ARKIV FÖR MATEMATIK Band 3 nr 3

Communicated 9 September 1953 by T. Nagell and Otto Frostman

Notes on the Diophantine equation $y^2 - k = x^3$

By Ove Hemer

The purpose of this article is to give some corrections and additions to my dissertation "On the Diophantine equation $y^2 - k = x^3$" (Uppsala 1952). In the following I denote that paper by H and refer to the bibliography given there as e.g. (H, [4]). In fact I have succeeded in solving all the equations with $0 < k \leq 100$.

The problem of solving an equation $y^2 - k = x^3$ is equivalent to solving a finite number of equations $(a, b, c, d) = 1$, where (a, b, c, d) is a binary cubic form. To be short I name this form soluble and (u, v) a solution of the form, if there is any integer solution (u, v) of $(a, b, c, d) = 1$. In the first part of H it is shown how to determine those equations and further their solubility is discussed. A soluble form may be written

$$F(u, v) = u^3 + p u^2 v + q u v^2 + r v^3 = (1, p, q, r) \tag{1}$$

and corresponds to a cubic ring $R(\theta)$, where

$$F(\theta, -1) = \theta^3 - p\theta^2 + q\theta - r = 0. \tag{2}$$

If $k > 0$, the form $F(u, v)$ has always a negative discriminant. Then every integer solution of (1) corresponds to a unit of the type

$$\varepsilon^n = u + v\theta \tag{3}$$

and vice versa, where ε is the fundamental unit of the ring $R(\theta)$. Hence the decisive question is to determine all such units (3).

If $0 < \varepsilon < 1$, the case $n < 0$ can easily be examined by H, Lemma 7, p. 25. This lemma was inserted a short time before the printing and hence it is not applied all through. Further, for want of space, the proof was too short. Hence I repeat the lemma here with a detailed proof:

Lemma 7. *A soluble irreducible form can always by a unimodular substitution be written $F(u, v) = (1, p, q, r)$, where $p \leq 1$ and $r > 0$. Suppose $D(F) < 0$ and $0 < \varepsilon < 1$, where ε is the fundamental unit in the corresponding cubic ring. Then, if v_1 and v_2 are positive integers and if $D\left(1, p, q, r - \frac{1}{v_1^3}\right)$ and $D\left(1, p, q, r + \frac{1}{v_2^3}\right)$*

are negative, a solution of (3) *with* $n<0$ *implies that* $-v_2<v<v_1$. *If specially* $p=0$, $n<0$ *implies that* $0<v<3\cdot\sqrt[3]{\frac{2r}{|D(F)|}}$ $\left(\textit{or, if } D(F)=-108k,\ 0<v<\sqrt[3]{\frac{r}{2k}}\right)\cdot$

Proof. Consider $D(r)=p^2q^2-4q^3+(18pq-4p^3)r-27r^2$ as a function of r. Then $p\leq 1$, $r>0$, $D(r)<0$, $D\left(r-\frac{1}{v_1^3}\right)<0$ implies $D(r-t)<0$, if $0<t<\frac{1}{v_1^3}\cdot$ This is immediately clear, if we get $D_{\max}$ for $r\leq 0$, i.e. $9pq-2p^3\leq 0$, or if $D(0)\geq 0$, i.e. $p^2q^2-4q^3\geq 0$. Then we have to examine $q>\frac{p^2}{4}>0$, but $p<0$ gives $9pq-$ $-2p^3<0$ and $p=1$, $q\geq 1$ gives $D_{\max}<0$. Since $\theta>0$ is defined by $F(\theta,-1)=0$, we then have $uv\leq 0$ for $v\geq v_1$. The case $uv=0$, $r=1$, $v=v_1=1$ corresponds to no solution of (3) with $n<0$, by *H*, Lemma 6 (NAGELL *H*, [3], Hilfssatz III). Hence we can suppose $uv<0$, if $v\leq -v_2$ or $v\geq v_1$ (the case $v\leq -v_2$ may be treated analogously). Then

$$(u+v\theta')(u+v\theta'')=u^2+(p-\theta)\cdot uv+\frac{r}{\theta}\cdot v^2>1$$

$\left(\text{since } \frac{1}{\theta}-\left(\frac{1-\theta}{2}\right)^2>1, \text{ if } 0<\theta<1\right)$. Hence $\varepsilon^n=u+v\theta<1$, i.e. $n>0$. The special result for $p=0$ follows immediately from the expression of $D(F)$.

By the examination of (3) for $n>0$ in the special cases I have sometimes used an incorrect "method". Suppose $\varepsilon^n=a_n\theta^2+b_n\theta+c_n$ and $a_n\equiv 0 \pmod{p^m}$, p a rational prime. Then a substitution $\theta=A\varphi+B$, $(p,A)=1$, gives $\varepsilon^n=$ $=a_n'\varphi^2+b_n'\varphi+c_n'$, where a_n and a_n' are divisible by the same power of p. Hence congruence conditions for n satisfying $a_n'\equiv 0 \pmod{p^m}$ cannot contradict the corresponding conditions for n satisfying $a_n\equiv 0 \pmod{p^m}$. The following faults in *H* result from this mistake:

$\boldsymbol{y^2-40=x^3}$, the form $(1,0,-18,32)$, p. 63, line 4, B.

$\boldsymbol{y^2-44=x^3}$, the form $(1,3,-12,12)$, p. 64, the last 7 lines. Further the relation (3), p. 63, shall be $\varepsilon^3+213\varepsilon^2+14283\varepsilon-1=0$.

$\boldsymbol{y^2-19=x^3}$, the form $(1,0,-15,24)$, p. 72, (4').

$\boldsymbol{y^2-37=x^3}$, the form $(1,0,-9,16)$, p. 77, at the bottom of the page. The relation (5), p. 77, shall be $\varepsilon^3+921\varepsilon^2+271191\varepsilon-1=0$. Further on p. 77, line 19, we shall have the factorizations $(\alpha)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}$ and $(1-\alpha)=\mathfrak{p}^2$ instead of $(\alpha)=\mathfrak{p}^2\mathfrak{q}$ and $(1-\alpha)=\mathfrak{p}_1\mathfrak{p}_2$. This gives wrongly $(2,-3,6,3)=1$ insoluble, though there is the solution $(2,-5)$, i.e. the form is equivalent to $(1,45,-54,16)$ and the equation has the further solution $(243,\pm 3788)$.

Further errors of calculation give the following faults:

$\boldsymbol{y^2-8=x^3}$, the form $(1,0,-6,8)$, p. 37, line 17. There is a third duadic solution but, as we shall see below, no more integer solution.

$\boldsymbol{y^2-28=x^3}$, the form $(1,0,-6,12)$, p. 56. The relation (8) shall be $b_{k+31}\equiv$ $\equiv b_k \pmod 5$ and then the conclusion is invalid.

Below we shall treat all the named forms definitely.

Finally, on p. 42, line 17, $\gamma = \mathfrak{p}_1$ is a misprint. It shall be $\lambda = \mathfrak{p}_1$. On p. 60, line 13, λ and μ shall change places. A small number of such errors in the tables shall be corrected in the tables in this article.

By the following examinations we very often use results of Delaunay and Nagell connected with H, Lemma 8 and mentioned on p. 27. I repeat Lemma 8 and give the other results more explicitly as Lemma 8 a and 8 b.

Lemma 8. *Let α be an integer (not necessarily a unit) in $R(\theta)$ and suppose that*

$$\alpha = a p \varphi^2 + b p \varphi + c,$$

where p is an odd prime, $\varphi = p^t \theta$, $t \geq 0$, $(\alpha, p) = 1$ and $(a, p) = 1$. Then no power α^m (m positive or negative) can be a binom $A\theta + B$.

Proof. If $m > 0$, the coefficient for φ^2 in α^m is

$$m \cdot c^{m-1} \cdot p \cdot a + \sum_{i=2}^{i=m} \binom{m}{i} \cdot c^{m-i} \cdot p^i \cdot A_i,$$

where A_i are rational integers. If $p > 2$, every term in the sum contains a higher power of p than the first term and hence the coefficient cannot be 0. Since $(c, p) = 1$, $\alpha \cdot \alpha^{-1} = 1$ gives $\alpha^{-1} = a' p \varphi^2 + b' p \varphi + c'$, where $(a', p) = 1$, an hence the lemma is proved even for $m < 0$.

Lemma 8 a. *Let $F(u, v) = (1, P, Q, R) = 1$, $F(\theta, -1) = 0$ and $\varepsilon = a\theta^2 + b\theta + c$ the fundamental unit of $R(\theta)$, $(a, b) = d$. Let further p be an odd prime, divisor of $k = \dfrac{N(-a\theta + b + aP)}{d^2}$, and $\varepsilon^m = a_m \theta^2 + b_m \theta + c_m$ be the least power of ε, where $a_m \equiv b_m \equiv 0 \pmod{p}$. Then, if $a_m \not\equiv 0 \pmod{p^2}$, the relation $\varepsilon^n = u + v\theta$ is impossible for $n \neq 0$.*

If $P = 0$, we get $N(-a\theta + b) = F(b, -a)$, i.e. $k = \dfrac{F(b, -a)}{d^2}$.

Proof. $\varepsilon^n = u + v\theta$ gives immediately

$$\varepsilon'^n - \varepsilon''^n = (\theta' - \theta'') \cdot v,$$

i.e. v must be divisible by $\dfrac{\varepsilon' - \varepsilon''}{\theta' - \theta''} = -a\theta + b + aP$, and this proves the lemma by Lemma 8, since n must be a multiple of m.

If $\varepsilon = c \pm \theta$, we get $k = \pm 1$, but then we can write (3)

$$\varepsilon^n = u + v\varepsilon.$$

Then n even implies $N(\varepsilon' + \varepsilon'')/v$ and, since $\varepsilon^{n-1} = u \cdot \varepsilon^{-1} + v$, n odd implies $N(\varepsilon' + \varepsilon'')/u$. We have

Lemma 8 b. *Let ε be a unit in a cubic ring and let the odd prime p be a divisor of $N(\varepsilon' + \varepsilon'')$. Suppose further that $\varepsilon^m = a_m \varepsilon^2 + b_m \varepsilon + c_m$ is the least power* *of* ε *with* $m > 0$, *where* $a_m \equiv b_m \equiv 0$ *(mod* p*). Then* $\varepsilon^n = u + v\varepsilon$ *has no even solution except* $n = 0$, *if* $a_m \not\equiv 0$ *(mod* p^2*), and no odd solution except* $n = 1$, *if* $c_{m+2} \not\equiv 0$ *(mod* p^2*).*

Proof. Denote $\varepsilon^{-m} = A\varepsilon^{-2} + B\varepsilon^{-1} + C$. Then

$$\varepsilon^m \varepsilon^{-m} = 1 \equiv c_m A \varepsilon^{-2} + c_m B \varepsilon^{-1} + c_m C \pmod{p},$$

i.e $A \equiv B \equiv 0$ (mod p) and hence, as proved by Lemma 8,

$$c_{m+2} \equiv b_{m+2} \equiv 0 \pmod{p}$$

since $\varepsilon^m = c_{m+2}\varepsilon^{-2} + b_{m+2}\varepsilon^{-1} + a_{m+2}$. Conversely $c_{m+2} \equiv b_{m+2} \equiv 0$ implies $a_m \equiv b_m \equiv 0$ (mod p). Then the result follows from Lemma 8.

By examining the special cases I begin with the forms mentioned above and then go on with the incompletely treated forms, occurring in the remaining cases $0 < k < 100$.

$\boldsymbol{y^2 - 8 = x^3}$. $\mathbf{(1, 0, -6, 8) = 1}$ (H, p. 33, (3)). The form is equivalent to (1, 9, 21, 1), i.e. $\varepsilon^3 = 9\varepsilon^2 - 21\varepsilon + 1$. We get $N(\varepsilon' + \varepsilon'') = N(9 - \varepsilon) = 4 \cdot 47$. By Lemma 8 b we find $p = 47$, $m = 92$, $a_{92} \equiv 940$ and $c_{94} \equiv 1081$ (mod 47^2). Then the form has only two solutions. (This result is pointed out by NAGELL). Hence the equation has exactly the four solutions given in H.

$\boldsymbol{y^2 - 28 = x^3}$. $\mathbf{(1, 0, -6, 12) = 1}$ (H, p. 56, (4)). We have $\alpha^3 - 6\alpha - 12 = 0$ and $\varepsilon = -3\alpha^2 + 11\alpha - 5$. Examining ε^n modulo 9 we find $\varepsilon^9 \equiv 1$ and $a_n \equiv 0$, if $n \equiv 0$ (mod 9). Since $\varepsilon^3 \equiv 3\alpha^2 - 2$ (mod 9), the form has the only solution (1, 0) by Lemma 8 and the equation has exactly the two solutions given in H.

$\boldsymbol{y^2 - 40 = x^3}$. $\mathbf{(1, 0, -18, 32) = 1}$ (H, p. 62, (7)). We have $\theta^3 - 18\theta - 32 = 0$ and $\varepsilon = 5\theta^2 - 31\theta + 31$. Now $\varepsilon^3 \equiv 1$ (mod 3) and $a_n \equiv -1$ (mod 3), if $n \not\equiv 0$. Since $a_3 \equiv 3$ (mod 9), the form has only one solution by Lemma 8 and the equation has the only solution given in H.

$\boldsymbol{y^2 - 44 = x^3}$. $\mathbf{(1, 3, -12, 12) = 1}$ (H, p. 64, (5)). A substitution $\gamma = \theta + 1$ in (6) p. 64 gives $\theta^3 - 15\theta - 26 = 0$ and we get $\varepsilon = 13\theta^2 - 15\theta - 201$. Then $-k = F(15, 13) = 2^3 \cdot 53^2$ and $p = 53$. By Lemma 8 a we find $m = 13$ and $a_{13} \equiv -583$ (mod 53^2), i.e. the form has only one solution. Hence the equation has exactly the two solutions given in H.

$\boldsymbol{y^2 - 19 = x^3}$. $\mathbf{(1, 0, -15, 24) = 1}$ (H, p. 72, (1)). We have $\varrho^3 - 15\varrho - 24 = 0$ and $\varepsilon = -36\varrho^2 + 202\varrho - 179$. As shown in H, $\varepsilon^n = u + v\varrho$, $n \neq 0$ implies $n \equiv -1$ (mod 4). Now we find $\varepsilon^8 \equiv 1$ (mod 16) and $n \equiv 0$ or 3 (mod 8) and further $\varepsilon^8 \equiv 1$ (mod 5) and $n \equiv 0$ or -1 (mod 8). Then $n = 0$ gives the only solution and the equation has exactly the solution given in H.

$\boldsymbol{y^2 - 37 = x^3}$. $\mathbf{(1, 0, -9, 16) = 1}$ (H, p. 77, (3)). We have $\theta^3 - 9\theta - 16 = 0$ and $\varepsilon = 57\theta^2 - 31\theta - 649$ and since $-k = 8 \cdot 41 \cdot 6361$, we put $p = 41$. By Lemma 8 a we find $m = 4$ and $a_4 \equiv 451$ (mod 41^2). The form has only one solution.

$\mathbf{(2, -3, 6, 3) = 1}$ (H, p. 77, (4)). The form is equivalent to $(1, 0, -729, 7576)$, i.e. $\theta_1^3 = 729\theta_1 + 7576$ and $\varepsilon = 360\theta_1^2 - 5602\theta_1 - 175267$. We get $-k = 2 \cdot 41 \cdot 6361$

and put $p=41$. As before we find $m=4$ and $a_4 \equiv 943 \pmod{41^2}$ and hence the form has only one solution. Then $y^2-37=x^3$ has exactly the three solutions $(-1, \pm 6)$, $(3, \pm 8)$ and $(243, \pm 3788)$.

In H, mom. 25, p. 87, I state that the equations with $k=22$, 26, 30, 35, 38, 71, 92 and 94 have exactly the solutions given there, if the calculated units are the fundamental units of the corresponding rings. Now I have examined that this is the fact in all the named cases and then the result follows by Lemma 8 a. I treat the first equation $y^2-22=x^3$ in detail and render the other analogous cases more briefly.

$\mathbf{y^2-22=x^3}$. $\mathbf{(1, 0, -9, 14)=1}$. We have $\varrho^3-9\varrho-14=0$ and $\varepsilon=185\varrho^2-609\varrho-199$. $\varepsilon=\eta^m$, $m>1$, implies by a method of NAGELL (H, p. 22 and [7], p. 7) $\eta=u+v\varrho$ with $|v|<1993$. It is more convenient to examine u and since $\theta<3{,}592$, we get $|u|<3{,}592\cdot 1993<7160$. We have the congruence conditions

$$\begin{cases} u\equiv -35 \pmod{288} \\ v\equiv 6 \pmod{12} \end{cases}, \quad \begin{cases} u\equiv 433 \pmod{1152} \\ v\equiv 12 \pmod{24} \end{cases} \quad \text{or} \quad \begin{cases} u\equiv 1 \text{ or } -575 \pmod{2304} \\ v\equiv 0 \pmod{24} \end{cases}.$$

Further $u\not\equiv -1 \pmod 5$ or $0 \pmod 7$ and $v\not\equiv -2 \pmod 5$. We get less than 50 values of u, which easily can be shown impossible. Hence ε is the fundamental unit of the ring. Now $7/F(609, 185)$, i.e. $p=7$, $\varepsilon^2\equiv 2 \pmod 7$ and $a_2\equiv 28 \pmod{49}$. Hence, by Lemma 8 a, $(1, 0)$ is the only solution of the form. That the other units all are fundamental is shown analogously and we get:

$\mathbf{y^2-26=x^3}$. $\mathbf{(1, 0, 3, 10)=1}$. $\varepsilon=-281\varrho^2-651\varrho+1917$, $p=7$, $\varepsilon^{16}\equiv 2 \pmod 7$ and $a_{16}\equiv -14 \pmod{49}$.

$\mathbf{y^2-30=x^3}$. $\mathbf{(1, 0, -57, 166)=1}$. $\varepsilon=-1349\varrho^2+6913\varrho+42293$, $p=3$, $\varepsilon^3\equiv 1 \pmod 3$ and $a_3\equiv 3 \pmod 9$.

$\mathbf{y^2-35=x^3}$. $\mathbf{(1, 0, -3, 12)=1}$. $\varepsilon=-1343\varrho^2+15347\varrho-31823$, $p=31$, $\varepsilon^{10}\equiv -6 \pmod{31}$ and $a_{10}\equiv 93 \pmod{961}$.

$\mathbf{y^2-38=x^3}$. $\mathbf{(1, 0, -33, 74)=1}$. $\varepsilon=539\varrho^2-1177\varrho-15971$, $p=11$, $\varepsilon\equiv 1 \pmod{11}$ and $a\equiv 55 \pmod{121}$.

$\mathbf{y^2-71=x^3}$. $\mathbf{(1, 0, -15, 28)=1}$. $\varepsilon=562\varrho^2-1290\varrho-5931$, $p=7$, $\varepsilon^2\equiv -3 \pmod 7$ and $a_2\equiv 14 \pmod{49}$.

$\mathbf{y^2-92=x^3}$. $\mathbf{(1, 0, -6, 20)=1}$. $\varepsilon=68\alpha^2+965\alpha-4121$, $p=5$, $\varepsilon^4\equiv 1 \pmod 5$ and $a_4\equiv 5 \pmod{25}$. The equation $(2, 3, 12, 3)=1$ is shown insoluble in H.

$\mathbf{y^2-94=x^3}$. $\mathbf{(1, 0, -9, 22)=1}$. $\varepsilon=-361\varrho^2-131\varrho+5821$, $p=5$, $\varepsilon^4\equiv 1 \pmod 5$ and $a_4\equiv -5 \pmod{25}$.

Finally I treat the remaining four cases $k=63$, 76, 55 and 91.

$\mathbf{y^2-63=x^3}$. $\mathbf{(1, 0, 9, 12)=1}$ (H, p. 59, (16)) and $\mathbf{(2, 0, 9, 3)=1}$ (H, p. 59, (18)). I have found that the calculated units (see the last table) are fundamental in the corresponding rings. This is easily seen in (18), but even in (16) we only need examine about 200 values u, though we get the limit $|u|<181700$ from $v^6\leq \frac{1}{4}\cdot\frac{D(\varepsilon)}{D(\theta)}$. Then, as pointed out in H, (16) has the only solution $(1, 0)$ and (18) is insoluble.

(2, −3, 6, 5) = 1 (*H*, p. 59, (17)). In this case the coefficients in the calculated unit are very great, but SKOLEM has shown me that the form is insoluble, irrespective of whether the unit is fundamental or not. I render his proof here:

As in *H* we consider the equivalent form $(2, 9, 18, 6) = 1$ and with the notations in *H*, p. 60, (20) and the factorizations given there we find $(2) = \mathfrak{p}^2 \cdot \mathfrak{p}_1$ and $\mathfrak{p} = \left(\frac{\alpha^3 (1-\alpha)^2}{48}\right)$. Then if $2 = \pi^2 \pi_1$, we can write $\pi = \frac{\alpha^3 (1-\alpha)^2}{48}$. If now (u, v) is a solution of the form, we get $N(2u + v\alpha) = 8u^3 + 36u^2v + 72uv^2 + 24v^3 = 4$ and it is easily seen that we can write

$$F(u, v) = (2, 9, 18, 6) = N\left(\pi_1 \cdot u + \frac{\alpha}{\pi_2} \cdot v\right) = 1$$

(cp. *H*, p. 20–22, DELAUNAY [4] t. 1, p. 258, and SKOLEM [1] Kap. VI, § 3). Then we have to examine

$$(4) \qquad 2u + v\alpha = \pi^2 \cdot \eta^n,$$

where η is the fundamental unit of $R(1, \alpha, \beta)$. Considering congruences modulo 5 we find $\alpha^3 \equiv -\alpha^2 - \alpha - 1$, i.e. $\alpha^4 \equiv 1 \pmod 5$. Since $\alpha\beta = 12$, we also get $\beta^4 \equiv 1$. Let $\tau = a\alpha + b\beta + c$ be an arbitrary integer in the ring. Then $\tau^5 \equiv \tau$, i.e. if $(\tau, 5) = 1$, we get $\tau^4 \equiv 1 \pmod 5$. Now $\varepsilon = \frac{1}{3} \cdot (27\alpha^2 - 121\alpha + 81)^3 \equiv \alpha - 1 \pmod 5$ and $\varepsilon^2 \equiv \alpha^2 - 2\alpha + 1$, i.e. ε is no square of a unit in the ring. Then $\varepsilon = \eta^m$ implies m odd and we can find an m' such that $mm' \equiv 1 \pmod 4$, i.e.

$$\varepsilon^{m'} \equiv \eta^{mm'} \equiv \eta \pmod 5$$

and hence every power of η is congruent to a power of ε modulo 5.

Since $\varepsilon^4 \equiv 1 \pmod 5$, we have to examine $\pi^2, \pi^2\varepsilon, \pi^2\varepsilon^2$ and $\pi^2\varepsilon^3$. Now $\pi \equiv -2\alpha^2 - 1$, $\pi^2 \equiv -\alpha^2$, $\pi^2\varepsilon \equiv 2\alpha^2 + \alpha + 1$, $\pi^2\varepsilon^2 \equiv 2\alpha^2 - 2\alpha + 2$ and $\pi^2\varepsilon^3 \equiv -\alpha^2 + 2\alpha + 1 \pmod 5$ and hence (4) can never be satisfied. Then the form is insoluble and the equation has exactly the two solutions given in *H*.

$y^2 - 76 = x^3$. **(4, 18, 12, 3) = 1** (*H*, p. 73, (6)). A trial of the same method gives the condition

$$2u + (\varrho + 3)v = \pi \cdot \varepsilon^n,$$

where $2 = \pi^2 \pi_1$, ϱ is defined by $\varrho^3 - 15\varrho - 24 = 0$ (*H*, p. 72, (2)) and $\varepsilon = -36\varrho^2 + 202\varrho - 179$. We can write $\pi = \frac{\varrho + 3}{2\varrho - 9} = 10\varrho^2 + 45\varrho + 53$ and get the condition

$$(5) \qquad U + V\varrho = (10\varrho^2 + 45\varrho + 53) \cdot \varepsilon^n.$$

We have $\varepsilon^{16} \equiv 2 \pmod 7$ and examining $n = 0, 1, 2, \ldots, 15$ in (5) we find the condition $n \equiv 2 \pmod{16}$. However, $\varepsilon^2 \equiv 1 \pmod 4$ implies n odd and hence the form is insoluble and the equation has the only solution given in *H*.

In the last two cases, 55 and 91, the calculated units are very great. I have used a method of solving the corresponding forms without showing that the units are fundamental, which may be generally available in similar cases. At first we shall state some self-evident facts, which we shall use below without references.

Suppose $\varepsilon=\eta^m$, $m>0$ and that ε^N is the first power of the unit ε with the property $\varepsilon^N\equiv c_N \pmod{p}$, p a rational prime. Then

$$\eta^{N_1}\equiv c \pmod{p} \text{ implies that } N/N_1.$$

Let $N_1=hN$ be the first exponent with this property. Then

$$h/m.$$

If there is any unit in the ring of the type $ap\theta^2+bp\theta+c$ with $(a,p)=1$, then η^{hN} is of the same type.

We alway shave an m' such that $mm'\equiv h \pmod{hN}$ and $\eta^h\equiv\varepsilon^{m'} \pmod{p}$. Then we can consider ε instead of η except if $h>1$.

Now we examine the possibilities $\eta\equiv a\theta^2+b\theta+c \pmod{p}$, where a, b and c assume complete systems of residues modulo p. At first we have the necessary condition for a unit

$$N(\eta)=\eta\cdot\eta'\cdot\eta''=1\equiv P_3(a,b,c) \pmod{p}.$$

This restricts the number of possible cases. In the remaining cases we determine h and examine those giving $h>1$. They can often be shown impossible on account of the necessary conditions h/m or h the same for η and η^r, if $(r,hN)=1$. Now we return to the two equations.

$\boldsymbol{y^2-55=x^3}$. $\mathbf{(1,0,-27,56)=1}$ (H, p. 88). We have $\varrho^3-27\varrho-56=0$ and $\varepsilon=\frac{1}{9}\cdot(25\varrho^2-97\varrho-323)^3$. At first we shall prove that we can consider powers of ε, irrespective of whether ε is fundamental or not. We examine congruences modulo 5 and find $\varepsilon^{10}\equiv 1 \pmod{5}$. Then we consider the different expressions $\eta\equiv a\varrho^2+b\varrho+c \pmod{5}$, where at first $\eta\cdot\eta'\cdot\eta''=1$ implies

$$a^3-2a^2b-a^2c+2abc-ac^2+b^3-2b^2c+c^3\equiv 1 \pmod{5}.$$

It is easily seen that ε is no square and no cube. Then $h=2$ or 3 is impossible and the only other case giving $h>1$ is $\eta\equiv-\varrho^2-2\varrho-2 \pmod{5}$, where $h=5$, i.e. $\eta^{50}\equiv 1 \pmod{5}$ as the first power. Now we get $\eta^2\equiv 2\varrho-2\equiv\varepsilon^7 \pmod{5}$ implying $h=2$ and there is no unit of the examined type. (Further, since $m=5$ implies $\eta\equiv-\varrho^2-2\varrho-2$, m cannot be divisible by 5.) Then we can examine powers of ε and we find modulo 5 $n\equiv 0$ or 7 (mod 10) and since $\varepsilon\equiv\varrho^2+\varrho+1$ and $\varepsilon^2\equiv 1 \pmod{2}$, n even. Hence $n\equiv 0 \pmod{10}$ and since $a_{10}\equiv 10 \pmod{25}$ there is no solution $n\neq 0$ and the equation has exactly the solution given in H.

$\boldsymbol{y^2-91=x^3}$. $\mathbf{(1,0,9,16)=1}$ (H, p. 88). We have $\varrho^3+9\varrho-16=0$ and $\varepsilon=\frac{1}{9}\cdot$ $\cdot(-23\varrho^2-167\varrho+289)^3$. Even in this case we examine modulo 5 and here we find $\varepsilon^8\equiv 1 \pmod{5}$, i.e. $N=8$. $\eta\equiv a\varrho^2+b\varrho+c \pmod{5}$ shall satisfy

$$a^3-a^2b+a^2c+2abc+2ac^2+b^3-b^2c+c^3\equiv 1 \pmod{5}.$$

We easily see that ε is no square and no cube and since h is divisible by 2 or 3 in all the cases with $h>1$, we must have $h=1$ and can consider the powers ε^n. Examination modulo 5 gives $n \equiv 0$ or 1 (mod 8) and modulo 2 we get n even, i.e. $n \equiv 0$ (mod 8). Since $\varepsilon^8 \equiv 1$ (mod 5) and $a_8 \equiv -10$ (mod 25) we get no solution $n \neq 0$ and the equation has exactly the solution given in H.

The cases $k < 0$ are treated in passing in H, Ch. II, mom. 26. By carelessness I have passed over a "trivial" solution of the reducible form corresponding to the equation $y^2 + 56 = x^3$. This equation has exactly one solution (18, ±76). The omission in my tables of this solution and the third solution of $y^2 - 37 = x^3$ has been pointed out by D. H. LEHMER. He mentions a table by ROBINSON in MTAC (Math.tabls and other aids to computation), to which I have no access. Now I have ealculated all the irreducible forms corresponding to the cases $0 < -k \leq 100$ by using H, Theorems 4 or 5. As an example we take the case$k = -53$. The class number $h(K\sqrt{-53})$ is 6. $(3) = \mathfrak{p}_3 \cdot \mathfrak{p}_3'$ and we find that (1), $\mathfrak{p}_3^2$ and $\mathfrak{p}_3'^2$ represent the ideal classes of third degree in the group of ideal classes in $K(\sqrt{-53})$. Since $\mathfrak{p}_3^6 = (\beta) = (26 + \sqrt{-53})$, the irreducible form comes from

$$9^3 \cdot (\pm y + \sqrt{-53}) = (26 + \sqrt{-53})\,(a + b\sqrt{-53})^3$$

by the relation in H, p. 15, line 3 from below. In this relation p need not be a prime. It is very easy to see that Theorem 5 gives no new equations in the actual cases with h divisible by 3.

The tables in this article give the results of H corrected and completed in some points. There are 22 undecided cases in the second table for $k < 0$, where no number N of solutions with $y \geq 0$ is stated. The forms which are not definitely solved in those cases are given in the third table. All the cases excluded in the two first tables, correspond to provably insoluble equations. The last table gives the fundamental rings and units in the occurring cubic fields. All the square-free numbers $1 < k < 50$ are considered and further every such value $50 < k < 100$, corresponding to a soluble equation. A form $(1, p, q, r)$ defines the ring $R(\varrho)$ by $F(\varrho, -1) = 0$ and a form (a, b, c, d) the ring $R(1, \alpha, \beta)$, where $F(\alpha, -a) = 0$ and $F(-d, \beta) = 0$. D is the discriminant of the field.

H, Table 3, treating the equations $y^2 + 27k = x^3$ with $-50 \leq k \leq 50$ (H, Ch. III), is excluded here.

Solutions of the equations $y^2 - k = x^3$ *with* $-100 \leq k \leq 100$

k	N	Solutions
1	3	(−1, 0), (0, 1), (2, 3)
2	1	(−1, 1)
3	1	(1, 2)
4	1	(0, 2)
5	1	(−1, 2)
8	4	(−2, 0), (1, 3), (2, 4), (46, 312)
9	5	(−2, 1), (0, 3), (3, 6), (6, 15), (40, 253)
10	1	(−1, 3)
12	2	(−2, 2), (13, 47)
15	2	(1, 4), (109, 1138)
16	1	(0, 4)
17	8	(−2, 3), (−1, 4), (2, 5), (4, 9), (8, 23), (43, 282), (52, 375), (5234, 378661)
18	1	(7, 19)
19	1	(5, 12)
22	1	(3, 7)
24	4	(−2, 4), (1, 5), (10, 32), (8158, 736844)
25	1	(0, 5)
26	1	(−1, 5)
27	1	(−3, 0)
28	2	(−3, 1), (2, 6)
30	1	(19, 83)
31	1	(−3, 2)
33	1	(−2, 5)
35	1	(1, 6)
36	4	(−3, 3), (0, 6), (4, 10), (12, 42)

k	N	Solutions	k	N	Solutions
37	3	(−1, 6), (3, 8), (243, 3788)	71	1	(5, 14)
38	1	(11, 37)	72	1	(−2, 8)
40	1	(6, 16)	73	6	(−4, 3), (2, 9), (3, 10), (6, 17), (72, 611), (356, 6717)
41	1	(2, 7)	76	1	(−3, 7)
43	1	(−3, 4)	79	1	(45, 302)
44	2	(−2, 6), (5, 13)	80	4	(−4, 4), (1, 9), (4, 12), (44, 292)
48	1	(1, 7)	81	1	(0, 9)
49	1	(0, 7)	82	1	(−1, 9)
50	1	(−1, 7)	89	4	(−4, 5), (−2, 9), (10, 33), (55, 408)
52	1	(−3, 5)	91	1	(−3, 8)
54	1	(3, 9)	92	1	(2, 10)
55	1	(9, 28)	94	1	(3, 11)
56	1	(2, 8)	97	1	(18, 77)
57	3	(−2, 7), (4, 11), (7, 20)	98	1	(7, 21)
63	2	(−3, 6), (1, 8)	99	1	(1, 10)
64	3	(−4, 0), (0, 8), (8, 24)	100	6	(−4, 6), (0, 10), (5, 15), (20, 90), (24, 118), (2660, 137190)
65	4	(−4, 1), (−1, 8), (14, 53), (584, 14113)			
68	2	(−4, 2), (152, 1874)			

$-k$	N	Solutions	$-k$	N	Solutions
1	1	(1, 0)	48	2	(4, 4), (28, 148)
2	1	(3, 5)	49	1	(65, 524)
4	2	(2, 2), (5, 11)	53		(9, 26), (29, 156)
7		(2, 1), (32, 181)	54	1	(7, 17)
8	1	(2, 0)	55		(4, 3), (56, 419)
11	2	(3, 4), (15, 58)	56	1	(18, 76)
13	1	(17, 70)	60		(4, 2), (136, 1586)
15		(4, 7)	61		(5, 8)
18		(3, 3)	63		(4, 1) (568, 13537)
19	1	(7, 18)	64	1	(4, 0)
20	1	(6, 14)	67	1	(23, 110)
23		(3, 2)	71		(8, 21)
25		(5, 10)	72		(6, 12)
26		(3, 1), (35, 207)	74	1	(99, 985)
27	1	(3, 0)	76	2	(5, 7), (101, 1015)
28		(4, 6), (8, 22), (37, 225)	79		(20, 89)
35	1	(11, 36)	81	1	(13, 46)
39		(4, 5), (10, 31), (22, 103)	83	1	(27, 140)
40	1	(14, 52)	87		(7, 16)
44	1	(5, 9)	89		(5, 6)
45		(21, 96)	95		(6, 11)
47		(6, 13), (12, 41), (63, 500)	100		(5, 5), (10, 30), (34, 198)

Forms which are not definitely treated

$-k$	Form (=1)	Solutions	x
7	(1, 0, −6, 2)	(1, 0), (1,3)	2, 32
15	(1, −6, 0, 2)	(1, 0)	4
18	(1, 0, −9, 6)	(1, 0)	3
23	(1, 0, −9, 4)	(1, 0)	3
25	(1, −6, −3, 2)	(1, 0)	5
26	(1, 0, −9, 2)	(1, 0)	3
28	(1, 0, −12, 12)	(1, 0), (1, 1)	4, 8
39	(1, 0, −12, 10)	(1, 0), (−1, −1), (3, 1)	4, 10, 22
45	(1, 12, −15, 4)	(1, 0)	21
47	(1, −6, −6, 2)	(1, 0), (−1, 1)	6, 12
53	(1, 6, −15, 6)	(1, 0), (1, 2)	9, 29

$-k$	Form $(=1)$	Solutions	x
55	$(1, 0, -12, 6)$	$(1, 0)$, $(1, 2)$	4, 56
60	$(1, 0, -12, 4)$	$(1, 0)$, $(1, 3)$	4, 136
61	$(1, 0, -15, 16)$	$(1, 0)$	5
63	$(1, 0, -12, 2)$	$(1, 0)$, $(1. 6)$	4, 568
71	$(1, 6, -12, 2)$	$(1, 0)$	8
72	$(1, -6, -6, 4)$	$(1, 0)$	6
	$(4, 0, -9, 3)$		
79	$(1, 12, -12, 2)$	$(1, 0)$	20
87	$(1, -9, 6, 4)$	$(1, 0)$	7
89	$(1, 0, -15, 12)$	$(1, 0)$	5
95	$(1, -6, -6, 6)$	$(1, 0)$	6
100	$(1, 0, -15, 10)$	$(1, 0)$	5
	$(1, 6, -18, 8)$	$(1, 0)$	10

Occurring cubic fields (except for $k=1$, i.e. $y^2 - f^2 = x^3$)

k	$-D$	Fundamental ring and unit	
2	216	$(1, 0, 3, 2)$	$\varepsilon = -\varrho^2 - \varrho + 1$
$2 \cdot 7^2$	$108 \cdot 98$	$(1, 0, -21, 42)$	$\varepsilon = 3\varrho^2 + 15\varrho - 167$
	$108 \cdot 98$	$(3, 6, 3, 4)$	
	$108 \cdot 98$	$(2, 3, 12, 2)$	
3	324	$(1, 0, -3, 4)$	$\varepsilon = \varrho^2 + \varrho - 7$
5	135	$(1, 0, 3, 1)$	$\varepsilon = \varrho$
6	648	$(2, 0, 3, 2)$	$\varepsilon = \alpha - 1$
7	756	$(2, 0, -3, 3)$	$\varepsilon = 11\alpha - 6\beta - 23$
$7 \cdot 3^2$	$108 \cdot 63$	$(1, 0, 9; 12)$	$\varepsilon = 36669\varrho^2 - 163545\varrho + 140365$
	$108 \cdot 63$	$(2, 9, 18, 6)$	*$\varepsilon = \frac{1}{3} \cdot (122\alpha + 54\beta - 891)^3$
	$108 \cdot 63$	$(2, 0, 9, 3)$	$\varepsilon = -1602\alpha - 15792\beta + 146521$
10	1080	$(1, 0, 3, 6)$	$\varepsilon = -21\varrho^2 - 11\varrho + 49$
11	$108 \cdot 11$	$(2, 0, 3, 3)$	$\varepsilon = -2\alpha + 24\beta - 95$
13	351	$(1, 3, 6, 1)$	$\varepsilon = \varrho$
14	$108 \cdot 14$	$(2, 0, -3, 4)$	$\varepsilon = -63\alpha - 8\beta + 227$
15	$108 \cdot 15$	$(1, 0, -3, 8)$	$\varepsilon = 5 - 2\varrho$
17	459	$(1, 0, -6, 7)$	$\varepsilon = 2\varrho^2 - 2\varrho - 11$
	$108 \cdot 17$	$(1, 0, -6, 10)$	$\varepsilon = \varrho - 3$
	204	$(1, 1, 1, 3)$	$\varepsilon = -\varrho^2 + \varrho + 1$
	$108 \cdot 17$	$(1, 0, 6, 6)$	$\varepsilon = -\varrho + 1$
19	$108 \cdot 19$	$(1, 0, -15, 24)$	$\varepsilon = -36\varrho^2 + 202\varrho - 179$
21	567	$(1, 0, -3, 5)$	$\varepsilon = -\varrho^2 + \varrho + 3$
22	$108 \cdot 22$	$(1; 0, -9, 14)$	$\varepsilon = 185\varrho^2 - 609\varrho - 199$
23	$108 \cdot 23$	$(2, 0, -3, 5)$	$\varepsilon = 965\alpha + 136\beta - 3713$
26	$108 \cdot 26$	$(1, 0, 3, 10)$	$\varepsilon = -281\varrho^2 - 651\varrho + 1917$
29	87	$(1, -1, 2, 1)$	$\varepsilon = \varrho$
30	$108 \cdot 30$	$(1, 0, -57, 166)$	$\varepsilon = -1349\varrho^2 + 6913\varrho + 42293$
31	$108 \cdot 31$	$(1, 0, 9, 4)$	$\varepsilon = 821\varrho^2 + 109\varrho - 203$
33	891	$(1, 0, 6, 1)$	$\varepsilon = \varrho$
	$108 \cdot 33$	$(1, 0, 6, 10)$	$\varepsilon = -\varrho^2 - \varrho + 3$
	44	$(1, -1, 1, 1)$	$\varepsilon = \varrho$
	$108 \cdot 33$	$(3, 0, 6, 2)$	$\varepsilon = -\alpha + 1$
34	$108 \cdot 34$	$(2, 0, -3, 6)$	*$\varepsilon = -1724\alpha - 678\beta + 8431$
35	$108 \cdot 35$	$(1, 0, -3, 12)$	$\varepsilon = -1343\varrho^2 + 15347\varrho - 31823$
37	999	$(2, 3, 3, 4)$	$\varepsilon = 140\alpha + 26\beta - 473$
38	$108 \cdot 38$	$(1, 0, -33, 74)$	$\varepsilon = 539\varrho^2 - 1177\varrho - 15971$
39	$108 \cdot 39$	$(3, 0, 3; 4)$	*$\varepsilon = 661\alpha + 1863\beta - 10832$

* ε not definitely proved to be fundamental.

k	$-D$	Fundamental ring and unit	
41	$27 \cdot 41$	$(3, -3, -3, 4)$	$\varepsilon = 2\alpha - 2\beta + 1$
	492	$(1, -1, 3, 3)$	$\varepsilon = 2\varrho^2 - 1$
	$108 \cdot 41$	$(2, 6, 12, 3)$	$\varepsilon = \alpha + \beta - 11$
	$108 \cdot 41$	$(2, 6, -6, 3)$	$\varepsilon = -\alpha + \beta + 7$
42	$108 \cdot 42$	$(2, 3, 0, 6)$	$\varepsilon = 6\alpha - \beta - 23$
43	516	$(2, 4, 3, 3)$	$\varepsilon = 23 - 7\alpha$
46	$108 \cdot 46$	$(2, 6, -3, 3)$	$^*\varepsilon = 244\alpha + 5380\beta - 8519$
47	$108 \cdot 47$	$(2, 0, -3, 7)$	$^*\varepsilon = -4838\alpha + 2736\beta + 7449$
55	$108 \cdot 55$	$(1, 0, -27, 56)$	$^*\varepsilon = \frac{1}{9} \cdot (25\varrho^2 - 97\varrho - 323)^3$
57	$27 \cdot 57$	$(1, 0, 6, 5)$	$\varepsilon = 2\varrho^2 + 34\varrho - 27$
	$108 \cdot 57$	$(1, 0, 6, 14)$	$\varepsilon = \varrho^2 - \varrho - 1$
	76	$(1, 1, 3, 1)$	$\varepsilon = \varrho$
	$108 \cdot 57$	$(1, 0, -12, 22)$	$\varepsilon = -\varrho^2 + 2\varrho + 9$
65	$27 \cdot 65$	$(2, -3, 3, 3)$	$\varepsilon = 28\alpha - 14\beta + 43$
	780	$(1, -2, 0, 6)$	$\varepsilon = 5\varrho^2 + 3\varrho - 13$
	$108 \cdot 65$	$(1, 0, 12, 2)$	$\varepsilon = 1 - 6\varrho$
	$108 \cdot 65$	$(1, 12, 6, 2)$	$\varepsilon = 3\varrho^2 - 33\varrho - 17$
71	$108 \cdot 71$	$(1, 0, -15, 28)$	$\varepsilon = 562\varrho^2 - 1290\varrho - 5931$
73	$27 \cdot 73$	$(2, 3, -3, 3)$	$\varepsilon = 8\alpha + 50\beta - 101$
	876	$(3, 0, -2, 2)$	$\varepsilon = 4\alpha - 7\beta - 1$
	$108 \cdot 73$	$(1, 15, 57, 1)$	$\varepsilon = \varrho$
	$108 \cdot 73$	$(1, 0, 12, 6)$	$\varepsilon = 1 - 2\varrho$
79	948	$(1, -1, 0, 6)$	$\varepsilon = 17\varrho^2 - 45\varrho + 29$
	$108 \cdot 79$	$(2, -3, 6, 6)$	
	$108 \cdot 79$	$(2, 0, 9, 5)$	
	$108 \cdot 79$	$(2, 3, -6, 7)$	
82	984	$(2, 1, 0, 3)$	$\varepsilon = 33\alpha + 7\beta - 104$
89	$27 \cdot 89$	$(1, 0, -6, 11)$	$\varepsilon = -10\varrho^2 + 50\varrho - 59$
	1068	$(3, 0, 2, 2)$	$\varepsilon = -3\alpha + 9\beta - 23$
	$108 \cdot 89$	$(1, 9, -3, 3)$	$\varepsilon = -2\varrho^2 + 17\varrho + 16$
	$108 \cdot 89$	$(1, 0, 12, 10)$	$\varepsilon = \varrho^2 + 3\varrho - 3$
91	$108 \cdot 91$	$(1, 0, 9, 16)$	$^*\varepsilon = \frac{1}{9} \cdot (-23\varrho^2 - 167\varrho + 289)^3$
94	$108 \cdot 94$	$(1, 0, -9, 22)$	$\varepsilon = -361\varrho^2 - 131\varrho + 5821$
97	$27 \cdot 97$	$(1, 6, -6, 3)$	$\varepsilon = 2\varrho^2 - 14\varrho + 1$
	$108 \cdot 97$	$(2, 12, 6, 3)$	$\varepsilon = \alpha - 11$
	1164	$(3, 6, -14, 6)$	$\varepsilon = -9\alpha + 9\beta + 79$
	$108 \cdot 97$	$(2, 18, 42, 3)$	$\varepsilon = 20\alpha + 3\beta - 125$

Tryckt den 16 januari 1954

Uppsala 1954. Almqvist & Wiksells Boktryckeri AB