Conspectus materiae tomi XX, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de
la Rédaction
et de l'échange

Address of the
Editorial Board
and of the exchange

Die Adresse der
Schriftleitung und
des Austausches

Адрес редакции
и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, Warszawa 1

Les volumes IV
et suivants sont
à obtenir chez

Volumes from IV
on are available
at

Die Bände IV und
folgende sind zu
beziehen durch

Томы IV и следующие можно получить через

Ars Polona-Ruch, Krakowskie Przedmieście 7, Warszawa 1

Prix d'un fascicule

Price of an issue

Preis für ein Heft

Цена номера

$ 4.00

Les volumes I–III
sont à obtenir chez

Volumes I–III
are available at

Die Bände I–III sind
zu beziehen durch

Томы I–III можно
получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XX (1972)

Waring's problem in quadratic number fields

by

J. H. E. Cohn (London)

For each square-free integer $d \neq 1$, the algebraic integers in the field $Z(d^{1/2})$ form a ring $Z[\theta]$, with integral basis $1, \theta$ where $\theta = d^{1/2}$ if $d \equiv 2$ or $3 \pmod 4$ and $\theta = \frac{1}{2}(1+d^{1/2})$ if $d \equiv 1 \pmod 4$. For each rational integer $k \geqslant 2$, denote by J_k the set of elements of $Z[\theta]$ which can be written as a finite sum $\pm\alpha_1^k \pm \alpha_2^k \pm \ldots \pm \alpha_s^k$ with $\alpha_1, \alpha_2, \ldots, \alpha_s \in Z[\theta]$, and by P_k the set of elements which can be written similarly, but with only positive signs. Clearly P_k is a subset of J_k, and J_k is a subring of $Z[\theta]$. The object of this paper is to determine J_k and P_k, for each d and k.

We have attempted to make the paper self-contained, and this has involved specialising some results of Siegel ([2], [3]). Thus for example, Siegel has given a result corresponding to our Theorem 2, applicable to any algebraic number field. He also gives a finite number of congruence conditions modulo powers of prime ideals in the field, which together are necessary and sufficient for an element of the field to belong to J_k, and shows that all totally positive elements of J_k with sufficiently large norms also belong to P_k.

Throughout we shall refer to the case $d \equiv 2$ or $3 \pmod 4$ as Case I, and to $d \equiv 1 \pmod 4$ as Case II. For $\nu \in Z[\theta]$ we have $\nu = x+y\theta$ with $x, y \in Z$ and write $\operatorname{rat}\nu = x$, $\operatorname{ir}\nu = y$. It should be noted that in Case II, $\operatorname{ir} d^{1/2} = 2$, since then $d^{1/2} = -1+2\theta$.

In the first place we observe that $Z \subset J_k$ and since

$$k!\,\xi = -\tfrac{1}{2}(k-1)(k!)+\sum_{r=0}^{k-1}(-1)^{k-1-r}\binom{k-1}{r}(\xi+r)^k,$$

it follows that if $k! \mid \operatorname{ir}\nu$, then $\nu \in J_k$. This well-known condition is sufficient, not only for quadratic fields, but with suitable modifications in notation for all algebraic number fields, but it is not necessary; for in $Z[2^{1/2}]$ we find that $17+12\cdot 2^{1/2} = (1+2^{1/2})^4 \in J_4$. We make the

Definition. Let $w(k) = \text{g.c.d.}\{\operatorname{ir}(x+y\theta)^k \mid x, y \in Z\}$.

Lemma 1. *There exist* $\alpha, \beta \in Z[\theta]$ *with*

$$w(k) = \text{g.c.d.}\{\operatorname{ir}(\alpha^k), \operatorname{ir}(\beta^k)\}.$$

Proof. Let $\alpha \in Z[\theta]$ with $\operatorname{ir}(\alpha^k) \neq 0$. Such an α certainly exists. Let $a = w^{-1}\operatorname{ir}(\alpha^k)$. By the definition of w, if p is prime and $p^c \| w$, $c \geqslant 0$, there exist x_p, y_p such that $p^c \| \operatorname{ir}(x+y\theta)^k$ for $x, y = x_p, y_p$ and so obviously for $x, y \equiv x_p, y_p \pmod{p^{c+1}}$. Letting p range over the prime factors of a, and using the Chinese Remainder Theorem, there exist x, y such that w is the g.c.d. of aw and $\operatorname{ir}(x+y\theta)^k$.

THEOREM 1. $J_k = \{\nu \mid w(k)|\operatorname{ir}\nu\}$.

Proof. (i) It is obvious from the definition of $w(k)$ that if $w(k) \nmid \operatorname{ir}\nu$, then $\nu \notin J_k$.

(ii) Suppose that $w(k)|\operatorname{ir}\nu$. Choose α, β as in Lemma 1. Then we can find rational integers A, B such that

$$\operatorname{ir}\nu = A\operatorname{ir}(\alpha^k)+B\operatorname{ir}(\beta^k) = \operatorname{ir}(A\alpha^k+B\beta^k),$$

and so $\nu = A\alpha^k+B\beta^k+x$, where $x \in Z \subset J_k$, which concludes the proof.

THEOREM 2. *If $d < 0$, or if k is odd and $d > 0$, then $J_k = P_k$.*

Proof. If k is odd, the result is trivial since $-\alpha^k = (-\alpha)^k$. If $d < 0$, it is sufficient to prove that $-1 \in P_k$. Choose $\alpha \in Z[\theta]$ with $2\pi/3k \leqslant \arg\alpha \leqslant \pi/k$, and then α^k has negative real part. Thus $\alpha^k+\bar{\alpha}^k$ is real and negative, and so equals a negative rational integer, $-n$, say. Then

$$-1 = \alpha^k+\bar{\alpha}^k+(n-1)1^k \in P_k.$$

THEOREM 3.

$$w(k) = 2^n \prod p^l \prod q^m$$

where p runs over all odd primes with $(d|p) = -1$, $(p+1)|k$ and $l = L+1$, where $L \geqslant 0$, $p^L \| k$; q runs over all odd primes with $q|d$, $q|k$ and $m = M$ where $q^M \| k$, except that if $q = 3$, $k > 3$ and $d \equiv 6 \pmod 9$ then $m = M+1$; and n is given by

(a) *in Case* I, $n = 0$ *if k is odd,*
$= 1$ *if* $k = 2$,
$= N$ *if* $2^N \| k$, $N \geqslant 1$ *if d is even,*
$= N+1$ *if* $2^N \| k$, $N \geqslant 1$ *if d is odd,* $k > 2$;

(b) *in Case* II, $n = 0$ *if* $d \equiv 1 \pmod 8$,
$= 0$ *if* $d \equiv 5 \pmod 8$ *and* $3 \nmid k$,
$= 1$ *if* $d \equiv 5 \pmod 8$ *and* $3|k, 2 \nmid k$,
$= N+2$ *if* $d \equiv 5 \pmod 8$, $3|k$, $2^N \| k$, $N \geqslant 1$.

The proof, for Case I, is contained in the following five lemmas. For Case II, the proof is entirely similar and is omitted.

LEMMA 2. *If p is an odd prime with $(d|p) = 1$, then $p \nmid w(k)$ for any k.*

Proof. Since $(d|p) = 1$, we can find $z \in Z$ such that $z^2 \equiv d \pmod p$, and so we can find $x, y \in Z$ such that $x^2-dy^2 = Ap$, and $p \nmid A$. For, let

$z^2-d = Bp$. If $p \nmid B$, then we take $x = z$, $y = 1$. If $p|B$, then we can take $z = x$, $y = p+1$ for then

$$x^2-dy^2 = z^2-d(p+1)^2 = p(B-dp-2d) = pA, \text{ say},$$

and since $p|B$, $p \nmid d$, it follows that $p \nmid A$.

We shall show that with this choice of x and y $p \nmid \operatorname{ir}(x+y\theta)^k$. For suppose that $p|\operatorname{ir}(x+y\theta)^k$. Then in $Z[\theta]$,

$$(x+y\theta)^k \equiv (x-y\theta)^k \pmod{[p]},$$

where as usual $[p]$ denotes the principal ideal generated by p. Now the discriminant Δ of the field equals $4d$, and so $(\Delta|p) = (d|p) = 1$, from which it follows that the ideal $[p]$ factorises into distinct prime ideals $[p] = P_1P_2$. Now

$$(x+y\theta)(x-y\theta) = x^2-dy^2 = Ap \in P_1$$

and so

$$(x+y\theta)^{2k} \equiv \{(x+y\theta)(x-y\theta)\}^k \pmod{P_1} \equiv 0 \pmod{P_1}.$$

But P_1 is a prime ideal and so $(x+y\theta) \in P_1$. Similarly $(x-y\theta) \in P_1$ and so

$$Ap = (x+y\theta)(x-y\theta) \in P_1^2.$$

Similarly $Ap \in P_2^2$ and so since P_1, P_2 are distinct prime ideals, $Ap \in P_1^2P_2^2 = [p^2]$, i.e. $p^2|Ap$, which is impossible since $p \nmid A$.

LEMMA 3. *If p is an odd prime with $(d|p) = -1$, then $p|w(k)$ if and only if $(p+1)|k$.*

Proof. (i) Since $(\Delta|p) = (d|p) = -1$, it follows that $[p]$ is a prime ideal. Suppose that $p|w(k)$. Then for $z = 0, 1, 2, \ldots, p-1$, $p|\operatorname{ir}(z+\theta)^k$, i.e.

$$(z+\theta)^k \equiv (z-\theta)^k \pmod{[p]}.$$

Also $(z+\theta)(z-\theta) = z^2-d \not\equiv 0 \pmod{[p]}$ since $(d|p) = -1$. Thus $z \pm \theta \not\equiv 0 \pmod{[p]}$ and so for $z = 0, 1, \ldots, p-1$ $(z+\theta)/(z-\theta)$ all satisfy $\xi^k = 1$ in the field $F = Z[\theta]/[p]$, a finite field with p^2 elements. Also these p solutions are distinct from the solution $\xi = 1$ and from each other; for $1 = (z+\theta)/(z-\theta)$ in F would imply $z+\theta \equiv z-\theta \pmod{[p]}$, which is impossible, and

$$\frac{z+\theta}{z-\theta} = \frac{z^*+\theta}{z^*-\theta}$$

in F would imply $2\theta(z-z^*) \equiv 0 \pmod{[p]}$ and this is not the case $z \neq z^*$, for the values of z considered.

Furthermore, 1 and these p solutions of $\xi^k = 1$ in F, form a subgroup of the set of all solutions of $\xi^k = 1$ in F; for let

$$\eta = \frac{z+\theta}{z-\theta}\cdot\frac{z^*+\theta}{z^*-\theta} = \frac{(zz^*+d)+(z+z^*)\theta}{(zz^*+d)-(z+z^*)\theta}.$$

If $z+z^* \equiv 0 \pmod{p}$, then $zz^*+d \equiv -z^2+d \not\equiv 0 \pmod{p}$, since $(d|p) = -1$, and so $\eta = 1$; if $z+z^* \not\equiv 0 \pmod{p}$ then there exists a t in the set $\{0, 1, \ldots, p-1\}$ such that $t(z+z^*) \equiv (zz^*+d) \pmod{p}$, and then $\eta = (t+\theta)/(t-\theta)$.

Now the multiplicative group of the field F is a cyclic group of order p^2-1 and so the subgroup of all solutions of $\xi^k = 1$ has order (k, p^2-1). But we have seen that this subgroup itself has a subgroup of order $p+1$ and so $(p+1)|k$.

(ii) Conversely, suppose that $(p+1)|k$. Let $k = (p+1)l$. Let $(x+y\theta)^l = X+Y\theta$. Then,

$$\begin{aligned}\mathrm{ir}(x+y\theta)^k &= \mathrm{ir}(X+Y\theta)^{p+1}\\ &= (p+1)X^pY+\binom{p+1}{3}X^{p-2}Y^3d+\ldots\\ &\quad \ldots+\binom{p+1}{p-2}X^3Y^{p-2}d^{\frac12(p-3)}+(p+1)XY^pd^{\frac12(p-1)}\\ &\equiv X^pY+XY^pd^{\frac12(p-1)} \pmod{p}\\ &\equiv XY(1+d^{\frac12(p-1)}) \pmod{p}\\ &\equiv 0 \pmod{p}\end{aligned}$$

since $d^{\frac12(p-1)} \equiv -1 \pmod{p}$, since $(d|p) = -1$.

This concludes the proof.

Lemma 4. *If p is an odd prime with $(d|p) = -1, (p+1)|k$ and if $p^L\|k$, with $L \geqslant 0$, then $p^{L+1}\|w(k)$.*

Proof. Let $k = (p+1)p^Ln$, where $p \nmid n$. Let $S = p^L$. For every $x, y \in Z$, we have by the previous lemma, that if $(x+y\theta)^{(p+1)n} = X+Y\theta$, then $p|Y$. Thus

$$\begin{aligned}\mathrm{ir}(x+y\theta)^k &= \mathrm{ir}(X+Y\theta)^S\\ &= X^{S-1}YS+\binom{S}{3}X^{S-3}Y^3d+\ldots \equiv 0 \pmod{pS}\end{aligned}$$

and so $p^{L+1}|w(k)$.

On the other hand we find that

$$\begin{aligned}\mathrm{ir}(p+\theta)^k &= p^{k-1}k+\binom{k}{3}p^{k-3}d+\ldots+\binom{k}{k-3}p^3d^{\frac12k-2}+pkd^{\frac12k-1}\\ &\equiv pkd^{\frac12k-1} \pmod{p^{L+2}} \not\equiv 0 \pmod{p^{L+2}}\end{aligned}$$

and so $p^{L+2} \nmid w(k)$.

Lemma 5. *If q is an odd prime with $q|d$, then $q|w(k)$ if and only if $q|k$. If $q^M\|k$, then $q^M\|w(k)$, except that if $q = 3$, $d \equiv 6 \pmod{9}$ and $k > 3$, then $3^{M+1}\|w(k)$.*

Proof. We have, since $q|d$,

$$\mathrm{ir}(x+y\theta)^k = kx^{k-1}y+\binom{k}{3}x^{k-3}y^3d+\ldots \equiv kx^{k-1}y \pmod{q}$$

and so $q|\mathrm{ir}(x+y\theta)^k$ for all choices of $x, y \in Z$ if and only if $q|k$.

We also have if $q^M\|k$, and if $q \neq 3$, then

$$\mathrm{ir}(x+y\theta)^k \equiv kx^{k-1}y \pmod{q^{M+1}}$$

and the result follows if $q \neq 3$.

If $q = 3$, this last argument needs modification, since then $3^{M-1}\|\binom{k}{3}$. If however $9|d$, then the previous argument still works. We suppose therefore that $9 \nmid d$. Then

$$\begin{aligned}\mathrm{ir}(x+y\theta)^k &\equiv kx^{k-1}y+\binom{k}{3}x^{k-3}y^3d \pmod{3^{M+1}}\\ &\equiv kx^{k-3}y\left\{x^2+\frac{(k-1)(k-2)}{2}\cdot\frac{d}{3}y^2\right\} \pmod{3^{M+1}}\\ &\equiv kx^{k-3}y\left\{x^2+\frac{d}{3}y^2\right\} \pmod{3^{M+1}}.\end{aligned}$$

Now, if $k = 3$, and therefore $M = 1$, we see that with $x = 0, y = 1$ the right hand side is divisible by 3 but not by 9, whereas for all x, y the right hand side is divisible by 3. Thus the general result is true in this case. Moreover, if $d \equiv 3 \pmod{9}$, then for all $k, x = y = 1$ leaves the right hand side divisible only by 3^M. However if $k \neq 3$ and also $d \equiv 6 \pmod{9}$, then for all x, y the right hand side is divisible by 3^{M+1}, and so $3^{M+1}|w(k)$. However, it is easily seen that in this case, $3^{M+2} \nmid w(k)$; for

$$\mathrm{ir}(1+3\theta)^k = 3k+\binom{k}{3}3^3d+\ldots \equiv 3k \pmod{3^{M+2}}.$$

This concludes the proof.

Lemma 6. *If k is odd, then $2 \nmid w(k)$. If $2^N\|k$ with $N \geqslant 1$, then $2^N\|w(k)$ if d is even, and $2^{N+1}\|w(k)$ if d is odd, except that $w(2) = 2$.*

Proof. (i) If k is odd, then $2 \nmid w(k)$; for if d is odd then

$$\mathrm{ir}(\theta)^k = d^{\frac12(k-1)} \equiv 1 \pmod{2},$$

whereas if d is even, then

$$\mathrm{ir}(1+\theta)^k = k+\binom{k}{3}d+\binom{k}{5}d^2+\ldots \equiv 1 \pmod{2}.$$

(ii) If d is even and $2^N\|k$, with $N \geqslant 1$, then we find that

$$\mathrm{ir}(x+y\theta)^k = kx^{k-1}y+\binom{k}{3}x^{k-3}y^3d+\ldots \equiv kx^{k-1}y \pmod{2^{N+1}}$$

and so $2^N\|w(k)$.

(iii) If d is odd, consider first $w(2^n)$. We have
$$(x+y\theta)^2 = (x^2+dy^2)+2\theta xy,$$
and so clearly $w(2) = 2$.

Now define for each x, y, n
$$x_n+y_n\theta = (x+y\theta)^{2^n}.$$
Then
$$x_{n+1} = x_n^2+dy_n^2; \qquad y_{n+1} = 2x_n y_n.$$
Since d is odd, we find that for all x, y, $4\,|\,x_1y_1$; for if either x or y is even, then $4\,|\,y_1$ whereas if x, y are both odd, then both x_1 and y_1 are even. Thus $2^3\,|\,y_2$, and so by a simple induction, $2^{n+1}\,|\,y_n$ for $n \geqslant 2$. On the other hand if $x = 1$, $y = 2$ then x_1 is odd and $2^2\|y_1$. We then find that x_n is odd and $2^{n+1}\|y_n$. Thus $2^{n+1}\|w(2^n)$. Now let $k = 2^N r$ where r is odd, $r > 1$ and $N \geqslant 1$. Then,
$$\mathrm{ir}(x+y\theta)^k = \mathrm{ir}(x_N+y_N\theta)^r = rx_N^{r-1}y_N+\binom{r}{3}x_N^{r-3}y_N^3 d+\ldots$$
Now it is easily seen that if $r > 1$, 2^{N+1} divides each term on the right, even if $N = 1$. On the other hand if $x = 1$, $y = 2$ then as we have seen above, x_N is odd and $2^{N+1}\|y_N$, whence 2^{N+2} does not divide the right hand side. This concludes the proof.

Lemmas 2–6 between them prove Theorem 3 in Case I. The proof for Case II is entirely similar, and in fact only the proof of the result corresponding to Lemma 6 is essentially different. The details are omitted.

We have therefore determined J_k completely, and so in view of Theorem 2, the remaining problem is to determine P_k when $d > 0$ and k is even. In the following, we restrict our attention to Case I, as some of the details are simpler; similar results can no doubt be proved in Case II. Clearly if $\nu\in P_k$ then also $\nu'\in P_k$, where ν' denotes the conjugate of ν. Thus we consider $\nu = x+y\theta$ where $y > 0$, the case $y = 0$ being trivial. Since k is even and every element in the field is real, for $\nu\in P_k$, we must have $\nu \geqslant 0$ and $\nu' \geqslant 0$ and so we need only consider $x > y\theta > 0$. We have in fact

Lemma 7. *In Case* I, $d > 0$, *k even, $x+y\theta\in P_k$ is possible only if $x > |y|\,\theta > 0$ with $w(k)\,|\,y$ or $x \geqslant 0$, $y = 0$.*

However, these necessary conditions for $\nu\in P_k$ are not always sufficient. For consider $d = 3$, $k = 4$. Then by Theorem 3, $w = 8$. However $14+8\cdot 3^{1/2}\notin P_4$, although $14 > 8\cdot 3^{1/2} > 0$. For we find if $\alpha = x+y\cdot 3^{1/2}$, then $\alpha^4 = (x^4+18x^2y^2+9y^4)+4xy(x^2+3y^2)3^{1/2}$, and so $14+8\cdot 3^{1/2} = \sum\alpha_r^4$ would imply
$$2 = \sum x_r y_r(x_r^2+3y_r^2),$$
$$14 = \sum (x_r^4+18x_r^2y_r^2+9y_r^4),$$

and these are impossible, since if $\mathrm{ir}\,\alpha^4 \neq 0$, we must have $\mathrm{rat}\,\alpha^4 \geqslant 28$. Actually, we see without difficulty that $n+8\cdot 3^{1/2}\notin P_4$ for any $n \leqslant 180$. For if this were possible, we see that for each r, $|y_r| \leqslant 2$, since otherwise $9y_r^4 > 180$. Also if $|y_r| = 2$, then $x_r = 0$, since otherwise $\mathrm{rat}\,\alpha^4 \geqslant 1+72+144 > 180$. Therefore for all terms which contribute to the irrational part, we have $y_r = \pm 1$. Again we may show that $x_r = 1$ or 2, and so the only possible summands in such a representation of $n+8\cdot 3^{1/2}$ are
$$(1\pm 3^{1/2})^4 = 28\pm 16\cdot 3^{1/2} \quad\text{and}\quad (2\pm 3^{1/2})^4 = 97\pm 56\cdot 3^{1/2}.$$
It is now easily seen that the smallest value of n for which a representation exists is 181, given by
$$181+8\cdot 3^{1/2} = (2+3^{1/2})^4+3(1-3^{1/2})^4.$$

It is now clear that $n+8\cdot 3^{1/2}$ has a representation as the sum of fourth powers if and only if $n \geqslant 181$. This type of behaviour is not exceptional, and we prove,

Theorem 4. *In Case* I, *let $d > 0$, $2\,|\,k$ and $w(k)\,|\,y$, where $y > 0$. Then there exists a least positive integer $f(y)$, which exceeds $y\theta$, such that $x+y\theta\in P_k$ if and only if $x \geqslant f(y)$.*

Proof. It is clear that to prove the theorem, we must find one value of x for which $x+y\theta\in P_k$ for each given y, satisfying the conditions. We choose α, β as in Lemma 1, with $aw(k) = \mathrm{ir}\,\alpha^k$ and $bw(k) = \mathrm{ir}\,\beta^k$ where $(a, b) = 1$ and we may assume, taking conjugates if necessary, that both a and b are positive. Then there exist positive integers A, B such that $y/w(k) = aA-bB$. But then $y = \mathrm{ir}\{A\alpha^k+B(\beta')^k\}$, and the result follows.

It is clear that the sum of two members of P_k is again a member, which yields

Lemma 8. $f(y_1+y_2) \leqslant f(y_1)+f(y_2)$.

To proceed, let ε_1 denote the fundamental unit in $Z[\theta]$ with $\varepsilon_1 > 1$. Let $\varepsilon = \varepsilon_1^k = a+u(k)\theta$. Since k is even, $N(\varepsilon) = 1$, i.e. $\varepsilon\varepsilon' = 1$. Thus $a > u\theta > 0$. Let $2\theta p_n = \varepsilon^n-\varepsilon'^n$; $2q_n = \varepsilon^n+\varepsilon'^n$. Then $u(k)\,|\,p_n$ for each n. Also $w(k)\,|\,u(k)$, since $u(k) = \mathrm{ir}\,\varepsilon_1^k$.

We prove

Lemma 9. $f(p_n) = q_n$ *for* $n > 0$.

For, $q_n+p_n\theta = \varepsilon^n = (\varepsilon_1^n)^k\in P_k$ and so $q_n \geqslant f(p_n)$. But, $(q_n+p_n\theta)\times(q_n-p_n\theta) = \varepsilon^n\varepsilon'^n = 1$ since $N(\varepsilon) = 1$. Thus $q_n-p_n\theta < 1$, and so $f(p_n) > p_n\theta > q_n-1$, which concludes the proof.

In what follows $[x]$ denotes the greatest integer not exceeding x. We have

Theorem 5. *If $u(k)\,|\,y$, $y > 0$, then $f(y) = 1+[y\theta]$.*

Proof. Clearly $f(y) \geqslant 1+[y\theta]$. We have $u|p_n$ for every $n \geqslant 1$, and $p_1 = u$. Also since $\varepsilon\varepsilon' = 1$ and $\varepsilon+\varepsilon' = 2a$, $p_{n+2} = 2ap_{n+1}-p_n$, and so $p_{n+2} < 2ap_{n+1}$ for $n \geqslant 1$. Now suppose that $p_n \leqslant y < p_{n+1}$. Then we may write $y = A_n p_n + y_1$, where $1 \leqslant A_n \leqslant 2a-1$, and $p_n > y_1 \geqslant 0$. If $y_1 > 0$ we may proceed in like fashion until we obtain

$$y = \sum_{r=1}^{n} A_r p_r + A_0,$$

with $1 \leqslant A_n \leqslant 2a-1$, $0 \leqslant A_r \leqslant 2a-1$ for $r = 1, 2, \ldots, n-1$, and $0 \leqslant A_0 < p_1$. But $u|A_0$ since $u|y$, and u divides each p_n. But $p_1 = u$ and so it follows that $A_0 = 0$. Thus we have

$$y = \sum_{r=1}^{n} A_r p_r.$$

We then have in view of Lemma 8

$$\begin{aligned} f(y) &\leqslant \sum_{r=1}^{n} A_r f(p_r) \\ &= \sum_{r=1}^{n} A_r q_r \quad \text{by Lemma 9} \\ &= \tfrac{1}{2}\sum_{r=1}^{n} A_r(\varepsilon^r - \varepsilon'^r) + \sum_{r=1}^{n} A_r \varepsilon'^r \\ &= \theta \sum_{r=1}^{n} A_r p_r + \sum_{r=1}^{n} A_r \varepsilon'^r \\ &= y\theta + \sum_{r=1}^{n} A_r \varepsilon'^r, \end{aligned}$$

and so the proof will be complete if it can be shown that

$$\sum_{r=1}^{n} A_r \varepsilon'^r \leqslant 1.$$

Now we recall that each A_r was chosen so that if $y = \sum_{r=m+1}^{n} A_r p_r + y_{n-m}$, then $0 \leqslant y_{n-m} < p_{m+1}$. Thus for each $m = 1, 2, \ldots, n-1$ we have

$$p_{m+1} > \sum_{r=1}^{m} A_r p_r,$$

and as before $0 \leqslant A_r \leqslant 2a-1$.

But it is easily verified that

$$p_{m+1} = (2a-1)p_1 + (2a-2)\sum_{r=2}^{m-1} p_r + (2a-1)p_m,$$

and so there are three possibilities

(a) $A_1 \leqslant 2a-2$,

(b) $A_1 = 2a-1$, $A_2 = A_3 = \ldots = A_{m-1} = 2a-2$, $A_m \leqslant 2a-3$ for some $m < n$,

(c) $A_1 = 2a-1$, $A_2 = A_3 = \ldots = A_n = 2a-2$.

We consider these possibilities in turn.

$$\text{(a)}\quad -1+\sum_{r=1}^{n} A_r \varepsilon'^r < -1+(2a-1)\sum_{r=1}^{\infty} \varepsilon'^r - \varepsilon' = -1+\frac{2a-1}{\varepsilon-1}-\frac{1}{\varepsilon} = \frac{2-\varepsilon}{\varepsilon(\varepsilon-1)} < 0,$$

since $\varepsilon = a+u\theta \geqslant 1+\theta > 2$.

$$\begin{aligned} \text{(b)}\quad -1+\sum_{r=1}^{n} A_r \varepsilon'^r &< -1+\varepsilon'+(2a-2)\sum_{r=1}^{m} \varepsilon'^r - \varepsilon'^m + (2a-1)\sum_{r=m+1}^{\infty} \varepsilon'^r \\ &= -1+\varepsilon'+\frac{2a-2}{\varepsilon-1}(1-\varepsilon'^m) - \varepsilon'^m + \frac{(2a-1)\varepsilon'^m}{\varepsilon-1} \\ &= -\frac{\varepsilon'^m}{\varepsilon-1}(\varepsilon-2) < 0. \end{aligned}$$

$$\begin{aligned} \text{(c)}\quad -1+\sum_{r=1}^{n} A_r \varepsilon'^r &= -1+\varepsilon'+(2a-2)\sum_{r=1}^{n} \varepsilon'^r \\ &< -1+\varepsilon'+\frac{2a-2}{\varepsilon-1} = 0. \end{aligned}$$

This concludes the proof.

The converse of Theorem 5 is however false in general. Thus for example in $Z[3^{1/2}]$ we find that $\varepsilon_1 = 2+3^{1/2}$, $\varepsilon = 97+56\cdot 3^{1/2}$, and so $u(4) = 56$. On the other hand $5404+3120\cdot 3^{1/2} = (5+3\cdot 3^{1/2})^4$ and $56 \nmid 3120$ yet $5403 = [3120\cdot 3^{1/2}]$.

Lemma 10. *For all $y > 0$ with $w(k)|y, f(y) \leqslant y\theta+\lambda$, where λ is a constant depending only upon d and k, and not upon y.*

Proof. Since $w|y$ and $w|u$ we find unique s, t such that $y/w = s+tu/w$ with $0 \leqslant s < u/w$. Then $y = sw+tu$ and so in view of Lemmas 8 and 9, and Theorem 5, we find that

$$f(y) \leqslant f(sw)+f(ut) \leqslant f(sw)+\theta ut+1 = f(sw)-\theta sw+\theta y+1 \leqslant \lambda+\theta y,$$

where λ is the greatest value of $1+f(sw)-\theta sw$ for $s = 1, 2, \ldots, -1+u/w$, and depends only upon d and k.

Lemma 11. *For all $y > 0$ with $w(k)|y, f(y) \leqslant [(dy^2+N)^{1/2}]+1$ where N is an integer depending upon d and k only. For all sufficiently large such $y, f(y) \leqslant [y\theta]+2$.*

Proof. We observe in the first place that for any ν and rational integer r, ν and $\nu\varepsilon^r$ both belong to P_k or neither belongs to P_k, since

$\varepsilon^r = (\varepsilon_1^r)^k$. Now suppose that $\nu = x + y\theta$ where $w \mid y$ and $x > y\theta > 0$. Let $M = N(\nu) = x^2 - dy^2 > 0$. Now let $x_r + y_r\theta = (x+y\theta)\varepsilon'^r$. Then

$$2y_r\theta = (x+y\theta)\varepsilon'^r - (x-y\theta)\varepsilon^r,$$

from which it follows that $y_r > y_{r+1}$. Also as $r \to \infty$, $y_r \to -\infty$, and so we may choose r to be the largest integer for which $y_r \geqslant 0$. For brevity write $X = x_r$, $Y = y_r$. If $Y = 0$, then clearly $\nu \in P_k$. We suppose then that $Y > 0$. Since $y_{r+1} < 0$, we find that $aY < uX$, and since $M = N(\nu) = N(\nu\varepsilon^r) = X^2 - dY^2$, we find that $Y < uM^{1/2}$, $X < aM^{1/2}$. Thus

$$X - Y\theta = \frac{M}{X+Y\theta} > M^{1/2}\varepsilon',$$

and so it follows from the previous lemma, that if $M \geqslant \lambda\varepsilon^2$, then $X + Y\theta$, and hence also $x + y\theta$ belong to P_k. Thus if $N = [\lambda\varepsilon^2]+1$, $f(y) \leqslant [(dy^2+N)^{1/2}]+1$. The last part is trivial, since

$$(dy^2+N)^{1/2} = \theta y\left\{1+\frac{N}{dy^2}\right\}^{1/2} < \theta y\left\{1+\frac{N}{2dy^2}\right\} < \theta y + 1$$

for all sufficiently large y.

We see therefore that for all sufficiently large y, $f(y)$ must equal $[y\theta]+1$ or $[y\theta]+2$. It is natural to ask whether this result can be improved to exclude the latter possibility. That this is not possible in general follows from

Lemma 12. *$f(y) = [y\theta]+1$ for all sufficiently large y if and only if $f(y) = [y\theta]+1$ for all y.*

Proof. Suppose there exists $\nu = x + y\theta$ with $x > y\theta > 0$, and $w(k) \mid y$ but with $\nu \notin P_k$. Then also $\nu\varepsilon^n \notin P_k$. Let

$$X_n + Y_n\theta = \nu\varepsilon^n = (x+y\theta)(q_n + p_n\theta) = (xq_n + dyp_n) + (yq_n + xp_n)\theta.$$

Thus $Y_n \to \infty$ as $n \to \infty$, and $w(k) \mid Y_n$. Also

$$X_n - Y_n\theta = \frac{x^2 - dy^2}{X_n + Y_n\theta} \to 0 \quad \text{as} \quad n \to \infty.$$

Thus for all sufficiently large n, $X_n - Y_n\theta < 1$, that is $X_n = [Y_n\theta]+1$, yet $X_n + Y_n\theta \notin P_k$, and this proves the result.

Lemma 13. *$f(y) = [y\theta]+1$ for all $y > 0$ with $w(k) \mid y$ only in the three cases $d = 2$, $k = 2$; $d = 2$, $k = 4$; $d = 3$, $k = 2$.*

Proof. Suppose that $x = [y\theta]+1$, and that

$$x + y\theta = \sum_{r=1}^{m} \alpha_r^k = \sum_{r=1}^{m} (x_r + y_r\theta)^k.$$

Since for this y, x is minimal, it follows that for no r is x_r or y_r zero. Without loss of generality, we assume that each $x_r > 0$. Then also each $y_r > 0$, since otherwise changing the sign of y_r would increase y, and leave x unaltered. Since $x = [y\theta]+1$, this would be impossible. Now if $f(y) = [y\theta]+1$ for all y divisible by w, it follows in particular that $f(w) = [w\theta]+1$. For a representation as a sum of kth powers of $f(w) + w\theta$, it is clear that there can be only one summand, since the irrational part of each kth power is divisible by w. Then

$$w = \mathrm{ir}(X+Y\theta)^k = X^{k-1}Yk + \binom{k}{3}X^{k-3}Y^3d + \ldots \geqslant \mathrm{ir}(1+\theta)^k,$$

and so it follows that $f(w) + w\theta = (1+\theta)^k$. But then $(1-\theta)^k = f(w) - w\theta < 1$, and this can be satisfied only if $\theta < 2$, that is $d = 2$ or 3.

Consider $d = 2$. Then we have

$$w = \frac{(2^{1/2}+1)^k - (2^{1/2}-1)^k}{2\cdot 2^{1/2}} > \frac{1}{3}(2^{1/2}+1)^k. \tag{1}$$

Now suppose that there are exactly r odd primes p with $(p+1) \mid k$, with $p_1 > p_2 > \ldots > p_r$. Then $p_1 + 1 \leqslant k$, $p_2 + 1 \leqslant k/2$, $\ldots$, $p_r + 1 \leqslant k/r$, and so

$$p_1p_2\ldots p_r \leqslant (k-1)\left(\frac{k}{2}-1\right)\left(\frac{k}{3}-1\right)\ldots\left(\frac{k}{r}-1\right) \tag{2}$$

$$= \frac{(k-1)!}{r!(k-1-r)!} < 2^{k-2}.$$

Now by Theorem 3, $w(k) = 2^n \prod p^{l+1}$ where $2^n \| k$, and p runs over all primes $\equiv \pm 3 \pmod 8$ with $(p+1) \mid k$ and $p^l \| k$. Thus $w(k) \leqslant kp_1p_2\ldots p_r < k\cdot 2^{k-2}$ by (2). Thus by (1) we should have to have

$$k\cdot 2^{k-2} > \tfrac{1}{3}(1+2^{1/2})^k$$

or

$$\frac{4}{3k}\log\frac{3k}{4} > \frac{4}{3}\log\frac{1+2^{1/2}}{2}.$$

Now for $x > e$, the function $x^{-1}\log x$ is monotonically decreasing, and so since the above inequality is not satisfied for $k = 12$, it is clearly not satisfied for any greater value. Thus we need only consider $n = 2, 4, 6, 8$ and 10. We find that

$$\begin{aligned} w(2) &= 2 = \mathrm{ir}(1+2^{1/2})^2 = \mathrm{ir}\,\varepsilon = u(2), \\ w(4) &= 12 = \mathrm{ir}(1+2^{1/2})^4 = \mathrm{ir}\,\varepsilon = u(4), \\ w(6) &= 10, \quad \mathrm{ir}(1+2^{1/2})^6 > 10, \\ w(8) &= 24, \quad \mathrm{ir}(1+2^{1/2})^8 > 24, \\ w(10) &= 2, \quad \mathrm{ir}(1+2^{1/2})^{10} > 2, \end{aligned}$$

and so using Theorem 5, we see that $k = 2$ and $k = 4$ do indeed give the only k with $d = 2$.

Consider $d = 3$. We need, writing x for $f(w)$

$$x+w\cdot 3^{1/2} = (3^{1/2}+1)^k = (4+2\cdot 3^{1/2})^{k/2}, \qquad x-w\cdot 3^{1/2} = (3^{1/2}-1)^k$$

whence

$$x^2-3w^2 = 2^k.$$

Also

$$2^k(2+3^{1/2})^k = (x+w\cdot 3^{1/2})^2 = x^2+3w^2+2xw\cdot 3^{1/2}$$

and so $2^k w \mid \mathrm{ir}\, 2^k(2+3^{1/2})^k = 2xw$. Thus $x = 2^{k-1}x_1$. Thus

$$2^{2k-2}x_1^2-3w^2 = 2^k.$$

But if $k>4$, we may divide through by 2^k, and then the resulting equation is impossible modulo 8. Thus $k = 2$ or $k = 4$. But $k = 4$ can be dismissed, since $w(4) = 4$ and $\mathrm{ir}(1+3^{1/2})^4 > 4$. There remains the case $k = 2$. We find that $w(2) = 2$, $\varepsilon_1 = 2+3^{1/2}$, $\varepsilon = \varepsilon_1^2 = 7+4\cdot 3^{1/2}$, and so $u(2) = 4$. Thus Theorem 5 is only applicable for $y \equiv 0 \pmod 4$, and we shall have to verify that if y is an odd multiple of 2, then indeed $x+y\cdot 3^{1/2} \in P_2$ for each $x > y\cdot 3^{1/2}$. The proof consists of applying our previous lemmas to reduce the amount of calculation required, and then performing this.

Using Lemma 10, we see that the result is true provided $x \geqslant y\cdot 3^{1/2}+\lambda$, where $\lambda = 1+f(2)-2\cdot 3^{1/2}$, that is $\lambda = 5-2\cdot 3^{1/2}$. We then use Lemma 11, in the course of the proof of which we saw that the result is true provided

$$x^2-3y^2 > \lambda\varepsilon^2 = (5-2\cdot 3^{1/2})(7+4\cdot 3^{1/2})^2 = 297\cdot 956.$$

Thus we need only consider values of x, y with $N = x^2-3y^2 \leqslant 297$. For such x, y let

$$X+Y\cdot 3^{1/2} = (x+y\cdot 3^{1/2})\,\varepsilon'^r.$$

Then clearly, we need only show that $X+Y\cdot 3^{1/2} \in P_2$. We now choose r so that $|Y|$ is minimal. It is then easily seen, since $\varepsilon' = 7-4\cdot 3^{1/2}$ that we then get $|Y| \leqslant N^{1/2}$, and so we see that we need only verify the result for $Y = 2, 6, 10, 14$ since the values divisible by 4 are treated using Theorem 5. We find in these cases

$$[2\cdot 3^{1/2}] = 3 \quad \text{and} \quad 4+2\cdot 3^{1/2} = (1+3^{1/2})^2,$$
$$[6\cdot 3^{1/2}] = 10 \quad \text{and} \quad 11+6\cdot 3^{1/2} = (1+3^{1/2})^2+(2+3^{1/2})^2,$$
$$[10\cdot 3^{1/2}] = 17 \quad \text{and} \quad 18+10\cdot 3^{1/2} = (1+3^{1/2})^2+2(2+3^{1/2})^2,$$
$$[14\cdot 3^{1/2}] = 24 \quad \text{and} \quad 25+14\cdot 3^{1/2} = (1+3^{1/2})^2+3(2+3^{1/2})^2.$$

This completes the proof.

Combining these results, together with similar ones for Case II, details of which are omitted, we obtain finally,

THEOREM 6. *If $d>0$, k even, P_k consists of all totally positive members of J_k only in the nine cases $d = 2$, $k = 2$ or 4; $d = 3$, $k = 2$ and $d = 5$, $k = 2, 4, 6, 8, 12$ or 24. In the other cases there exists an effectively computable $N = N(d, k) > 1$, such that P_k consists of all totally positive members of J_k with norm at least N, together with some but not all of the other totally positive members of J_k.*

We have seen at the beginning of this paper that $k! \mid \mathrm{ir}\,\nu$ is a sufficient condition for $\nu \in J_k$, and so clearly $w(k)$ must be a factor of $k!$. However, we observe that $w(k)$ is far smaller that $k!$, for all but very small values of k. We prove the following result, although the constants in the actual bound are easily improved:

THEOREM 7. *For every d, $w(k) < 3k\cdot 2^k$. As $k\to\infty$, $\log w(k) = o(k^\delta)$ for every $\delta > 0$.*

Proof. In virtue of Theorem 3, we find that

$$\frac{w(k)}{k} \leqslant 12\prod p,$$

where the product is taken over odd primes, p, such that $p+1 \mid k$ and $(d\mid p) = -1$. Thus if there are exactly r such primes, with $p_1 > p_2 > \ldots > p_r$, then

$$p_1 \leqslant k-1, \qquad p_2 \leqslant \frac{k}{2}-1, \qquad \ldots, \qquad p_r \leqslant \frac{k}{r}-1.$$

Thus

$$w(k) \leqslant 12k\,\frac{(k-1)(k-2)\ldots(k-r)}{r!} = 12k\binom{k-1}{r} < 12k\cdot\frac{1}{2}\cdot 2^{k-1} = 3k\cdot 2^k.$$

To prove the second part, we observe that $r \leqslant d(k)$, where $d(k)$ denotes the number of divisors of k, and then using the well-known result that $d(k) = o(k^\varepsilon)$, we find that since $p_r \geqslant 3$, $r \leqslant \frac{1}{4}k$, and so

$$\log w(k) \leqslant \log 12+\log k+\log\binom{k-1}{d(k)}$$
$$< \log 12+\log k+d(k)\log k = o(k^\delta),$$

where ε was chosen smaller than δ.

We have not considered the question of how many kth powers might be needed to represent any element of J_k (or P_k), and we make only two observations. From Theorems 3 and 6 it follows that every element of $Z[5^{1/2}]$ is the sum of squares provided it is totally positive. Maass [1] has proved the extraordinary result that three squares always suffice, and moreover has given a formula for the number of representations as the sum of three squares. We prove, in any quadratic field a result for cubes, viz.

THEOREM 8. *Any element of J_3 can be represented by at most five cubes.*

Proof. The idea of the proof is very simple; from the two well-known identities

$$6t = (t+1)^3+(t-1)^3-2t^3,$$
$$6t+3 = t^3+(4-t)^3+(2t-5)^3+(4-2t)^3$$

we see that if $\nu \in J_3$, then ν can be represented as the sum of at most five cubes if we can find l, m such that

$$\operatorname{rat}\{\nu-(l+m\theta)^3\} \equiv 0 \pmod 3$$

and also

$$\operatorname{ir}\{\nu-(l+m\theta)^3\} \equiv 0 \pmod 6.$$

We shall show that this is always possible, but the proof is rather long in view of the many cases that arise.

Case I. (a) $3 \nmid d$. Then $w(3) = 1$. We then need to choose l, m if possible so that, since $\theta^2 = d$,

$$a \equiv l^3 \pmod 3, \qquad b \equiv 3l^2m+m^3d \pmod 6.$$

The first of these is satisfied if $l \equiv a \pmod 3$. The second requires simultaneously, $b \equiv md \pmod 3$ and $b \equiv m(l+d) \pmod 2$ and it is clear that these are consistent. Thus $a+b\theta$ can be expressed as the sum of five cubes for each a, b.

(b) $3 | d$. Then $w(3) = 3$. We then have $\nu = a+3b\theta$, and so must choose l, m if possible so that

$$a \equiv l^3 \pmod 3, \qquad b \equiv l^2m+m^3\frac{d}{3} \pmod 2,$$

and again it is clear that these can be satisfied.

Case II. (a) $d \equiv 1 \pmod{24}$. Then $w(3) = 1$. We now have

$$\theta^2 = \theta+\frac{d-1}{4} \equiv \theta \pmod 6, \quad \text{and so} \quad \theta^3 \equiv \theta^2 \equiv \theta \pmod 6.$$

Thus

$$(l+m\theta)^3 \equiv l^3+3l^2m\theta+3lm^2\theta+m^3\theta \pmod 6 \equiv l+m\theta \pmod 6$$

and so

$$a+b\theta = (a+b\theta)^3+6\xi,$$

and the result follows.

(b) $d \equiv 5 \pmod{24}$. Then $w(3) = 2$, $\nu = a+2b\theta$. Then

$$\theta^2 = \theta+\frac{d-1}{4} \equiv \theta+1 \pmod 6 \quad \text{and} \quad \theta^3 \equiv 2\theta+1 \pmod 6.$$

Thus

$$(l+m\theta)^3 \equiv l^3+3l^2m\theta+3lm^2(\theta+1)+m^3(2\theta+1) \pmod 6$$

and so we require

$$a \equiv l^3+m^3 \equiv l+m \pmod 3, \qquad b \equiv m^3 \equiv m \pmod 3$$

and it is clear that these can be satisfied simultaneously.

(c) $d \equiv 9 \pmod{24}$. Then $w(3) = 3$, $\nu = a+3b\theta$. In this case we find that

$$\theta^2 \equiv \theta+2, \qquad \theta^3 \equiv 3\theta+2 \pmod 6$$

and so

$$(l+m\theta)^3 \equiv l^3+3l^2m\theta+3lm^2(\theta+2)+m^3(3\theta+2) \pmod 6$$
$$\equiv l+2m+3m\theta \pmod 6$$

and so we require that

$$b \equiv m \pmod 2, \qquad a \equiv l+2m \pmod 3,$$

and again these are consistent.

(d) $d \equiv 13 \pmod{24}$. Then $w(3) = 2$, $\nu = a+2b\theta$. Then

$$\theta^2 \equiv \theta+3, \qquad \theta^3 = -2\theta+3 \pmod 6,$$

and we find as before that

$$(l+m\theta)^3 \equiv l-2m\theta \pmod 6,$$

and so we can have $l = a$, $m = -b$.

(e) $d \equiv 17 \pmod{24}$. Then $w(3) = 1$, $\nu = a+b\theta$. Then

$$\theta^2 \equiv \theta-2, \qquad \theta^3 = -\theta-2 \pmod 6,$$

whence

$$(l+m\theta)^3 \equiv (l-2m)-m\theta \pmod 6$$

and so we require $a \equiv l-2m \pmod 3$, $b \equiv -m \pmod 6$, and again we can find such l, m.

(f) $d \equiv 21 \pmod{24}$. Then $w(3) = 6$, $\nu = a+6b\theta$. Thus $\nu = a^3+6\xi$, and the result follows.

From the method of proof it is clear that the representation as the sum of five cubes can be carried out in infinitely many ways. This raises the question as to whether four cubes might not suffice. In some cases this is so — for example if $d = -1$ we have the ring of Gaussian integers, and in this case I have been able to find a number of identities which together show that four cubes suffice. But I have not been able to prove a similar result in general; perhaps this is not altogether surprising, since the corresponding result is unproven even in Z.

References

[1] H. Maass, *Darstellung total positiver Zahlen des Körpers $R(5^{1/2})$ als Summe von drei Quadraten*, Hamburger Abhandlungen, 14 (1941), pp. 185–191.

[2] C. L. Siegel, *Generalisation of Waring's problem to algebraic number fields*, Amer. Journ. Math. 66 (1944), pp. 122–136.

[3] — *Sums of m-th powers of algebraic integers*, Ann. of Math. (2) 46 (1945), pp. 313–339.

ROYAL HOLLOWAY COLLEGE
Englefield Green, Surrey

Received on 22. 1. 1970 (26)

ACTA ARITHMETICA
XX (1972)

Об оценке количества представлений специальным классом бинарных кубических форм положительного дискриминанта

Э. Т. Аванесов (Кисловодск)

Пусть $F(x, y) = x^3 + \sum_{i=1}^{3} a_i x^{3-i} y^i$ — неприводимая бинарная кубическая форма с целыми коэффициентами и дискриминантом D. Если $D < 0$, то задача определения всех целых решений (x, y) неопределенного уравнения

$$F(x, y) = x^3 + \sum_{i=1}^{3} a_i x^{3-i} y^i = 1 \tag{1}$$

разрешается с помощью результатов Делоне [9] и Нагелла [13]. При $D > 0$ их метод оказывается, вообще говоря, неприменимым.

На основании известных результатов Бэйкера (см. например, [4]) для возможных целых решений (x, y) уравнения (1) справедлива следующая оценка:

$$\max(|x|, |y|) < \exp(3^{1536^2} \cdot H^{41472}),$$

где

$$H = \max_i |a_i|.$$

Очевидно, применение последней оценки на конкретных примерах должно приводить к чрезвычайно большому объему вычислений, требующему использования мощной электронно-вычислительной техники (см. [5]).

В связи с этим возникает необходимость развития методов фактического определения решений или понижения оценки Бэйкера, например, для уравнения (1) в случае положительного дискриминанта.

Мы исследуем специальный класс бинарных кубических форм положительного дискриминанта

$$x^3 - mx^2y - (m+3)xy^2 - y^3 = 1, \tag{2}$$

m — произвольное целое число.

Это классическое уравнение (частным случаям его, получающимся при $m = 0$, -1 и 2, посвящены соответственно работы [12], [6] и [1])

U
B W