ON A THEOREM OF DELAUNAY AND SOME RELATED RESULTS

BASIL GORDON AND S. P. MOHANTY
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 \( \epsilon = \alpha \phi^2 + \beta \phi + c \) is a unit in the ring \( \mathbb{Z}[\theta] \), where \( \theta^4 - P\theta^2 + Q\theta - R = 0 \), \( p \) is an odd prime, \( \phi = \rho^\iota \theta \), \( \iota \geq 0 \) and \( p \nmid \alpha \), 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 \( \epsilon = \alpha \theta^2 + \beta \theta + c \) is a unit in \( \mathbb{Z}[\theta] \), where \( \theta^4 = d \theta^2 + e \theta + f \) and \( p^a \| a \), \( p^b \| b \), \( p \) being a prime, then \( \epsilon^n = u + v\theta \) is impossible for \( n \neq 0 \) in the following cases:

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

As an application of this and some other similar theorems, all integer solutions of the equation \( y^2 = x^4 + 113 \) are determined.

First we prove two simple lemmas.

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

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

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

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

If \( p \| n \) and \( p \nmid i \) then \( p \nmid r \) for \( i = p^q + r \). Then

\[
\binom{n - p^q}{r} = \binom{n - p^q}{r} \binom{n - p^q - 1}{r - 1}.
\]
is divisible by \( p \). Hence \( p^{a+1} \mid \binom{n}{i} \).

Again from

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

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

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

(i) \( \alpha \leq \beta < 2\alpha \)

(ii) \( \beta \leq \alpha < 2\beta \)

For \( \alpha \leq \beta \) we have \( p^\alpha \parallel a' \) and \( p^\beta \mid b' \).

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

\[
\begin{align*}
&\quad a'a'd^2 + ab'd + a'bd + aa'e + ac' + ca' + bb' = 0, \\
&\quad aa'f + aa'de + ab'e + a'be + bc' + b'c = 0, \\
&\quad aa'df + ab'f + a'bf + cc' = 1.
\end{align*}
\]

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

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

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

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 $(r\theta^2 + s\theta)' = a\theta^2 + b\theta + c$, with $a_i$, $b$, and $c_i$ rational integers. Then

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

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

\[
nc^{n-1} p^n r + \binom{n}{2} c^{n-2} p^{2n} a_2 + \cdots + p^n a_n = 0.
\]

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 $\alpha \geq 2$ 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

\[
nc^{n-1} p^\beta r + \binom{n}{2} c^{n-2} p^{2\beta} a_2 + \cdots + p^{\beta} a_n,
\]

where $(r\theta^2 + s\theta)' = a\theta^2 + b\theta + c$, 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 $p^\alpha \| a'$, $p^\beta \| b'$ for $\alpha \leq \beta$, and $p^\alpha \| a'$, $p^\beta \| b'$ for $\beta \leq \alpha < 2\beta - 1$, $\alpha \leq \beta < 2\alpha$ and $\beta \leq \alpha < 2\beta$. 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 
\( e^n = u + v\theta \) is possible for \( n > 3 \); examples are given in [2, page 417]. Very often the following theorem is useful.

**Theorem 4.** Let \( e = a_1\theta^2 + b_1\theta + c_i \) be a unit in \( \mathbb{Z}[\theta] \), where \( \theta^3 - p_1\theta - q_1 = 0 \). If \( p_1 \equiv 0 \pmod{3} \), then

\[
(6) \quad e^n = u + v\theta
\]

is impossible for \( n \neq 0 \) provided \( a_i \not\equiv 0 \pmod{3} \), \( b_1^2 + 2a_1c_1 \not\equiv 0 \pmod{3} \), and \( b_1^2c_1 + a_1^2 + a_1b_1q_1 \not\equiv 0 \pmod{3} \).

**Proof.** Let \( e^n = a_n\theta^2 + b_n\theta + c_n \). 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

\[
a_3 = a_1^3p_1^2 + 3a_1b_1^2p_1 + 3a_1^2c_1p_1 + 3b_1^2c_1 + 3a_1c_1^2 + 3a_1^2b_1q_1, \quad b_3 = 2a_1^3p_1q_1 + 3a_1b_1^2q_1 + 3a_1^2c_1q_1 + 3a_1^2b_1p_1^2 + b_1^3p_1 + 6a_1b_1c_1p_1 + 3b_1c_1^2, \quad c_3 = 3a_1^2b_1^2p_1q_1 + b_1^3q_1 + 6a_1b_1c_1q_1 + a_1^3q_1^2 + c_1^3.
\]

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 \( e^3 \) 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

\[
\epsilon \cdot (e^3)^m = u + v\theta,
\]

or

\[
(a_1\theta^2 + b_1\theta + c_i)(\pm 1)^m \equiv u + v\theta \pmod{3}.
\]

This congruence is impossible unless \( a_i \equiv 0 \pmod{3} \). Hence if \( a_i \not\equiv 0 \pmod{3} \), 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. \( b_1^2 + 2a_1c_1 \equiv 0 \).
(mod 3). Hence if \( b_i^2 + 2a_ic \neq 0 \) (mod 3), then \( n \equiv 2 \) (mod 3) is impossible. Finally suppose \( n = 3m \) in (6). Then we get

\[
(a_3\theta^2 + b_3\theta + c_3)^m = u + v\theta.
\]

Now \( a_3 \equiv b_3 \equiv 0 \) (mod 3), and \( a_3 \equiv 3b_1^2c_1 + 3a_1c_1^2 + 3a_1^2b_1q_1 \) (mod 9). If \( b_1^2c_1 + a_1c_1^2 + a_1^2b_1q_1 \neq 0 \) (mod 3), then \( a_3 \neq 0 \) (mod 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 \( \mathbb{Z}[\theta] \) 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 \( \mathbb{Z}[\theta] \), where \( \theta^3 - P\theta^2 + Q\theta - R = 0 \). If \( \theta^3 \equiv 0 \) (mod \( p^2 \)), where \( p \) is a prime, then \( p \not| c \) and \( \epsilon^n = u + v\theta \) is impossible for \( n > 1 \).

**Proof.** We have \((\epsilon - c)^3 \equiv 0 \) (mod \( p^2 \)). If \( p | c \) then \( \epsilon^3 \equiv 0 \) (mod \( p \)) where \( p^3 | N(\epsilon^3) = \pm 1 \). Hence \( p \not| c \). Let \( \epsilon^n = u + v\theta, n > 1 \). Then

\[
(c \pm \theta)^n = c^n + \binom{n}{1} c^{n-1}(\pm \theta) + \binom{n}{2} c^{n-2}\theta^2 + \binom{n}{3} c^{n-3}(\pm \theta)^3 + \cdots
\]

\[+ (\pm \theta)^n = u + v\theta.\]

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

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

As \( \theta^3 \equiv 0 \) (mod \( p^2 \)), we have \( r_i \equiv 0 \) (mod \( p^{2i/3} \)). Since \( p \not| c \), \( p | \binom{n}{2} \). Suppose \( p^k \| \binom{n}{2} \). If \( p = 2 \) then \( 2^k \| \binom{n}{2} \). If \( p \neq 2 \) then \( p^k \| \binom{n}{2}, \binom{n}{3}, \ldots, \binom{n}{p-1} \) and \( p^{k-1} \| \binom{n}{p} \). Using Lemma 2, we see that each term of (8) except the first is divisible by at least \( p^{k+1} \). Hence \( p^{k+1} \| \binom{n}{2} \), a contradiction.

**Theorem 7.** Let \( \epsilon = \pm \theta + c_i \) be a unit of the ring \( \mathbb{Z}[\theta] \), where \( \theta^3 - 3P\theta^2 + 3Q\theta - R = 0 \). If \( c_i + P \neq 0 \) (mod 3) and \( c_i^2 + 2c_iP + Q \neq 0 \) (mod 3), then \( \epsilon^n = u + v\theta \) is impossible for \( n > 1 \).
Proof. Let \( \varepsilon = \theta + c_1 \). Then \( \theta = \varepsilon - c_1 \). So from

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

we get

\[
(\varepsilon - c_1)^3 - 3P(\varepsilon - c_1)^2 + 3Q(\varepsilon - c_1) - R = 0,
\]

or

\[
\varepsilon^3 = 3(c_1 + P)\varepsilon^2 - 3(c^2 + 2c_1P + Q)\varepsilon + (c^3 + 3c^2P + 3c_1Q + R).
\]

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

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

\[
(3r\varepsilon^2 - 3s\varepsilon \pm 1)^m = u_1 + v_1\varepsilon.
\]

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

\[
\varepsilon(3r\varepsilon^2 - 3s\varepsilon \pm 1)^m = u_1 + v_1\varepsilon,
\]

or

\[
(3r\varepsilon^2 - 3s\varepsilon \pm 1)^m = v_1 \pm u_1(\varepsilon^2 - 3r\varepsilon + 3s).
\]

Let \( (r\varepsilon^2 - s\varepsilon)^i = r_1\varepsilon^2 + s_1\varepsilon + t_1 \), where \( r_1, s_1, t_1 \) are rational integers. Then

\[
\begin{align*}
(\pm 1)^m & + \binom{m}{1}(\pm 1)^{m-1}(r_1\varepsilon^2 - s_1\varepsilon) + \binom{m}{2}(\pm 1)^{m-2}3^2(r_2\varepsilon^2 + s_2\varepsilon + t_2) \\
& + \cdots + 3^m(r_m\varepsilon^2 + s_m\varepsilon + t_m) = \pm u_1\varepsilon^2 \pm 3ru_1\varepsilon + (v_1 \pm 3su_1).
\end{align*}
\]

On equating coefficients of \( \varepsilon^2 \) and \( \varepsilon \), we obtain

\[
(\pm 1)^{m-1}3mr + (\pm 1)^{m-2}3^2 \binom{m}{2} r_2 + (\pm 1)^{m-3}3^3 \binom{m}{3} r_3 + \cdots + 3^mr_m = \pm u_1,
\]

and
(11) \(- (\pm 1)^{n-1}3ms + (\pm 1)^{n-2}3^2 \binom{m}{2} s_2 + (\pm 1)^{n-3}3^3 \binom{m}{3} s_3 + \cdots + 3^n s_m\)

\(- \mp 3ru_1.\)

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

\[ (\pm 1)^{n-1}3^m (3r^2 - s) + (\pm 1)^{n-2}3^2 \binom{m}{2} (3r^2 + s_2) \]

\[ + (\pm 1)^{n-3}3^3 \binom{m}{3} (3r^3 + s_3) + \cdots + 3^n (3r^nr + s_m) = 0. \]

We see from this that \(3|m(3r^2 - s).\) As \(3 \not| s,\) we have \(3|m.\) Suppose \(3^k \parallel m.\) 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 \(n \geq 0.\)

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 \(n \geq 0,\) 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 \(b_1 | v\) 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

\begin{align*}
(12) & b_1a'P + b_1b' + c_1a' = 0, \\
(13) & -b_1a'Q + b_1c' + c_1b' = 0,
\end{align*}
and

\[(14) \quad b_1 a'R + c_1 c' = 1.\]

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

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

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

\[\epsilon^n = u + \frac{v(\epsilon - c_1)}{b_1} = (u - vc_1/b_1) + ve/b_1 = x + ye,
\]

where \(x\) and \(y\) are rational integers. Then by Lemma 9, \(n \geq 0\). 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 \(n \geq 4\).

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 \(0 < k \leq 100\) it is known that \(y^2 - k = x^3, k = 17\) has the maximum number of solutions. In the range \(100 < k \leq 200\) 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:

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

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

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

\[ x = \left( 113b^2 - a^2 \right)/2, \]

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

\[ x = \left( 113b^2 - a^2 \right)/2. \]

On equating irrational parts we have respectively

(15) \[ 3a^2b + 113b^3 = 8, \]

(16) \[ 73(a^3 + 3 \cdot 113ab^2) + 776(3a^2b + 113b^3) = 8, \]

(17) \[ (a^3 + 3 \cdot 113ab^2) + 11(3a^2b + 113b^3) = 8, \]

(18) \[ 1579(a^3 + 3 \cdot 113ab^2) + 16785(3a^2b + 113b^3) = 8, \]

(19) \[ -27(a^3 + 3 \cdot 113ab^2) + 287(3a^2b + 113b^3) = 8. \]

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

(20) \[ 73(u_1^3 + 3 \cdot 113u_1v_1^2) + 776(3u_1^2v_1 + 113v_1^3) = 1. \]

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

(21) \[ F(u, v) = u^3 - 33uv^2 + 76v^3 = 1. \]

This corresponds to the ring \( \mathbb{Z}[\theta] \), where \( \theta^3 - 33\theta - 76 = 0 \). In this ring the fundamental unit is \( e = 4\theta^2 - 16\theta - 71 \). 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

(22) \[ u_1^3 - 24u_1v_1^2 + 176v_1^3 = 8. \]

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

(23) \[ F(u, v) = u^3 - 6uv^2 + 22v^3 = 1. \]
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

\[(2\theta - 7)^n = u + v\theta.\]

By Theorem 8, $n \geq 0$ and by Lemma 5, $n \leq 1$. 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

\[8v_1^3 + 12v_1^2u_1 - 42v_1u_1^2 + 27u_1^3 = 8.\]

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

\[F(u, v) = u^3 - 24uv^2 + 50v^3 = 1.\]

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

\[v_1^3 - 312v_1u_1^2 - 2128u_1^3 = 8.\]

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

\[F(u, v) = v^3 + 12vu^2 + 14u^3 = 1.\]

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,

\[\epsilon^n = (\theta^3 - 1)^n = v + u\theta\]

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 $a_m \not\equiv 0 \pmod{23^3}$. 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


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
Ann K. Boyle, M. G. Deshpande and Edmund H. Feller, *On nonsingularity k-primitive rings* .......................................................... 303
Rolando Basim Chuaqui, *Measures invariant under a group of transformations* .......................................................... 313
Wendell Dan Curtis and Forrest Miller, *Gauge groups and classification of bundles with simple structural group* ......... 331
Garret J. Etgen and Willie Taylor, *The essential uniqueness of bounded nonoscillatory solutions of certain even order differential equations* .......................................................... 339
Paul Ezust, *On a representation theory for ideal systems* .................... 347
Richard Carl Gilbert, *The deficiency index of a third order operator* .......... 369
John Norman Ginsburg, *S-spaces in countably compact spaces using Ostaszewski’s method* ........................................... 393
Basil Gordon and S. P. Mohanty, *On a theorem of Delaunay and some related results* .......................................................... 399
Douglas Lloyd Grant, *Topological groups which satisfy an open mapping theorem* .......................................................... 411
Charles Lemuel Hagopian, *A characterization of solenoids* .................... 425
Kyong Taik Hahn, *On completeness of the Bergman metric and its subordinate metrics. II* .......................................................... 437
G. Hochschild and David Wheeler Wigner, *Abstractly split group extensions* .......................................................... 447
Gary S. Itzkowitz, *Inner invariant subspaces* .................................. 455
Jiang Luh and Mohan S. Putcha, *A commutativity theorem for non-associative algebras over a principal ideal domain* ........ 485
Akio Osada, *On the distribution of a-points of a strongly annular function* .......................................................... 491
Jeffrey Lynn Spielman, *A characterization of the Gaussian distribution in a Hilbert space* .......................................................... 497
Robert Moffatt Stephenson Jr., *Symmetrizable-closed spaces* .................. 507
Peter George Trotter and Takayuki Tamura, *Completely semisimple inverse Δ-semigroups admitting principal series* ......... 515
Charles Irvin Vinsonhaler and William Jennings Wickless, *Torsion free abelian groups quasi-projective over their endomorphism rings* .......................................................... 527
Frank Arvey Wattenberg, *Topologies on the set of closed subsets* ............. 537
Richard A. Zalik, *Integral representation of Tchebycheff systems* .......... 553