MATH. SCAND. 4 (1956), 95–107

ON SOME DIOPHANTINE EQUATIONS OF THE TYPE $y^2 - f^2 = x^3$

OVE HEMER

This paper contains some notes on cubic forms with negative discriminant, with applications to the special equations $y^2 - f^2 = x^3$, where $f = 11, 12, \ldots, 25$.

An equation $AU^3 + BU^2V + CUV^2 + DV^3 = M$ or more briefly

(1) $$F_1(U, V) = (A, B, C, D) = M$$

may often be shown insoluble by consideration of congruences modulo powers of some prime p (e.g. Mordell [5]), but $(A, B, C, D) \equiv M \pmod{p^k}$ for every p and k does not imply that (1) is soluble (see Skolem [9] and [10]). If $N(\mu)$ denotes the norm of μ, (1) can be looked upon as

(2) $$N(\varkappa U + \lambda V) = M$$

with some necessary conditions for solubility, above all that $\varkappa$ and λ must be integers in the ring $R(1, \alpha, \beta)$, where $F_1(\alpha, -A) = 0$ and $F_1(-D, \beta) = 0$ (see Delaunay [2]). The equation (2) can be transformed into

(3) $$N(kU + V\varrho) = m\,,$$

where k is a rational integer, $\varkappa | k$, and $m = MN(k/\varkappa)$, i.e. (1) is equivalent to

(4) $$F(u, v) = (1, P, Q, R) = m\,,$$

and we can concentrate on equations of this type.

If F has a negative discriminant, (4) can be replaced by the equations

(5) $$u + v\varrho = \mu_i \varepsilon^n\,,$$

where μ_i represents all the different, i.e. non-associated, integers in the ring $R(\varrho)$ with the norm $N(\mu_i) = m$, while ϱ is defined by $F(\varrho, -1) = 0$, and ε is the fundamental unit in $R(\varrho)$. Already Lagrange has shown that (4) can be replaced by a number of equations $G_i(w, z) = 1$, corresponding to the different solutions u_i of the congruence

(6) $$F(u, 1) \equiv 0 \pmod{m}$$

Received September 23, 1955.

(and $F(u, d) \equiv 0 \pmod{m}$, corresponding to $d|\mu_i$ in (5) if $d^3|m$). We can suppose that μ_i contains no rational integer and then a solution of (5) implies $(v, m)=1$, i.e. we have a v' such that $vv' \equiv 1 \pmod{m_i}$ and $uv' \equiv u_i \pmod{m_i}$, where m_i is the least rational integer containing μ_i, i.e. $m_i|m$. Then $(u_i+\varrho, m)=\mu_i$ and (6) is satisfied by every $u \equiv u_i \pmod{m_i}$, which gives an equation $G_i=1$. Otherwise (5) is insoluble (cf. (18) p. 106). Conversely $u_j \not\equiv u_i \pmod{m_i}$ implies $\mu_j \neq \mu_i$. We also find (no rational integer dividing μ_i or μ_j) the following

Lemma 1. *If $(\mu_i, \mu_j)=\delta \neq 1$, $N\delta=d$, then a necessary condition that both μ_i and μ_j give soluble equations* (5) *is that none of them contain ideals prime to δ but not to d.*

Proof. Suppose that $(u_i+\varrho, m)=\mu_i$ and $(u_j+\varrho, m)=\mu_j$. Let p be a prime divisor of d. Then p contains an ideal $\mathfrak{p}$ such that $\mathfrak{p}|\delta$. Suppose that p contains another ideal $\mathfrak{q}$ prime to δ but a divisor of μ_i. We get $\mathfrak{p}$ a divisor of both $(u_i+\varrho)$ and $(u_j+\varrho)$ and hence $p|(u_i-u_j)$. Since $\mathfrak{q}|(u_i+\varrho)$ and $\mathfrak{q}|p$ we further get $\mathfrak{q}|(u_j+\varrho)$, i.e. $\mathfrak{q}|\delta$. This contradiction shows that if $(u_i+\varrho, m)=\mu_i$, we cannot have $(u_j+\varrho, m)=\mu_j$, and the lemma is proved.

Lemma 1 restricts the number of equations (5). However we do not need it for the special applications in this paper.

Further the well-known theorem by Delaunay and Nagell about the number of representations of 1 by cubic forms with negative discriminant (Delaunay [1], Nagell [7], and related in Nagell [8]) immediately gives

Lemma 2. *A necessary condition that* (5) *have more than two solutions (u, v) is that there is a unit η in the corresponding field such that $t^6D(\eta)=m^2D(F)$, where $t|m$. There are never more than three solutions, except if* (5) *is equivalent to an equation $G=1$ with $D(G)=-23$, -31 or -44, in which cases there are* 5, 4 *and* 4 *solutions respectively.*

Proof. As stated above a soluble equation (5) corresponds to a single equation $G=1$.

As an example the examination of the equation $y^2-33\cdot 3^2=x^3$ (Hemer [3, p. 74]) gives $F=3\cdot(1, -1, 1, 1)=3$, corresponding to four of the nine solutions of $y^2-297=x^3$. In order to decide whether there can be a third solution of (5), it is generally more simple, however, to determine the equation $G=1$ and use the necessary condition $D(\varepsilon)=D(G)$.

If we write $\varepsilon^n=a_n\varrho^2+b_n\varrho+c_n$, (5) can be replaced by a condition

$$ta_n+sb_n+rc_n = 0, \tag{7}$$

which often may be shown impossible modulo some prime-power p^k. Below I shall give some results concerning the often occurring case $r=0$, i.e. $ta_n+sb_n=0$, but first I give a general theorem which is a generalization of lemma 7 in Hemer [4].

THEOREM 1. *Suppose* $P \leqq 1$, $R>0$ *in* (4) (*always achievable by a unimodular substitution*), $D(F)<0$ *and* $0<\varepsilon<1$. *Let* v_1 *be the least positive integer such that* $D\,(1, P, Q, R-v_1^{-3})<0$. *Then a solution of* (4) *with* $uv>0$ *implies* $0<v<v_1 m^{\frac{1}{3}}$. *If further* $uv<0$, *a solution of* (5) *with* $n<0$ *implies*

$$n > \frac{\log m - \log \mu}{\log \varepsilon} \qquad (m \text{ and } \mu \text{ positive})\,.$$

PROOF. Put $u=vz$. Then (4) gives $v^3F(z,1)=m$. The equation $F(z,1)=f(z)=0$ has only one real solution $z=-\varrho$. We get the possible $f_{\min}>v_1^{-3}$ for $z=-\frac{1}{3}P+\frac{1}{3}(P^2-3Q)^{\frac{1}{2}} \geqq 0$, and since $f(0) \geqq 1$, $uv>0$ implies that $0<v^3<v_1{}^3 m$. The case $uv=0$ is trivial and $uv<0$ gives

$$(u+v\varrho')(u+v\varrho'') = u^2+(P-\varrho)uv+\frac{R}{\varrho}v^2 > 1$$

since $\varrho>0$. Hence $u+v\varrho<m$, i.e. $\varepsilon^n\mu<m$, which proves the last part of the theorem.

Now we return to the special case $r=0$ in (7) and begin with a simple generalization of lemma 8 in Hemer [4].

LEMMA 3. *Let* $\alpha=a\varrho^2+b\varrho+c$ *be an integer in the ring* $R(\varrho)$ *and suppose that* $a\equiv b\equiv 0 \pmod{p^k}$, *p an odd prime*, $(\alpha, p)=1$, *and* $ta+sb \not\equiv 0 \pmod{p^{2k}}$; *t, s and k rational integers*, $k>0$. *Then, if* $\alpha^n=a_n\varrho^2+b_n\varrho+c_n$, $ta_n+sb_n \neq 0$ *for any* $n \neq 0$.

PROOF. Suppose

$$p^h \| n,\; h \geqq 0\,.$$

Then, if $n>0$ and $p>2$, we find modulo p^{2k+h}

$$a_n \equiv nc^{n-1}a \quad \text{and} \quad b_n \equiv nc^{n-1}b\,,$$

i.e. $ta_n+sb_n \not\equiv 0 \pmod{p^{2k+h}}$. Further $\alpha^n\alpha^{-n}=1$ gives

$$ta_{-n}+sb_{-n} \equiv -c_{-n}{}^2(ta_n+sb_n) \pmod{p^{2k+2h}}\,,$$

and the lemma is proved even for $n<0$.

Further we shall generalize a lemma by Delaunay (lemma 8a, Hemer [4]).

Lemma 4. *Suppose* $\alpha = a\varrho^2 + b\varrho + c$, *where* $F(\varrho, -1) = 0$, F *defined by* (4), *and let* p *be an odd prime, divisor of* $d^{-1}N(aP+b-a\varrho)$, *where* $d = \big(N(aP+b-a\varrho), N(sP-t-s\varrho)\big)$, *that is* $\big(F(aP+b, -a), F(sP-t, -s)\big)$, $(\alpha, p) = 1$, *and* $(t, s) = 1$. *Let further* α^r *be the least power of* α *with* $a_r \equiv 0 \pmod{p}$. *Then firstly* $p|b_r$, *and secondly* $ta_n + sb_n = 0$ *implies that* $r|n$, *i.e. lemma* 3 *may be applied to* α^r.

Proof. The equation $\alpha^n = a_n\varrho^2 + b_n\varrho + c_n$ gives

$$\alpha'^n - \alpha''^n = (\varrho' - \varrho'')\big(a_n(P-\varrho) + b_n\big),$$

i.e. $(aP+b-a\varrho)|(a_nP+b_n-a_n\varrho)$ and thus $p|a_n$ implies $p|b_n$. Also, if $ta_n = -sb_n = std_n$, we find $(aP+b-a\varrho)|d_n(sP-t-s\varrho)$ and

$$N(aP+b-a\varrho)|dd_n^3.$$

Hence $p|a_n$ and $r|n$.

If $ta_r + sb_r \equiv 0 \pmod{p^{2k}}$ for every p satisfying lemma 4, or if it is possible to show that $r|n$, we may get new values of p, if we start from α^r instead of α.

Now consider the powers of

$$\alpha^i \equiv a_i\varrho^2 + b_i\varrho + c_i \pmod{p}, \tag{8}$$

where $(\alpha, p) = 1$, and the triples $T_i = (a_i, b_i, c_i)$, where a_i, b_i and c_i assume complete systems of residues modulo p. Since there are exactly p^2 such triples with $a_i = 1$, there is always an $i \leqq p^2 + 1$ such that either $a_i = 0$ or $T_i = kT_j$, $j < i$, that is $\alpha^i \equiv k\alpha^j \pmod{p}$. In the last case suppose $i = j + r$. Then, since $(\alpha, p) = 1$, we get

$$\alpha^r \equiv k \pmod{p},$$

and since (8) is defined by a recursion formula, this implies that $a_r \equiv b_r \equiv 0 \pmod{p}$. Hence there is always an $i \leqq p^2 + 1$ such that $a_i \equiv 0 \pmod{p}$ (and an $i \leqq p^2 + p + 1$ such that $a_i \equiv b_i \equiv 0 \pmod{p}$) for every prime p.

If p is no prime in $K(\varrho)$, it is possible to find lower limits by the generalized theorem of Fermat

$$\alpha^{N(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}},$$

where $\mathfrak{p}$ is a prime ideal. If $(\alpha, \mathfrak{p}) = 1$, $\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$, and we have the following four cases:

1. $(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$, which gives $\alpha^{p-1} \equiv 1 \pmod{p}$,
2. $(p) = \mathfrak{p} \cdot \mathfrak{q}$ ($\mathfrak{q}$ a prime ideal of the second degree) and $\alpha^{p^2-1} \equiv 1 \pmod{p}$,
3. $(p) = \mathfrak{p}^3$. Since $\mathfrak{p}$ is an ideal of the first degree we always have a

rational integer h such that $\alpha \equiv h \pmod{\mathfrak{p}}$, i.e. $\alpha = h+\pi$, $\mathfrak{p}|(\pi)$, and then we find $\alpha^p = (h+\pi)^p \equiv h^p \equiv h \pmod{p}$ if $p>2$, and $\alpha^4 \equiv 1 \pmod{2}$ if $p=2$.

4. $(p) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2$. As above, putting $\alpha = a\varrho^2 + b\varrho + c$, we can suppose $\mathfrak{p}_1|(\varrho)$. (Otherwise $\varrho \equiv h \pmod{\mathfrak{p}_1}$ and we find $\varrho_1 = \varrho - h$ divisible by $\mathfrak{p}_1$). Then $\varrho^3 \equiv P\varrho^2 \pmod{p}$, $p \nmid P$ and $\alpha^p \equiv P^{p-2}(aP+b)\varrho^2 + c \pmod{p}$. In particular, if we consider the case $p|F(b+aP, -a)$, i.e. that p satisfies lemma 4, we get

$$F \equiv (b+aP)^2 b \equiv 0 \pmod{p},$$

i.e. $p|b$ or $p|(b+aP)$.

If $p|b$ then $\alpha^p \equiv a\varrho^2 + c \equiv \alpha \pmod{p}$, i.e. $\alpha^{p-1} \equiv 1 \pmod{p}$, and if $p|(b+aP)$ then $\alpha^p \equiv c \pmod{p}$.

Then the least exponent r for which $\alpha^r \equiv k \pmod{p}$ is a divisor of the exponents given above.

For the following applications to some equations $y^2 - f^2 = x^3$ we shall use the results above, and in the special case of (1)

$$(A, 0, 0, D) = M, \tag{9}$$

$M = 1$ or 3, A and D positive, the theorem by Nagell (Nagell [6] and [8]):

THEOREM 2. *The equation* (9) *has at most one solution* (u, v), $uv \neq 0$, *except in the case* $(1, 0, 0, 2) = 3$, *which has exactly the two solutions* $(1, 1)$ *and* $(-5, 4)$. *Since* (9) *belongs to the field* $K(\sqrt[3]{D/A})$, *there is only one soluble equation for each field, except for the fields* $K(\sqrt[3]{2})$ *and* $K(\sqrt[3]{20})$, *which have the three soluble equations* $(1, 0, 0, 2) = 1$ *and* 3 *and* $(1, 0, 0, 4) = 3$, *and the two equations* $(1, 0, 0, 20) = 1$ *and* $(2, 0, 0, 5) = 3$, *respectively.*

Applications.

An equation $y^2 - f^2 = x^3$ can be replaced by the "reducible" equation $(1, 0, 0, 1) = 2f$ and $\frac{1}{2}(3^r - 1)$ equations $(A, 0, 0, D) = 2fA^{-1}D^{-1}$ if $2f$ contains r different primes (see Hemer [3], theorem 2). Now I shall give the complete solutions of the equations $y^2 - f^2 = x^3$ with $f = 11, 12, \ldots, 25$.

$\boldsymbol{y^2 - 11^2 = x^3}$. Solutions (0, 11) and (12, 43).

Corresponding forms	Solutions
(1, 0, 0, 1) = 22	impossible modulo 9.
(1, 0, 0, 2) = 11	(3, −2).
(1, 0, 0, 11) = 2	no solutions.
(2, 0, 0, 11) = 1	impossible modulo 9.
(1, 0, 0, 22) = 1	(1, 0).

$(1, 0, 0, 2) = 11$. Put $\varrho^3 = 2$. Then $(3 - 2\varrho)$ is the only ideal in $K(\varrho)$ with the norm 11, and we obtain

$$u + v\varrho = (3 - 2\varrho)(\varrho - 1)^n,$$

which gives $3a_n - 2b_n = 0$. We find $n \equiv 0 \pmod 3$ and $\varepsilon^3 = -3\varrho^2 + 3\varrho + 1$, and hence by lemma 3 there is no solution with $n \neq 0$.

$(1, 0, 0, 11) = 2$. Put $\varrho^3 = 11$. The only ideal in $K(\varrho)$ with the norm 2 is not principal (the square of it is $(5 - \varrho^2)$). Hence the equation is insoluble.

$(1, 0, 0, 22) = 1$. We have $\varrho^3 = 22$ and $\varepsilon = -4\varrho^2 + 3\varrho + 23$. $F(3, 4) = 5 \cdot 7 \cdot 41$ is divisible by 5 and 7 and $\varepsilon^2 \equiv 21\varrho^2 + 1 \pmod{7^2}$. Hence $(1, 0)$ is the only solution by lemma 4.

$\boldsymbol{y^2 - 12^2 = x^3}$. Solution $(0, 12)$.

$(1, 0, 0, 1) = 24$	impossible modulo 9.
$(1, 0, 0, 2) = 12$	impossible modulo 8.
$(1, 0, 0, 3) = 8$	$(2, 0)$.
$(1, 0, 0, 6) = 4$	impossible modulo 8.
$(2, 0, 0, 3) = 4$	impossible modulo 8.

$(1, 0, 0, 3) = 8$. If $\varrho^3 = 3$, we get $(2) = (\varrho - 1)(\varrho^2 + \varrho + 1)$, i.e.

$$u + v\varrho = 2(\varrho^2 - 2)^n \tag{10}$$

and

$$u + v\varrho = (\varrho - 1)^3(\varrho^2 - 2)^n. \tag{11}$$

Since $F(0, -1) = -3$ and $\varepsilon^3 \equiv 3\varrho^2 + 1 \pmod 9$, (10) has only the solution $n = 0$ by lemma 4. In (11) we get the condition $2a_n + 3b_n - 3c_n = 0$. This implies modulo 3 that $n \equiv 0 \pmod 3$ and modulo 2 that $n \equiv 1 \pmod 3$, i.e. (11) is insoluble.

$\boldsymbol{y^2 - 13^2 = x^3}$. Solutions $(0, 13)$, $(3, 14)$ and $(78, 689)$.

$(1, 0, 0, 1) = 26$	$(3, -1)$.
$(1, 0, 0, 2) = 13$	impossible modulo 9.
$(1, 0, 0, 13) = 2$	impossible modulo 9.
$(1, 0, 0, 26) = 1$	$(1, 0)$, $(3, -1)$, and no more by theorem 2.
$(2, 0, 0, 13) = 1$	impossible modulo 9.

$\boldsymbol{y^2 - 14^2 = x^3}$. Solutions $(-3, 13)$, $(0, 14)$ and $(84, 770)$.

$(1, 0, 0, 1) = 28$ $(3, 1)$.

$(1, 0, 0, 2) = 14$, $(1, 0, 0, 7) = 4$, and $(1, 0, 0, 14) = 2$ all insoluble modulo 9.

$(1, 0, 0, 28) = 1$ $(1, 0)$, $(-3, 1)$, and no more by theorem 2.

$\boldsymbol{y^2-15^2=x^3}$. Solutions $(-6, 3)$, $(-5, 10)$, $(0, 15)$, $(4, 17)$, $(6, 21)$, $(10, 35)$, $(15, 60)$, $(30, 165)$, $(60, 465)$, $(180, 2415)$, $(336, 6159)$, $(351, 6576)$ and $(720114, 611085363)$.

$(1, 0, 0, 1)$	$= 30$	impossible modulo 9.
$(1, 0, 0, 2)$	$= 15$	$(-1, 2)$.
$(1, 0, 0, 3)$	$= 10$	$(13, -9)$.
$(1, 0, 0, 5)$	$= 6$	$(1, 1)$.
$(1, 0, 0, 6)$	$= 5$	$(-1, 1)$ and $(467, -257)$.
$(2, 0, 0, 3)$	$= 5$	$(1, 1)$ and $(-8, 7)$.
$(1, 0, 0, 10)$	$= 3$	impossible modulo 9.
$(2, 0, 0, 5)$	$= 3$	$(-1, 1)$ and no more by theorem 2.
$(1, 0, 0, 15)$	$= 2$	no solutions.
$(3, 0, 0, 5)$	$= 2$	$(-1, 1)$.
$(1, 0, 0, 30)$	$= 1$	$(1, 0)$ and no more by theorem 2, since $(9, 0, 0, 10)=1$ is soluble.
$(2, 0, 0, 15)$	$= 1$	$(2, -1)$ and no more by theorem 2.
$(3, 0, 0, 10)$	$= 1$	$(3, -2)$ and no more by theorem 2.
$(5, 0, 0, 6)$	$= 1$	$(-1, 1)$ and no more by theorem 2.

$(1, 0, 0, 2)=15$. We have $\varrho^3=2$. Since $(3)=(\varrho+1)^3$ and only one ideal exists with the norm 5, we only get

$$u+v\varrho = (2\varrho-1)(\varrho-1)^n$$

with the condition $2b_n-a_n=0$. We find $3|n$ and $\varepsilon^3\equiv 1 \pmod 3$, but lemma 3 fails. The corresponding equation $G=1$ is $(1, 6, 0, 18)=1$ with the fundamental unit $\eta=3\theta^2-12\theta-47$, and now lemma 3 can be used.

$(1, 0, 0, 3)=10$. We have $\varrho^3=3$ and, since there is only one ideal in $K(\varrho)$ with the norm 2 and one with the norm 5, we get

$$u+v\varrho = (\varrho^2+1)(\varrho^2-2)^n$$

with the condition $a_n+c_n=0$. We find $n\equiv 2 \pmod 3$ and a solution $n=2$. By theorem 1 we have $n>0$. Putting $n=2+3^r n_1$, $3\nmid n_1$, we get $a_n+c_n\equiv \pm 3^r \pmod{3^{r+1}}$, and there are no other solutions.

$(1, 0, 0, 5)=6$. We have $\varrho^3=5$, $(3)=(2-\varrho)^3$ and only one ideal in $K(\varrho)$ with the norm 2. Then we obtain

$$u+v\varrho = (\varrho+1)(2\varrho^2-4\varrho+1)^n$$

with the condition $a_n+b_n=0$. By lemma 4 we get $p=13$ and, since $\varepsilon^4\equiv -4 \pmod{13}$ and $a_4+b_4\equiv -39 \pmod{13^2}$, there is no solution for $n\neq 0$.

$(1, 0, 0, 6)=5$. We have $\varrho^3=6$, and, since (5) contains only one prime of the first degree, we get

$$u+v\varrho = (\varrho-1)(3\varrho^2-6\varrho+1)^n$$

with the condition $-a_n+b_n=0$. We obtain solutions for $n=0$ and 2, and by lemma 2 there is no further solution. This may be stated more easily by the equivalent equation $(1, 0, -18, 42)=1$, which has the fundamental unit $\eta=42\theta-215=\varepsilon^2$.

$(2, 0, 0, 3)=5$. This can be replaced by $(1, 0, 18, 6)=1$ with $\varepsilon=-3\theta+1$, and hence there are only two solutions by lemma 2.

$(1, 0, 0, 15)=2$. We have $\varrho^3=15$. The only ideal with the norm 2 is not principal (the square of it is $\varrho^2+2\varrho-11$), and the equation is insoluble.

$(3, 0, 0, 5)=2$. This can be replaced by $(1, 12, 3, 4)=1$ with

$$\varepsilon = 189\theta^2-2391\theta+1951 .$$

Lemma 4 is satisfied by $p=37$. Since $\varepsilon^{12}\equiv -11 \pmod{37}$ and

$$a_{12} \equiv 16\cdot 37 \pmod{37^2} ,$$

there is no solution with $n \neq 0$.

13 solutions might be the greatest number stated for any equation $y^2-k=x^3$, and the solution (720114, 611085363) is probably the greatest one pointed out to any equation stated previously.

$y^2-16^2=x^3$. Solution (0, 16).

$(1, 0, 0, 1) = 32$	impossible modulo 9.
$(1, 0, 0, 2) = 16$	(0, 2).

$(1, 0, 0, 2)=16$. This can be replaced by $(1, 0, 0, 4)=1$ with $\varrho^3=2$, which gives

$$u+v\varrho^2 = (\varrho-1)^n ,$$

i.e. $b_n=0$. We find $3|n$, $\varepsilon^3\equiv 1 \pmod 3$, and $b_3=3$, and there is no solution with $n\neq 0$ by lemma 3.

$y^2-17^2=x^3$. Solutions $(-4, 15)$, $(0, 17)$ and $(68, 561)$.

$(1, 0, 0, 1) = 34$	no solutions.
$(1, 0, 0, 2) = 17$	(1, 2).
$(1, 0, 0, 17) = 2$	no solutions.
$(1, 0, 0, 34) = 1$	(1, 0).
$(2, 0, 0, 17) = 1$	$(-2, 1)$ and no more by theorem 2.

$(1, 0, 0, 2)=17$. We have $\varrho^3=2$ and $(17)=(2\varrho+1)(4\varrho^2-2\varrho+1)$, and this gives

$$u+v\varrho = (2\varrho+1)(\varrho-1)^n$$

with the condition $a_n+2b_n=0$. Modulo 5 we find $8|n$ and

$$\varepsilon^8 = -80\varrho^2+100\varrho+1 ,$$

i.e. there are no solutions with $n \neq 0$ by lemma 3.

(1, 0, 0, 17) = 2. We have $\varrho^3=17$ and $\varepsilon=-7\varrho+18$, and (2) contains only one prime of the first degree, $\frac{1}{3}(\varrho^2+2\varrho+7)$, which does not belong to the ring $R(\varrho)$. Hence there are no solutions to the equation.

(1, 0, 0, 34) = 1. We have $\varrho^3=34$ and $\varepsilon=-51\varrho^2-24\varrho+613$, i.e. there is no more solution by lemma 3.

$y^2-18^2=x^3$. Solution (0, 18).

(1, 0, 0, 1) = 36 no solution.

(1, 0, 0, 4) = 9, (1, 0, 0, 9) = 4, and (4, 0, 0, 9) = 1 all impossible modulo 9.

(1, 0, 0, 36) = 1 (1, 0).

(1, 0, 0, 36) = 1. We have $\varrho^3=6$, and $\varepsilon=3\varrho^2-6\varrho+1$, and this gives

$$u+v\varrho^2 = (3\varrho^2-6\varrho+1)^n$$

with the condition $b_n=0$, which is impossible for $n \neq 0$ by lemma 3.

$y^2-19^2=x^3$. Solution (0, 19).

(1, 0, 0, 1) = 38 no solution.

(1, 0, 0, 2) = 19, (1, 0, 0, 19) = 2, and (2, 0, 0, 19) = 1 all impossible modulo 19.

(1, 0, 0, 38) = 1 (1, 0).

(1, 0, 0, 38) = 1. We have $\varrho^3=38$, $\varepsilon=-3\varrho^2+55\varrho-151$ and $13|F(55, 3)$. Since $\varepsilon^4 \equiv 1 \pmod{13}$ and $a_4 \equiv 6\cdot 13 \pmod{13^2}$, there is no further solution by lemma 4.

$y^2-20^2=x^3$. Solution (0, 20).

(1, 0, 0, 1) = 40 impossible modulo 9.

(1, 0, 0, 2) = 20, (1, 0, 0, 10) = 4 and (2, 0, 0, 5) = 4 all impossible modulo 8.

(1, 0, 0, 5) = 8 (2, 0).

(1, 0, 0, 5) = 8. We have $\varrho^3=5$ and only one ideal exists with the norm 2. We obtain

$$u+v\varrho = 2(2\varrho^2-4\varrho+1)^n \tag{12}$$

and

$$u+v\varrho = (\varrho^2+\varrho+2)(2\varrho^2-4\varrho+1)^n . \tag{13}$$

In (12) we get the condition $a_n=0$ and, by lemma 4, $n=0$ is the only solution since $13 \mid F(-4, -2)$, $\varepsilon^4 \equiv -4 \pmod{13}$, and $a_4 \equiv 26 \pmod{13^2}$. In (13) we have the condition $2a_n+b_n+c_n=0$, which is impossible since $\varepsilon \equiv 1 \pmod 2$.

$\boldsymbol{y^2-21^2=x^3}$. Solutions $(-6, 15)$, $(0, 21)$, $(7, 28)$ and $(42, 273)$.

$(1, 0, 0, 1) = 42$ impossible modulo 9.

$(1, 0, 0, 2) = 21$, $(1, 0, 0, 3) = 14$, $(2, 0, 0, 3) = 7$, $(1, 0, 0, 14) = 3$, $(2, 0, 0, 7) = 3$, $(1, 0, 0, 21) = 2$, $(3, 0, 0, 7) = 2$, $(2, 0, 0, 21) = 1$, and $(3, 0, 0, 14) = 1$ all impossible modulo 7.

$(1, 0, 0, 6) = 7$ $(1, 1)$.

$(1, 0, 0, 7) = 6$ $(-1, 1)$.

$(1, 0, 0, 42) = 1$ $(1, 0)$, and no more by theorem 2 since $(49, 0, 0, 6)=1$ is soluble.

$(7, 0, 0, 6) = 1$ $(1, -1)$, and no more by theorem 2.

$(1, 0, 0, 6)=7$. Then $\varrho^3=6$, and we get

$$u+v\varrho = (\varrho+1)(3\varrho^2-6\varrho+1)^n, \tag{14}$$

$$u+v\varrho = (2\varrho^2+4\varrho+7)(3\varrho^2-6\varrho+1)^n \tag{15}$$

and

$$u+v\varrho = (\varrho^2+\varrho-5)(3\varrho^2-6\varrho+1)^n. \tag{16}$$

Equation (14) gives $a_n+b_n=0$, and this has the only solution $n=0$ by lemma 3. In (15) we get the condition $7a_n+4b_n+2c_n=0$ and in (16) $-5a_n+b_n+c_n=0$, both of which are impossible modulo 3.

$(1, 0, 0, 7)=6$. Then $\varrho^3=7$ and we only get

$$u+v\varrho = (\varrho-1)(2-\varrho)^n$$

with the condition $-a_n+b_n=0$. Modulo 3 we find $3 \mid n$ and

$$\varepsilon^3 = 6\varrho^2-12\varrho+1 .$$

Since $5 \mid F(-12, -6)$, $\varepsilon^{12} \equiv 1 \pmod 5$, and $-a_{12}+b_{12} \equiv 10 \pmod{25}$, there are no more solutions by lemma 4.

$\boldsymbol{y^2-22^2=x^3}$. Solution $(0, 22)$.

$(1, 0, 0, 1) = 44$ no solution.

$(1, 0, 0, 4) = 11$, $(1, 0, 0, 11) = 4$, and $(4, 0, 0, 11) = 1$ all impossible modulo 9.

$(1, 0, 0, 44) = 1$ $(1, 0)$.

$(1, 0, 0, 44)=1$. Then $\varrho^3=44$, but the field is defined by the form

(1, 5, 1, 3) with the corresponding fundamental unit $\eta = 5\theta^2 - 37\theta + 61$, where $\theta^3 - 5\theta^2 + \theta - 3 = 0$. In $R(\varrho)$ we get $\varepsilon = \eta^2 = -213\varrho^2 + 303\varrho + 1585$ and there is, according to lemma 3, no further solution.

$y^2 - 23^2 = x^3$. Solution (0, 23).

(1, 0, 0, 1) = 46 no solution.

(1, 0, 0, 2) = 23, (1, 0, 0, 23) = 2 and (2, 0, 0, 23) = 1 all impossible modulo 9.

(1, 0, 0, 46) = 1 (1, 0).

(1, 0, 0, 46) = 1. We have $\varrho^3 = 46$ and $\varepsilon = 309\varrho^2 + 48\varrho - 4139$, i.e. no further solution by lemma 3.

$y^2 - 24^2 = x^3$. Solutions (−8, 8), (0, 24) and (160, 2024).

(1, 0, 0, 1) = 48, (1, 0, 0, 3) = 16 and (2, 0, 0, 3) = 8 all impossible modulo 9.

(1, 0, 0, 2) = 24 (2, 2) and (−10, 8).

(1, 0, 0, 6) = 8 (2, 0).

(1, 0, 0, 2) = 24. Then $\varrho^3 = 2$ and, since (2) and (3) are cubes, we only get

$$u + v\varrho = 2(\varrho + 1)(\varrho - 1)^n$$

corresponding to the equation (1, 0, 0, 2) = 3, which occurred as an exception in theorem 2.

(1, 0, 0, 6) = 8. Then $\varrho^3 = 6$ and (2) a cube gives

$$u + v\varrho = 2(3\varrho^2 - 6\varrho + 1)^n,$$

and there is no further solution by lemma 3.

$y^2 - 25^2 = x^3$. Solutions (0, 25), (6, 29) and (75, 650).

(1, 0, 0, 1)	= 50 and (1, 0, 0, 10) = 5	both impossible modulo 9.
(1, 0, 0, 2)	= 25	(3, −1).
(1, 0, 0, 5)	= 10	(−5, 3).
(1, 0, 0, 50)	= 1	(1, 0), and no more by theorem 2, last part.

(1, 0, 0, 2) = 25. We have $\varrho^3 = 2$ and $5 = (\varrho^2 + 1)(-\varrho^2 + 2\varrho + 1)$, where $(\varrho - 1)(\varrho^2 + 1)^2 = 3 - \varrho$ and $(-\varrho^2 + 2\varrho + 1)$ is a prime of the second degree. We get

$$u + v\varrho = (3 - \varrho)(\varrho - 1)^n \tag{17}$$

with the condition $3a_n - b_n = 0$, and

$$(18) \qquad u+v\varrho = (-\varrho^2+2\varrho+1)(\varrho-1)^n$$

with the condition $a_n+2b_n-c_n=0$. In (17) we find $3|n$ and

$$3a_3-b_3 \equiv -3 \pmod 9 ,$$

i.e. $n=0$ gives the only solution by lemma 3. Further $\varepsilon^8\equiv 1 \pmod 5$, and (18) is impossible modulo 5, as is shown by examining n modulo 8. As stated in this paper just before lemma 1, we also find (18) impossible since the congruence (6), i.e. $u^3+2\equiv 0 \pmod{25}$, is satisfied by $u\equiv -3 \pmod{25}$, but not otherwise modulo 5, though $-\varrho^2+2\varrho+1$ is a divisor of 5.

$(1, 0, 0, 5)=10$. Then $\varrho^3=5$, and we only get

$$u+v\varrho = (3\varrho-5)(2\varrho^2-4\varrho+1)^n$$

with the condition $-5a_n+3b_n=0$. Since $13|F(4, 2)$, but $13\nmid F(5, -3)$, $\varepsilon^4\equiv -4 \pmod{13}$ and $-5a_4+3b_4\equiv 13 \pmod{13^2}$, $n=0$ gives the only solution by lemma 4.

Finally I will complete my dissertation (Hemer [3]), in the case $y^2-6^2=x^3$, the equation $(1, 0, 0, 3)=4$ (p. 28) by

$$u+v\varrho = (\varrho^2+\varrho+1)(\varrho^2-2)^n, \qquad a_n+b_n+c_n = 0 ,$$

and in the case $y^2-10^2=x^3$, the equation $(1, 0, 0, 5)=4$ (p. 31) by

$$u+v\varrho = (3\varrho^2+5\varrho+9)(2\varrho^2-4\varrho+1)^n, \qquad 9a_n+5b_n+3c_n = 0 ,$$

and these relations are both impossible modulo 2.

BIBLIOGRAPHY

1. B. Delaunay, *Sur le nombre des représentations d'un nombre par une forme cubique binaire à discriminant négatif*, C. R. Acad. Sci. Paris 171 (1920), 336–338.
2. B. Delaunay, *Über den Algorithmus der Erhöhung*, J. Soc. Phys. Math. Léningrade 1 (1927), 257–267.
3. O. Hemer, *On the Diophantine equation $y^2-k=x^3$*, Dissertation, Uppsala, 1952.
4. O. Hemer, *Notes on the Diophantine equation $y^2-k=x^3$*, Ark. Mat. 3 (1954), 67–77.
5. L. J. Mordell, *The Diophantine equation $y^2-k=x^3$*, Proc. London Math. Soc. 13 (1913), 60–80.
6. T. Nagell, *Solution complète de quelques équations cubiques à deux indéterminées*, J. Math. Pures Appl. (9), 4 (1925), 209–270.
7. T. Nagell, *Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante*, Math. Z. 28 (1928), 10–29.
8. T. Nagell, *L'analyse indéterminée de degré supérieur*, Mémor. Sci. Math. 39 (1929), 1–63.

9. Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen,* Avh. Norske Vid. Akad. Oslo, I, Mat.-Naturv. Klasse, 1937, No. 12, 1–16.
10. Th. Skolem, *Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist,* Avh. Norske Vid. Akad. Oslo, I, Mat.-Naturv. Klasse, 1942, No. 4, 1–28.

LINKÖPING, SWEDEN