ARKIV FÖR MATEMATIK Band 3 nr 6

Read 11 November 1953

On the Diophantine equation $x^2 + 8D = y^n$

By Trygve Nagell

§ 1.

In a previous paper[1] I showed that the Diophantine equation

$$x^2 + 8 = y^n \quad (n \geqq 3) \tag{1}$$

has no solution in positive integers x and y when n is not a prime $\equiv \pm 1 \pmod 8$. If n is a prime $\equiv \pm 1 \pmod 8$, there is at most one solution in positive integers.

It is, however, possible to obtain the following improvement of this result:

Theorem 1. *The Diophantine equation* (1), *where n is an integer $\geqq 3$, has no solution in positive integers x and y.*

The proof will be given in § 5.

In this paper we shall examine the more general equation

$$x^2 + 8D = y^n, \tag{2}$$

where D is a square-free, odd integer $\geqq 1$, and where n is an integer $\geqq 3$.

We begin by proving the following lemma:

Lemma 1. The equation (2) *has no solution in even integers x and y if $n \geqq 4$.*

If $n = 3$ and if the number of ideal classes in the quadratic field $\boldsymbol{K}(\sqrt{-2D})$ is not divisible by 3, *the equation* (2) *is solvable in even integers x and y only when $D = 6a^2 \mp 1$, a integer; corresponding to this value of D there is the single integral solution $y = 16a^2 \mp 2$.*

Proof. Let x, y be a solution of (2) in integers. If x is even, y is so. Then y^n is divisible by 8. Hence by (2) x is divisible by 4. Since D is odd, y^n must be divisible by exactly 8, and this implies $n = 3$. If we put $x = 4x_1$ and $y = 2y_1$, we get

$$(2x_1)^2 + 2D = 2y_1^3. \tag{3}$$

The ideal factors $(2x_1 + \sqrt{-2D})$ and $(2x_1 - \sqrt{-2D})$ of the left-hand side have the greatest common divisor $(2, \sqrt{-2D})$. Hence it follows from (3)

[1] See Nagell [1], § 2. Figures in [ ] refer to the Bibliography at the end of this paper.

$$(2x_1+\sqrt{-2D})=(2,\sqrt{-2D})\,\mathfrak{j}^3, \tag{4}$$

where $\mathfrak{j}$ is an ideal with the norm y_1 in $\boldsymbol{K}(\sqrt{-2D})$. Since

$$(2,\sqrt{-2D})^2=(2),$$

we get

$$(2x_1+\sqrt{-2D})^2=(2)\,\mathfrak{j}^6. \tag{5}$$

Thus $\mathfrak{j}^6$ is a principal ideal. Since, by hypothesis, the class number is not divisible by 3, it is evident that $\mathfrak{j}^2$ is a principal ideal. Then it follows from (5)

$$(2x_1+\sqrt{-2D})^2=2\,(u+v\sqrt{-2D})^3, \tag{6}$$

where u and v are rational integers, such that

$$y_1^2=(N\,\mathfrak{j})^2=u^2+2Dv^2. \tag{7}$$

u is odd, since y_1 is so. It follows from (6) that

$$u+v\sqrt{-2D}=(a\sqrt{2}+b\sqrt{-D})^2, \tag{8}$$

where a and b are rational integers. Combining this equation with (6) we get

$$x_1\sqrt{2}+\sqrt{-D}=(a\sqrt{2}+b\sqrt{-D})^3, \tag{9}$$

whence

$$1=6a^2b-Db^3.$$

This implies $b=\pm 1$ and

$$D=6a^2\mp 1. \tag{10}$$

Then we get from (7) and (8)

$$y_1=N\,\mathfrak{j}=2a^2+Db^2=2a^2+D=8a^2\mp 1, \tag{11}$$

and from (9)

$$x_1=2a^3-3Dab^2=-16a^3\pm 3a. \tag{11'}$$

§ 2.

We shall now consider equation (2) for an odd solution x. Let n be the power of an odd prime q, thus $n=q^\alpha$. Further we suppose that the number of ideal classes in the quadratic field $\boldsymbol{K}(\sqrt{-2D})$ is not divisible by n.

When x is odd, y is also odd, and the ideal factors $(x+2\sqrt{-2D})$ and $(x-2\sqrt{-2D})$ of the left-hand side of (2) are relatively prime. Hence

$$(x+2\sqrt{-2D})=\mathfrak{j}^n, \tag{12}$$

where $\mathfrak{j}$ is an ideal. If the class number h in $\boldsymbol{K}(\sqrt{-2D})$ is divisible by q^{β} $(0 \leqq \beta < \alpha)$ and not by $q^{\beta+1}$, there exist two rational integers f and g such that

$$f q^{\alpha} - g h = q^{\beta}.$$

Then by (12) we get the following equivalence

$$\lambda^{q^{\beta}} \sim \lambda^{f q^{\alpha}} \sim 1.$$

Hence we obtain from (12)

$$x + 2\sqrt{-2D} = (u + v\sqrt{-2D})^{q},$$

where u and v are rational integers, such that

$$y^{n} = (u^{2} + 2Dv^{2})^{q}.$$

u is odd since x is so. Then, equating the coefficients of $\sqrt{-2D}$, we get the relation

$$2 = \sum_{k=0}^{\frac{1}{2}(q-1)} \binom{q}{2k+1} u^{q-2k-1} v^{2k+1} (-2D)^{k}. \tag{13}$$

From this equation it is obvious that v is a divisor of 2 and that $q u^{q-1} v$ is even. Hence $v = \pm 2$ since q and u are odd. All the terms on the right-hand side in (13) are divisible by q, except the last term (for $k = \frac{1}{2}(q-1)$). Thus we get, if D is not divisible by q,

$$2 \equiv v^{q} (-2D)^{\frac{1}{2}(q-1)} \equiv v \left(\frac{-2D}{q}\right) \pmod{q},$$

whence

$$v = 2\left(\frac{-2D}{q}\right).$$

If D is divisible by q, equation (13) is impossible.

Then, on dividing (13) by v, we have

$$\left(\frac{-2D}{q}\right) = \sum_{k=0}^{\frac{1}{2}(q-1)} \binom{q}{2k+1} u^{q-2k-1} (-8D)^{k}. \tag{14}$$

Taking equation (14) as a congruence modulo 8 we get

$$\left(\frac{-2D}{q}\right) \equiv q u^{q-1} \equiv q \pmod{8}, \tag{15}$$

whence it follows

$$q \equiv \pm 1 \pmod{8}.$$

Hence, taking in consideration Lemma 1, we have the following result:

Theorem 2. *Let n be the power of an odd prime q, $n \geqq 3$, and suppose that the class number in $\boldsymbol{K}(\sqrt{-2D})$ is not divisible by n.*

If $q \equiv \pm 3 \pmod 8$, *the Diophantine equation* (2) *has no solution in integers* x *and* y, *apart from the case when* $n = 3$ *and* x *and* y *are even. Likewise, if* D *is divisible by* q, *equation* (2) *has no integral solution.*

We may also state

Lemma 2. Let n *be the power of a prime* $q \equiv \pm 1 \pmod 8$, *and suppose that the class number in* $\mathbf{K}(\sqrt{-2D})$ *is not divisible by* n.

If the Diophantine equation (2) *is solvable in integers* x *and* y, *we must have*

$$y^{\frac{n}{q}} = u^2 + 8D,$$

where u *is an odd integer satisfying equation* (14).

§ 3.

Now suppose that the prime q in (14) is $\equiv \pm 1 \pmod 8$. If we put $X = u^2$ and $Y = -8D$, the right-hand side of (14) becomes a form of the degree $\frac{1}{2}(q-1)$ in X and Y with integral coefficients. By the theorem of EISENSTEIN it is obvious that this form is irreducible. Hence, according to a famous theorem of THUE, equation (14) holds only for a finite number of integral values X and Y. Thus we have proved:

Theorem 3. *Let* n *be the power of an odd prime* $\equiv \pm 1 \pmod 8$, *and suppose that the class number in* $\mathbf{K}(\sqrt{-2D})$ *is not divisible by* n. *For a given* $n \geqq 7$, *there is only a finite number of square-free odd integers* $D \geqq 1$, *such that the Diophantine equation* (2) *is solvable in integers* x *and* y.

§ 4.

When $q \equiv -1 \pmod 8$ it follows from (15)

$$-1 \equiv q \equiv \left(\frac{-2D}{q}\right) \equiv -\left(\frac{D}{q}\right) \pmod 8.$$

When $q \equiv +1 \pmod 8$ it follows

$$1 \equiv q \equiv \left(\frac{-2D}{q}\right) \equiv \left(\frac{D}{q}\right) \pmod 8.$$

Hence, in both cases D must be a quadratic residue modulo q. Thus we can state

Theorem 4. *Let* n *be the power of an odd prime* $q \equiv \pm 1 \pmod 8$, *and suppose that the class number in* $\mathbf{K}(\sqrt{-2D})$ *is not divisible by* n. *If* D *is a quadratic non-residue modulo* n, *the Diophantine equation* (2) *has no solution in integers* x *and* y.

§ 5.

Now we suppose that $D \equiv 1 \pmod 3$.
If $q \equiv -1 \pmod 8$ it follows from (14)

$$-1 \equiv \sum_{k=0}^{\frac{1}{2}(q-1)} \binom{q}{2k+1} u^{q-2k-1} \pmod 3.$$

This is impossible when u is divisible by 3, since, in that case, the right-hand side is $\equiv 1 \pmod 3$. If u is not divisible by 3, we get

$$-1 \equiv \binom{q}{1} + \binom{q}{3} + \cdots + \binom{q}{q} \pmod 3.$$

But this congruence is impossible since the value of the right-hand side is 2^{q-1} and thus $\equiv 1 \pmod 3$.

If $q \equiv 1 \pmod 8$ it follows from (14)

$$q-1+q(u^{q-1}-1) = -\sum_{k=1}^{\frac{1}{2}(q-1)} \binom{q}{2k+1} u^{q-2k-1}(-8D)^k. \tag{16}$$

Suppose $q-1 = 2^r q_1$ where q_1 is odd. Then $u^{q-1}-1$ is divisible by 2^{r+2}. The general term in the right-hand sum in (16) may be written

$$\frac{q(q-1)}{2k(2k+1)} \binom{q-2}{2k-1} u^{q-2k-1}(-8D)^k. \tag{17}$$

Here the numerator is divisible by 2^{r+3k}. The denominator is divisible by a power of 2 which is $\leqq 2k$. Since for all $k \geqq 1$

$$2^{3k} = 8^k > 4k,$$

we conclude that the number (17) is divisible at least by 2^{r+1}. Hence equation (16) is impossible, for $q-1$ is divisible by 2^r but not by 2^{r+1}.

Thus we can state

Theorem 5. *Let n be the power of an odd prime $q \equiv \pm 1 \pmod 8$, and suppose that the class number in $\boldsymbol{K}(\sqrt{-2D})$ is not divisible by n. If $D \equiv 1 \pmod 3$, the Diophantine equation (2) has no solution in integers x and y.*

This result is contained in the more general

Theorem 6. *Let n be an odd integer >3, and suppose that the class number in $\boldsymbol{K}(\sqrt{-2D})$ is not divisible by n. If $D \equiv 1 \pmod 3$ the Diophantine equation (2) has no solution in integers x and y.*

Proof. Suppose that equation (2) is solvable in integers x and y. There must exist a prime factor q of n with the following property: q^α is a factor of n but not of the class number h. Let us put $m=q^\alpha$, $n=mr$ and $z=y^r$. Then the equation

$$(2') \qquad x^2+8D=z^m$$

should be solvable in integers x and z. But by Theorem 2 this is impossible when $q\equiv\pm 3 \pmod 8$ and $m=q^\alpha>3$. When $m=q^\alpha=3$, it follows from Lemma 1 and Theorem 2 that

$$z=y^r=16a^2\mp 2;$$

but this is impossible since $r=\frac{n}{3}>1$.

When $q\equiv\pm 1 \pmod 8$ equation (2′) is impossible in virtue of Theorem 5.

In the special case $D=1$ we easily get Theorem 1. In fact, the class number in $\boldsymbol{K}(\sqrt{-2})$ is $=1$. The equation

$$x^2+8=y^2$$

is possible only for $|x|=1$, $|y|=3$. By Lemma 1 the equation

$$x^2+8=y^3$$

is satisfied only for $x=0$, $y=2$.

§ 6.

We shall prove the following theorem:

Theorem 7. *Let n be the power of an odd prime $q\equiv\pm 1 \pmod 8$, and suppose that the class number in $\boldsymbol{K}(\sqrt{-2D})$ is not divisible by n. Then the Diophantine equation (2) has at most one solution in positive integers x and y.*

Proof. Suppose that equation (14) was satisfied for two values u and u_1 $(u\neq\pm u_1)$. Thus

$$\left(\frac{-2D}{q}\right)=\sum_{k=0}^{\frac{1}{2}(q-1)}\binom{q}{2k+1}u_1^{q-2k-1}(-8D)^k.$$

Subtracting this equation from equation (14) we get, on dividing by $u^2-u_1^2$:

$$(18) \qquad -q\,\frac{u^{q-1}-u_1^{q-1}}{u^2-u_1^2}=\sum_{k=1}^{\frac{1}{2}(q-3)}\binom{q}{2k+1}\frac{u^{q-2k-1}-u_1^{q-2k-1}}{u^2-u_1^2}(-8D)^k.$$

We need the following lemma:

Lemma 3. Suppose that $m=2^\mu r$, where m, μ and r are positive integers, r odd. Suppose further that u and u_1 are odd integers $u\neq\pm u_1$. Then the integer

$$\frac{u^m-u_1^m}{u^2-u_1^2}$$

is divisible by exactly $2^{\mu-1}$ and not by 2^μ.

Proof. The lemma is true for $m=2$, independently of the value of r. For, since r is odd, the number

$$\frac{u^{2r}-u_1^{2r}}{u^2-u_1^2}=u^{2r-2}+u^{2r-4}u_1^2+\cdots+u_1^{2r-2}$$

is odd. Suppose that the lemma is true for the even exponent m. Then we shall show that it is also true for the exponent $2m$. In fact, we have

$$\frac{u^{2m}-u_1^{2m}}{u^2-u_1^2}=(u^m+u_1^m)\frac{u^m-u_1^m}{u^2-u_1^2},$$

and $u^m+u_1^m$, being the sum of two odd squares, is even but not divisible by 4. Thus Lemma 3 is established by induction.

It is easy to see that equation (18) is impossible when $q\equiv -1 \pmod 8$. For, by Lemma 3, the left-hand side of (18) is odd in this case. But the right-hand side is divisible by 8.

Suppose next $q\equiv 1 \pmod 8$ and $q-1=2^\mu r$, where r is odd and $\mu\geqq 3$. Then, by Lemma 2, the left-hand side of (18) is divisible by $2^{\mu-1}$ and not by 2^μ. The general term in (18) may be written

$$\binom{q-2}{2k-1}\frac{q(q-1)}{2k(2k+1)}2^{3k}\cdot\frac{u^{q-2k-1}-u_1^{q-2k-1}}{u^2-u_1^2}(-D)^k.$$

Since for all $k\geqq 1$

$$2^{3k}>2k,$$

this number is divisible at most by 2^μ. Hence the right-hand side of (18) is divisible by 2^μ. But we have just shown that the left-hand side of (18) is divisible by $2^{\mu-1}$ and not by 2^μ. Thus equation (14) is satisfied by at most one value of u^2. The corresponding value of y is given by the relation

$$y^n=(u^2+8D)^q. \tag{19}$$

This proves Theorem 7.

§ 7.

Further we prowe

Theorem 8. *Let n be an odd integer >3, and suppose that n and the class number in $\boldsymbol{K}(\sqrt{-2D})$ are relatively prime. If the Diophantine equation* (2) *has a solution in integers x and y, n is a prime* $\equiv \pm 1 \pmod 8$.

Proof. Suppose that n is divisible by a prime $q\equiv \pm 3 \pmod 8$. Put

$$z=y^{\frac{n}{q}}$$

and consider the equation

$$x^2+8D=z^q.$$

The class number h in $K(\sqrt{-2\,D})$ is not divisible by q. If $q=3$, we get by Lemma 1

$$z=16\,a^2\mp 2=y^{\frac{n}{3}}.$$

But this is clearly impossible since $\frac{n}{3}>1$. If $q>3$, it follows from Theorem 2 that equation (2) is impossible.

Hence n is a product of primes $\equiv \pm 1 \pmod 8$. Let q be the least of these primes and suppose that $n>q$. Put

$$z=y^{\frac{n}{q}}$$

and consider the equation

$$x^2+8\,D=z^q.$$

Since the class number h is not divisible by q, it follows by Lemma 2 that

$$z=u^2+8\,D,$$

where u is an odd integer satisfying equation (14). $\frac{n}{q}$ is divisible by a prime p which is $\geqq q$ and $\equiv \pm 1 \pmod 8$. Now put

$$z_1=y^{\frac{n}{p\,q}}$$

and consider the equation

$$u^2+8\,D=z_1^p.$$

Since the class number h is not divisible by p, it follows by Lemma 2 that

$$z_1=u_1^2+8\,D,$$

where u_1 is an odd integer. Hence we have

$$z=y^{\frac{n}{q}}=(u_1^2+8\,D)^p\geqq(1+8\,D)^q. \tag{20}$$

From equation (14) it follows that

$$(8\,D)^{\frac{1}{2}(q-1)}\equiv\left(\frac{2\,D}{q}\right) \pmod{u^2 q},$$

whence

$$u^2 q\leqq(8\,D)^{\frac{1}{2}(q-1)}+1.$$

Thus we get

$$z=u^2+8\,D\leqq\frac{1}{q}\left[(8\,D)^{\frac{1}{2}(q-1)}+1\right]+8\,D.$$

But this contradicts the inequality (20). In fact, it is easily seen that for all $D\geqq 1$ and all $q\geqq 7$, we have

$$(1+8D)^q > \frac{1}{q}[(8D)^{\frac{1}{2}(q-1)}+1]+8D.$$

Hence n must be a prime $\equiv \pm 1 \pmod 8$, and Theorem 8 is proved.

§ 8.

Finally we prove

Theorem 9. *Let n be an odd integer >3, and let D be a positive integer of the form*

$$D = \tfrac{1}{8}(y^n - x^2), \tag{21}$$

where x and y are odd integers. Then there exists a number D_0 such that the class number in the imaginary quadratic field $\boldsymbol{K}(\sqrt{-2D})$ is divisible by n for all square-free $D \geqq D_0$.

Proof. Suppose that the class number is not divisible by n. Then there exists a prime factor q of n with the following property: q^α is a factor of n but not of the class number. Let us put $m = q^\alpha$, $n = mr$ and $z = y^r$. Then it follows from (21)

$$x^2 + 8D = z^m. \tag{22}$$

But by Theorem 2 this relation is not possible for integral values of x and z when $q \equiv \pm 3 \pmod 8$ and $m = q^\alpha > 3$. When $m = q^\alpha = 3$, it follows from Theorem 2 that (22) is not possible for even x and z. When $q \equiv \pm 1 \pmod 8$, in virtue of Theorem 3, the relation (22) is possible only for a finite number of values D.

This proves Theorem 9.

Remark. It may be shown that there are infinitely many positive and square-free integers D of the form (21); compare [2], § 2.

§ 9.

There are several similar results on other Diophantine equations of the type

$$x^2 + B = y^n, \tag{23}$$

where B and n are positive integers, n odd and $\geqq 3$. Thus LEBESGUE showed that the equation

$$x^2 + 1 = y^n$$

has no solution in integers x and y for $x \neq 0$; see [3].

In a previous paper I examined equation (23) when B is a positive square-free integer which is either $\equiv 1$ or $\equiv 2 \pmod 4$, and showed how all integral solutions may be found in many cases; see [4], § 2. Example: For $B = 5$ and $n \geqq 3$ equation (23) has no integral solution.

LJUNGGREN has treated the case in which B is a positive square-free integer of the form

$$B=1+2^{2m+1}(2h-1),$$

where m and h are positive integers; when the class number in the field $\boldsymbol{K}(\sqrt{-B})$ is not divisible by n, he showed that equation (23) has no integral solution; see [5] and [6]. Example: For $B=9$ and $n\geqq 3$ equation (23) cannot be satisfied by any integers x and y.

Equation (23) is a special case of the Diophantine equation

$$ax^2+bx+c=dy^n, \tag{24}$$

where the left-hand side is an irreducible polynomial of the second degree having integral coefficients; d is an integer $\neq 0$. It was shown by THUE that this equation has only a finite number of integral solutions x, y, when $n\geqq 3$; see [7]. This result was subsequently discovered again by LANDAU and OSTROWSKI; see [8]. However, no general method is known for determining all integral solutions x and y of a given equation of the form (24).

BIBLIOGRAPHY

[1]. T. NAGELL, Verallgemeinerung eines FERMAT-schen Satzes, Archiv der Mathematik, Bd V, S. 53, Zürich 1954.

[2]. —— Zur Arithmetik der Polynome, Berichte d. mathem. Seminars d. Hamburgischen Universität, Bd I, § 2, S. 185, Hamburg 1922.

[3]. V. A. LEBESGUE, Sur l'impossibilité en nombres entiers de l'équation $x^m=y^2+1$, Nouvelles Annales de Mathématiques (1), tome 9, p. 178, Paris 1850.

[4]. T. NAGELL, Sur l'impossibilité de quelques équations à deux indéterminées, Norsk Matematisk Forenings Skrifter, Ser. I, Nr. 13, Kristiania 1923.

[5]. W. LJUNGGREN, On the Diophantine equation $x^2+p^2=y^n$, Kong. Norske Videnskabers Selskab, Forhandl. Bd XVI, Nr. 8, Trondhjem 1943.

[6]. —— On the Diophantine equation $x^2+D=y^n$, Kong. Norske Videnskabers Selskab, Forhandl. Bd XVI, Nr. 23, Trondhjem 1944.

[7]. A. THUE, Über die Unlösbarkeit der Gleichung $ax^2+bx+c=dy^n$ in grossen ganzen Zahlen x und y, Archiv for Mathematik og Naturvidenskab, Bd XXXIV, Kristiania 1916.

[8]. E. LANDAU and A. OSTROWSKI, On the Diophantine equation $ay^2+by+c=dx^n$, Proceedings of the London Mathematical Society, Ser. 2, Vol. 19, London 1919.

Tryckt den 13 april 1954

Uppsala 1954. Almqvist & Wiksells Boktryckeri AB