Pacific Journal of
Mathematics

# ON A THEOREM OF DELAUNAY AND SOME RELATED RESULTS

BASIL GORDON AND S. P. MOHANTY

Vol. 68, No. 2 April 1977

PACIFIC JOURNAL OF MATHEMATICS
Vol 68 No 2, 1977

# ON A THEOREM OF DELAUNAY AND SOME RELATED RESULTS

B. GORDON AND S. P. MOHANTY

*Dedicated to the memory of Professor T. S. Motzkin*

**Delaunay has proved that if $\epsilon = ap\phi^2 + bp\phi + c$ is a unit in the ring $Z[\theta]$, where $\theta^3 - P\theta^2 + Q\theta - R = 0$, $p$ is an odd prime, $\phi = p^t\theta$, $t \geqq 0$ and $p \nmid a$, then no power $\epsilon^m$ ($m$ positive) can be a binorm, i.e. $\epsilon^m = u + v\theta$ is impossible for $m$ a positive integer. Hemer has pointed out that in the above situation, $\epsilon^m = u + v\theta$ is also impossible for $m$ a negative integer.**

**In this paper the above result is extended as follows.**

THEOREM 1. *If $\epsilon = a\theta^2 + b\theta + c$ is a unit in $Z[\theta]$, where $\theta^3 = d\theta^2 + e\theta + f$ and $p^\alpha \| a$, $p^\beta \| b$, $p$ being a prime, then $\epsilon^n = u + v\theta$ is impossible for $n \neq 0$ in the following cases:*

(i) *When $1 \leqq \alpha \leqq \beta$ and $p$ is odd,*
(ii) *When $2 \leqq \alpha \leqq \beta$ and $p = 2$,*
(iii) *When $\beta \leqq \alpha < 2\beta$ and $p$ is odd,*
(iv) *When $\beta \leqq \alpha < 2\beta - 1$ and $p = 2$.*

**As an application of this and some other similar theorems, all integer solutions of the equation $y^2 = x^3 + 113$ are determined.**

First we prove two simple lemmas.

LEMMA 2. *If $p^\alpha \| \binom{n}{p^q}$ then $p^\alpha \mid \binom{n}{i}$, where the prime $p$ satisfies $p^q < i < p^{q+1}$ and $p^{\alpha-1}$ a $\binom{n}{p^{q+1}}$. Furthermore if $p \mid n$ and $p \nmid i$ then $p^{\alpha+1} \mid \binom{n}{i}$.*

*Proof.* Let $i = p^q + r$. Then $0 < r < p^{q+1} - p^q$. Hence

$$\binom{n}{i} = \binom{n}{p^q}\binom{n - p^q}{r}\frac{r!}{\prod_{j=1}^{r}(p^q + j)}.$$

Since $\prod_{j=1}^{r}(p^q + j)/r!$ is an integer not divisible by $p$ and $p^\alpha \| \binom{n}{p^q}$, we have $p^\alpha \mid \binom{n}{i}$.

If $p \mid n$ and $p \nmid i$ then $p \nmid r$ for $i = p^q + r$. Then

$$\binom{n - p^q}{r} = \left(\frac{n - p^q}{r}\right)\binom{n - p^q - 1}{r - 1}$$

is divisible by $p$. Hence $p^{\alpha+1} \mid \binom{n}{i}$.

Again from

$$\binom{n}{p^{q+1}} = \binom{n}{p^q}\binom{n-p^q}{p^{q+1}-p^q}\frac{s!}{\prod_{j=1}^{s}(p^{q+1}-j)}\left(\frac{p^{q+1}-p^q}{p^{q+1}}\right),$$

where $s = p^{q+1} - p^q - 1$, we see that $p^{\alpha-1} \mid \binom{n}{p^{q+1}}$, and the lemma is proved.

LEMMA 3. *Let* $\epsilon = a\theta^2 + b\theta + c$ *be a unit in* $Z[\theta]$, *where* $\theta^3 = d\theta^2 + e\theta + f$, *and* $\epsilon^{-1} = a'\theta^2 + b'\theta + c'$. *If* $p^\alpha \| a$, $p^\beta \| b$, *where* $p$ *is a prime and* $\alpha\beta \neq 0$, *then* $p^\alpha \| a'$ *and* $p^\beta \| b'$ *in the following cases*:

(i) $\alpha \leqq \beta < 2\alpha$

(ii) $\beta \leqq \alpha < 2\beta$

*For* $\alpha \leqq \beta$ *we have* $p^\alpha \| a'$ *and* $p^\alpha \mid b'$.

*Proof.* Since $(a\theta^2 + b\theta + c)(a'\theta^2 + b'\theta + c') = 1$, we have,

$$aa'd^2 + ab'd + a'bd + aa'e + ac' + ca' + bb' = 0, \tag{1}$$

$$aa'f + aa'de + ab'e + a'be + bc' + b'c = 0, \tag{2}$$

and

$$aa'df + ab'f + a'bf + cc' = 1. \tag{3}$$

From (3) it follows that $p \nmid c'$.

*Case* (i). From (1) we have $ca' \equiv 0 \pmod{p^\alpha}$ as $\alpha \leqq \beta$. Since $p \nmid c$ we get $a' \equiv 0 \pmod{p^\alpha}$. From (2) we obtain $b'c \equiv 0 \pmod{p^\alpha}$ for $\alpha \leqq \beta$, whence $b' \equiv 0 \pmod{p^\alpha}$. If $\beta < 2\alpha$, then (2) gives $b'c \equiv 0 \pmod{p^\beta}$, or $b' \equiv 0 \pmod{p^\beta}$. If $p^{\alpha+1} \mid a'$, then from (1) we have $ac' \equiv 0 \pmod{p^{\alpha+1}}$. Since $p \nmid c'$ we get $a \equiv 0 \pmod{p^{\alpha+1}}$, a contradiction. Hence $p^\alpha \| a'$. Similarly if $p^{\beta+1} \mid b'$, then from (2) we get $bc' \equiv 0 \pmod{p^{\beta+1}}$ when $\beta < 2\alpha$. Again we arrive at a contradiction since $p \nmid c'$ and $p^\beta \| b$. Hence $p^\beta \| b'$.

*Case* (ii). Since $\beta \leqq \alpha$, (2) yields $b'c \equiv 0 \pmod{p^\beta}$. Then we have $b' \equiv 0 \pmod{p^\beta}$ for $p \nmid c$. Using $\alpha < 2\beta$, we get $a'(bd + c) \equiv 0 \pmod{p^\alpha}$ from (1). Then $a' \equiv 0 \pmod{p^\alpha}$ as $p \nmid (bd + c)$. If $b' \equiv$

$0 \pmod{p^{\beta+1}}$, then from (2) we see that $bc' \equiv 0 \pmod{p^{\beta+1}}$, a contradiction. Hence $p^\beta \| b'$. If $a' \equiv 0 \pmod{p^{\alpha+1}}$ we have from (1) $ac' + bb' \equiv 0 \pmod{p^{\alpha+1}}$. We get a contradiction for $\alpha < 2\beta$. Hence $p^\alpha \| a'$.

*Proof of Theorem* 1. Let $n > 0$. Case (i) and (ii). Let $1 \leqq \alpha \leqq \beta$. Since $\epsilon$ is a unit, $p \nmid c$. Moreover $\epsilon = a\theta^2 + b\theta + c = p^\alpha(r\theta^2 + s\theta) + c$ where $p \nmid r$. Let $(r\theta^2 + s\theta)^i = a_i\theta^2 + b_i\theta + c_i$, with $a_i$, $b_i$ and $c_i$ rational integers. Then

$$\epsilon^n = (a\theta^2 + b\theta + c)^n = [c + p^\alpha(r\theta^2 + s\theta)]^n = c^n + \binom{n}{1} c^{n-1}p^\alpha(r\theta^2 + s\theta)$$
$$+ \binom{n}{2} c^{n-2}p^{2\alpha}(a_2\theta^2 + b_2\theta + c_2) + \cdots + p^{n\alpha}(a_n\theta^2 + b_n\theta + c_n) = u + v\theta.$$

Comparing the coefficients of $\theta^2$, we have

$$nc^{n-1}p^\alpha r + \binom{n}{2} c^{n-2}p^{2\alpha}a_2 + \cdots + p^{n\alpha}a_n = 0. \tag{4}$$

If $p$ is an odd prime, we see using Lemma 2 that the first term of (4) is divisible by a lower power of $p$ than the others. If $p = 2$ and $\alpha \geqq 2$ the same conclusion holds. Hence (4) can never be satisfied. So $\epsilon^n$ can never be of the form $u + v\theta$ in these cases.

*Cases* (iii) *and* (iv). Now $\epsilon = p^\beta(r\theta^2 + s\theta) + c$, where $p^{\alpha-\beta} \| r$. Then the coefficient of $\theta^2$ in $\epsilon^n = [c + p^\beta(r\theta^2 + s\theta)]^n$ is

$$nc^{n-1}p^\beta r + \binom{n}{2} c^{n-2}p^{2\beta}a_2 + \cdots + p^{n\beta}a_n, \tag{5}$$

where $(r\theta^2 + s\theta)^i = a_i\theta^2 + b_i\theta + c_i$ with $a_i$, $b_i$ and $c_i$ rational integers. Again using Lemma 2 and the fact that $\alpha < 2\beta$, we see that the first term of (5) is divisible by a lower power of $p$ than the others if $p$ is an odd prime.

In case $p = 2$ and $\alpha < 2\beta - 1$ the same conclusion holds. Hence (5) can never be zero, i.e. $\epsilon^n = u + v\theta$ is impossible. This proves the theorem for $n > 0$.

We next consider $\epsilon^n = u + v$ for $n < 0$.

Let $n = -m$ and $\epsilon^{-1} = a'\theta^2 + b'\theta + c'$. Then we have $\epsilon^n = (\epsilon^{-1})^m = (a'\theta^2 + b'\theta + c')^m$ where $m > 0$. From Lemma 3, we see that $p^\alpha \| a'$, $p^\alpha | b'$ for $\alpha \leqq \beta$, and $p^\alpha \| a'$, $p^\beta \| b'$ for $\beta \leqq \alpha < 2\beta - 1$, $\alpha \leqq \beta < 2\alpha$ and $\beta \leqq \alpha < 2\beta$. Hence $(a'\theta^2 + b'\theta + c')^m = u + v\theta$ is impossible for $m > 0$. Combining these results we see that $\epsilon^n = u + v\theta$ is impossible for $n \neq 0$, and the theorem is proved.

We note that if the conditions of Theorem 1 are not fulfilled, then $\epsilon^n = u + v\theta$ is possible for $n > 3$; examples are given in [**2**, page 417].

Very often the following theorem is useful.

THEOREM 4. *Let* $\epsilon = a_1\theta^2 + b_1\theta + c_1$ *be a unit in* $Z[\theta]$, *where* $\theta^3 - p_1\theta - q_1 = 0$. *If* $p_1 \equiv 0 \pmod 3$, *then*

$$\epsilon^n = u + v\theta \tag{6}$$

*is impossible for* $n \not\equiv 0$ *provided* $a_1 \not\equiv 0 \pmod 3$, $b_1^2 + 2a_1c_1 \not\equiv 0 \pmod 3$, *and* $b_1^2c_1 + a_1c_1^2 + a_1^2b_1q_1 \not\equiv 0 \pmod 3$.

*Proof.* Let $\epsilon^n = a_n\theta^2 + b_n\theta + c_n$. Then we have

$$a_{n+1} = a_n(a_1p_1 + c_1) + b_nb_1 + c_na_1,$$

$$b_{n+1} = a_n(a_1q_1 + b_1p_1) + b_n(c_1 + a_1p_1) + c_nb_1,$$

and

$$c_{n+1} = a_nb_1q_1 + b_na_1q_1 + c_nc_1.$$

Hence we get $a_2 = a_1^2p_1 + b_1^2 + 2a_1c_1$, $b_2 = a_1^2q_1 + 2b_1c_1 + 2a_1b_1p_1$, and $c_2 = c_1^2 + 2a_1b_1q_1$. Then $a_3 = a_1^3p_1^2 + 3a_1b_1^2p_1 + 3a_1^2c_1p_1 + 3b_1^2c_1 + 3a_1c_1^2 + 3a_1^2b_1q_1$, $b_3 = 2a_1^3p_1q_1 + 3a_1b_1^2q_1 + 3a_1^2c_1q_1 + 3a_1^2b_1p_1^2 + b_1^3p_1 + 6a_1b_1c_1p_1 + 3b_1c_1^2$, and $c_3 = 3a_1^2b_1p_1q_1 + b_1^3q_1 + 6a_1b_1c_1q_1 + a_1^3q_1^2 + c_1^3$. Suppose $p_1 \equiv 0 \pmod 3$. Then $a_3 \equiv 0 \pmod 3$, $b_3 \equiv 0 \pmod 3$, and $c_3 \equiv b_1q_1 + a_1q_1^2 + c_1 \pmod 3$.

Since $\epsilon^3$ is a unit, $c_3 \not\equiv 0 \pmod 3$ as $a_3 \equiv b_3 \equiv 0 \pmod 3$. Hence we have $c_3 \equiv 1$ or $2 \pmod 3$.

Suppose $n \equiv 1 \pmod 3$, and put $n = 1 + 3m$ in (6). We get

$$\epsilon \cdot (\epsilon^3)^m = u + v\theta,$$

or

$$(a_1\theta^2 + b_1\theta + c_1)(\pm 1)^m \equiv u + v\theta \pmod 3.$$

This congruence is impossible unless $a_1 \equiv 0 \pmod 3$. Hence if $a_1 \not\equiv 0 \pmod 3$, then $n \not\equiv 1 \pmod 3$. Suppose $n \equiv 2 \pmod 3$, and let $n = 2 + 3m$. Then (6) gives

$$(a_2\theta^2 + b_2\theta + c_2)(\pm 1)^m \equiv u + v\theta \pmod 3.$$

This is impossible unless $a_2 \equiv 0 \pmod 3$, i.e. $b_1^2 + 2a_1c_1 \equiv 0$

$\pmod 3$. Hence if $b_1^2+2a_1c_1\not\equiv 0 \pmod 3$, then $n\equiv 2 \pmod 3$ is impossible. Finally suppose $n=3m$ in (6). Then we get

$$(a_3\theta^2+b_3\theta+c_3)^m=u+v\theta. \tag{7}$$

Now $a_3\equiv b_3\equiv 0 \pmod 3$, and $a_3\equiv 3b_1^2c_1+3a_1c_1^2+3a_1^2b_1q_1 \pmod 9$. If $b_1^2c_1+a_1c_1^2+a_1^2b_1q_1\not\equiv 0 \pmod 3$, then $a_3\not\equiv 0 \pmod 9$ and hence by Theorem 1, (7) is impossible for $m$ an integer, positive or negative.

Therefore $n=0$ is the only solution to (6).

LEMMA 5 (Delaunay [2, page 385]). *If $b\theta+c$, where $b\neq 0,\pm 1$, is a positive unit of $Z[\theta]$ where $\theta^3-P\theta^2+Q\theta-R=0$, then no power $>1$ of $b\theta+c$ can be a binomial unit.* (In other words all the positive powers of the positive unit $b\theta+c$ are of the form $L\theta^2+M\theta+N$, where $L\neq 0$).

We prove two theorems which are useful when $b=\pm 1$.

THEOREM 6. *Let $\epsilon=\pm\theta+c$ be a unit in $Z[\theta]$, where $\theta^3-P\theta^2+Q\theta-R=0$. If $\theta^3\equiv 0 \pmod{p^2}$, where $p$ is a prime, then $p\nmid c$ and $\epsilon^n=u+v\theta$ is impossible for $n>1$.*

*Proof.* We have $(\epsilon-c)^3\equiv 0 \pmod{p^2}$. If $p\mid c$ then $\epsilon^3\equiv 0 \pmod p$ where $p^3\mid N(\epsilon^3)=\pm 1$. Hence $p\nmid c$. Let $\epsilon^n=u+v\theta$, $n>1$. Then

$$\begin{aligned}(c\pm\theta)^n=c^n+\binom{n}{1}c^{n-1}(\pm\theta)+\binom{n}{2}c^{n-2}\theta^2+\binom{n}{3}c^{n-3}(\pm\theta)^3+\cdots\\ +(\pm\theta)^n=u+v\theta.\end{aligned}$$

Let $\theta^n=r_n\theta^2+s_n\theta+t_n$. Then

$$\binom{n}{2}c^{n-2}+\binom{n}{3}c^{n-3}(\pm r_3)+\cdots+(\pm r_n)=0. \tag{8}$$

As $\theta^3\equiv 0 \pmod{p^2}$, we have $r_i\equiv 0 \pmod{p^{2[i/3]}}$. Since $p\nmid c$, $p\mid\binom{n}{2}$. Suppose $p^k\parallel\binom{n}{2}$. If $p=2$ then $2^k\parallel\binom{n}{2}$. If $p\neq 2$ then $p^k\Big\|\binom{n}{2},\binom{n}{3}\cdots\binom{n}{p-1}$ and $p^{k-1}\Big\|\binom{n}{p}$. Using Lemma 2, we see that each term of (8) except the first is divisible by at least $p^{k+1}$. Hence $p^{k+1}\Big|\binom{n}{2}$, a contradiction.

THEOREM 7. *Let $\epsilon=\pm\theta+c_1$ be a unit of the ring $Z[\theta]$, where $\theta^3-3P\theta^2+3Q\theta-R=0$. If $c_1+P\not\equiv 0 \pmod 3$ and $c_1^2+2c_1P+Q\not\equiv 0 \pmod 3$, then $\epsilon^n=u+v\theta$ is impossible for $n>1$.*

*Proof.* Let $\varepsilon = \theta + c_1$. Then $\theta = \epsilon - c_1$. So from

$$\theta^3 - 3P\theta^2 + 3Q\theta - R = 0,$$

we get

$$(\epsilon - c_1)^3 - 3P(\epsilon - c_1)^2 + 3Q(\epsilon - c_1) - R = 0,$$

or

$$\epsilon^3 = 3(c_1 + P)\epsilon^2 - 3(c^2 + 2c_1P + Q)\epsilon + (c_1^3 + 3c_1^2P + 3c_1Q + R).$$

Now $N(\epsilon) = c_1^3 + 3c_1^2P + 3c_1Q + R = \pm 1$.

For convenience we write $\epsilon^3 = 3r\epsilon^2 - 3s\epsilon \pm 1$. Now by hypothesis $3 \nmid r$ and $3 \nmid s$. Let $\epsilon^n = u + v\theta$. Then $\epsilon^n = u + v(\epsilon - c_1) = u_1 + v_1\epsilon$, say. Suppose $n \equiv 2 \pmod 3$. Then $\epsilon^2(\epsilon^3)^m = u_1 + v_1\epsilon$, where $n = 2 + 3m$. As $\epsilon^3 \equiv \pm 1 \pmod 3$, we have $\pm\epsilon^2 \equiv u_1 + v_1\epsilon \pmod 3$, which is impossible. Let $n \equiv 0 \pmod 3$ and $n \neq 0$. Putting $n = 3m$, we get

$$(3r\epsilon^2 - 3s\epsilon \pm 1)^m = u_1 + v_1\epsilon. \tag{9}$$

But this is impossible by Theorem 1, whether $m$ is a positive or a negative integer, for $3 \nmid r$. Hence if $n \neq 0$, the only possibility is $n \equiv 1 \pmod 3$.

Let $n = 1 + 3m$, where $m > 0$. Then

$$\epsilon(3r\epsilon^2 - 3s\epsilon \pm 1)^m = u_1 + v_1\epsilon,$$

or

$$(3r\epsilon^2 - 3s\epsilon \pm 1)^m = v_1 \pm u_1(\epsilon^2 - 3r\epsilon + 3s).$$

Let $(r\epsilon^2 - s\epsilon)^i = r_i\epsilon^2 + s_i\epsilon + t_i$, where $r_i$, $s_i$, $t_i$ are rational integers. Then

$$(\pm 1)^m + \binom{m}{1}(\pm 1)^{m-1}3(r\epsilon^2 - s\epsilon) + \binom{m}{2}(\pm 1)^{m-2}3^2(r_2\epsilon^2 + s_2\epsilon + t_2)$$
$$+ \cdots + 3^m(r_m\epsilon^2 + s_m\epsilon + t_m) = \pm u_1\epsilon^2 \mp 3ru_1\epsilon + (v_1 \pm 3su_1).$$

On equating coefficients of $\epsilon^2$ and $\epsilon$, we obtain

$$(\pm 1)^{m-1}3mr + (\pm 1)^{m-2}3^2\binom{m}{2}r_2 + (\pm 1)^{m-3}3^3\binom{m}{3}r_3 + \cdots + 3^m r_m = \pm u_1, \tag{10}$$

and

$$(11)\quad -(\pm 1)^{m-1}3ms + (\pm 1)^{m-2}3^2\binom{m}{2}s_2 + (\pm 1)^{m-3}3^3\binom{m}{3}s_3 + \cdots + 3^m s_m$$
$$= \mp 3ru_1.$$

Multiplying both sides of (10) by $3r$ and then adding to (11), we obtain

$$(\pm 1)^{m-1}3m(3r^2 - s) + (\pm 1)^{m-2}3^2\binom{m}{2}(3r_2r + s_2)$$
$$+ (\pm 1)^{m-3}3^3\binom{m}{3}(3r_3r + s_3) + \cdots + 3^m(3r_mr + s_m) = 0.$$

We see from this that $3 \mid m(3r^2 - s)$. As $3 \nmid s$, we have $3 \mid m$. Suppose $3^k \| m$. Using Lemma 2, we easily see that all the terms except the first are divisible by $3^{k+2}$, while the first is exactly divisible by $3^{k+1}$, which is impossible. Hence $m = 0$, i.e. $n = 1$.

So if $n$ is a nonnegative integer and $\epsilon^n = u + v\theta$, then $n = 0$ or $n = 1$. The proof for $\epsilon = -\theta + c$, is completely analogous.

THEOREM 8. *If* $\epsilon = b_1\theta + c_1$ *is a positive unit in* $Z[\theta]$, *where* $\theta^3 - P\theta^2 + Q\theta - R = 0$ *with* $D(\theta)$ *negative and* $\neq -23$, *then* $\epsilon^n = u + v\theta$ *implies that* $n \geqq 0$.

To prove this theorem we need the following well-known result.

LEMMA 9 (Nagell [8]). *If* $\eta$ *is a unit,* $D(\eta) < 0$, $0 < \eta < 1$, *then* $\eta^n = x + y\eta$ *implies that* $n \geqq 0$, *except in the case when* $\eta^3 + \eta^2 - 1 = 0$. *In this case* $\eta^{-2} = 1 + \eta$ *and* $D(\eta) = -23$.

*Proof of Theorem* 8. Let $\epsilon = b_1\theta + c_1$ be a positive unit in $Z[\theta]$. Then $0 < \epsilon < 1$. Since $\epsilon$ is contained in $Z[\theta]$, we get $D(\epsilon) = \delta^2 \cdot D(\theta)$. Hence $D(\epsilon) < 0$ and $\neq -23$.

Let $\epsilon^n = u + \theta$. Since $\epsilon = b_1\theta + c_1$ we have

$$(b_1\theta + c_1)^n = u + v\theta.$$

Then $b_1 \mid v$ when $n$ is a positive integer. In case $n$ is negative, we put $n = -m$ where $m$ is positive. Let $\epsilon^{-1} = a'\theta^2 + b'\theta + c'$. Then $\theta^3 = P\theta^2 - Q\theta + R$ and $\epsilon\epsilon^{-1} = 1$ imply

$$(12)\qquad b_1a'P + b_1b' + c_1a' = 0,$$

$$(13)\qquad -b_1a'Q + b_1c' + c_1b' = 0,$$

and

$$b_1a'R + c_1c' = 1. \tag{14}$$

Since $(b_1, c_1) = 1$, $\epsilon = b_1\theta + c_1$ being a unit, we conclude that $b_1 | a'$ and $b_1 | b'$ from (12) and (13) respectively. Then from

$$(b_1\theta + c_1)^n = (a'\theta^2 + b'\theta + c')^m = u + v\theta,$$

we see that $b_1 | v$.

Since $\epsilon = b_1\theta + c_1$, we have $\theta = (\epsilon - c_1)/b_1$, and hence $\epsilon^n = u + v\theta$ can be written as

$$\epsilon^n = u + \frac{v(\epsilon - c_1)}{b_1} = (u - vc_1/b_1) + v\epsilon/b_1 = x + y\epsilon,$$

where $x$ and $y$ are rational integers. Then by Lemma 9, $n \geqq 0$. For binorms in fields of degree higher than three, one can see **[9]**. Recently Bernstein **[1]** has shown that units of the form $\epsilon = 1 + xw + yw^2$, $x, y \in Q$ exist for infinitely many algebraic number fields $Q(w)$ of degree $n \geqq 4$.

Now we solve $y^2 - 113 = x^3$ to show the application of some of the above theorems. The above equation is a special case of the well-known Mordell Equation $y^2 - k = x^3$, which has interested mathematicians for more than three centuries, and has played an important role in the development of number theory. In the range $0 < k \leqq 100$ it is known that $y^2 - k = x^3$, $k = 17$ has the maximum number of solutions. In the range $100 < k \leqq 200$ it is found **[6]** that $y^2 - k = x^3$, $k = 113$ has the maximum number of solutions. The complete solution of this equation is given below.

The fundamental unit of $Q(\sqrt{113})$ is $\eta = 776 + 73\sqrt{113}$, and $h(Q\sqrt{113}) = 1$. 2 splits into two different prime ideals in the field $Q(\sqrt{113})$. Hence by Theorem 5 of Hemer **[4]**, all the integral solutions of $y^2 - 113 = x^3$ can be obtained from the following equations:

$$\pm y + \sqrt{113} = \left(\frac{a + b\sqrt{113}}{2}\right)^3, \quad x = \frac{a^2 - 113b^2}{4},$$

$$\pm y + \sqrt{113} = (776 + 73\sqrt{113})\left(\frac{a + b\sqrt{113}}{2}\right)^3, \quad x = (113b^2 - a^2)/4,$$

$$\frac{1}{2}(\pm y + \sqrt{113}) = \left(\frac{11 + \sqrt{113}}{2}\right)\left(\frac{a + b\sqrt{113}}{2}\right)^3, \quad x = (a^2 - 113b^2)/2,$$

$$\frac{1}{2}(\pm y+\sqrt{113})=\left(\frac{11+\sqrt{113}}{2}\right)(776+73\sqrt{113})\left(\frac{a+b\sqrt{113}}{2}\right)^3,$$
$$x=(113b^2-a^2)/2,$$

$$\frac{1}{2}(\pm y+\sqrt{113})=\left(\frac{11+\sqrt{113}}{2}\right)(776-73\sqrt{113})\left(\frac{a+b\sqrt{113}}{2}\right)^3,$$
$$x=(113b^2-a^2)/2.$$

On equating irrational parts we have respectively

$$3a^2b+113b^3=8, \tag{15}$$

$$73(a^3+3\cdot 113ab^2)+776(3a^2b+113b^3)=8, \tag{16}$$

$$(a^3+3\cdot 113ab^2)+11(3a^2b+113b^3)=8, \tag{17}$$

$$1579(a^3+3\cdot 113ab^2)+16785(3a^2b+113b^3)=8, \tag{18}$$

$$-27(a^3+3\cdot 113ab^2)+287(3a^2b+113b^3)=8. \tag{19}$$

Clearly (15) has no solution in integers. From (16) it is easily seen that $a$ and $b$ are both even. Putting $a=2u_1$, $b=2v_1$ in (16), we obtain

$$73(u_1^3+3\cdot 113u_1v_1^2)+776(3u_1^2v_1+113v_1^3)=1. \tag{20}$$

The substitution $u_1=21u-52v$, $v_1=-2u+5v$ in (20) yields

$$F(u,v)=u^3-33uv^2+76v^3=1. \tag{21}$$

This corresponds to the ring $Z[\theta]$, where $\theta^3-33\theta-76=0$. In this ring the fundamental unit is $\epsilon=4\theta^2-16\theta-71$. By Theorem 1,

$$(4\theta^2-16\theta-71)^n=u+v\theta$$

is only possible for $n=0$. Then $u=1$, $v=0$, and so $a=42$, $b=-4$. Hence $x=11$, $y=\pm 38$.

The substitution $a=u_1-11v_1$, $b=v_1$ in (17) gives

$$u_1^3-24u_1v_1^2+176v_1^3=8. \tag{22}$$

Hence $u_1\equiv 0 \pmod 2$. Putting $u_1=2u$, $v_1=v$ in (22), we get

$$F(u,v)=u^3-6uv^2+22v^3=1. \tag{23}$$

This corresponds to the ring $Z[\theta]$, where $\theta^3-6\theta-22=0$; $Z[\theta]$ has fundamental unit $\epsilon=2\theta-7$.

Now we consider

$$(2\theta-7)^n=u+v\theta. \tag{24}$$

By Theorem 8, $n\geqq 0$ and by Lemma 5, $n\leqq 1$. Therefore (24) has only the two solutions $n=0$, $n=1$. These solutions correspond to $x=2$, $y=\pm 11$ and $x=422$, $y=\pm 8669$ respectively.

Substituting $a=-21u_1+53v_1$, $b=2u_1-5v_1$ in (18), we get

$$8v_1^3+12v_1^2u_1-42v_1u_1^2+27u_1^3=8. \tag{25}$$

We put $u_1=2v$, $v_1=u-v$ in (25), since $u_1\equiv 0 \pmod 2$. This gives

$$F(u,v)=u^3-24uv^2+50v^3=1. \tag{26}$$

This corresponds to the ring $Z[\theta]$, where $\theta^3-24\theta-50=0$, with the fundamental unit $\epsilon=-3\theta^2+10\theta+41$. We see that $\epsilon\equiv 2\theta^2+1 \pmod 5$ and $\epsilon^2\equiv 1 \pmod 5$ while $\epsilon^2\equiv -5\theta^2+5\theta+6 \pmod{25}$. Hence $\epsilon^2=a_1\theta^2+b_1\theta+c_1$ implies that $5\|a_1$, $5\|b_1$. Hence, by Theorem 1, $\epsilon^n=u+v\theta$ is impossible for an even integer $n\neq 0$. When $n$ is odd we have

$$2\theta^2+1\equiv u+v\theta \pmod 5.$$

This is impossible. So we have $n=0$. Then $u=1$, $v=0$ and hence $x=8$, $y=\pm 25$.

The substitution $a=111u_1+10v_1$, $b=11u_1+v_1$ in (19) yields

$$v_1^3-312v_1u_1^2-2128u_1^3=8. \tag{27}$$

Since (27) implies $v_1\equiv 0 \pmod 2$, we put $v_1=12u+10v$, $u_1=-u-v$ and get

$$F(u,v)=v^3+12vu^2+14u^3=1. \tag{28}$$

The fundamental unit of the ring $Z[\theta]$, where $\theta^3+12\theta-14=0$, is $\epsilon=\theta-1$, satisfying $\epsilon^3+3\epsilon^2+15\epsilon-1=0$.

Then by Theorems 8 and 6,

$$\epsilon^n=(\theta-1)^n=v+u\theta$$

has only two solutions, viz. $n=0$ and 1.

Incidentally, we cannot reach this conclusion by using the standard criterion of Hemer **[4]**, which is as follows:

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

Now $N(\epsilon' + \epsilon'') = N(-3 - \epsilon) = -46$ has only the odd prime divisor $p = 23$. The least exponent $m$ such that $a_m \equiv b_m \equiv 0 \pmod{23}$ is $m = 22$, and $a_m \not\equiv 0 \pmod{23^2}$. But unfortunately $c_{24} \equiv 0 \pmod{23^2}$.

When $n = 0,\ u = 0,\ v = 1;\ a = -11,\ b = -1;\ x = -4,\ y = \pm 7.$

When $n = 1,\ u = 1,\ v = -1;\ a = 20,\ b = 2;\ x = 26,\ y = \pm 133.$

Hence the Diophantine equation $y^2 - 113 = x^3$ has exactly 6 solutions in integers. They are $(x, y) = (11, \pm 38)$, $(8, \pm 25)$, $(2, \pm 11)$, $(-4, \pm 7)$, $(422, \pm 8669)$ and $(26, \pm 133)$.

ACKNOWLEDGEMENT. We are thankful to the referee for comments for the improvement of the paper.

## REFERENCES

1. Leon Bernstein, *Truncated units in infinitely many algebraic number fields of degree $n \geqq 4$*, Math. Ann., **213** (1975), 275–279.

2. B. N. Delaunay and D. K. Faddeev, *The theory of irrationalities of the third degree*, Amer. Math. Soc., Providence, Rhode Island (1964).

3. R. Finkelstein and H. London, *On Mordell's Equations $y^2 - k = x^3$*, Bowling Green State University Press.

4. O. Hemer, *On the Diophantine equation $y^2 - k = x^3$*, Diss. Uppsala (1952).

5. L. J. Mordell, *Diophantine equations*, Pure and Appl. Math., **30**, Academic Press, New York, (1969), 238–254.

6. S. P. Mohanty, *On the Diophantine equation $y^2 - k = x^3$*, Diss. UCLA (1971).

7. ———, *On consecutive integer solutions for $y^2 - k = x^3$*, Proc. Amer. Math. Soc., **48** (1975), 281–285.

8. T. Nagell, *Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante*, Ibid Bd. **28** (1928).

9. Hans-Joachim Stender, *Lösbare Gleichungen $ax^n - by^n = C$ and Grundeinheiten für einige algebraische Zahlkörper vom Grade $n$, $n = 3, 4, 6$*; Habilitation paper, University of Cologne (1975).

Received November 3, 1975. The preparation of this paper was partly supported by NSF grant GP-23113.

UNIVERSITY OF CALIFORNIA, LOS ANGELES
AND
I. I. T. KANPUR, KANPUR-16, INDIA

# PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate, may be sent to any one of the four editors. Please classify according to the scheme of Math. Reviews, Index to Vol. 39. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

100 reprints are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: $72.00 a year (6 Vols., 12 issues). Special rate: $36.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION
Printed at Jerusalem Academic Press, POB 2390, Jerusalem, Israel.

# Pacific Journal of Mathematics

Vol. 68, No. 2 April, 1977