COLLOQUIUM MATHEMATICUM

VOL. 98 2003 NO. 2

THE DIOPHANTINE EQUATION $Dx^2 + 2^{2m+1} = y^n$

BY

J. H. E. COHN (London)

Abstract. It is shown that for a given squarefree positive integer D, the equation of the title has no solutions in integers $x > 0$, $m > 0$, $n \geq 3$ and y odd, nor unless $D \equiv 14 \pmod{16}$ in integers $x > 0$, $m = 0$, $n \geq 3$, $y > 0$, provided in each case that n does not divide the class number of the imaginary quadratic field containing $\sqrt{-2D}$, except for a small number of (stated) exceptions.

1. Introduction. Ljunggren [3] proved that the equation $x^2 + 2 = y^n$ in positive integers x, y and $n \geq 3$ has only the solution $x = 5$, and Nagell [7, Theorem 24] has shown that if $D \geq 3$ is an odd squarefree integer, $n \geq 3$ is odd and provided n does not divide h, the class number of the quadratic field $\mathbb{Q}[\sqrt{-2D}]$, then the equation $Dx^2 + 2 = y^n$ has no solution. Cohn [2] has completely solved the equation $x^2 + 2^{2m+1} = y^n$, and it is the object of this note to generalise these results.

2. The case $m = 0$. In the first place, the restriction to n odd in Nagell's result can be removed. Since $D > 1$, and is odd, $2D$ has at least two prime factors and so h is even. So if $n = 2N$ with N odd, the result follows directly from Nagell's. Otherwise, it suffices to consider just $n = 2^r$, a power of 2. In the field $\mathbb{Q}[\sqrt{-2D}]$ the principal ideal $[2]$ is the square of the ideal $\varrho = [2, \sqrt{-2D}]$ and we find that since y must be odd,

$$\varrho^2[y]^n = [2 + x\sqrt{-2D}][2 - x\sqrt{-2D}],$$

the two ideals on the right having ϱ as their common factor. So $[2 + x\sqrt{-2D}] = \varrho\pi^n$ for some ideal π, with π^{2n} a principal ideal. Since $n = 2^r$ does not divide h, we may suppose that $h = 2^s j$ where j is odd and $1 \leq s < r$. Thus for some rational integers f and g, $2^s = fh - gn$ and so not only is π^{2n} a principal ideal, but so is $\pi^{2^{s+1}}$. Hence

$$[2 + x\sqrt{-2D}]^2 = [2]\pi^{2^{r+1}} = [2]\sigma^{2^{r-s}}$$

where σ is principal. Since the only units in the field are ± 1, for some rational integers A and B, $(2 + x\sqrt{-2D})^2 = \pm 2(A + B\sqrt{-2D})^2$. But the upper sign

2000 *Mathematics Subject Classification*: Primary 11D61; Secondary 11B37.

would give $\sqrt{2}+x\sqrt{-D}=\pm(A+B\sqrt{-2D})$, which is impossible, and the lower sign yields $-\sqrt{-2}+x\sqrt{D}=\pm(A+B\sqrt{-2D})$, which cannot occur as $D>1$ and is squarefree.

THEOREM 1. *Given a positive squarefree* $D\not\equiv 14 \pmod{16}$, *the equation* $Dx^2+2=y^n$ *has no solutions in positive integers* x, y *and* $n\ge 3$ *unless* n *divides the class number* h *of the quadratic field containing* $\sqrt{-2D}$ *with just the two exceptions* $x=5$, $n=3$, $y=3$ *for* $D=1$ *and* $x=1$, $n=3$, $y=2$ *for* $D=6$.

Proof. For $D=1$ this is Ljunggren's result, and by the above, the theorem holds for odd $D>1$. For even D we have $D=2d$ with d odd and $y=2Y$, and then $dx^2+1=2^{n-1}Y^n$. Since by supposition $d\not\equiv 7 \pmod 8$, the only possibility is $n=3$ with $d\equiv 3 \pmod 8$, x and Y both odd and $3\nmid h$. Then unless $d=3$, we obtain

$$\frac{1}{2}(1+x\sqrt{-d})=\left\{\frac{1}{2}(A+B\sqrt{-d})\right\}^3,$$

where A and B are rational integers of like parity, since the only units in this field, ±1, can be absorbed into the cube. But then $4=A(A^2-3dB^2)$, which is easily seen to be impossible. On the other hand if $d=3$, then we have the equation $y^3=6x^2+2$ leading to the Mordell equation $(6y)^3=(36x)^2+432$, known [6, p. 247] to have only the rational solutions given by $y=2$. This concludes the proof.

In §4, we consider some of the cases with $D<100$ in which n does divide h.

3. The case $m>0$. Although in proving Theorem 1, we were able to deal with some even values of y, Nagell's method depended rather crucially on y being odd. In considering the more general equation of the title, we shall always assume y to be odd, and m positive. This necessarily requires both D and x to be odd as well. We prove

THEOREM 2. *Given a positive squarefree integer* D, *and positive integer* m, *the equation* $Dx^2+2^{2m+1}=y^n$ *has no solutions in positive integers* x, y *and* $n\ge 3$ *with* y *odd, unless* n *divides the class number* h *of the quadratic field containing* $\sqrt{-2D}$ *with the exception of the case* $D=1$, $m=2$, $y=3$, $n=4$ *and a family of exceptions with* D *the squarefree part of* $\frac{1}{3}(2^{2m+1}+1)$, $y=\frac{1}{3}(2^{2m+3}+1)$ *and* $n=3$.

Proof. For $D=1$, as is shown in [2], the only solution is as stated. We suppose therefore that $D\ge 3$. Consider first the case in which n is odd; it clearly suffices to consider only powers of odd primes, $n=p^r$, and suppose that h, which is not divisible by n, equals $p^s j$ where $0\le s<r$ and $p\nmid j$.

Then with the ideal $\varrho = [2, \sqrt{-2D}]$ as above, we find that

$$[2^{m+1} + x\sqrt{-2D}][2^{m+1} - x\sqrt{-2D}] = \varrho^2 [y]^n$$

and since y is assumed odd, this gives $[2^{m+1} + x\sqrt{-2D}] = \varrho\pi^n$ for some ideal π for which π^{2n} is principal. But since $(h, n) = p^s$, there exist rational integers f and g such that $p^s = fh - gn$ and so in fact π^{2p^s} is principal. Hence, since the only units in the field are ± 1, for some rational integers a and b we have $(2^{m+1} + x\sqrt{-2D})^2 = 2(a + b\sqrt{-2D})^p$, and so

$$(a + b\sqrt{-2D})^p = (2^m\sqrt{2} + x\sqrt{-D})^2.$$

Suppose now that $(a + b\sqrt{-2D})^{(p-1)/2} = l + m\sqrt{-2D}$. Then

$$\begin{aligned} a + b\sqrt{-2D} &= \left(\frac{2^m\sqrt{2} + x\sqrt{-D}}{l + m\sqrt{-2D}}\right)^2 = \left(\frac{(2^m\sqrt{2} + x\sqrt{-D})(l - m\sqrt{-2D})}{l^2 + 2Dm^2}\right)^2 \\ &= (c\sqrt{2} + d\sqrt{-D})^2 \end{aligned}$$

for some rational quantities c, d. Suppose now that the least common multiple of the denominators of c and d is k, so that $c = c_1/k$, $d = d_1/k$ with $(c_1, d_1) = 1$. Then $bk^2 = 2c_1d_1$ and $ak^2 = 2c_1^2 - Dd_1^2$. Since D is odd and squarefree, it is easily seen that no prime can divide k, whence both c and d must be integers, and so changing their signs if necessary, we obtain $2^m\sqrt{2} + x\sqrt{-D} = (c\sqrt{2} + d\sqrt{-D})^p$. Then

$$y^{2n} = (2^{2m+1} + Dx^2)^2 = (2c^2 + Dd^2)^{2p},$$

and so d is odd. Also,

$$2^m = c\sum_{i=0}^{(p-1)/2} \binom{p}{2i+1} 2^i c^{2i} (-Dd^2)^{(p-2i-1)/2},$$

and so $c = \pm 2^m$ since the second factor is odd.

Thus $2^{m+1/2} + x\sqrt{-D} = (\pm 2^{m+1/2} + d\sqrt{-D})^p = \alpha^p$, say, and then with $\beta = \overline{\alpha}$,

$$2^{m+3/2} = \alpha^p + \beta^p = (\alpha + \beta)\left(\frac{\alpha^{2p} - \beta^{2p}}{\alpha^2 - \beta^2}\right)\Big/\left(\frac{\alpha^p - \beta^p}{\alpha - \beta}\right)$$

and so

$$\frac{\alpha^{2p} - \beta^{2p}}{\alpha^2 - \beta^2} = \pm\frac{\alpha^p - \beta^p}{\alpha - \beta}.$$

Now α, β is a Lehmer pair since $(\alpha + \beta)^2 = 2^{2m+3}$ and $\alpha\beta = 2^{2m+1} + Dd^2$, and so the Lehmer number $(\alpha^{2p} - \beta^{2p})/(\alpha^2 - \beta^2)$ has no primitive divisors. It then follows from [1, Theorems C and 1.4] that there can be no solution except possibly if $p = 5$ or 3. But there is none for $p = 5$, since equating real parts would give $1 = \pm(2^{4m+2} - 10 \cdot 2^{2m+1}d^2D + 5d^4D^2)$ and here the lower sign is impossible modulo 4 and the upper sign modulo 5. For $p = 3$ we obtain

$1 = \pm(2^{2m+1} - 3d^2D)$ and the upper sign is impossible modulo 3, whence D is the squarefree part of $\frac{1}{3}(2^{2m+1}+1)$ and then $y^{n/3} = \frac{1}{3}(2^{2m+3}+1)$, where n would have to be a power of 3.

To conclude the proof for n odd, we have to show that $n = 3$ is the only possibility here. The contrary case would imply that the equation $Y^3 = \frac{1}{3}(2^{2m+3}+1)$ had a solution. Now this equation is impossible modulo 7 unless $m \equiv -1 \pmod 3$ and then writing $m = 3M-1$ and $X = -2^{2M}$ we obtain $3Y^3 + 2X^3 = 1$. It follows from [5] that this equation has but the single solution $Y = 1$, $X = -1$, and this leads to no solution of our problem.

Finally, if n is even, then if $n = 2N$ with N odd, since $D \geq 3$ and is odd, h is even and so $n \nmid h$ implies that $N \nmid h$ and the result follows since even $Dx^2 + 2^{2m+1} = y^N$ has no solutions and $\frac{1}{3}(2^{2m+3}+1)$ cannot be a square. For the remaining case $n = 2^r$ with $r \geq 2$. In the field $\mathbb{Q}[\sqrt{-2D}]$ the principal ideal [2] is the square of the ideal $\varrho = [2, \sqrt{-2D}]$ and we find that since x and y must be odd,

$$\varrho^2[y]^n = [2^{m+1} + x\sqrt{-2D}][2^{m+1} - x\sqrt{-2D}],$$

the two ideals on the right having ϱ as their common factor. Thus $[2^{m+1} + x\sqrt{-2D}] = \varrho\pi^n$ for some ideal π, with π^{2n} a principal ideal. Since $n = 2^r$ does not divide h, we may suppose that $h = 2^s j$ where j is odd and $1 \leq s < r$. Thus for some rational integers f and g, $2^s = fh - gn$ and so not only is π^{2n} a principal ideal, but so is $\pi^{2^{s+1}}$. Hence

$$[2^{m+1} + x\sqrt{-2D}]^2 = [2]\pi^{2^{r+1}} = [2]\sigma^{2^{r-s}}$$

where σ is principal. Since the only units in the field are ± 1, for some rational integers A and B, $(2^{m+1} + x\sqrt{-2D})^2 = \pm 2(A + B\sqrt{-2D})^2$. But the upper sign would give $2^m\sqrt{2} + x\sqrt{-D} = \pm(A + B\sqrt{-2D})$, which is impossible, and the lower sign yields $-2^m\sqrt{-2} + x\sqrt{D} = \pm(A + B\sqrt{-2D})$, which cannot occur as $D > 1$ and is squarefree.

This concludes the proof, but raises the problem of determining, for a given D, whether it is the squarefree part of $\frac{1}{3}(2^{2m+1}+1)$ for one or more values of m. Firstly, we may prove without difficulty that it can never occur for more than one such value. For if D were the squarefree part of both $\frac{1}{3}(2^a+1)$ and $\frac{1}{3}(2^b+1)$ for odd $a > b$, then $(2^a+1)/(2^b+1)$ would be the square of a rational; since $(2^a+1, 2^b+1) = 2^{(a,b)}+1$, it would follow that both $(2^a+1)/(2^{(a,b)}+1)$ and $(2^b+1)/(2^{(a,b)}+1)$ would be square integers, and by [4] this cannot occur.

Secondly, we need only consider $D \equiv 3 \pmod 8$ and for every prime factor p of D, it would follow that $(-2 \mid p) = 1$, i.e., that $p \equiv 1$ or $3 \pmod 8$. Next for each such p, we determine $\sigma(p)$, the least integer with $2^\sigma \equiv -1 \pmod p$, a factor of $\frac{1}{2}(p-1)$. Then $2m+1$ must be a multiple of $\sigma(p)$, and so impossible if $\sigma(p)$ is even.

Using these results, we find that $3 = \frac{1}{3}(2^3+1)$, $11 = \frac{1}{3}(2^5+1)$, $3^2 \cdot 19 = \frac{1}{3}(2^9+1)$, and $43 = \frac{1}{3}(2^7+1)$, whereas 35 is impossible because $5 \mid 35$ and 51 is impossible since $\sigma(17) = 4$. However, 59 would appear to present greater difficulties, although here $3 \mid h$ in any case.

4. The equation $Dx^2 + 2 = y^n$ for $D < 100$

THEOREM 3. *For squarefree $D < 100$, other than 14, 30, 46, 62, 78 and 94, there are the unique solutions $x = 5$ for $D = 1$ and $x = 1$ for $D = 6$. There is the solution $x = 1$ for $D = 79$. Otherwise there are no other solutions, except possibly for $(D, n) = (53, 3)$, $(55, 3)$, $(79, 4)$, $(87, 3)$ and $(97, 5)$.*

Proof. We have excluded the values for which $D \equiv 14 \pmod{16}$, and have proved the result for $D = 1$ and 6. For the remaining values of D there are no solutions save possibly for fourteen for which the corresponding h has an odd prime factor p, leading to $Dx^2 + 2 = y^p$, and twenty-eight for which h is divisible by 4, leading to $Dx^2 + 2 = y^4$.

Of the fourteen with odd prime factors, six can be eliminated using very simple congruence arguments, as follows:

D	h of the field $\mathbb{Q}[\sqrt{-2D}]$	Only possible value of p	Impossible mod
13	6	3	13
19	6	3	19
61	10	5	61
85	12	3	9
91	12	3	7
93	12	3	9

and four other only slightly more complicated ones, which we prove below:

D	h of the field $\mathbb{Q}[\sqrt{-2D}]$	Only possible value of p
37	10	5
43	10	5
67	14	7
83	10	5

(a) $y^5 = 37x^2 + 2$ would imply $y \equiv 7 \pmod 8$ and $y \equiv 24 \pmod{37}$ but a contradiction arises from

$$37x^2 \equiv -1 \left(\bmod \frac{y-1}{2}\right)$$

whence

$$-1 = \left(37 \,\middle|\, \frac{y-1}{2}\right) = \left(\frac{y-1}{2} \,\middle|\, 37\right) = -(y-1 \mid 37) = -(23 \mid 37) = 1.$$

(b) $y^5 = 43x^2 + 2$ would imply $y \equiv 5 \pmod 8$ and $y \equiv 8 \pmod{43}$ but then

$$43x^2 \equiv -1 \left(\bmod \frac{y-1}{4}\right)$$

gives

$$1 = \left(-43 \,\middle|\, \frac{y-1}{4}\right) = \left(\frac{y-1}{4} \,\middle|\, 43\right) = (y-1 \,|\, 43) = (7 \,|\, 43) = -1,$$

which is impossible.

(c) $y^7 = 67x^2 + 2$ would imply $y \equiv 5 \pmod 8$ and $y \equiv 13 \pmod{67}$ but then

$$67x^2 \equiv -1 \left(\bmod \frac{y-1}{4}\right)$$

gives

$$1 = \left(-67 \,\middle|\, \frac{y-1}{4}\right) = \left(\frac{y-1}{4} \,\middle|\, 67\right) = (y-1 \,|\, 67) = (12 \,|\, 67) = -1,$$

which is impossible.

(d) $y^5 = 83x^2 + 2$ would imply $y \equiv 5 \pmod 8$ and $y \equiv 71 \pmod{83}$. So

$$83x^2 \equiv -3 \left(\bmod \frac{y+1}{2}\right)$$

and then

$$\left(83 \,\middle|\, \frac{y+1}{2}\right) = -\left(\frac{y+1}{2} \,\middle|\, 83\right) = -1 = \left(-3 \,\middle|\, \frac{y+1}{2}\right) = \left(\frac{y+1}{2} \,\middle|\, 3\right),$$

whence $3 \,|\, y$, which is impossible since it would imply that $x^2 \equiv -1 \pmod 3$.

The remaining four cases:

D	h of the field $\mathbb{Q}[\sqrt{-2D}]$	No solutions except perhaps if $p =$
53	6	3
55	12	3
87	12	3
97	20	5

appear to be more difficult.

Of the twenty-eight with $4 \,|\, h$, all but six, 7, 23, 31, 47, 71 and 79, can be eliminated because $v^2 - Du^2 = 2$ has no solutions. The cases $D = 7$, 23 and 71 yield no solutions, because for them $D \equiv 7 \pmod{16}$ and then $Dx^2 + 2 = y^4$ would imply $x^2 \equiv 9 \pmod{16}$, whence $x \equiv \pm 3 \pmod 8$ and then $(2 \,|\, x) = -1$.

There are no solutions for $D = 31$, for we should find from $y^4 - 31x^2 = 2$ that $y^2 + x\sqrt{31} = (39 + 7\sqrt{31})(1520 + 273\sqrt{31})^k$, whence

$$y^2 + x\sqrt{31} \equiv -(1 + \sqrt{31})(\sqrt{31})^k \pmod 8,$$

yielding $y^2 \equiv -1 \pmod 8$ if $k \equiv 0$ or $3 \pmod 4$, and

$$y^2 + x\sqrt{31} \equiv (1 + 7\sqrt{31})(7\sqrt{31})^k \pmod{19}$$

with $y^2 \equiv -1 \pmod{19}$ if $k \equiv 1$ or $2 \pmod 4$.

Similarly, there are no solutions for $D = 47$, since then

$$y^2 + x\sqrt{47} = (7 + \sqrt{47})(48 + 7\sqrt{47})^k \equiv (-1 + \sqrt{47})(-\sqrt{47})^k \pmod 8,$$

giving $y^2 \equiv -1 \pmod 8$ if $k \equiv 0$ or $3 \pmod 4$, and

$$y^2 + x\sqrt{47} = (7 + \sqrt{47})(48 + 7\sqrt{47})^k \equiv (1 + \sqrt{47})(\sqrt{47})^k \pmod 3,$$

whence $y^2 \equiv -1 \pmod 3$ if $k \equiv 1$ or $2 \pmod 4$.

Finally, for the case $D = 79$ the equation $79x^2 + 2 = y^4$ has the solution $x = 1$, and to prove that this is the only solution appears to be more difficult.

5. A curious corollary

THEOREM 4. *Let $c^2d = (2a + 1)^n - 2^{2m+1} > 0$ with d squarefree, for any integers $m \geq 0$, $n > 2$, and $a > \frac{1}{2}(2^{(2m+1)/n} - 1)$. Then the class number of the field $\mathbb{Q}[\sqrt{-2d}]$ is divisible by n except for a family of cases with $n = 3$, $m \geq 0$, $a = \frac{1}{3}(2^{2m+2} - 1)$ and the single case $n = 4$, $m = 2$, $a = 1$.*

For, the equation $dx^2 + 2^{2m+1} = y^n$ has the solution $x = c$, $y = 2a + 1$ and the exceptions are just those of the theorems above.

The author would like to express his sincere thanks to the referee for a number of valuable suggestions.

REFERENCES

[1] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. 539 (2001), 75–122.

[2] J. H. E. Cohn, *The diophantine equation $x^2 + 2^k = y^n$*, Arch. Math. (Basel) 59 (1992), 341–344.

[3] W. Ljunggren, *Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen*, Ark. Mat. Astr. Fys. 29A (1943), no. 13.

[4] —, *Noen setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$* [Some theorems on indeterminate equations of the form $(x^n - 1)/(x - 1) = y^q$], Norsk Mat. Tiddskr. 25 (1943), 17–20.

[5] —, *On an improvement of a theorem of T. Nagell concerning the Diophantine equation $Ax^3 + By^3 = C$*, Math. Scand. 1 (1953), 297–309.

[6] L. J. Mordell, *Diophantine Equations*, Academic Press, London & New York, 1969.

[7] T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Soc. Sci. Upsal. (4) 16 (1955), no. 2.

23, Highfield Gardens
London NW11 9HD, U.K.
E-mail: J.Cohn@rhul.ac.uk

Received 19 February 2003;
revised 28 May 2003 (4316)