TOKYO J. MATH.
VOL. 11, NO. 1, 1988

The Diophantine Equation $x^2 \pm ly^2 = z^l$ Connected with Fermat's Last Theorem

Norio ADACHI

Waseda University

Dedicated to late Professor M. Kinoshita

Introduction.

Let l be an odd prime number and put $l^* = (-1)^{(l-1)/2} l$. Fermat's Last Theorem was proved by Euler for the exponent $l=3$ ([3]) and by Dirichlet for the exponent $l=5$ ([1]). Their proofs, which will be reproduced in §2 in modern terms (cf. Edwards [2]), are based on the fact that the implication

$$a^2 - l^* b^2 = l\text{-th power} \quad \Longrightarrow \quad \exists u, v;\ a + b\sqrt{l^*} = (u + v\sqrt{l^*})^l$$

is justified for $l=3$ or $l=5$ under some subsidiary conditions. It is often said that their success is due to the unique factorization property in the maximal order of the quadratic field $\boldsymbol{Q}(\sqrt{l^*})$ for $l=3$ or $l=5$, respectively. But, this point of view is not exact, as will be seen in §1; for the above implication is true virtually for any prime l (Theorem 1, Theorem 2). The examples in §2 will show that the difficulty lies in finding the step of "infinite descent", not in the failure of the unique factorization.

§1. The Diophantine equation $x^2 - l^* y^2 = z^l$.

Let l be an odd prime number fixed throughout the present paper and put $l^* = (-1)^{(l-1)/2} l$. We use roman small letters such as $a, b, u, v, \cdots$ to designate rational integers. We say that a and b have the property (P), if they are relatively prime, of opposite parity, and $a^2 - l^* b^2$ is an l-th power of a rational integer.

We consider here whether the following implication $(*)$ is justified:

$$(*) \qquad \text{(P)} \quad \Longrightarrow \quad \exists u, v;\ a + b\sqrt{l^*} = (u + v\sqrt{l^*})^l$$

Received March 12, 1987

In his Algebra [3], Euler used the fact that the implication (*) is valid in the case $l=3$. While his proof was incomplete, we know that the assertion is true. In 1825 Dirichlet presented a paper ([1]), where he proved that the implication is valid in the case $l=5$ under the subsidiary condition that b is divisible by 5, which is obviously a necessary condition. We generalize their results as follows:

THEOREM 1. *The implication* (*) *is always valid in the case* $l\equiv -1 \pmod 4$.

COROLLARY. *Suppose* $l\equiv -1 \pmod 4$ *and* a^2+lb^2 *to be a* $2l$*-th power, where* a, b *are relatively prime and of opposite parity. Then there exist* u, v *such that* $a+b\sqrt{-l}=\pm(u+v\sqrt{-l})^{2l}$.

THEOREM 2. *In the case* $l\equiv 1 \pmod 4$, *we suppose that the Bernoulli number* $B_{(l-1)/2}$ *is not divisible by* l. *Then the implication* (*) *is valid under the condition that* b *is divisible by* l.

COROLLARY. *Suppose* $l\equiv 1 \pmod 4$ *and* a^2-lb^2 *to be a* $2l$*-th power, where* a, b *are relatively prime and of opposite parity. In addition, suppose that* $B_{(l-1)/2}$ *is not divisible by* l. *Then there exist* u, v *such that* $a+b\sqrt{l}=\pm(u+v\sqrt{l})^{2l}$.

The theorems immediately follow from the following four lemmas.

LEMMA 1. *Suppose that* a *and* b *have the property* (P). *Then* $a+b\sqrt{l^*}$ *and* $a-b\sqrt{l^*}$ *are relatively prime in the maximal order of the quadratic field* $\boldsymbol{Q}(\sqrt{l^*})$.

PROOF. Suppose that there is a prime ideal $\mathfrak{p}$ in the maximal order which divides both $a+b\sqrt{l^*}$ and $a-b\sqrt{l^*}$. The number 2 is not divisible by $\mathfrak{p}$, since $a^2-l^*b^2$ is odd. Hence $\mathfrak{p}$ divides $b\sqrt{l^*}$ as well as a. If $\mathfrak{p}$ does not divide $\sqrt{l^*}$, then $\mathfrak{p}$ divides both a and b, which is impossible, since a is supposed to be prime to b. Therefore $\mathfrak{p}$ divides $\sqrt{l^*}$, hence also l. It follows from this that a is divisible by l. Thus l divides $a^2-l^*b^2$, which is an l-th power by the assumption. This means that b is also divisible by l. This contradiction completes the proof of the lemma.

While the following is a known result, its proof will be given, for the author cannot find one in the literatures at hand:

LEMMA 2. *Let* K *be the quadratic field with discriminant* d. *Then the class number* h_K *of* K *is smaller than* $d/4$, *if* $d>0$, *and* $|d|/3$, *if* $d<0$.

PROOF. Let D denote the number $\sqrt{d}/2$, if $d>0$, and $\sqrt{|d|/3}$, if $d<0$. It is well known that in each ideal class of K there exists an ideal A whose norm is smaller than D (cf., e.g. Hasse [4], p. 565). Let n be any positive integer $<D$, and $p_1 \cdots p_m$ the decomposition of n into prime factors. Then for each n there are at most 2^m ideals whose norms are n. On the other hand we have

$$2^m \leqq p_1 \cdots p_m = n < D .$$

Therefore there are at most D ideals whose norms are a given number $<D$. This implies that h_K is smaller than D^2.

LEMMA 3. *Suppose that a and b have the property* (P) *and, in case* $l \equiv 1 \pmod 4$), *that b is divisible by l and that the Bernoulli number $B_{(l-1)/2}$ is not divisible by l. Then there exist x and y such that $a+b\sqrt{l^*}=(x+y\omega)^l$, where ω denotes* $(1+\sqrt{l^*})/2$.

PROOF. By Lemma 1, $a+b\sqrt{l^*}$ and $a-b\sqrt{l^*}$ are relatively prime. So there is an ideal A of the quadratic field $K=\boldsymbol{Q}(\sqrt{l^*})$ such that

$$a+b\sqrt{l^*}=A^l .$$

By Lemma 2, the class number h_K of the field K is smaller than l, hence prime to l. Therefore A is a principal ideal. Hence there are an algebraic integer $x+y\omega$ and a unit ε of the maximal order of the field K such that

$$a+b\sqrt{l^*}=\varepsilon(x+y\omega)^l .$$

If $l \equiv -1 \pmod 4$ and $l \neq 3$, then the units of the maximal order of K are ± 1; hence the assertion is clear in this case. Suppose $l \equiv 1 \pmod 4$ and write

$$x+y\omega=\frac{c+d\sqrt{l^*}}{2}$$

and

$$\left(\frac{c+d\sqrt{l^*}}{2}\right)^l=\frac{c_1+d_1\sqrt{l^*}}{2} .$$

Then it must hold that $c_1 \not\equiv 0 \pmod l$, whereas $d_1 \equiv 0 \pmod l$. Write $\varepsilon=(s+t\sqrt{l^*})/2$. Then we have

$$\begin{aligned} a+b\sqrt{l^*} &= \frac{s+t\sqrt{l^*}}{2}\cdot\frac{c_1+d_1\sqrt{l^*}}{2} \\ &= \frac{(c_1s+d_1tl^*)+(c_1t+d_1s)\sqrt{l^*}}{4} . \end{aligned}$$

Since d_1 is divisible by l and c_1 is not, we have $c_1t+d_1s\equiv 0 \pmod{l}$, if and only if $t\equiv 0 \pmod{l}$. Now it holds that $c_1t+d_1s\equiv 0 \pmod{l}$, since it is assumed that b is divisible by l; hence t must be divisible by l.

Let $E=(u+v\sqrt{l^*})/2$ be a fundamental unit of the maximal order of the field K. Then we may assume that there is a positive integer m such that $\varepsilon=\pm E^m$. It remains to show that m is divisible by l. The following congruence is known (cf., e.g. Washington [5], p. 81);

$$h_K\cdot\frac{v}{u}\equiv B_{(l-1)/2} \pmod{l}\ .$$

By Lemma 2 and the assumption of our lemma, neither h_K nor $B_{(l-1)/2}$ is divisible by l. Hence v is not divisible by l. Therefore, it follows from the binomial expansion of $(u+v\sqrt{l^*})^m$ that m is divisible by l, since t is divisible by l.

Finally, we treat the case $l=3$. Note that $(x+y\omega)^3=((c+d\sqrt{-3})/2)^3\in \boldsymbol{Z}[\sqrt{-3}]$ and that it is prime to 2. Therefore, $\varepsilon=(a+b\sqrt{-3})/(x+y\omega)^3$ is an element of $\boldsymbol{Z}[\sqrt{-3}]$. If we write ε as $\pm((1+\sqrt{-3})/2)^j$, where $j=0$, 1 or 2, then j must be 0. Hence the proof of the lemma is complete.

LEMMA 4. *Put $\omega=(1+\sqrt{l^*})/2$. If $a+b\sqrt{l^*}$ is an l-th power in the field $K=\boldsymbol{Q}(\sqrt{l^*})$, say $(x+y\omega)^l$, then y is divisible by 2.*

PROOF. Let ζ be a primitive l-th root of unity and $\bar{\omega}$ the conjugate of ω. Then we have

$$\begin{aligned}
a&=\frac{1}{2}\{(a+b\sqrt{l^*})+(a-b\sqrt{l^*})\}\\
&=\frac{1}{2}\{(x+y\omega)^l+(x+y\bar{\omega})^l\}\\
&=\frac{1}{2}\left\{\left(\frac{c+d\sqrt{l^*}}{2}\right)^l+\left(\frac{c-d\sqrt{l^*}}{2}\right)^l\right\}\\
&=\frac{c}{2}\prod_{j=1}^{l-1}\left(\frac{c+d\sqrt{l^*}}{2}+\zeta^j\frac{c-d\sqrt{l^*}}{2}\right)\,.
\end{aligned}$$

Let $\mathfrak{p}$ be a prime divisor of 2 in the cyclotomic field $\boldsymbol{Q}(\zeta)$, and suppose that $\mathfrak{p}$ divides some factor of the above product, say $(c+d\sqrt{l^*})/2+\zeta(c-d\sqrt{l^*})/2$. Then we have

$$\begin{aligned}
&c(1+\zeta)+d(1-\zeta)\sqrt{l^*}\equiv 0 \pmod{2\mathfrak{p}}\ ,\\
\therefore\quad &c(1+\zeta)\equiv d(\zeta-1)\sqrt{l^*} \pmod{2\mathfrak{p}}\ .
\end{aligned}$$

Squaring both sides, we obtain

$$c^2(1+\zeta)^2 \equiv d^2(\zeta-1)^2 l^* \pmod{4\mathfrak{p}} .$$

What we have to show is that c is even. Suppose the contrary; then $c \equiv d \equiv 1 \pmod 2$. If we take m so that $l^*=4m+1$, we obtain the congruence

$$m\zeta^2+\zeta+m \equiv 0 \pmod{\mathfrak{p}} ,$$

since $c^2 \equiv d^2 \equiv 1 \pmod 8$. It follows from this that $\zeta \equiv 0 \pmod{\mathfrak{p}}$ or $\zeta^2+\zeta+1 \equiv 0 \pmod{\mathfrak{p}}$, according as m is even or not. But both ζ and $\zeta^2+\zeta+1$ are units, unless $l=3$. This is a contradiction. Therefore c must be even; so is y.

It remains to take care of the case $l=3$. It is easily seen that

$$(1) \qquad (x+y\omega)^3=(x\omega+y\omega^2)^3=(-y+(x-y)\omega)^3$$

and

$$(2) \qquad (x+y\omega)^3=(x\omega^2+y)^3=(y-x-x\omega)^3 .$$

If y is even, we have nothing to do. Suppose that y is odd. If x is odd, the equalities (1) show that we have only to substitute $-y$ or $x-y$ for x or y, respectively; if x is even, the equalities (2) show that we have only to substitute $y-x$ or $-x$ for x or y, respectively. Thus the proof of the lemma is complete.

PROOF OF COROLLARY TO THEOREM 1. The class number of the quadratic field $K=\boldsymbol{Q}(\sqrt{-l})$ is not divisible by 2, since the discriminant of K has no prime divisor other than l. Hence we can write

$$\begin{aligned} a+b\sqrt{-l} &= \pm(x+y\omega)^{2l} \\ &= \pm\left\{\left(x^2-\frac{l+1}{4}y^2\right)+(2xy+y^2)\omega\right\}^l \end{aligned}$$

where $\omega=(1+\sqrt{-l})/2$. By Lemma 4, $2xy+y^2 \equiv 0 \pmod 2$; hence $y \equiv 0 \pmod 2$.

The proof of Corollary to Theorem 2 is almost the same as above. In fact, substitute l for $-l$, and $\pm\varepsilon$ for $\pm$, where ε is a suitable positive unit in the maximal order of the field $K=\boldsymbol{Q}(\sqrt{l})$. It is clear that ε has positive norm. Hence ε is a square of another unit, since any of the fundamental units have negative norm, provided $l \equiv 1 \pmod 4$. The corollary follows from this and Theorem 2.

§ 2. Connection with Fermat's Last Theorem.

Let l be an odd prime number fixed as in the preceding section, and consider the Fermat equation

$$x^l+y^l+z^l=0 \tag{3}$$

Suppose that the equation (3) has a non-trivial solution (x, y, z) such that x, y and z are relatively prime and one of them is divisible by l, say we suppose $z\equiv 0 \pmod{l}$. Moreover, we suppose, for simplicity, that z is also even (if this is not the case, we must use a slight variant of our theorems in § 1; cf. Edwards [2], pp. 70–73);

$$z\equiv 0 \pmod{2l} . \tag{4}$$

This is the case which Dirichlet first treated in his paper [1] in 1825.

Since x and y are odd, we can set $x+y=2u$, $x-y=2v$. Then we have $x=u+v$, $y=u-v$.

LEMMA 5. *Let the notations be as above. Then u and v are of opposite parity and relatively prime. Moreover, u is divisible by $2l$.*

PROOF. The first part is clear, since x and y are relatively prime. And also it is clear that u is divisible by l, since z is divisible by l. As x and y are odd, $x^{l-1}+x^{l-2}y+\cdots+y^{l-1}$ is also odd. Hence $x+y=2u$ is divisible by 2^l, for z^l is divisible by 2^l. This completes the proof of the lemma.

Let ζ be a primitive l-th root of unity. Denote by L the cyclotomic field $\boldsymbol{Q}(\zeta)$, and by N_L the norm map from the field L to the rational number field $\boldsymbol{Q}$. We can set $u=lw$ by Lemma 5. Then we have

$$\begin{aligned} x^l+y^l &= (u+v)^l+(u-v)^l \\ &= 2uN_L((u+v)+\zeta(u-v)) \\ &= 2lwN_L(1-\zeta)N_L\left(v+\frac{1+\zeta}{1-\zeta}lw\right) \\ &= 2l^2wN_L\left(v+\frac{1+\zeta}{1-\zeta}lw\right), \end{aligned}$$

since $N_L(1-\zeta)=l$. It follows from Lemma 5 and $N_L(v+((1+\zeta)/(1-\zeta))lw)\equiv v^l \pmod{1-\zeta}$ that $2l^2w$ and $N_L(v+((1+\zeta)/(1-\zeta))lw)$ are relatively prime. By (3), x^l+y^l is an l-th power. Hence we have

$$(5)\qquad \begin{cases} 2l^2 w = l\text{-th power}\,, \\ N_L\left(v+\dfrac{1+\zeta}{1-\zeta}lw\right) = l\text{-th power}\,. \end{cases}$$

LEMMA 6. *The number $N_L(v+((1+\zeta)/(1-\zeta))lw)$ can be written in the form $p^2-l^*q^2$ where p and q are rational integers which have opposite parity and relatively prime.*

PROOF. As is well known, $\sqrt{l^*}\in L$. Let K be the quadratic field $\boldsymbol{Q}(\sqrt{l^*})$ which is contained in the field L. Then we have

$$\begin{aligned} N_L\left(v+\frac{1+\zeta}{1-\zeta}lw\right) &= N_K N_{L/K}\left(v+\frac{1+\zeta}{1-\zeta}lw\right) \\ &= N_K(p+q\sqrt{l^*}) \\ &= p^2-l^*q^2\,. \end{aligned}$$

Indeed p and q are rational integers, since u and hence w is even by Lemma 5. And it is also clear that they are of opposite parity, since $p^2-l^*q^2$ is odd. They are relatively prime, because $p+\sqrt{l^*}q$ and $p-\sqrt{l^*}q$ must be relatively prime.

Applying Lemma 6 to the second equation of (5), we have

$$(6)\qquad \begin{cases} 2l^2 w = l\text{-th power}\,, \\ p^2-l^*q^2 = l\text{-th power}\,, \end{cases}$$

where p and q are polynomials of v and w.

EXAMPLE 1 (the case $l=3$; $l^*=-3$). In this case, we have $p=v$ and $q=w$. The relations (6) are

$$(7)\qquad 2\cdot 3^2 w = \text{cube}$$

and

$$v^2+3w^2 = \text{cube}\,.$$

By Theorem 1 there are s and t such that

$$v+\sqrt{-3}w=(s+\sqrt{-3}t)^3\,.$$

Then we have

$$v=s(s+3t)(s-3t)$$

and

$$w=3t(s+t)(s-t)\ .$$

It follows that s is odd and t is divisible by $2\cdot 3$, since v is odd and w is divisible by $2\cdot 3$. Substituting $3t(s+t)(s-t)$ for w in (7), we have

$$2t(s+t)(s-t)=\text{cube}\ .$$

As $2t$, $s+t$ and $s-t$ are pairwise relatively prime, we can conclude that all of them are cubic numbers;

$$s-t=a^3\ ,\quad s+t=b^3 \quad\text{and}\quad 2t=c^3\ .$$
$$\therefore\quad a^3+(-b)^3+c^3=0\ .$$

Furthermore, c is divisible by $2\cdot 3$. It is easily seen that $|c|$ is smaller than $|z|$ in (3). This supplies the step of infinite descent.

EXAMPLE 2 (the case $l=5$; $l^*=5$). In this case, we have $p=v^2+5^2w^2$ and $q=2\cdot 5w^2$; for the calculation, see Example 3 below. The relations (6) are written as follows in this case:

$$(8)\qquad \begin{cases} 2\cdot 5^3 q=\text{fifth power}\ , \\ p^2-5q^2=\text{fifth power}\ . \end{cases}$$

Since $q\equiv 0 \pmod 5$, applying Theorem 2 to the second relation of (8), we have

$$p+\sqrt{5}\,q=(a+\sqrt{5}\,b)^5$$

for some a and b. Put

$$\alpha=a+\sqrt{5}\,b\ .$$

Then we have

$$\begin{aligned} q&=\frac{1}{2\sqrt{5}}\{(a+\sqrt{5}\,b)^5-(a-\sqrt{5}\,b)^5\} \\ &=b\prod_{j=1}^{l-1}(\alpha-\zeta^j\bar{\alpha}) \\ &=bN_L(\alpha-\zeta\bar{\alpha}) \qquad (\because\ 5\equiv 1 \pmod 4 \text{ and } \alpha\in K) \\ &=5bN_L\Big(a+\frac{1+\zeta}{1-\zeta}\sqrt{5}\,b\Big) \\ &=5b(u^2-5v^2)\ , \end{aligned}$$

where $u=a^2+5b^2$, $v=2b^2$. Substituting $5b(u^2-5v^2)$ for q in the first relation of (8), we have

$$2\cdot 5^4 b(u^2-5v^2) = \text{fifth power} .$$

Therefore

$$\begin{cases} 2\cdot 5^4 b = \text{fifth power} , \\ u^2-5v^2 = \text{fifth power} . \end{cases}$$

Since $v=2b^2$, we have

$$\begin{cases} 2\cdot 5^3 v = \text{fifth power} , \\ u^2-5v^2 = \text{fifth power} . \end{cases}$$

Thus u and v satisfy the same conditions satisfied by p and q in (8), and $|q|>|v|>0$. Therefore the argument can be repeated indefinitely and this leads to an impossible infinite descent.

EXAMPLE 3 (the case $l=7$; $l^*=-7$). Let K be the quadratic field $\boldsymbol{Q}(\sqrt{-7})$, and $\omega=(1+\sqrt{-7})/2$. In order to determine p and q in Lemma 6, we need the minimal polynomial of ζ over the field K:

LEMMA 7. *Let ζ be the normalized 7-th root of unity; $\zeta=e^{2\pi i/7}$. Then the minimal polynomial of ζ, or $(1+\zeta)/(1-\zeta)$ over K is*

$$x^3+(1-\omega)x^2-\omega x-1 ,$$

or

$$x^3-\sqrt{-7}x^2-x+\frac{1}{\sqrt{-7}} ,$$

respectively.

PROOF. By the well known theorem of Gaussian sum we have

$$\zeta+\zeta^2-\zeta^3+\zeta^4-\zeta^5-\zeta^6=\sqrt{-7} .$$

On the other hand, ζ satisfies the equation

$$\zeta^6+\zeta^5+\zeta^4+\zeta^3+\zeta^2+\zeta+1=0 . \tag{9}$$

Therefore we have

$$\zeta^4+\zeta^2+\zeta+1-\omega=0 .$$

From this and (9) we obtain the assertion for ζ. Calculation of the minimal equation for $(1+\zeta)/(1-\zeta)$ is straightforward from the one for ζ.

By Lemma 7 we obtain

$$N_{L/K}\left(v+\frac{1+\zeta}{1-\zeta}7w\right)=(v^3-7^2vw^2)+(7v^2w+7^2w^3)\sqrt{-7}\ ;$$

hence

$$\begin{cases} p=v(v+7w)(v-7w)\ , \\ q=7w(v^2+7w^2)\ . \end{cases}$$

The same method would be applied to the case $l>7$; for example, if $l=13$, then for (6) we obtain

$$\begin{cases} 2\cdot 13^2w = 13\text{-th power}\ , \\ p^2-13q^2 = 13\text{-th power}\ , \end{cases}$$

where

$$\begin{cases} p=v^6+11\cdot 13^2v^4w^2+15\cdot 13^4v^2w^4+5\cdot 13^6w^6\ , \\ q=2\cdot 13^2w^2\{(v^2+13^2w^2)^2-13(2\cdot 13w^2)^2\}\ . \end{cases}$$

However, there seems to be no easy way of finding the step of infinite descent for $l>5$. Though we could also give the modern version of Dirichlet's proof for the case for which the exponent is 14, using Corollary to Theorem 1 (cf. Edwards [2], pp. 74–75), the trial to generalize it to a larger even exponent $2l$ is confronted with analogous difficulties.

References

[1] G. L. Dirichlet, Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré, J. Reine Angew. Math. (Crelles J.), **3** (1928), 354–375 (Werke, vol. 1, 21–46).

[2] H. M. Edwards, *Fermat's Last Theorem*, Springer, 1977.

[3] L. Euler, Vollständige Einleitung zur Algebra, *Opera Omnia*, Ser. 1, Vol. 1, St. Petersburg, 1770.

[4] H. Hasse, *Number Theory*, Springer, 1980 (Translation of "Zahlentheorie").

[5] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1982.

Present Address:
Department of Mathematics
School of Science and Engineering, Waseda University
Okubo, Shinjuku-ku, Tokyo 160, Japan