TSUKUBA J. MATH.
Vol. 8 No. 1 (1984). 131–157

SOLUTION OF A DIOPHANTINE PROBLEM

By

Saburô UCHIYAMA

Ivan Matveevič Vinogradov
in memoriam

We shall concern in the present paper with one of the Diophantine problems arising from the study of relations between two kinds of figurate numbers, or more specifically, between pyramidal and triangular numbers P_x and t_y, defined respectively by

$$P_x=\frac{1}{6}x(x+1)(2x+1)$$

and

$$t_y=\frac{1}{2}y(y+1).$$

As an unsolved problem in number theory, the problem has been proposed in [3; D 3] to determine when the equality $t_y=P_x$ does occur. In fact, it has been conjectured that the integer solutions x, y of the equation

$$\frac{1}{2}y(y+1)=\frac{1}{6}x(x+1)(2x+1) \tag{1}$$

are those that are given by

$$x=-1,\ 0,\ 1,\ 5,\ 6 \text{ and } 85. \tag{2}$$

It will be proved in the following that this is in fact the case, namely, that the Diophantine equation (1) has the solutions x, y with x listed in (2) and only these. Thus, we have just four natural numbers, 1, 55, 91 and 208335, which are simultaneously triangular and pyramidal.

It will be of some interest to note that a similar Diophantine equation

$$\frac{1}{2}y(y+1)=\frac{1}{6}x(x+1)(x+2) \tag{3}$$

where the right-hand side is a tetrahedral number T_x, was treated by È. T.

Received July 29, 1983

Avanesov [5], who showed that the solutions x, y of (3) are those that are given by

$$x=1,\ 3,\ 8,\ 20 \text{ and } 34$$

apart from $x=-2,\ -1$ and 0 which are trival. Our methods of reasoning are alike in principle but the respective proofs differ from each other considerably in many details.

Now, if we put

$$X=2x+1,\quad Y=2y+1,$$

then the equation (1) becomes

$$3Y^2=X^3-X+3. \tag{4}$$

It is well known that the elliptic equation

$$ey^2=ax^3+bx^2+cx+d \qquad (a\neq 0),$$

where the coefficients are integers and where the cubic polynomial on the right-hand side has no squared linear factor in x, admits only a finite number of integer solutions x, y, and these solutions can be effectively determined (cf. [4; Chaps. 27 & 28]).

We shall prove the

THEOREM. *The only solutions of the Diophantine equation* (4) *in rational integers* X, Y *are given by*

$$X=-1,\ 0,\ 1,\ 3,\ 8,\ 11,\ 13,\ 171 \text{ and } 1704. \tag{5}$$

Needless to say, the odd values only of X in (5) correspond to the values of x listed in (2) for the solutions of (1).

1. Reducing the original equation.

1.1 Throughout in what follows we shall denote by $\boldsymbol{Z}$ the ring of rational integers and by $\boldsymbol{Q}$ the field of rational numbers.

Put

$$g(x)=x^3-x+3.$$

The polynomial $g(x)$ is irreducible in $\boldsymbol{Z}[x]$ and has discriminant $D_g=-239$. Thus, the equation $g(x)=0$ has a real root and a pair of conjugate complex roots. Let λ be a generic root of the equation $g(x)=0$. Then λ generates a cubic field $K=\boldsymbol{Q}(\lambda)$. The field discriminant of K is $D_K=-239$, and an integral basis of K is $\Delta=\{1, \lambda, \lambda^2\}$.

According to Dirichlet's units theorem, the field K has the unit group generated by a fundamental unit ε, and we see from a table in [7; p. 113] that we can take

$$\varepsilon=\lambda^2+\lambda-1.$$

The cyclotomic units in K are ± 1. Moreover, K has the class number $h_K=1$.

It is immediate to see that we have in $\mathcal{O}$, the ring of integers of K,

$$(3)=(\lambda)(\lambda-1)(\lambda+1) \tag{6}$$

and

$$(239)=(3\lambda^2-1)^2(3\lambda^2-4), \tag{7}$$

where each of the ideals appearing in the right-hand side of (6) and (7) is a prime ideal of $\mathcal{O}$.

Now, the equation (4) can be rewritten in the form

$$(X-\lambda)(X^2+\lambda X+\lambda^2-1)=\zeta\lambda(\lambda-1)(\lambda+1)Y^2, \tag{8}$$

where ζ is a unit of K.

We have

$$(X-\lambda, X^2+\lambda X+\lambda^2-1)=(X-\lambda, 3\lambda^2-1).$$

We see that $X-\lambda\equiv 0 \pmod{3\lambda^2-1}$ if and only if $X\equiv 124 \pmod{239}$. Here, if $X\equiv 124 \pmod{239}$ then

$$g(X)\equiv 0 \pmod{239}$$

but

$$g(X)\not\equiv 0 \pmod{239^2},$$

since we have

$$g(124)=3\cdot 239\cdot 2659 \text{ and } g'(124)=193\cdot 239.$$

It follows that the equation (4) is impossible for any X with $X\equiv 124 \pmod{239}$. We may assume, therefore, that in (8) the two factors on the left-hand side are co-prime.

We note that

$$(X-\lambda, 3)=\begin{cases}(\lambda) & \text{if } X\equiv 0 \pmod 3,\\ (\lambda\mp 1) & \text{if } X\equiv \pm 1 \pmod 3.\end{cases}$$

We have also, for any a, b, c in $\boldsymbol{Z}$,

$$(a+b\lambda+c\lambda^2)^2=A+B\lambda+C\lambda^2,$$

where

$$(9)\qquad \begin{cases} A=a^2-6bc, \\ B=2ab+2bc-3c^2, \\ C=b^2+2ac+c^2. \end{cases}$$

We distinguish three cases according as $X\equiv 0$, 1 or -1 (mod 3).

1.2 *Case of* $X\equiv 0$ (mod 3). Here we have from (8)

$$X-\lambda=\pm\lambda\varepsilon^k(a+b\lambda+c\lambda^2)^2$$

for some a, b, c, and k in $\boldsymbol{Z}$, where one may assume without loss of generality that $k=0$ or 1.

If $k=0$ then

$$\begin{aligned} X-\lambda &= \pm\lambda(a+b\lambda+c\lambda^2)^2 \\ &= \pm\lambda(A+B\lambda+C\lambda^2) \\ &= \pm(-3C+(A+C)\lambda+B\lambda^2). \end{aligned}$$

It follows from this that

$$\begin{aligned} 0&=B, \\ \mp 1&=A+C, \\ \mp X&=3C. \end{aligned}$$

In view of (9) we find that c must be even, and hence $\mp 1\equiv a^2+b^2$ (mod 4); therefore, a, b have different parity and we must take the lower sign $+$. Thus we have

$$X=3(b^2+2ac+c^2)$$

and

$$(10)\qquad \begin{cases} 2b(a+c)=3c^2 \\ (a+c)^2+b^2-6bc=1. \end{cases}$$

Suppose first that $bc=0$. If $b=0$ then we have from (10) $a+c=\pm 1, c=0$, and so $a=\pm 1$, which gives the solution

$$X=0.$$

If $c=0$ and $b\neq 0$ then, from (10) again, $a^2+b^2=1, a=0, b=\pm 1$, which gives

$$X=3.$$

Suppose then that $bc>0$. We note that $(b, a+c)=1$, and so $(2b, a+c)=1$ or 2.

If $a+c$ is odd, then X, as well as b, is even. There are two cases to be distinguished.

(i) $a+c=\pm 3u^2, b=\pm 2^{2m-1}v^2, c=\pm 2^m uv$ for some u, v and m in $\boldsymbol{Z}$ with u, v

odd, $m \geqq 1$.

If we write $U=u$, $V=2^{m-1}v$, then the second equality in (10) gives

$$9U^4-24UV^3+4V^4=1.$$

This equation has, however, no integer solutions U, V with odd U, since the congruence

$$9U^4-24UV^3+4V^4 \equiv 1 \pmod{16}$$

is insoluble in U, V with $U \equiv 1 \pmod 2$.

(ii) $a+c=\pm u^2, b=\pm 3\cdot 2^{2m-1}v^2, c=\pm 2^m uv$ for some u, v and m in $\boldsymbol{Z}$ with u, v odd, $m \geqq 1$.

If we write $U=u$, $V=2^{m-1}v$, then we have, from the second equality in (10) again,

$$U^4-72UV^3+36V^4=1. \tag{11}$$

There are solutions $U=\pm 1$, $V=\pm 2$, which as we shall see later are the only solutions of (11) (apart from the trivial ones $U=\pm 1$, $V=0$) and which give $a=\mp 3$, $b=\pm 24, c=\pm 4$ and so

$$X=3\cdot 568=1704.$$

Incidentally, the equation (11) is impossible modulo 8 if $m=1$.

Next, if $a+c$ is even, then X, as well as b, is odd. There are two cases again.

(iii) $a+c=\pm 3\cdot 2^{2m-1}u^2, b=\pm v^2, c=\pm 2^m uv$ for some u, v and m in $\boldsymbol{Z}$ with u, v odd, $m \geqq 1$.

If we put $U=2^{m-1}u$, $V=v$, then we have

$$36U^4-12UV^3+V^4=1, \tag{12}$$

which admits, as we shall see later, no solutions U, V (apart from the trivial solutions $U=0$, $V=\pm 1$).

The equation (12) is impossible modulo 16 for $m=2$.

(iv) $a+c=\pm 2^{2m-1}u^2, b=\pm 3v^2, c=\pm 2^m uv$ for some u, v and m in $\boldsymbol{Z}$ with u, v odd, $m \geqq 1$.

If we put $U=2^{m-1}u$, $V=v$, then we get

$$4U^4-36UV^3+9V^4=1. \tag{13}$$

There are solutions $U=\pm 2$, $V=\pm 1$, which as we shall see later are the only solutions of (13) and which give $a=\pm 4, b=\pm 3, c=\pm 4$, and hence

$$X=3\cdot 57=171.$$

The equation (13) is impossible modulo 16 if $m \geqq 3$.

If $k=1$ then we have

$$\begin{aligned} X-\lambda &= \pm\lambda\varepsilon(a+b\lambda+c\lambda^2)^2 \\ &= \pm(\lambda^2-3)(A+B\lambda+C\lambda^2) \\ &= \pm(-3(A+B)-(2B+3C)\lambda+(A-2C)\lambda^2), \end{aligned}$$

whence

$$0=A-2C, \tag{14}$$

$$\pm 1=2B+3C, \tag{15}$$

and

$$\mp X=3(A+B).$$

In view of (9), from (14) it follows that $a\equiv 0 \pmod 2$, and from (15) that $\pm 1\equiv 3b^2-3c^2 \pmod 4$, or $b+c\equiv 1 \pmod 2$. But then, from (14) again we get $0\equiv -2 \pmod 4$, an absurd relation. Hence, there are no solutions X under the circumstances.

1.3 *Case of* $X\equiv 1 \pmod 3$. In this case we have

$$X-\lambda=\pm(\lambda-1)\varepsilon^k(a+b\lambda+c\lambda^2)^2$$

for some a, b, c, and k in $\boldsymbol{Z}$, where as before we may assume that $k=0$ or 1.

If $k=0$ then we have

$$\begin{aligned} X-\lambda &= \pm(\lambda-1)(a+b\lambda+c\lambda^2)^2 \\ &= \pm(\lambda-1)(A+B\lambda+C\lambda^2) \\ &= \pm(-(A+3C)+(A-B+C)\lambda+(B-C)\lambda^2), \end{aligned}$$

so that

$$\begin{aligned} 0&=B-C, \\ \mp 1&=A-B+C, \\ \mp X&=A+3C. \end{aligned}$$

On account of (9) we find that $a\not\equiv 0 \pmod 3$, and so we must take the lower sign $+$ in the last two equalities, and that $b\equiv 0 \pmod 2$. Thus we have

$$X=3(b^2+2ac+c^2)+1$$

and

$$\begin{cases} (2a-b+c)(b-c)=3c^2, \\ a^2-6bc=1. \end{cases} \tag{16}$$

Suppose first that $bc=0$. If $b=0$ then $a=\pm 1, c=0$, which give

$$X=1.$$

If $c=0$ and $b\neq 0$ then $a=\pm 1, b=\pm 2$, which give

$$X=13.$$

Suppose then that $bc>0$. Since we must have $(a, 6bc)=1, (a, b-c)=1$ so that $(2a, b-c)=1$ or 2.

If $b-c$ is odd, then c is odd and X is even. There are two cases to be distinguished.

(i) $2a-b+c=\pm 3u^2, b-c=\pm v^2, |c|=uv$ for some u, v in $\boldsymbol{Z}, u, v$ odd.

If $c=uv>0$ then $b=\pm v^2+uv, bc=uv(u\pm v)$, where for the sign $-$ we must have $u-v>0$.

If $c=-uv<0$ then $b=\pm v^2-uv, bc=uv(u\mp v)$, where for the sign $-$ we must have $u-v>0$.

In either case we have $a=\pm(1/2)(3u^2+v^2)$. If we write $U=\pm u, V=v$, then we get from the second equality in (16)

$$9U^4-18U^2V^2+24UV^3+V^4=4.$$

However, this equation has no integer solutions U, V with $U\equiv V\equiv 1 \pmod 2$, since the congruence

$$9U^4-18U^2V^2+24UV^3+V^4\equiv 4 \pmod{16}$$

is impossible for $U\equiv V\equiv 1 \pmod 2$.

(ii) $2a-b+c=\pm u^2, b-c=\pm 3v^2, |c|=uv$ for some u, v in $\boldsymbol{Z}, u, v$ odd.

If $c=uv>0$ then $b=\pm 3v^2+uv, bc=uv^2(u\pm 3v)$, where for the sign $-$ we must have $u-3v>0$.

If $c=-uv<0$ then $b=\pm 3v^2-uv, bc=uv^2(u\mp 3v)$, where for the sign $-$ we must have $u-3v>0$.

We have, in either case, $a=\pm(1/2)(u^2+3v^2)$. If we write $U=\pm u, V=v$, then

$$U^4-18U^2V^2+72UV^3+9V^4=4,$$

where $U\equiv V\equiv 1 \pmod 2$. This equation is also impossible, as is seen by considering the both sides of it modulo 16.

If $b-c$ is even, then c is even and X is odd. We have to distinguish four cases.

(iii) $2a-b+c=\pm 3\cdot 2^{2m-1}u^2, b-c=\pm 2v^2$, where $2^m||c$, so that $|c|=2^muv$ with u, v odd, $m\geqq 1$.

If $c=2^muv>0$, then $b=\pm 2v^2+2^muv, bc=2^{m+1}uv^2(2^{m-1}u\pm v)>0$.

If $c=-2^muv<0$, then $b=\pm 2v^2-2^muv, bc=2^{m+1}uv^2(2^{m-1}u\mp v)>0$.

In either case we have $a=\pm(3\cdot 2^{2m-2}u^2+v^2)$. If we put $U=\pm 2^{m-1}u, V=v$, then we get from (16)

$$9U^4-18U^2V^2+24UV^3+V^4=1. \tag{17}$$

We shall show later that this equation has no solutions U, V (apart from the trivial ones $U=0, V=\pm 1$). The equation (17) has no solutions U, V with $U\equiv V\equiv 1 \pmod 2$, that is, in the case of $m=1$. This can be seen at once if we consider the equation modulo 4.

(iv) $2a-b+c=\pm 2^{2m-1}u^2, b-c=\pm 3\cdot 2v^2$, where $2^m||c$, so that $|c|=2^muv$ with u, v odd, $m\geqq 1$.

If $c=2^muv>0$, then $b=\pm 3\cdot 2v^2+2^muv, bc=2^{m+1}uv^2(2^{m-1}u\pm 3v)>0$.

If $c=-2^muv<0$, then $b=\pm 3\cdot 2v^2-2^muv, bc=2^{m+1}uv^2(2^{m-1}u\mp 3v)>0$.

We have in either case $a=\pm(2^{2m-2}u^2+3v^2)$. If we write $U=\pm 2^{m-1}u$, $V=v$, then

$$U^4-18U^2V^2+72UV^3+9V^4=1. \tag{18}$$

We shall show later that this equation has also no solutions U, V (apart from the trivial ones $U=\pm 1, V=0$). Again, the equation (18) has no solutions U, V with $U\equiv V\equiv 1 \pmod 2$, that is, in the case of $m=1$. For $m\geqq 3$ the equation turns out to be impossible, when considered modulo 16.

(v) $2a-b+c=\pm 3\cdot 2u^2, b-c=\pm 2^{2m-1}v^2$, where $2^m||c$, so that $|c|=2^muv$ with u, v odd, $m>1$.

If $c=2^muv>0$ then $b=\pm 2^{2m-1}v^2+2^muv, bc=2^{2m}uv^2(u\pm 2^{m-1}v)>0$.

If $c=-2^muv<0$ then $b=\pm 2^{2m-1}v^2-2^muv, bc=2^{2m}uv^2(u\mp 2^{m-1}v)>0$.

We have in either case $a=\pm(3u^2+2^{2m-2}v^2)$. If we put $U=\pm u$, $V=2^{m-1}v$, then we get

$$9U^4-18U^2V^2+24UV^3+V^4=1.$$

This equation is identical in form with (17); the only difference is in the parity of the solutions U, V sought. The equation is impossible modulo 16 for $m\geqq 3$.

(vi) $2a-b+c=\pm 2u^2, b-c=\pm 3\cdot 2^{2m-1}v^2$, where $2^m||c$, so that $|c|=2^muv$ with u, v odd, $m>1$.

If $c=2^muv>0$ then $b=\pm 3\cdot 2^{2m-1}v^2+2^muv, bc=2^{2m}uv^2(u\pm 3\cdot 2^{m-1}v)>0$.

If $c=-2^muv<0$ then $b=\pm 3\cdot 2^{2m-1}v^2-2^muv, bc=2^{2m}uv^2(u\mp 3\cdot 2^{m-1}v)>0$.

In either case we have $a=\pm(u^2+3\cdot 2^{2m-2}v^2)$. If we put $U=\pm u$, $V=2^{m-1}v$, then

$$U^4-18U^2V^2+72UV^3+9V^4=1.$$

This equation is identical in form with (18), with the difference only in the parity of the solutions U, V sought. The equation is impossible for $m=1$; this is also impossible modulo 16 for $m=2$.

If $k=1$ then

$$\begin{aligned} X-\lambda &= \pm(\lambda-1)\varepsilon(a+b\lambda+c\lambda^2)^2 \\ &= \mp(\lambda+2)(A+B\lambda+C\lambda^2) \end{aligned}$$

$$=\mp(2A-3C+(A+2B+C)\lambda+(B+2C)\lambda^2),$$

and we must have

(19) $$0=B+2C,$$

(20) $$\pm 1=A+2B+C,$$

(21) $$\mp X=2A-3C.$$

It follows from (21) that $a\not\equiv 0 \pmod 3$ and we have to take the upper sign, + in (20) and − in (21). The equality (19) modulo 4 gives $2ab+2b^2\equiv 0 \pmod 4$, i.e. $b(a+b)\equiv 0 \pmod 2$. The equality (20) modulo 4 yields $a^2+b^2\equiv 1 \pmod 4$, since, from (19) we have $c\equiv 0 \pmod 2$. It follows that $b\equiv 0 \pmod 2$ and $a\equiv 1 \pmod 2$. But, $b\equiv 0 \pmod 2$ implies $X\equiv 0 \pmod 2$. Since

$$X=-A-1=-(a^2-6bc)-1\equiv -2 \pmod 8,$$

it would follow that

$$3\equiv 3Y^2=X^3-X+3\equiv 5 \pmod 8,$$

an impossibility. Therefore, there are no solutions X in this situation.

1.4 *Case of* $X\equiv -1 \pmod 3$. In this case we have

$$X-\lambda=\pm(\lambda+1)\varepsilon^k(a+b\lambda+c\lambda^2)^2$$

for some a, b, c, and k in $\boldsymbol{Z}$, where we may assume as before that $k=0$ or 1.

If $k=0$ then we have

$$\begin{aligned} X-\lambda&=\pm(\lambda+1)(a+b\lambda+c\lambda^2)^2\\ &=\pm(\lambda+1)(A+B\lambda+C\lambda^2)\\ &=\pm(A-3C+(A+B+C)\lambda+(B+C)\lambda^2), \end{aligned}$$

from which follows that

(22) $$0=B+C,$$

(23) $$\mp 1=A+B+C,$$

(24) $$\pm X=A-3C.$$

It follows from (9) and (24) that $a\not\equiv 0 \pmod 3$ and we have to take the lower sign, + in (23) and − in (24). By (22) we have $b\equiv 0 \pmod 2$. We thus have

$$X=3(b^2+2ac+c^2)-1$$

and

(25) $$\begin{cases}(2a+b+c)(b+c)=3c^2,\\ a^2-6bc=1.\end{cases}$$

Suppose that $bc=0$. If $b=0$ then $a=\pm 1$; if further $c=0$ then this gives

$$X=-1;$$

and if $c\neq 0$ then $\pm 2+c=3c$, or $c=\pm 1$ and this gives

$$X=8.$$

If $b\neq 0$ then $c=0$, and so $\pm 2+b=0$, or $b=\mp 2$. This gives

$$X=11.$$

Suppose now that $bc>0$. Since we have $(a, 6bc)=1$, $(a, b+c)=1$ so that $(2a, b+c)=1$ or 2.

If $b+c$ is odd, then c is odd and X is even. There are two cases to be considered.

(i) $2a+b+c=\pm 3u^2, b+c=\pm v^2, c=\pm uv$ with u, v odd.

We have $a=\pm(1/2)(3u^2-v^2), b=\pm(v^2-uv)=\pm v(v-u)$, and so, by (25),

$$9u^4+18u^2v^2-24uv^3+v^4=4. \tag{26}$$

We shall see later that the only solutions of (26) are $u=v=\pm 1$, which will lead to $a=\pm 1, b=0, c=\pm 1$, a case we have already dealt with and now excluded.

(ii) $2a+b+c=\pm u^2, b+c=\pm 3v^2, c=\pm uv$ with u, v odd.

We have $a=\pm(1/2)(u^2-3v^2), b=\pm(3v^2-uv)=\pm v(3v-u)$ and so

$$u^4+18u^2v^2-72uv^3+9v^4=4.$$

This equation is impossible, as can be seen by considering it modulo 128.

If $b+c$ is even, then c is even and X is odd. We have to distinguish four cases.

(iii) $2a+b+c=\pm 3\cdot 2^{2m-1}u^2, b+c=\pm 2v^2$, where $2^m\|c$, so that $c=\pm 2^m uv$ with uv odd, $m\geqq 1$.

We have $a=\pm(3\cdot 2^{2m-2}u^2-v^2), b=\pm 2v(v-2^{m-1}u)$. If we write $U=2^{m-1}u$, $V=v$, then we get from (25) again

$$9U^4+18U^2V^2-24UV^3+V^4=1. \tag{27}$$

We shall show later that this equation has only trivial solutions $U=0$, $V=\pm 1$. We note that the equation (27) is impossible, modulo 4, for $m=1$; it is also impossible modulo 16 for $m=2$.

(iv) $2a+b+c=\pm 2^{2m-1}u^2, b+c=\pm 3\cdot 2v^2$, where $2^m\|c$, so that $c=\pm 2^m uv$ with uv odd, $m\geqq 1$.

We have $a=\pm(2^{2m-2}u^2-3v^2), b=\pm 2v(3v-2^{m-1}u)$. If we write $U=2^{m-1}u$, $V=v$, then

(28) $$U^4+18U^2V^2-72UV^3+9V^4=1.$$

We shall show later that this equation also has only trivial solutions $U=\pm1$, $V=0$. The equation (28) is impossible, modulo 4, for $m=1$; also, it is impossible, modulo 16, for $m\geqq3$.

(v) $2a+b+c=\pm3\cdot2u^2$, $b+c=\pm2^{2m-1}v^2$, where $2^m||c$, so that $c=\pm2^muv$ with uv odd, $m>1$.

We have $a=\pm(3u^2-2^{2m-2}v^2)$, $b=\pm2^mv(2^{m-1}v-u)$. If we put $U=u$, $V=2^{m-1}v$, then

$$9U^4+18U^2V^2-24UV^3+V^4=1.$$

This equation is identical in form with (27), except for the parity condition on the solutions U, V. The equation is impossible for $m=1$, and so is also for $m\geqq3$, modulo 16.

(vi) $2a+b+c=\pm2u^2$, $b+c=\pm3\cdot2^{2m-1}v^2$, where $2^m||c$, so that $c=\pm2^muv$ with uv odd, $m>1$.

We have $a=\pm(u^2-3\cdot2^{2m-2}v^2)$, $b=\pm2^mv(3\cdot2^{m-1}v-u)$. If we put $U=u$, $V=2^{m-1}v$, then

$$U^4+18U^2V^2-72UV^3+9V^4=1.$$

This equation is again identical in form with (28), except for the parity condition on the solutions U, V. The equation is impossible for $m=1$, and is also impossible modulo 16 for $m=2$.

If $k=1$ then we have

$$\begin{aligned}X-\lambda&=\pm(\lambda+1)\varepsilon(a+b\lambda+c\lambda^2)^2\\&=\pm(2\lambda^2+\lambda-4)(A+B\lambda+C\lambda^2)\\&=\pm(-(4A+6B+3C)+(A-2B-5C)\lambda\\&\quad+(2A+B-2C)\lambda^2)\end{aligned}$$

so that

(29) $$0=2A+B-2C,$$

(30) $$\mp1=A-2B-5C,$$

(31) $$\mp X=4A+6B+3C.$$

From (31) it follows that $a\not\equiv0 \pmod 3$ and we have to take the upper sign $-$ in (30) and (31). The equality (29) modulo 2 gives $c\equiv0 \pmod 2$, and the equality (30) modulo 4 gives $a^2-b^2\equiv-1 \pmod 4$, and so a is even and b odd. But then (29) modulo 4 will yield $-2b^2\equiv2\equiv0 \pmod 4$, an absurdity. Hence, there are no solutions X in the present situation.

1.5 We thus have completed the reduction of the problem of solving the

original Diophantine equation (4) to the study of eight Diophantine equations (11), (12), (13), (17), (18), (26), (27) and (28), each of them being of a norm form equation of fourth degree. Our task is now to resolve these equations.

2. Resolving the equations derived.

2.1 In the following we are going to work with the arithmetic in several quartic number fields $L=\boldsymbol{Q}(\theta)$ generated by certain algebraic integers θ of fourth degree over $\boldsymbol{Q}$. In each occurrence the defining monic polynomial $f(x)\in\boldsymbol{Z}[x]$ of θ has one and the same discriminant

$$D_f=-713650176=-2^{12}\cdot 3^6\cdot 239,$$

but, of course, the field discriminant of $L=\boldsymbol{Q}(\theta)$ may differ. In order to determine an integral basis of the field L, the algorithm of W. E. H. Berwick [1] will be useful.

Since $\deg f(x)=4$ and $D_f<0$, the equation $f(x)=0$ has two real roots and a pair of conjugate complex roots. The resolvent cubic of $f(x)$ has no rational roots, so that the Galois group of $L/\boldsymbol{Q}$ is the full symmetric group of degree 4. According to Dirichlet's units theorem, the unit group of L is generated by two independent units, so-called fundamental units. In L there are no cyclotomic units other than ± 1.

We have appealed to Berwick's criterion [2] to find a pair of fundamental units in L. In fact, if we assume that θ be real and denote, for any element $\alpha\in L=\boldsymbol{Q}(\theta)$, by α', and $\alpha'', \bar{\alpha}''$ the real, and the pair of complex conjugates of α, respectively, then two independent units are any two of the three units $\varepsilon_1, \varepsilon_2, \varepsilon_3$ defined by

(a) $\varepsilon>1$ and least, $|\varepsilon'|<1$, $\varepsilon''\bar{\varepsilon}''<1$;

(b) $|\varepsilon|<1, \varepsilon'>1$ and least, $\varepsilon''\bar{\varepsilon}''<1$;

(c) $|\varepsilon|<1, |\varepsilon'|<1, |\varepsilon''|=|\bar{\varepsilon}''|>1$ and least.

Here, there is no loss in generality in assuming $\varepsilon_1\varepsilon_2\varepsilon_3=1$. In this connexion one may refer also to [6].

2.2 PROPOSITION 1. *The only solutions of the Diophantine equation*

$$U^4-72UV^3+36V^4=1 \tag{11}$$

in rational integers U, V are

$$U=\pm 1,\ V=0 \text{ and } U=\pm 1,\ V=\pm 2.$$

PROOF. Put

$$f(x)=x^4-72x+36.$$

The discriminant D_f of $f(x)$ is negative, more precisely $D_f=-2^{12}\cdot 3^6\cdot 239$. Let θ be a real root of $f(x)=0$.

The quartic field $L=\boldsymbol{Q}(\theta)$ has an integral basis $\Delta=\{1,\omega_1,\omega_2,\omega_3\}$ with

$$\omega_1=\theta,\ \omega_2=\frac{1}{6}\theta^2,\ \omega_3=\frac{1}{6}\theta^3,$$

and the discriminant of L is $D=-2^8\cdot 3^2\cdot 239$.

We see that the units $\varepsilon_1,\varepsilon_2$ and ε_3, where

$$\begin{aligned}\varepsilon_1&=24-\omega_2-2\omega_3,\\ \varepsilon_2&=-208+364\omega_1+549\omega_2+138\omega_3,\\ \varepsilon_3&=-3+6\omega_1+8\omega_2-4\omega_3,\end{aligned}$$

respectively satisfy Berwick's conditions (a), (b) and (c). Hence, any two of the three units $\varepsilon_1,\varepsilon_2,\varepsilon_3$ form a pair of fundamental units in L. Therefore, the pair of units

$$\begin{aligned}\alpha&=\varepsilon_1^{-1}=\omega_2\\ \beta&=\varepsilon_1\varepsilon_3=8-4\omega_1+3\omega_2\end{aligned}$$

is a fundamental pair.

We have

$$\alpha^2=-(1-2\omega_1),$$

$$\beta^2\equiv -9(1-2\omega_1)+8(2\omega_2-3\omega_3) \pmod{2^5}.$$

We list some congruence relations related to the powers of α and β. Here, m,n and h are arbitrary rational integers, $h\geqq 1$. We put $\Omega=1-2\omega_1$.

$$\begin{aligned}\Omega^{4m}&\equiv 1-8m\omega_1+144m\omega_2 &&\pmod{2^5},\\ \Omega^{4m+1}&\equiv 1-2(4m+1)\omega_1+144m\omega_2 &&\pmod{2^5},\\ \Omega^{4m+2}&\equiv 1-4(2m+1)\omega_1+24(6m+1)\omega_2 &&\pmod{2^5},\\ \Omega^{4m+3}&\equiv 1-2(4m+3)\omega_1+72(2m+1)\omega_2-48\omega_3 &&\pmod{2^5};\\ (-1)^{n+1}\beta^{2n}\varepsilon_3&\equiv 3^{2n+1}\Omega^{n+1}-4\cdot 3^{2n-1}\Omega^n(2(2n+3)\omega_2-3(2n+1)\omega_3) &&\pmod{2^5};\\ \Omega^{2^h m}&\equiv 1-2^{h+1}m\omega_1+9\cdot 2^{h+2}m\omega_2 &&\pmod{2^{h+4}},\\ \Omega^{2^h m+1}&\equiv 1-2(2^h m+1)\omega_1+9\cdot 2^{h+2}m\omega_2 &&\pmod{2^{h+3}};\\ (-1)^{2^{h-1}}\beta^{2^h n}&\equiv 3^{2^h n}\Omega^{2^{h-1}n}-3^{2^h n-2}\cdot 2^{h+2}n\Omega^{2^{h-1}n-1}(2\omega_2-3\omega_3) &&\pmod{2^{h+4}}.\end{aligned}$$

Now, if $U,V\in\boldsymbol{Z}$ satisfy the equation (11), then we must have

$$\pm(U-V\theta)=\alpha^a\beta^b$$

for some rational integers a,b. Since we have

$$\alpha^{2m}\beta^{2n+1}\equiv\pm(\omega_2-2(m+n)\omega_3) \pmod 4,$$

$$\alpha^{2m+1}\beta^{2n}\equiv\pm(\omega_2-2(m+n)\omega_3) \pmod 4,$$

the exponents a, b must have the same parity.

We shall show that $a\equiv b\equiv 1 \pmod 2$ is impossible. For this purpose we write

$$\Omega^m\equiv 1-A(m)\omega_1+B(m)\omega_2-C(m)\omega_3 \pmod{2^5}$$

with

$$A(m)=2m \text{ for all } m,$$

and, according as $m\equiv 0, 1, 2,$ or $3 \pmod 4$,

$$B(m)=36m,\ 36(m-1),\ 12(3m-4),\ \text{or } 36(m-1)$$
$$C(m)=0,\ 0,\ 0,\ \text{or } 48.$$

We have

$$\alpha^{2m+1}\beta^{2n+1}=\alpha^{2m}\beta^{2n}\varepsilon_3,$$

so that, modulo 2^5,

$$\begin{aligned}\pm\alpha^{2m+1}\beta^{2n+1}&\equiv 3^{2n+1}\Omega^{m+n+1}\\&\quad-4\cdot 3^{2n-1}\Omega^{m+n}(2(2n+3)\omega_2-3(2n+1)\omega_3)\\&\equiv 3^{2n+1}(1+8(2n+1)A(m+n))\\&\quad-3^{2n}(4(2n+1)A(m+n)+3A(m+n+1))\omega_1\\&\quad-3^{2n-1}(8(2n+3)-9B(m+n+1))\omega_2\\&\quad+3^{2n-1}(4(3(2n+1)+2(2n+3)A(m+n))-9C(m+n+1))\omega_3,\end{aligned}$$

where, if $m+n+1\not\equiv 3 \pmod 4$ then the coefficient of ω_3 on the right is congruent to

$$3^{2n-1}\cdot 4(3(2n+1)+2(2n+3)A(m+n))\not\equiv 0 \pmod{2^5},$$

and if $m+n+1\equiv 3 \pmod 4$ then $m+n\equiv 2 \pmod 4$ and the coefficient of ω_3 on the right is again congruent to

$$3^{2n-1}(12(2n+1)-9\cdot 48)\equiv 3^{2n-1}\cdot 4(6n-1)\not\equiv 0 \pmod{2^5}.$$

This proves our assertion.

We thus have $a\equiv b\equiv 0 \pmod 2$. As before, we have, modulo 2^5,

$$\begin{aligned}\pm\alpha^{2m}\beta^{2n}&\equiv 3^{2n}\Omega^{m+n}\\&\quad-8\cdot 3^{2n-2}n\Omega^{m+n-1}(2\omega_2-3\omega_3)\\&\equiv 3^{2n}(16n+1)-3^{2n}A(m+n)\omega_1\\&\quad-3^{2n-2}(16n-9B(m+n))\omega_2\\&\quad+3^{2n-2}(24n-9C(m+n))\omega_3,\end{aligned}$$

where

$$3^{2n-2}(16n-9B(m+n))\not\equiv 0 \pmod{2^5},$$

provided $m+n\not\equiv 0$ or 1 (mod 4).

Suppose then that $m+n\equiv 0$ or 1 (mod 4). A necessary condition for

$$\pm(U-V\theta)=\alpha^{2m}\beta^{2n}$$

is that

$$3^{2n-2}\cdot 24n\equiv 0 \pmod{2^5}, \text{ i.e. } n\equiv 0 \pmod 4.$$

Let us suppose that $n\neq 0$ and $2^h\|n, h\geqq 2$. Write

$$n=2^h n', \quad (n',2)=1.$$

We have, modulo 2^{h+5},

$$\begin{aligned}\pm\alpha^{2m}\beta^{2^{h+1}n'}\equiv & 3^{2^{h+1}n'}\Omega^{m+2^h n'}\\ & -3^{2^{h+1}n'-2}\cdot 2^{h+3}n'\Omega^{m+2^h n'-1}(2\omega_3-3\omega_3)\\ \equiv & 3^{2^{h+1}n'}(2^{h+4}n'+1)-3^{2^{h+1}n'}A(m+2^h n')\omega_1\\ & -3^{2^{h+1}n'-1}(2^{h+4}n'-9B(m+2^h n'))\omega_2\\ & +3^{2^{h+1}n'-2}(3\cdot 2^{h+3}n'-9C(m+2^h n'))\omega_3.\end{aligned}$$

Since $m\equiv 0$ or 1 (mod 4), it follows from this that

$$3\cdot 2^{h+3}n'\equiv 0 \pmod{2^{h+5}}$$

which is impossible, however. Hence, the only possibility is that $a\equiv 0$ (mod 2) and $b=0$.

Now, if we have

$$\pm(U-V\theta)=\alpha^{2m}=\pm\Omega^m,$$

then we must have

$$m\equiv 0 \text{ or } 1 \pmod 4.$$

Suppose first that $m\equiv 0$ (mod 4) and $m\neq 0$. Let $2^h, h\geqq 2$, be the highest power of 2 that divides m and set $m=2^h m', (m',2)=1$. Then

$$\Omega^{2^h m'}\equiv 1-2^{h+1}m'\omega_1+9\cdot 2^{h+2}m'\omega_2 \pmod{2^{h+4}},$$

which implies $m'\equiv 0$ (mod 4), a contradiction. Therefore, the only possibility is $m=0$, giving

$$U=\pm 1, \quad V=0.$$

Suppose next that $m\equiv 1$ (mod 4) and $m\neq 1$. Let $2^h, h\geqq 2$, be the highest power of 2 that divides $m-1$, and write $m=2^h m'+1, (m',2)=1$. Then

$$\Omega^{2^h m'+1}\equiv 1-2(2^h m'+1)\omega_1+9\cdot 2^{h+2}m'\omega_2 \pmod{2^{h+3}},$$

which implies $m'\equiv 0$ (mod 2), a contradiction again. Thus, the only possibility is

$m=1$, and so

$$U=\pm 1,\quad V=\pm 2.$$

This completes the proof of Proposition 1.

2.3 PROPOSITION 2. *The only solutions of the Diophantine equation*

$$36U^4-12UV^3+V^4=1 \tag{12}$$

in rational integers U, V are the trivial ones,

$$U=0,\quad V=\pm 1.$$

PROOF. Put

$$f(x)=x^4-12x^3+36.$$

The discriminant of $f(x)$ is $D_f=-2^{12}\cdot 3^6\cdot 239$. Let θ be a real root of the equation $f(x)=0$ and put $L=\boldsymbol{Q}(\theta)$.

The quartic field L has an integral basis $\Delta=\{1,\omega_1,\omega_2,\omega_3\}$ with

$$\omega_1=\theta,\ \omega_2=\frac{1}{6}\theta^2,\ \omega_3=\frac{1}{6}\theta^3,$$

and the discriminant of L is $D=-2^8\cdot 3^2\cdot 239$.

Let ξ be any root of the equation $f(x)=0$. If we define the number ξ^* by $\xi\xi^*=6$, then ξ^* satisfies the equation $f^*(x)=0$, where

$$f^*(x)=x^4-72x+36. \tag{32}$$

Therefore, the number θ^* given by $\theta\theta^*=6$ generates a quartic field $\boldsymbol{Q}(\theta^*)=L$, and $\Delta^*=\{1,\omega_1^*,\omega_2^*,\omega_3^*\}$ with

$$\omega_1^*=\theta^*,\ \omega_2^*=\frac{1}{6}\theta^{*2},\ \omega_4^*=\frac{1}{6}\theta^{*3} \tag{33}$$

is another integral basis of L. In fact, we have

$$\Delta^*=M\Delta,$$

where Δ and Δ^* are taken to be column vectors and M is the matrix

$$M=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 12 & -1 \\ 0 & 2 & -1 & 0 \\ 12 & -1 & 0 & 0 \end{pmatrix}$$

with $\det M=1$.

Consequently, it is immediate to find a fundamental pair of units in L by

making use of a result in the proof of Proposition 1. Thus, the pair

$$\alpha=2\omega_1-\omega_2,$$
$$\beta=8+6\omega_1-51\omega_2+4\omega_3$$

is a fundamental pair of units in L.

Now, the solutions $U, V\in\boldsymbol{Z}$ of the equation (12) should satisfy

$$\pm(V-U\theta)=\alpha^a\beta^b$$

for some $a, b\in\boldsymbol{Z}$.

If $a+b\equiv1 \pmod 2$ then

$$\alpha^a\beta^b\equiv\pm\omega_2^{a+b}\equiv\pm\omega_2 \qquad (\mathrm{mod}\ 2),$$

which is obviously impossible.

We now suppose that $a+b\equiv0 \pmod 2$ and distinguish two cases.

If $a\equiv b\equiv1 \pmod 2$ then, writing $a=2m+1, b=2n+1$, we have

$$\alpha^a\beta^b\equiv1+2c(a,b)\omega_2+2\omega_3 \qquad (\mathrm{mod}\ 4),$$

where $c(a,b)=0$ if $m+n\equiv0 \pmod 2$, and $=(m+n-1)/2$ if $m+n\equiv1 \pmod 2$. This is impossible.

Next, we consider the case of $a\equiv b\equiv0 \pmod 2$. First suppose that $ab\neq0$. Write

$$a=2^hm,\ b=2^kn, \qquad (mn,2)=1.$$

Since $\omega_3^2\equiv0 \pmod 2$ we have

$$\alpha^a\equiv\pm(1+2^hm\omega_3) \qquad (\mathrm{mod}\ 2^{h+1}),$$
$$\beta^b\equiv\pm(1+2^kn\omega_3) \qquad (\mathrm{mod}\ 2^{k+1}),$$

and so

$$\alpha^a\beta^b\equiv\pm(1+(2^hm+2^kn)\omega_3) \qquad (\mathrm{mod}\ 2^{l+1})$$

with $l=\min(h,k)$. This implies that one at least of m, n is divisible by 2, provided $h\neq k$. If $h=k$ then, since $m\equiv n\equiv1 \pmod 2$, we have

$$\alpha^m\beta^n\equiv1+2c(m,n)\omega_2+2\omega_3 \qquad (\mathrm{mod}\ 4),$$

so that

$$\alpha^a\beta^b\equiv1+2^{h+1}c(m,n)\omega_2+2^{h+1}\omega_3 \qquad (\mathrm{mod}\ 2^{h+2}).$$

In any case we have an imposibility, and hence we must have $ab=0$.

Suppose then that $a\neq0, b=0$. Writing as before

$$a=2^hm,\ (m,2)=1,$$

we get

$$\alpha^a \equiv \pm(1+2^h m\omega_3) \pmod{2^{h+1}},$$

whence $m\equiv 0 \pmod 2$, a contradiction again. Similarly, the supposition $a=0, b\neq 0$ involves a contradiction.

Thus, the only possibility is that $a=b=0$, which gives the trivial solutions of (12),

$$U=0,\ V=\pm 1.$$

2.4 PROPOSITION 3. *The only solutions of the Diophantine equation*

$$4U^4-36UV^3+9V^4=1 \tag{13}$$

in rational integers U, V are

$$U=-2,\ V=-1 \text{ and } U=2,\ V=1.$$

PROOF. If we set $U=2u-v$, $V=u$, then the equation (13) becomes

$$u^4-92u^3v+96u^2v^2-32uv^3+4v^4=1. \tag{34}$$

In order to prove Proposition 3 we have to show that the equation (34) admits the trivial solutions $u=\pm 1, v=0$ only.

Let θ be a real root of the equation $f(x)=0$, where

$$f(x)=x^4-92x^3+96x^2-32x+4$$

is a polynomial whose discriminant is $D_f=-2^{12}\cdot 3^6\cdot 239$. The quartic field $L=\boldsymbol{Q}(\theta)$ has an integral basis $\Delta=\{1, \omega_1, \omega_2, \omega_3\}$ with

$$\omega_1=\theta,\ \omega_2=\frac{1}{6}(\theta^2+2\theta+4),\ \omega_3=\frac{1}{6}(\theta^3+2\theta^2+4\theta),$$

and the discriminant of L is $D=-2^8\cdot 3^2\cdot 239$.

Let ξ be any root of the equation $f(x)=0$. If we define the number ξ^* by $(4-\xi)\cdot\xi^*=2$, then ξ^* satisfies an equation $f^*(x)=0$, where $f^*(x)$ is the polynomial specified in (32). Therefore, the number θ^* given by $(4-\theta)\theta^*=2$ generates a quartic field $\boldsymbol{Q}(\theta^*)=L$, and $\Delta^*=\{1, \omega_1^*, \omega_2^*, \omega_3^*\}$ with $\omega_1^*, \omega_2^*, \omega_3^*$ as given in (33) is another integral basis of L. We have in fact

$$\Delta^*=M\Delta,$$

where

$$M=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 186 & 140 & -282 & 3 \\ -242 & -171 & 375 & -4 \\ 500 & 311 & -748 & 8 \end{pmatrix}$$

and $\det M=1$.

Thus, we may easily rewrite a fundamental pair of units in $\boldsymbol{Q}(\theta^*)$ in terms of the new basis Δ; the result is

$$\alpha=-242-171\omega_1+375\omega_2-4\omega_3,$$
$$\beta=-1462-1073\omega_1+2253\omega_2-24\omega_3.$$

Now, the solutions $u, v\in\boldsymbol{Z}$ of the equation (34) should satisfy

$$\pm(u-v\theta)=\alpha^a\beta^b$$

for some $a, b\in\boldsymbol{Z}$.

The rest of the proof can be carried out just as in the proof of Proposition 2, by making use of the congruence relations

$$\alpha\equiv-2-3\omega_1-\omega_2+4\omega_3 \pmod 8,$$
$$\beta\equiv 2-\omega_1-3\omega_2 \pmod 8,$$
$$\alpha^2\equiv\beta^2\equiv-1+4\omega_2-2\omega_3 \pmod 8,$$

and

$$\alpha\beta=3+4\omega_1+4\omega_2-2\omega_3 \pmod 8.$$

2.5 PROPOSITION 4. *The only solutions of the Diophantine equation*

$$U^4-18U^2V^2+72UV^3+9V^4=1 \tag{18}$$

in rational integers U, V are the trivial ones,

$$U=\pm1,\ V=0.$$

PROOF. Put

$$f(x)=x^4-18x^2+72x+9. \tag{35}$$

The discriminant of $f(x)$ is $D_f=-2^{12}\cdot3^6\cdot239$. Let θ be a real root of the equation $f(x)=0$ and put $L=\boldsymbol{Q}(\theta)$.

The quartic field L has an integral basis $\Delta=\{1, \omega_1, \omega_2, \omega_3\}$ where

$$\omega_1=\frac{1}{2}(\theta+1),\ \omega_2=\frac{1}{12}(\theta^2+3),\ \omega_3=\frac{1}{24}(\theta+3)(\theta^2+3), \tag{36}$$

and the discriminant of L is $D=-3^2\cdot239$.

We appeal again to Berwick's criterion to find a pair of fundamental units in L,

$$\alpha=1-\omega_1+\omega_2,$$
$$\beta=1-\omega_1-\omega_2.$$

If $U, V\in\boldsymbol{Z}$ satisfy the equation (18), then we must have as before

$$\pm(U-V\theta)=\pm(U+V-2V\omega_1)=\alpha^a\beta^b$$

for some $a, b\in\boldsymbol{Z}$.

Since $\alpha\equiv\beta \pmod 2$ and since

$$\alpha^m\equiv 1, \alpha, \omega_2, \omega_1+\omega_3, \omega_1, 1+\omega_3, \text{ or } \omega_2+\omega_3 \pmod 2$$

according as

$$m\equiv 0, 1, 2, 3, 4, 5, \text{ or } 6 \pmod 7,$$

it is necessary that $a+b\equiv 0 \pmod 7$. So we shall suppose in the following that

$$a+b\equiv 0 \pmod 7$$

so that

$$a-6b\equiv 6a-b\equiv 0 \pmod 7.$$

Suppose $a-6b\neq 0$ and $b\neq 0$. Put

$$a-6b=2^h\cdot 7e,\ b=2^kf, (ef, 2)=1,\ h\geqq 0,\ k\geqq 0.$$

If $k=0$ then $h\geqq 0$, and if $k>0$ then $h=0$.

Note that

$$\alpha^7\equiv -1+4\omega_2 \pmod 8,$$
$$\alpha^6\beta\equiv 1-2(\omega_1-\omega_2) \pmod 8.$$

Case of $k=0, h\geqq 0$: In this case we have

$$\alpha^{a-6b}\equiv\pm(1-2^{h+2}e\omega_2) \pmod{2^{h+3}},$$
$$\beta^b\equiv\alpha^{-6b}(1-2f(\omega_1-\omega_2)) \pmod 4.$$

It follows that

$$\alpha^a\beta^b\equiv\pm(1-2f(\omega_1-\omega_2)) \pmod 4,$$

and this implies that $f\equiv 0 \pmod 2$, a contradiction.

Case of $k>0$, $h=0$: Here, we have

$$\alpha^{a-6b}\equiv -(1-4e\omega_2) \pmod 8,$$
$$\beta^b\equiv\alpha^{-6b}(1-2^{k+1}f(\omega_1-\omega_2)) \pmod{2^{k+2}},$$

and so

$$\alpha^a\beta^b\equiv -1+2^{k+1}f\omega_1+4(e-2^{k-1}f)\omega_2 \qquad (\mathrm{mod}\ 8).$$

This implies that $f\equiv 0 \pmod 2$ if $k=1$, and $e\equiv 0 \pmod 2$ if $k>1$, an impossibility.

We thus have proved that we have

$$\text{either } a-6b=0 \text{ or } b=0.$$

In quite a similar manner we can show that we have

$$\text{either } 6a-b=0 \text{ or } a=0,$$

using the relations

$$\beta^7\equiv -3+2(\omega_1+\omega_2) \qquad (\mathrm{mod}\ 8),$$
$$\alpha\beta^6\equiv 3+4(\omega_1+\omega_2) \qquad (\mathrm{mod}\ 8).$$

We have, therefore, $a=b=0$ in any case, thus giving the trivial solutions of (18)

$$U=\pm 1,\ V=0.$$

2.6 PROPOSITION 5. *The only solutions of the Diophantine equation*

$$9U^4-18U^2V^2+24UV^3+V^4=1 \tag{17}$$

in rational integers U, V are the trivial ones,

$$U=0,\ V=\pm 1.$$

PROOF. Put

$$f(x)=x^4+24x^3-18x^2+9.$$

The discriminant of $f(x)$ is $D_f=-2^{12}\cdot 3^6\cdot 239$. Let θ be a real root of the equation $f(x)=0$ and put $L=\boldsymbol{Q}(\theta)$.

The quartic field L has an integral basis $\Delta=\{1,\omega_1,\omega_2,\omega_3\}$ where $\omega_1,\omega_2,\omega_3$ are defined by (36). The field L has the discriminant $D=-3^2\cdot 239$.

Let ξ be any root of the equation $f(x)=0$. If we define the number ξ^* by $\xi\xi^*=3$, then ξ^* satisfies an equation $f^*(x)=0$, where $f^*(x)$ is a polynomial specified in (35). Therefore, the number θ^* given by $\theta\theta^*=3$ generates a quartic field $\boldsymbol{Q}(\theta^*)=L$, and $\Delta^*=\{1,\omega_1^*,\omega_2^*,\omega_3^*\}$ with $\omega_1^*,\omega_2^*,\omega_3^*$ as given in (36), with θ^* in place of θ, is another integral basis of L; in fact, we find

$$\Delta^*=M\Delta,$$

where

$$M=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 9 & 7 & -42 & -4 \\ 4 & -4 & -1 & 0 \\ 18 & 6 & -75 & -7 \end{pmatrix}$$

and det $M=1$.

Thus, we may use a result in the proof of Proposition 4 to find a fundamental pair of units in L,

$$\alpha=-4-11\omega_1+41\omega_2+4\omega_3,$$
$$\beta=-12-3\omega_1+43\omega_2+4\omega_3.$$

Now, for each solution $U, V\in\boldsymbol{Z}$ of the equation (17) we have

$$\pm(V-U\theta)=\pm(U+V-2U\omega_1)=\alpha^a\beta^b$$

for some $a, b\in\boldsymbol{Z}$.

Since

$$\alpha\equiv\beta \pmod 2$$

and since

$$\alpha^m\equiv 1, \alpha, \omega_2, 1+\omega_1+\omega_2+\omega_3, 1+\omega_1, 1+\omega_2+\omega_3, \text{ or } \omega_3 \pmod 2$$

according as

$$m\equiv 0, 1, 2, 3, 4, 5, \text{ or } 6 \pmod 7,$$

we must have $a+b\equiv 0 \pmod 7$, and so

$$a-6b\equiv 6a-b\equiv 0 \pmod 7.$$

We note that

$$\alpha^7\equiv -1-2(\omega_1-\omega_2) \pmod 8,$$
$$\alpha^6\beta\equiv -1+4(\omega_1+\omega_2) \pmod 8,$$

and

$$\beta^7\equiv -1-2(\omega_1-\omega_2) \pmod 8,$$
$$\alpha\beta^6\equiv -1+4(\omega_1+\omega_2) \pmod 8.$$

The rest of the proof can be carried out along the same lines as in the proof of Proposition 4.

2.7 PROPOSITION 6. *The only solutions of the Diophantine equation*

$$U^4+18U^2V^2-72UV^3+9V^4=1 \tag{28}$$

in rational integers U, V are the trivial ones,

$$U=\pm 1,\ V=0.$$

PROOF. Put

$$f(x)=x^4+18x^2-72x+9. \tag{37}$$

The discriminant of $f(x)$ is $D_f=-2^{12}\cdot 3^6\cdot 239$. Let θ be a real root of the equation $f(x)=0$ and put $L=\boldsymbol{Q}(\theta)$.

An integral basis $\Delta=\{1, \omega_1, \omega_2, \omega_3\}$ of the quartic field L is given by

$$\omega_1=\theta,\ \omega_2=\frac{1}{6}(\theta^2+3),\ \omega_3=\frac{1}{6}(\theta^3+3\theta), \tag{38}$$

and the discriminant of L is $D=-2^8\cdot 3^2\cdot 239$.

As a fundamental pair of units in L we take the pair

$$\alpha=1+5\omega_1-3\omega_2-2\omega_3,$$
$$\beta=-7+15\omega_1+11\omega_2+4\omega_3.$$

Note that

$$\begin{aligned}
\alpha &\equiv 1-3\omega_1+3\omega_2-2\omega_3 \pmod 8,\\
\beta &\equiv 1-\omega_1+3\omega_2+4\omega_3 \pmod 8;\\
\alpha^2 &\equiv 3+2\omega_2-2\omega_3 \pmod 8,\\
\beta^2 &\equiv -1-2\omega_2+2\omega_3 \pmod 8;
\end{aligned}$$

and

$$\alpha\beta\equiv -1+2\omega_2 \pmod 8.$$

Now, for each solution $U, V\in\boldsymbol{Z}$ of the equation (28) we have

$$\pm(U-V\theta)=\alpha^a\beta^b$$

for some $a, b\in\boldsymbol{Z}$.

Since $\alpha^2\beta^2\equiv 1 \pmod 4$ and $\alpha\beta\equiv -1+2\omega_2 \pmod 4$, the only possibility for the values of $a, b \pmod 2$ is

$$a\equiv b\equiv 0 \pmod 2.$$

The rest of the proof is similar to that of Proposition 2. We thus have $a=b=0$ and our equation (28) has only the trivial solutions

$$U=\pm 1,\ V=0.$$

2.8 PROPOSION 7. *The only solutions of the Diophantine equation*

$$9U^4+18U^2V^2-24UV^3+V^4=1 \tag{27}$$

in rational integers U, V are the trivial ones,

$$U=0,\ V=\pm 1.$$

PROOF. Put

$$f(x)=x^4-24x^3+18x^2+9.$$

The discriminant of $f(x)$ is $D_f=-2^{12}\cdot 3^6\cdot 239$. Let θ be a real root of the equation $f(x)=0$ and write $L=\boldsymbol{Q}(\theta)$.

The quartic field L has an integral basis $\Delta=\{1,\omega_1,\omega_2,\omega_3\}$ with $\omega_1,\omega_2,\omega_3$ as given by (38), and the discriminant of L is $D=-2^8\cdot 3^2\cdot 239$.

Let ξ be any root of the equation $f(x)=0$. If we define the number ξ^* by $\xi\xi^*=3$, then ξ^* satisfies an equation $f^*(x)=0$, where $f^*(x)$ is a polynamial specified in (37). It follows from this that the number θ^* given by $\theta\theta^*=3$ defines a quartic field $\boldsymbol{Q}(\theta^*)=L$, and $\Delta^*=\{1,\omega_1^*,\omega_2^*,\omega_3^*\}$ with $\omega_1^*,\omega_2^*,\omega_3^*$ as given in (38), with θ^* in place of θ, is another integral basis of L. We thus find

$$\Delta^*=M\Delta$$

with

$$M=\begin{pmatrix} 1 & 0 & 0 & 0 \\ -24 & -5 & 48 & -2 \\ -2 & 4 & -1 & 0 \\ 72 & 12 & -120 & 5 \end{pmatrix}$$

and $\det M=1$.

Consequently, it is again immediate to find a fundamental pair of units in L by making use of a result in the proof of Proposition 6. Thus

$$\alpha=-257-37\omega_1+474\omega_2-23\omega_3,$$
$$\beta=-461+17\omega_1+232\omega_2-9\omega_3$$

form a fundamental pair of units in our L.

We have then

$$\alpha\equiv -1+3\omega_1+2\omega_2+\omega_3 \pmod 8,$$
$$\beta\equiv 3+\omega_1-\omega_3 \pmod 8;$$
$$\alpha^2\equiv 3+4\omega_1+4\omega_2+2\omega_3 \pmod 8,$$
$$\beta^2\equiv -1+4\omega_1+2\omega_3 \pmod 8;$$

and

$$\alpha\beta\equiv -1+2\omega_2+2\omega_3 \pmod 8.$$

Therefore, we see that the proof can be carried out just in the same way as in the proof of Proposition 2, on noting that

$$(\pm 1+\omega_3)^2\equiv 0 \pmod 2.$$

2.9 PROPOSITION 8. *The only solutions of the Diophantine equation*

$$9u^4+18u^2v^2-24uv^3+v^4=4 \tag{26}$$

in rational integers u, v are

$$u=v=\pm 1.$$

PROOF. If we set $u=x+y, v=x$, then the equation (26) becomes

$$4x^4+48x^3y+72x^2y^2+36xy^3+9y^4=4.$$

Hence, y must be even, and, by replacing y with $2y$ and then dividing by 4 the both sides of the resulting equation, we get

$$x^4+24x^3y+72x^2y^2+72xy^3+36y^4=1.$$

Again, by the transformation $U=x-6y$, $V=y$, we have

$$U^4-144U^2V^2+936UV^3-1692V^4=1. \tag{39}$$

Thus, in order to prove Proposition 8 it will suffice to show that the Diophantine equation (39) in rational integers U, V has only the trivial solutions $U=\pm 1$, $V=0$.

Define the polynomial

$$f(x)=x^4-144x^2+936x-1692$$

whose discriminant is $D_f=-2^{12}\cdot 3^6\cdot 239$. Let θ be a real root of the equation $f(x)=0$ and put $L=\boldsymbol{Q}(\theta)$.

An integral basis of L is $\Delta=\{1, \omega_1, \omega_2, \omega_3\}$, where

$$\omega_1=\theta,\ \omega_2=\frac{1}{6}\theta^2 \quad \omega_3=\frac{1}{6}\theta^3,$$

and the discriminant of L is $D=-2^8\cdot 3^2\cdot 239$.

Let ξ be any root of the equation $f(x)=0$. It is not difficult to verify that, if we define the number ξ^* by $(\xi-6)(\xi^*-3)=6$, then ξ^* satisfies an equation $f^*(x)=0$, where $f^*(x)$ is a polynomial specified in (37). It follows from this that the number θ^* satisfying $(\theta-6)(\theta^*-3)=6$ defines a quartic field $\boldsymbol{Q}(\theta^*)=L$, and $\Delta^*=\{1, \omega_1^*, \omega_2^*, \omega_3^*\}$ with $\omega_1^*, \omega_2^*, \omega_3^*$ as given in (38), with θ^* in place of θ, is another integral basis of L. We have in fact

$$\Delta^*=M\Delta,$$

where

$$M=\begin{pmatrix} 1 & 0 & 0 & 0 \\ -45 & 18 & -6 & -1 \\ 150 & -114 & 5 & 1 \\ -264 & 269 & 9 & 1 \end{pmatrix}$$

and det $M=1$.

In virtue of this relation we may easily translate the pair of fundamental units found and used in the proof of Proposition 6 to a pair of fundamental units in our field L. Thus, we take as a fundamental pair of units in L

$$\alpha=146+106\omega_1+63\omega_2+10\omega_3,$$
$$\beta=-88+92\omega_1+\omega_2.$$

We have

$$\alpha\equiv 2+2\omega_1-\omega_2+2\omega_3 \pmod 8,$$
$$\beta\equiv 4\omega_1+\omega_2 \pmod 8;$$
$$\alpha^2\equiv 3-2\omega_1+4\omega_2+4\omega_3 \pmod 8,$$
$$\beta^2\equiv -1-2\omega_1 \pmod 8;$$

and

$$\alpha\beta\equiv -3-2\omega_1+2\omega_2-2\omega_3 \pmod 8.$$

The rest of the proof can be carried out just as in the proof of Proposition 2 to conclude that the equation (39) admits only the trivial solutions $U=\pm 1$, $V=0$, as required.

This concludes the proof of our theorem stated in the Introduction.

2.10 Here is a final remark. So far we have treated eight Diophantine equations that have the form $F(U, V)=1$, directly or after suitably transformed, where each of the $F(U, V)$ is an irreducible binary quartic form in U, V with rational integral coefficients. It can be easily verified that no two of these forms $F(U, V)$ are equivalent under the unimodular transformation of the indeterminates U, V with integer coefficients. Thus, each of the eight equations $F(U, V)=1$ needed a separate consideration, as we have seen above.

References

[1] Berwick, W. E. H., Integral Bases. Cambridge Tracts in Math. and Math. Physics, No. 22. Cambridge Univ. Press, London 1927.

[2] Berwick, W. E. H., Algebraic number-fields with two independent units. Proc. London Math. Soc. **34** (1932), 360-378.

[3] Guy, Richard K., Unsolved Problems in Number Theory. Unsolved Problems in Intuitive Mathematics Vol. 1. Springer-Verl., New York et al. 1981.

Japanese edition (corrected and enlarged), translated by S. Hitotumatu: 数論における未解決問題集. Springer-Verl., Tokyo et al. 1983.

[4] Mordell, L. J., Diophantine Equations. Pure and Appl. Math. Vol. 30. Academic Press, London and New York 1969.

[5] Аванесов, Э. Т., Решение одной проблеме фигурных чисел. Acta Arith. **12** (1967), 409-420.

[6] Биллевич, К. К., Об единицах алгебраическнх полей третьего и четвертого порядков. Матем. Сборник **40** (**82**) (1956), 123-136.

[7] Делоне, Б. Н. и Фаддеев, Д. К., Теория иррациональностей третьей степени. Труды Матем. Ин-та им. В. А. Стеклова XI. АН СССР, Москва-Ленинград 1940. English Translation by E. Lehmer and S. A. Walker, The Theory of Irrationality of the Third Degree. Transl. Math. Monographs Vol. 10, Amer. Math. Soc., Providence, Rhode Island 1964.

Institute of Mathematics
University of Tsukuba
Ibaraki Pref.
305 Japan