence is given by

$$y_0 = 7,\ y_1 = 163,\ y_n = 115598 y_{n-1} - y_n.$$

It follows that $y_n \equiv 7 \pmod{13}$ and we have only to consider the equation

$$y_n = 7^m \cdot 19^{m''} \quad \text{with} \quad m + 7m'' \equiv 1 \pmod{12}.$$

If 19 divides y_n, then $n \equiv 3 \pmod{19}$ and $y_n \equiv 9 \pmod{37}$, which implies $m + m'' \equiv 2 \pmod{3}$; this contradicts $m + 7m'' \equiv 1 \pmod{12}$. Thus $m'' = 0$.
Now, our solution goes as follows,

$$M = 7 \text{ and } m \neq 0 \Rightarrow n \equiv 0 \pmod{2},$$
$$M = 9 \text{ and } m \equiv 1 \pmod{3} \Rightarrow n \equiv 0 \pmod{3},$$
$$M = 11 \text{ and } n \equiv 0 \pmod{6} \Rightarrow m \equiv 1 \pmod{10},$$
$$M = 17 \text{ and } n \equiv 0 \pmod{2} \Rightarrow m \equiv 1 \pmod{16},$$
$$m \equiv 1 \pmod{40} \Rightarrow y_n = 7^m \equiv 7 \pmod{41} \Rightarrow n \equiv 0, 4 \pmod{21}$$
$$\Rightarrow n \equiv 0 \pmod{7} \text{ [since 3 divides } n\text{]}$$
$$M = 49 \text{ and } m \geq 2 \Rightarrow n \equiv 8, 22 \pmod{28} \Rightarrow n \not\equiv 0 \pmod{7},$$

a contradiction. Then $m \in \{0,1\}$, so that the only solution is $y = 7$, $x = -30$ and $x = 31$, which gives

$$x^3 + 1 = -26999 = -7^2 \cdot 19 \cdot 29 \text{ and } x^3 + 1 = 29792 = 2^5 \cdot 7^2 \cdot 19.$$

6. The case $(1,1,0,0)$: $a = 21$.

In this case $X_0 = 9$, $Y_0 = 2$, $u = 55$, $v = 12$ and the linear recursive sequence is

$$y_0 = 1,\ y_1 = 109,\ y_n = 110 y_{n-1} - y_n.$$

If 7 or 13 divides y_n then $n \equiv 3 \pmod{7}$ and 43 divides y_n. Thus, we have only to consider the equation $y_n = 19^{m''}$. Since $y_n \equiv 1 \pmod{4}$ for every n, we see that m'' is even.

Now, if 19 divides y_n then $n \equiv 2 \pmod{5}$ and $y_n \equiv 12 \pmod{29}$, which is not a square mod 29. This shows that $m'' = 0$. We get $y = 1$, $x = -4$ and $x = 5$,

$$x^3 + 1 = -63 = -3^2 \cdot 7 \text{ and } x^3 + 1 = 126 = 2 \cdot 3^2 \cdot 7.$$

7. The case $(1,0,1,0)$: $a = 39$.

In this case $X_0 = 306$, $Y_0 = 49$, $u = 25$, $v = 4$ and we see that Y_n is odd for every n. There is no solution.

8. The case $(1,0,0,1)$: $a = 57$.

Here, $X_0 = 15$, $Y_0 = 2$, $u = 151$, $v = 20$ and

$$y_0 = 1,\ y_1 = 301,\ y_n = 302y_{n-1} - y_{n-2}.$$

It is easy to verify that

19 divides $y_n \Rightarrow$ 37 divides y_n, 7 divides $y_n \Rightarrow$ 43 divides y_n,

so that we only have to consider the equation $y_n = 13^{m'}$. We notice that

$$\forall n, y_n \equiv \pm 1 \pmod{151},\ \text{so that } m' \equiv 0 \pmod{75}.$$

Then,

$$m' \equiv 0 \pmod 3 \Rightarrow y_n \equiv 1, 10, 19 \pmod{27} \Rightarrow n \equiv 0, 2 \pmod 3,$$

but since $y_{-(n+1)} = y_n$ we may suppose $n \equiv 0 \pmod 3$,

$$\begin{aligned} &m' \equiv 0 \pmod 5 \text{ and } n \equiv 0 \pmod 3 \\ &\quad \Rightarrow y_n \equiv \pm 1 \pmod{11} \text{ and } n \equiv 0 \pmod 6, \\ &n \equiv 0 \pmod 6 \Rightarrow y_n \equiv 1 \pmod{43} \Rightarrow m' \equiv 0 \pmod 7 \\ &m' > 0 \text{ and } n \equiv 0 \pmod 2 \Rightarrow n \equiv 10 \pmod{14} \\ &\quad \Rightarrow y_n \equiv 5, 24 \pmod{29}, \end{aligned}$$

and the last congruences are impossible since $m' \equiv 0 \pmod 7$. This proves that $y = 1$ and $x = -7$ or $x = 8$,

$$x^3 + 1 = -2 \cdot 3^2 \cdot 19 \quad \text{or} \quad x^3 + 1 = 3^3 \cdot 19.$$

9. The case $(0,1,1,0)$: $a = 91$.

Then, $X_0 = 19$, $Y_0 = 2$, $u = 4954951$, $v = 519420$ and

$$y_0 = 1,\ y_1 = 9889441,\ y_n = 9909902\ y_{n-1} - y_{n-2},$$

and it is easy to verify that 19 never divides y_n, so that we only have to consider

$$y_n = 7^m \cdot 13^{m'}.$$

Since $y_n \equiv 1 \pmod{44}$ for all n, we see that the exponents m and m' must be even. This implies $y_n \equiv 1 \pmod 8$ and $n \equiv 0, 1 \pmod 4$.
Modulo 31, the period is 8 and y_n is not a square for $n = 4, 5$, so that $n \equiv 0, 1 \pmod 8$, $y_n \equiv 1 \pmod{16}$ and $m' \equiv 0 \pmod 4$.
But y_n must be a square modulo 787, and we have indeed $n \equiv 0 \pmod 8$.
Notice that

$$m > 0 \text{ and } n \equiv 0 \pmod 2 \Rightarrow n \equiv 6 \pmod{14} \Rightarrow y_n \equiv 13 \pmod{29} \Rightarrow$$
$$\Rightarrow m' \equiv 1 \pmod 2,$$

which contradicts the fact that m' is even: necessarily $m = 0$, $y_n = 13^{m'}$.
Now

$$m' > 0 \text{ and } n \equiv 0 \pmod 2 \Rightarrow n \equiv 6 \pmod{26} \Rightarrow y_n \equiv 4 \pmod{53} \Rightarrow$$
$$\Rightarrow m' \not\equiv 0 \pmod 4,$$

again a contradiction: $m' = 0$ too. We get $y = 1$, $x = -9$ or $x = 10$,

$$x^3 + 1 = -2^3 \cdot 7 \cdot 13 \quad \text{or} \quad x^3 + 1 = 7 \cdot 11 \cdot 13.$$

10. The case $(0, 1, 0, 1)$: $a = 133$.

Then $X_0 = 23$, $Y_0 = 2$, $u = 2588599$, $v = 224460$ and

$$y_0 = 1, \; y_1 = 5169889, \; y_n = 5177198\, y_{n-1} - y_{n-2},$$

and y_n is always a non-zero square modulo 13, so that

$$y_n = 7^m \cdot 19^{m''} \text{ with } m \equiv m'' \pmod 2.$$

Since m and m'' are of the same parity, y_n must be a square modulo 43, and this implies that n is even. Now

$$n \equiv 0 \pmod 2 \Rightarrow y_n \equiv 1 \pmod 5 \Rightarrow m'' \equiv 0 \pmod 2 \text{ and } m \equiv 0 \pmod 4.$$

Since m, m'' and n are even, a glance at $M = 8$ shows that 4 divides n, and

$$n \equiv 0 \pmod 4 \Rightarrow y_n \equiv 1 \pmod{13} \Rightarrow m + 7m'' \equiv 0 \pmod{12},$$

so that m and m'' are both multiples of 4.

Now we see that $m'' = 0$, because

$$m'' > 0 \Rightarrow n \equiv 8 \pmod{19} \Rightarrow y_n \equiv 9 \pmod{113},$$

which contradicts the fact that m and m'' are both multiples of 4. It follows that m is a multiple of 12.
The conclusion is easy:

$$M = 11 : n \equiv m \equiv 0 \pmod 2 \Rightarrow n \equiv 0, 1 \pmod 5,$$

$$M = 31 : n \equiv 0, 1 \pmod 5 \text{ and } m \equiv 0 \pmod 3 \Rightarrow n \equiv 0 \pmod 5,$$

$$M = 139 : m > 0 \text{ and } n \equiv 0 \pmod{10} \Rightarrow n \equiv 10 \pmod{70} \Rightarrow$$

$$\Rightarrow y_n \equiv 108 \pmod{139},$$

but 108 is not a square modulo 139. Thus, $m = 0$ and we obtain $y = 1$, $x = -11, 12$ and

$$x^3 + 1 = -2 \cdot 5 \cdot 7 \cdot 19 \quad \text{or} \quad x^3 + 1 = 7 \cdot 13 \cdot 19.$$

11. Tha case $(0, 0, 1, 1)$: $a = 247$.

One verifies that $X_0 = 1163$, $Y_0 = 74$, $u = 14549450527$, $v = -925759368$ so that the linear recursive sequence is defined by

$$y_0 = 37, \; y_1 = 597007, \; y_n = 29098901054 \, y_{n-1} - y_{n-2}.$$

Since for all n, $y_n \equiv 37 \pmod{67}$ the exponents m and m' are of the same parity, and

$$m \equiv m' \pmod 2 \Rightarrow y_n \text{ is a square modulo } 5 \Rightarrow n \equiv 2 \pmod 3,$$

$$n \equiv 2 \pmod 3 \Rightarrow y_n \equiv 58 \pmod{109} \Rightarrow m' \not\equiv m'' \pmod 2,$$

$$m = m' \not\equiv m'' \pmod 2 \Rightarrow y_n \equiv 3 \pmod 8,$$

which is impossible: there is no solution.

12. The case $(1, 1, 1, 0)$: $a = 273$.

Here, $X_0 = 33$, $Y_0 = 2$, $u = 727$, $v = 44$ and

$$y_0 = 1, \; y_1 = 1453, \; y_n = 1454 \, y_{n-1} - y_{n-2}.$$

When 7 divides y_n then y_n is a multiple of 43, therefore

$$y_n = 13^{m'} \cdot 19^{m''}.$$

Since $y_n \equiv 1 \pmod{44}$ for all n, the exponents m' and m'' are both even. We remark that

$$m' > 0 \Rightarrow n \equiv 6 \pmod{13} \Rightarrow y_n \equiv 85 \pmod{103},$$

and 85 is not a square modulo 103; hence $m' = 0$. Moreover,

$$m'' > 0 \Rightarrow n \equiv 1 \pmod 3 \Rightarrow y_n \equiv 3 \pmod 5,$$

and 3 is not a square modulo 5; hence $m'' = 0$. We get $y = 1$, $x = -16$ or $x = 17$ and

$$x^3 + 1 = -3^2 \cdot 5 \cdot 7 \cdot 13 \quad \text{or} \quad x^3 + 1 = 2 \cdot 3^3 \cdot 7 \cdot 13.$$

13. The case $(1,1,0,1)$: $a = 399$.

There is no element in $\mathbf{Z}\left[\sqrt{399}\right]$ of norm -3 (apply e.g. Theorem 108 a of [Na]) and thus no solution.

14. The case $(1,1,1,1)$: $a = 741$.

Here $X_0 = 3321$, $Y_0 = 122$, $u = 7352695$, $v = 270108$.
Since 122 and 270108 are both divisible by 61 one sees that y_n is always a multiple of 61, and consequently there is no solution.

15. The case $(0,1,1,1)$: $a = 1729$.

Here $X_0 = 122831$, $Y_0 = 2954$, $u = 44611924489705$, $v = 1072885712316$.
As usually, $y_0 = Y_0/2$, $y_1 = (uY_0 + vX_0)/2$ and $y_n = 2uy_{n-1} - y_{n-2}$. We notice that,

$$M = 5 : \forall n, y_n \equiv \pm 2 \Rightarrow m + m' \equiv 1 \pmod 2,$$

$$M = 11 : \forall n, y_n \equiv 3 \Rightarrow m + m' + m'' \equiv 0 \pmod 2,$$

(so that m'' is odd),

$$M = 49 : m > 1 \Rightarrow n \equiv 21 \pmod{49} \Rightarrow y_n \equiv 13 \pmod{97}$$

$$\Rightarrow m + m' + m'' \equiv 1 \pmod 2 : \text{ contradiction } (m \leq 1),$$

$$M = 4 : m \equiv m'' \equiv 1 \pmod 2 \Rightarrow y_n \equiv 1 \pmod 4 \Rightarrow n \equiv 0 \pmod 2,$$

$$M = 109 : n \equiv 0 \pmod 2 \Rightarrow m' + m'' \equiv 0 \pmod 2 \Rightarrow m' \equiv 0 \pmod 2.$$

Thus, $m \equiv 1 \pmod 2 \Rightarrow m' \equiv 1 \pmod 2$ which contradicts the relation $m' + m'' \equiv 1 \pmod 2$. It follows that m is even and, since $m \leq 1$, $m = 0$. Thus $m = 0$ and $m' \equiv m'' \equiv 1 \pmod 2$.

We have,

$$M = 8 : m' \equiv m'' \equiv 1 \pmod 2 \Rightarrow n \equiv 1 \pmod 4,$$

$$M = 109 : n \equiv 1 \pmod 4 \text{ and } m' \equiv m'' \equiv 1 \pmod 2 \Rightarrow n \equiv 5 \pmod{12},$$

$$M = 17 : n \equiv 5 \pmod{12} \Rightarrow y_n = 6, 8, 13$$

$$\Rightarrow 4m' + 14m'' \equiv 15, 10, 1 \pmod{16} \Rightarrow 4m' + 14m'' \equiv 10 \pmod{16}$$

$$\Rightarrow n \equiv 29 \pmod{36} \text{ and } m'' \equiv 3 \pmod 4,$$

$$M = 37 : n \equiv 29 \pmod{36} \Rightarrow y_n \equiv 12 \pmod{37} \Rightarrow m' + m'' \equiv 2 \pmod 3$$

$$M = 73 : n \equiv 29 \pmod{36} \Rightarrow y_n \equiv 34, 39 \pmod{73}$$

$$\Rightarrow m' + m'' \equiv 1 \pmod 3,$$

which contradicts the relation $m' + m'' \equiv 2 \pmod 3$ obtained just above. There is no solution.

16. The case $(1,1,1,1)$: $a = 5187$.

Then $X_0 = 72$, $Y_0 = 1$, $u = 3457$, $v = 48$. There is no solution since Y is always odd.
We gather our results in a table where we give all the solutions of the equation

$$x^3 + 1 = \pm 2^a\, 3^b\, 5^c\, 7^d\, 11^e\, 13^f\, 17^g\, 19^h.$$

x	x^3+1	a	b	c	d	e	f	g	h
−22	−10647	0	2	0	1	0	2	0	0
−18	−5831	0	0	0	3	0	0	1	0
−16	−4095	0	2	1	1	0	1	0	0
−11	−1330	1	0	1	1	0	0	0	1
−9	−728	3	0	0	1	0	1	0	0
−7	−342	1	2	0	0	0	0	0	1
−4	−63	0	2	0	1	0	0	0	0
−3	−26	1	0	0	0	0	1	0	0
−2	−7	0	0	0	1	0	0	0	0
0	1	0	0	0	0	0	0	0	0
1	2	1	0	0	0	0	0	0	0
2	9	0	2	0	0	0	0	0	0
3	28	2	0	0	1	0	0	0	0
4	65	0	0	1	0	0	1	0	0
5	126	1	2	0	1	0	0	0	0
8	513	0	3	0	0	0	0	0	1
10	1001	0	0	0	1	1	1	0	0
12	1729	0	0	0	1	0	1	0	1
17	4914	1	3	0	1	0	1	0	0
19	6810	2	0	1	3	0	0	0	0
23	12168	3	2	0	0	0	2	0	0
31	29792	5	0	0	2	0	0	0	1
69	328510	1	0	1	1	0	1	0	2

Consequence:

$$\boxed{P(x^3+1) \geq 31 \text{ if } x > 69 \text{ or } x < -22.}$$

2. A lower bound for $P(x^3 + 2)$

In this section we want to find all the integer solutions of $P(x^3+2) \leq 7$. Since the prime 7 never divides $x^3 + 2$ this condition is equivalent to the set of systems

$$x^3 - Dy^3 = -2, \quad P(y) \leq 5,$$

where D is cube–free and $P(D) \leq 5$.

Looking modulo 4, one sees that 4 does not divide D and that y must be odd. Modulo 9 the cubes are $0, \pm 1$, so that D mod 9 is different from 0, 4 and 5. We have only to consider the ten cases $D = 1, 2, 3, 6, 10, 15, 25, 30, 75, 150$.

We work in the fields $\mathbf{Q}(\Theta)$, where $\Theta = \sqrt[3]{D}$ and we replace each of the previous systems by the unique equation $\text{Norm}(x + y\Theta) = -2$. It is well known that the group of units of any order of such a field is of rank one and we shall choose a fundamental unit ε with norm equal to 1.

We put $\varepsilon = u + v\Theta + w\Theta^2$, where ε is a fundamental unit of $\mathbf{Z}[\Theta]$ or, sometimes, of the maximal order of $\mathbf{Q}(\Theta)$, if this makes the computations simpler.

The following lemma (proved in [Bo & Sh], chap. III, §7.1.) will also be used.

Lemma 2. – *Let O_K be the ring of integers of a number field K. Suppose that p is a prime number, and that $\wp_1, \ldots, \wp_k$ are the prime ideals of O_K of norm p. Then each element of O_K of norm equal to $\pm p$ belongs to some $\wp_i$ and each $\wp_i$ contains at most one class of associate elements of O_K of norm $\pm p$.*

When D is odd, the polynomial $X^3 - D$ has only one linear factor modulo 2, and there is one ideal of the field $\mathbf{Q}(\Theta)$ of norm 2. When D is even, then 2 is totally ramified and there is again only one ideal of norm 2. Lemma 2 implies that the set of the solutions of the equation $\text{Norm}(\beta) = -2$ in integers β of $\mathbf{Q}(\Theta)$ is either empty or equal to the set of values $\alpha\varepsilon^n$, where α is fixed with norm equal to -2 and n runs through $\mathbf{Z}$.

We put $\alpha = a + b\Theta + c\Theta^2$ and

$$\alpha\varepsilon^n = x_n + y_n\Theta + z_n\Theta^2, \text{ for every } n \in \mathbf{Z},$$

so that (z_n) is a linear recursive sequence and we want to find all its zeroes. We notice that

$$\begin{aligned} z_0 = c, \quad z_1 &= aw + bv + cu, \\ z_2 &= cu^2 + av^2 + Dbw^2 + 2buv + 2auw + 2Dcvw, \end{aligned}$$

and since $\varepsilon^3 = 3u \cdot \varepsilon^2 + 3(Dvw - u^2) \cdot \varepsilon + 1$, the z_n's satisfy the following linear relation

$$z_{n+3} = U \cdot z_{n+2} + V \cdot z_{n+1} + z_n, \quad \text{with } U = 3u \text{ and } V = 3(Dvw - u^2).$$

Remark. If $\varepsilon \equiv 1 \pmod 2$ then $z_n \equiv z_0 \pmod 2$ for all n, so that in that case z_n is never zero when the first term z_0 is odd.

To find all $n \in \mathbf{Z}$ for which $z_n = 0$ (these n's will be called the zeroes of this sequence) we propose the following method which, in general, can be adaptated to linear sequences of arbitrary order.

Suppose that some preliminary computations furnish us a set $\mathbf{I}$ of zeroes $i \in \mathbf{Z}$ of the sequence and that we want to prove that these are the only zeroes. Then we can apply the following theorem.

Theorem. – *Let p be an odd prime and k a positive integer such that $\varepsilon^k \equiv N \pmod p$ with a rational integer N. Let $M \in \mathbf{Z}$ such that $M \cdot N \equiv 1 \pmod{p^2}$. Put $\varepsilon^k = N + p\lambda$, where λ is an algebraic integer. Suppose that the following conditions hold:*

(c1) p does not divide Norm(λ) (this is the norm from $\mathbf{Q}(\Theta)$ to $\mathbf{Q}$),

(c2) $z_n \equiv 0 \pmod p \Rightarrow n \equiv i \pmod k$ for some $i \in \mathbf{I}$,

(c3) $M \cdot z_{2k+i} \equiv 2z_{k+i} \pmod{p^2}$ for every $i \in \mathbf{I}$,

(c4) for every $i \in \mathbf{I}$, p^2 does not divide z_{k+i}.

Then, $z_n = 0 \Rightarrow n \in \mathbf{I}$.

PROOF. Suppose that $z_n = 0$. In view of (c2), $n = m \cdot k + i$ for some $i \in \mathbf{I}$ and $m \in \mathbf{Z}$, and it suffices to prove that $m = 0$.

Write $M \cdot \varepsilon^k = 1 + p\beta$ for some algebraic integer $\beta \in \mathbf{Q}(\Theta)$. We have

$$z_{km+i} = \gamma\varepsilon^{km+i} + \gamma'\varepsilon'^{km+i} + \gamma''\varepsilon''^{km+i},$$

where γ is some algebraic number and γ', γ'' are its conjugates. Therefore,

$$(1) \quad M^m \cdot z_{km+i} = \omega(1+p\beta)^m + \omega'(1+p\beta')^m + \omega''(1+p\beta'')^m =: f(m)$$

for suitable algebraic numbers $\omega, \omega', \omega''$.

We can view (1) as a relation in the p–adic field $\mathbf{C}_p$. On expanding the binomials in the right-hand side of (1), we get

$$f(m) = \sum_{j=0}^{m} p^j \binom{m}{j} (\omega\beta^j + \omega'\beta'^j + \omega''\beta''^j) = \sum_{j=0}^{m} p^j \binom{m}{j} \Omega_j,$$

where we have put $\Omega_j = \omega\beta^j + \omega'\beta'^j + \omega''\beta''^j$. One the other hand,

$$\beta^j = p^{-j}\{(1+p\beta) - 1\}^j = p^{-j} \sum_{h=0}^{j} (-1)^{j-h} \binom{j}{h} (1+p\beta)^h,$$

and in view of (1) and the definition of Ω_j,

$$\Omega_j = p^{-j}\sum_{h=0}^{j}(-1)^{j-h}\binom{j}{h}f(h). \tag{2}$$

In view of (2), we get

$$\Omega_0 = f(0) = z_i = 0, \tag{3}$$

$$\Omega_1 = \frac{f(1)-f(0)}{p} = \frac{M\cdot z_{k+i}-z_i}{p} = \frac{M\cdot z_{k+i}}{p}, \tag{4}$$

$$\Omega_2 = \frac{f(2)-2f(1)+f(0)}{p^2} = \frac{M^2\cdot z_{2k+i}-2M\cdot z_{k+i}}{p^2}.$$

Moreover,

$$z_{k+i} = \gamma\varepsilon^{k+i}+\gamma'\varepsilon'^{k+i}+\gamma''\varepsilon''^{k+i} \equiv N(\gamma\varepsilon^i+\gamma'\varepsilon'^i+\gamma''\varepsilon''^i) \equiv$$
$$\equiv Nz_i \equiv 0 \pmod p;$$

therefore Ω_1 is a rational integer. In view of (c3), Ω_2 belongs also to $\mathbf{Z}$. Suppose now that $\beta^3 = A\beta^2+B\beta+C$, with $A,B,C,\in\mathbf{Z}$, is the characteristic equation of the algebraic integer β. We claim that p does not divide C. Indeed, p divides C iff it divides the norm of β. But, $\varepsilon^k = N+p\lambda$ and $1+p\beta = M\varepsilon^k = MN+pM\lambda \equiv 1+pM\lambda \pmod{p^2}$, so that $\beta \equiv M\lambda$ modulo p, and since $\operatorname{Norm}(M\lambda) = M^3\operatorname{Norm}(\lambda) \not\equiv 0 \pmod p$, our claim is proved.

The formula $\Omega_{j+3} = A\Omega_{j+2}+B\Omega_{j+1}+C\Omega_j$ for every j in $\mathbf{Z}$ shows that all the Ω's are p–adic integers. Consider now $f(m)$. In view of (3) and (4), we have

$$f(m) = 0 = \Omega_0+pm\Omega_1+\sum_{j=2}^{m}p^j\binom{m}{j}\Omega_j = Mmz_{k+i}+\sum_{j=2}^{m}p^j\binom{m}{j}\Omega_j. \tag{5}$$

Suppose for the moment that $m\neq 0$ and let $p^r\|m$, $r\geq 0$. It is easy to see that

$$\operatorname{ord}_p(p^jm/j!) > j+r-j/(p-1) \quad (\geq r+2 \text{ if } j\geq 4).$$

Also, it is straightforward to check that $\operatorname{ord}_p(p^jm/j!)\geq r+2$ for $j=2,3$. Henceforth,

$$\operatorname{ord}_p\left(p^j\binom{m}{j}\right)\geq r+2 \text{ for } j\geq 2,$$

and since the Ω's are p–adic integers it follows by (5) that $\mathrm{ord}_p(Mmz_{k+i}) \geq r+2$, which is equivalent to $\mathrm{ord}_p(z_{k+i}) \geq 2$, in contrast to (c4). This contradiction proves that $m = 0$, as required.

The following table shows how we apply the above theorem for various values of D. In all these cases, it is straightforward to check the validity of conditions (c1) and (c2) (remark: to check the validity of (c1) it suffices to know λ modulo p, i.e. ε^k modulo p^2)

D	(a,b,c)	(u,v,w)	(z_0,z_1,z_2)	(U,V)	(p,k)	(N,M)	$\lambda \bmod p$
2	(0,1,0)	[1](1,1,1)	(0,1,4)	(3,3)	(3,3)	(1,1)	$2\Theta+\Theta^2$
3	(−1,1,0)	[1](4,3,2)	(0,1,11)	(12,6)	(61,60)	(1,1)	$21\Theta+20\Theta^2$
6	(2,−1,0)	[1](1,−6,3)	(0,12,42)	(3,−327)	(37,12)	(10,100)	$21\Theta+19\Theta^2$
10	(2,−1,0)	[2](1,6,−3)	(0,−12,−42)	(3,−543)	(3,1)	(1,1)	$2\Theta-\Theta^2$
25	(3,−1,0)	[3](1,2,−4/5)	$(0,-\frac{12}{5},-\frac{64}{5})$	(3,−123)	(67,22)	(1,1)	$-8\Theta-11\Theta^2$

D	$i \in I$	$z_{k+i} \bmod p^2$	$z_{2k+i} \bmod p^2$
2	0	−3	3
3	0	61	122
6	0	37	−629
10	0	−3	3
25	0	−1072	−2144

[1] : $u+v\Theta+w\Theta^2$ is a fundamental unit of both $\mathbf{Z}[\Theta]$ and $\mathbf{Q}(\Theta)$,

[2] : $u+v\Theta+w\Theta^2$ is a fundamental unit of $\mathbf{Z}[\Theta]$ but not of $\mathbf{Q}(\Theta)$,

[3] : $u+v\Theta+w\Theta^2$ is a fundamental unit of $\mathbf{Q}(\Theta)$, which does not belong to $\mathbf{Z}[\Theta]$.

As we see from this table, the conditions (c2) and (c3) are satisfied for the above values of D.

The cases $D = 1, 15, 30, 75, 150$ remain.

The case $D = 1$ is trivial:

We have to solve $x^3 - y^3 = -2$. This gives $x = -1$ and $x^3 + 2 = 1$.

Also, the case $D = 75$ does not give any solution, because in this case

$$\varepsilon = 1081 - 312\Theta + \frac{66}{5}\Theta^2 \equiv 1 \pmod 2, \quad \alpha = 22 - \Theta + \Theta^2$$

and, according to the remark preceeding the theorem, there is no n with $z_n = 0$.

In cases $D = 15, 30$ and 150 there is no element in $\mathbf{Z}[\Theta]$ with norm -2.

In general, the problem of determining a complete set of pairwise non-associated elements of an order with given norm (or of deciding that such a set is empty) can be effectively solved; see for example [Bo & Sh], ch. 2, §5.4. In the Appendix below, we describe the way we worked in our particalar case.

To summarize, to solutions of $P(x^3+2) \leq 7$ are

$$x = -3, x^3+2 = -25;\ x = -2, x^3+2 = -6;\ x = -1, x^3+2 = 1;$$
$$x = 0, x^3+2 = 2;\ x = 1, x^3+2 = 3;\ x = 2, x^3+2 = 10.$$

Thus, $P(x^3+2) \geq 11$ if $x < -3$ or $x > 2$.

References

[Bo & Sh] Z. I. BOREVICH and I. R. SHAFAREVICH, Number Theory, *Academic Press, New York*, 1967.

[Bu & Wi] J. BUCHMANN and H. C. WILLIAMS, On principal ideal testing in algebraic number fields, *J. Symbolic Comp.*, v. **4**, 1987, pp. 11–19.

[De & Fa] B. N. DELONE and D. K. FADEEV, The irrationalities of the third degree, Transl. Math. Monographs, n° **10**, *Amer. Math. Soc., Providence, R. I.*, 1964.

[Lev] W. LEVEQUE, Topics in Number Theory; v. 1, *Addison–Wesley, Reading, Mass.*, 1958.

[Mi 1] M. MIGNOTTE, Une nouvelle résolution de l'équation $x^2 + 7 = 2^n$, *Rend. del Sem. Univ. Cagliari*, v. **54**, n° 2, (1984), 41–43.

[Mi 2] M. MIGNOTTE, $P(x^2+1) \geq 17$ si $x \geq 240$, *C. R. Acad. Sci. Paris*, t. **301**, serie I, n° 13 (1985), 661–664.

[Mi 3] M. MIGNOTTE, On the automatic resolution of certain diophantine equations, *Proceedings EUROSAM 84*, Lecture Notes in Computer Sci., **174**, *Springer Verlag, Berlin* (1984), 378–385.

[Mu] M. MUREDDU, A lower bound for $P(x^4+1)$, *Ann. Fac. Sci. Toulouse;* t. **8**, série V, fasc. 2, 1986/87, 109–120.

[Na] T. NAGELL, Introduction to Number Theory, *Chelsea Publ. Co., New York*, 1964.

[Pe] A. PETHŐ, On the solution of the diophantine equation $G_n = p^z$, *Proceedings EUROCAL 85*, Lecture Notes in Computer Sci., **204**, *Springer Verlag, Berlin* (1985), 503–512.

[Pe–W] A. PETHŐ and B. M. M. de WEGER, Products of prime powers in binary recurrence sequences I: The hyperbolic case, with an application to the generalized Ramanujan–Nagell equation, *Math. Comp.*, t. **47** (1986), 713–727.

[S] C. STØRMER, Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications, *Vid. – Selsk. Skrifter. Math. Naturv. Ke*, 1897.

[W1] B. de WEGER, Products of prime powers in binary recurrence sequences II: The elliptic case, with an application to a mixed quadratic – exponential equation, *Math. Comp.*, t. **47** (1986), 729–739.

[W2] B. de WEGER, Algorithms for diophantine equations, Thesis, *Leiden*, jan. 1988.

Appendix

Searching for the integral elements of a cubic field of negative discriminant, with a given norm

Let $K = \mathbf{Q}(\Theta)$ be a cubic field with negative discriminant. For $\alpha \in K$, we denote the conjugates of α in $\mathbf{C}$ by $\alpha^{(1)} \in \mathbf{R}$, $\alpha^{(2)}, \alpha^{(3)}$. Let O be the ring of integers in K.

The following method has been used to find all elements in K of norm C (in our case $C = 2$). If $\alpha \in K$ is of norm $C \in \mathbf{Z}$, then there is a principal ideal in O of norm $|C|$. Let

$$|C| = \prod_{i=1}^{k} p_i^{n_i}$$

be the decomposition of $|C|$ into prime numbers p_i and let

$$p_i O = \prod_{j=1}^{g_i} \wp_{ij}^{c_{ij}}$$

be the decomposition of the principal ideals $p_i O$ into a power product of prime ideals of O. Let f_{ij} be the degree of the residue class field $O/\wp_{ij}$, i.e. the norm of $\wp_{ij}$ is $N\wp_{ij} = p_i^{f_{ij}}$ $(1 \le i \le k,\ 1 \le j \le g_i)$.

Since K is a cubic field, this decomposition can be obtained very easily (see [De & Fa]). It is then an easy matter to determine the finite set S of all the ideals of norm $|C|$. This is particularly easy, if $|C|$ is a prime number and in this case, S contains at most three elements.

If S is empty, then there is no element in K of norm C. Otherwise we determine the set

$$R = \left\{ \frac{1}{\mu_1} O, \ldots, \frac{1}{\mu_r} O \right\}$$

of all the reduced principal ideals of O. Here $\mu_i \in O$ for $1 \le i \le r$. For every a in S we also calculate a reduced ideal $a' = \frac{1}{\alpha} a$ in the equivalence class of a. If a is equal to $\frac{1}{\mu_i} O$ for some $i \in \{1, \ldots, r\}$ then a is principal

and $\gamma = \alpha/\mu_i$ is of norm $|C|$ and we can easily check whether $N(\gamma) = C$. The calculation of the reduced ideals is described in [Bu & Wi].

J. BUCHMANN
FB – 10 INFORMATIK
UNIVERSITÄT DES SAARLANDES
SAARBRÜCKEN 6600, R.F.A.

K. GYŐRY
MATHEMATICAL INSTITUTE
LAJOS KOSSUTH UNIVERSITY
4010 DEBRECEN, HUNGARY

M. MIGNOTTE
MATHÉMATIQUE
UNIVERSITÉ LOUIS PASTEUR
67084 STRASBOURG, FRANCE

N. TZANAKIS
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CRETE
IRAKLION, CRETE, GREECE

(Received July 31, 1989)