ACTA ARITHMETICA
LXV.4 (1993)

The diophantine equation $x^2 + C = y^n$

by

J. H. E. Cohn (London)

1. Introduction. Many special cases of the equation of the title, where x and y are positive integers and $n \geq 3$, have been considered over the years, but most results for general n are of fairly recent origin. The earliest reference seems to be an assertion by Fermat that he had shown that when $C = 2$, $n = 3$, the only solution is given by $x = 5$, $y = 3$; a proof was published by Euler [14]. The first result for general n is due to V. A. Lebesgue [18] who proved that when $C = 1$ there are no solutions. Nagell [29] proved that there are no solutions for $C = 3$ and 5, but did not complete a proof for $C = 2$. Ljunggren [20] generalised Fermat's result and proved that for $C = 2$ the equation has no solution other than $x = 5$, a result rediscovered by Nagell [31], who also showed [32] that when $C = 4$ the only solutions are $x = 2$ and $x = 11$. Chao Ko [6] proved that $x = 3$ is the only solution for $C = -1$, a result which had been sought for many years as a special case of the Catalan conjecture.

It follows from [36, Theorem 12.2], itself an extension of a deep analytical result [35], that for any given C there are but finitely many solutions, which are effectively computable in the usual sense, viz., that it is possible to find them all by considering all values of x up to a bound $K(C)$ which can be explicitly calculated. In practice, the power of that method is limited by the huge size of the K that arises, but it provides a theoretical method for solving such problems.

The case in which n is even is easily treated, since then C is to be expressed as the difference of two integer squares; for n odd there is no loss of generality in considering only odd primes p, which we shall assume in what follows. We shall only consider positive values of C; in theory, much of the following applies also to the case $C < 0$, but the reason for the restriction to positive C will become evident below. It clearly suffices to find the possible values of x.

The special case $p = 3$ has received extensive treatment, and some results are known for the special cases $p = 5$ [2, 37] and $p = 7$ [3].

The method for $C = 1$, 2 and 4 consists of two parts. Firstly, using unique prime factorisation in the fields $\mathbb{Q}[\sqrt{-1}]$ and $\mathbb{Q}[\sqrt{-2}]$, it is shown that $y = a^2 + C$ for some a. Then the fundamental unit in the field $\mathbb{Q}[\sqrt{a^2+C}]$ is expressed simply in terms of a. For other values of C, even if the first step can be followed, the second cannot, and a different method is required to complete the proof. Nagell [33] found such a method for $C = 8$, and proved that there are no solutions.

As the list of references shows, there are quite a few results for general p. Many of these are not so well known, perhaps because they are published in journals which are not so readily available. There are numerous cases of duplication of known results. Thus for example the case $C = 2$, first proved by Ljunggren [20], was duplicated by Nagell [31]. For $C = 3$, the result first proved by Nagell [29] was duplicated by Brown [4], and subsequently, I am ashamed to say, by Cohn [10]. The early papers mainly use *ad hoc* methods for the special values of C considered. Ljunggren's result in [19] is incomplete as he himself points out in [21]; in particular, the case $C = 25$ remained and remains unsolved. However, a series of papers by Korhonen [15, 16, 17] deals with numerous values, and the author wishes to thank Professor Schinzel for drawing his attention to them.

This note, which attempts to be self-contained, attempts to collect together some of the known results, and to prove some new ones using some new techniques. The examples in Section 4 are expository in nature, and it is not suggested that all the results are new; Section 5 contains all the results we have managed to prove for values of C under 100, and gives complete solutions in 77 of these cases, of which more than half appear to be new. We have attempted to list the authors of previously known results, although in view of the duplication mentioned earlier inadvertent omission is quite possible.

The author wishes to thank the referee most sincerely for suggesting some improvements in the presentation of Section 2.

2. Preliminaries. The obvious starting point is to factorise the equation in the imaginary quadratic field in which $\sqrt{-C}$ lies, $(x+\sqrt{-C})(x-\sqrt{-C}) = y^p$, and then it is clear that if for integers a and b,

$$\text{(A)} \qquad \pm x + \sqrt{-C} = (a + b\sqrt{-C})^p$$

then indeed x will be a solution with $y = a^2 + b^2C$. It is not of course suggested that (A) is *necessary* for a solution; this would only be the case if

(1) $C \not\equiv 3 \pmod 4$;

(2) a question of units did not arise;

(3) the field had unique factorisation;

(4) C were square-free; and

(5) the factors $\pm x + \sqrt{-C}$ had no common factor,

but what is true in any event is that (A) is a *sufficient* condition for a solution. Since this possibility must be considered for every C, we prove some results concerning it in the next section. Before doing so, however, we consider the above questions.

Firstly, if $C \equiv 3 \pmod 4$, we obtain in addition to (A) the sufficient condition

$$\text{(B)} \qquad \pm x + \sqrt{-C} = (\tfrac{1}{2}(A + B\sqrt{-C}))^p, \qquad A \equiv B \equiv 1 \pmod 2)$$

with $y = \frac{1}{4}(A^2 + B^2 C)$. This can occur only if $p = 3$. For, equating imaginary parts in (B) yields

$$2^p = B \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} A^{p-2r-1}(-B^2C)^r ,$$

and so since B is odd, $B = \pm 1$. Thus

$$\pm 2 \equiv \pm 2^p \equiv (-C)^{(p-1)/2} \equiv (-C \,|\, p) \equiv 0, \pm 1 \pmod p ,$$

which implies that $p = 3$, and then $\pm 8 = 3A^2 - C$. Thus we have

LEMMA 1. *Case* (B) *occurs if and only if* $C = 3A^2 \pm 8$ *and gives only the solution* $p = 3$, $x = A^3 \pm 3A$.

We next consider the question of units. If $p \neq 3$, the units in the field can be absorbed into the power in (A) whatever the value of C. Even if $p = 3$, this is still usually the case, since unless $C = 3d^2$ the only units are ± 1 and possibly $\pm i$. However, if $C = 3d^2$, there are six units, ± 1, $\pm\omega$ and $\pm\omega^2$. Apart from (A) or (B), this leads to

$$\text{(C)} \qquad \pm x + d\sqrt{-3} = \omega(\tfrac{1}{2}(A + Bd\sqrt{-3}))^3, \qquad A \equiv B \pmod 2 .$$

LEMMA 2. *Case* (C) *occurs if and only if* $C = 48D^6$, $x = 4D^3$, $p = 3$.

Proof. Equating imaginary parts gives $16d = A^3 - 9AB^2d^2 - 3A^2Bd + 3B^3d^3$ and so if $r = A - Bd$, then $16d = r^3 - 12rB^2d^2 - 8B^3d^3$, whence $r = 2s$ and so $2d = s^3 - 3sB^2d^2 - B^3d^3$. Since the right hand side is to be even, both s and Bd are even, and so the right hand side is actually divisible by 8. Then with $d = 4\delta$, $s = 2\sigma$ we obtain $\delta = \sigma^3 - 12\sigma B^2\delta^2 - 8B^3\delta^3$, whence $\sigma^3 = \delta(1 + 12\sigma B^2\delta + 8B^3\delta^2)$, the factors on the right being coprime. Thus $\delta = D^3$, $\sigma = D\tau$, and $\tau^3 = 1 + 12\tau B^2D^4 + 8B^3D^6$, whence $1 = \tau^3 - 3\tau\varrho^2 - \varrho^3$ with $\varrho = 2BD^2$. It is known [28, Chap. 23, Th. 8] that this equation has just the six solutions in integers, $(\tau, \varrho) = (-3, 2)$, $(-1, 1)$, $(1, 0)$, $(0, -1)$, $(1, -3)$ and $(2, 1)$. Since $\varrho = 2BD^2$ must be even and $\tau > 0$, it follows that the only possibility is $B = 0$, $d = 4D^3$, $A = 4D$, $C = 48D^6$ and so $\pm x + 4D^3\sqrt{-3} = 8\omega D^3$, whence $x = 4D^3$, which concludes the proof.

If we were to allow $C < 0$, then the question of units would be very much more complicated, and this explains our restriction to $C > 0$.

The next question concerns the uniqueness of factorisation in the field. There are only nine imaginary quadratic fields in which this holds, so that it might be thought that our discussion was of limited application. This, however, is not the case. Consider the example $C = 6$; here the field $\mathbb{Q}[\sqrt{-6}]$ has class number $h = 2$. For any possible solution of the equation, $(x, 6) = 1$ and p is odd. Then the principal ideal π generated by $x + \sqrt{-6}$ and its conjugate π' are coprime with product $[y]^p$. Thus for some ideal ξ, $\pi = \xi^p$, but the conclusion we desire, that $x + \sqrt{-6} = (a + b\sqrt{-6})^p$, does not follow immediately from this, since ξ is not known to be principal. However, since $h = 2$, it follows that ξ^2 is principal and hence $(x + \sqrt{-6})^2$ must equal the pth power of an element in the field. Since p is odd, it then follows that $x + \sqrt{-6}$ itself is such a power. It will then follow from Lemmas 4 and 5 below that the equation has no solutions at all if $C = 6$.

The same argument can be applied in other cases; what is important is not that $h = 1$, but that $p \nmid h$. This will hold for all odd primes if h happens to be a power of 2. Even for other values of h, it will hold for all but finitely many primes, and only these have to be treated by other methods. Thus for example, for $C = 26$, $h = 6$, and so the above method applies unless $p = 3$, which must be considered separately.

Next, if C is not square-free, say $C = cd^2$ where c is square-free, then we obtain in addition to (A) also

$$\text{(D)} \qquad \pm x + d\sqrt{-c} = (a + b\sqrt{-c})^p$$

and if $c \equiv 3 \pmod 4$ also

$$\text{(E)} \qquad \pm x + d\sqrt{-c} = (\tfrac{1}{2}(A + B\sqrt{-c}))^p, \qquad A \equiv B \equiv 1 \pmod 2 .$$

Here we obtain from (D) equating imaginary parts

$$d = b \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} a^{p-2r-1}(-b^2c)^r ,$$

from which it follows that b divides d, and then

$$d/b \equiv (-b^2c)^{(p-1)/2} \equiv (-b^2c \,|\, p) \equiv 0,\ 1 \text{ or } -1 \pmod p .$$

Here $b = \pm d$ leads back to (A) and otherwise p is limited to a finite set for each such b, and there is then no difficulty is solving the resulting polynomial equations for a. Treatment of (E) is even simpler for we observe that $(\frac{1}{2}(A + B\sqrt{-c}))^p \in \mathbb{Z}[\sqrt{-c}]$ only if $c \equiv 3 \pmod 8$ and $p = 3$ and then solutions arise only for $B \,|\, d$ and $8d/B = 3A^2 - B^2c$ with $8x = |A^3 - 3AB^2c|$.

The most serious difficulties arise from possible common factors, and here no method seems to be available. Thus for example if $C = 7$, and x

is odd, the factors $\pm x + \sqrt{-7}$ are both divisible by $\frac{1}{2}(1+\sqrt{-7})$ and by $\frac{1}{2}(1-\sqrt{-7})$, which leads to great difficulties. The special case, $y = 2$, of the equation proposed by Ramanujan [34] was solved by Nagell [30] thirty five years later. It is now known as the Ramanujan–Nagell equation, and there is an excellent survey article [9] concerning it.

Possible common factors arise in one of two ways. As above, there are the prime factors of 2 in $\mathbb{Q}[\sqrt{-C}]$ if $C \equiv 7 \pmod 8$. Secondly, if $C = cd^2$ say, where c is square-free, then it sometimes happens that x shares a factor with d which splits into distinct primes in the field $\mathbb{Q}[\sqrt{-c}]$. Thus if $C = 25$, then if $5 \nmid x$ the methods outlined in Section 3 can be applied, but if $x = 5X$, $y = 5Y$ then $(X+i)(X-i) = 5^{p-2}Y^p$. Since $5 = (1+2i)(1-2i)$, this can occur; in fact, it does with $x = 10$. However, if no prime factor of d splits in $\mathbb{Q}[\sqrt{-c}]$, this cannot happen; for example if $C = 9$ we cannot have $3 \mid x$ since otherwise $x = 3X$, $y = 3Y$, and X^2+1 would be divisible by 3. It is easily seen that if q is a prime dividing (x, C) and q does not split in $\mathbb{Q}[\sqrt{-c}]$, then $p \mid \kappa$ where q^κ is the highest power of q dividing C; in particular, if C is free of prime factors which split in $\mathbb{Q}[\sqrt{-c}]$ then $(x, C) = 1$.

Summarising the above, we obtain the following

THEOREM 1. *Let $C > 0$, $C = cd^2$, c square-free, $c \not\equiv 7 \pmod 8$. If p is an odd prime and $x^2 + C = y^p$ for coprime positive integers x, y then either*

(a) *there exist integers a, b with $b \mid d$, $y = a^2 + b^2c$ and $\pm x + d\sqrt{-c} = (a + b\sqrt{-c})^p$; or*

(b) *$c \equiv 3 \pmod 8$, $p = 3$ and there exist odd integers A, B with $B \mid d$, $y = \frac{1}{4}(A^2 + B^2c), \pm x + d\sqrt{-c} = \frac{1}{8}(A + B\sqrt{-c})^3$; or*

(c) *$p \mid h$, the class number of the field $\mathbb{Q}[\sqrt{-c}]$; or*

(d) *$C = 3A^2 \pm 8$, $p = 3$, $x = A^3 \pm 3A$; or*

(e) *$C = 48D^6$, $p = 3$, $x = 4D^3$.*

3. Treatment of (A).

From (A) equating imaginary parts gives

$$1 = b \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} a^{p-2r-1}(-b^2C)^r$$

and so $b = \pm 1$. Thus

$$\pm 1 = \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} a^{p-2r-1}(-C)^r \tag{1}$$

and it is from this that the remaining conclusions will follow. It is clear from (1) that a and C must have opposite parity, for if a and C were both even then the right hand side of (1) would be even, whereas if they were both odd then we should obtain

$$\pm 1 \equiv \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} = 2^{p-1} \equiv 0 \pmod 2 .$$

Lemma 3. *Let q be any odd prime dividing a, satisfying* (1). *Then* $C^{q-1} \equiv 1 \pmod{q^2}$; *unless $p = q = 3$, $q^\alpha \,\|\, a$ implies $q^{2\alpha} \,\|(C^{q-1} - 1)$.*

Proof. From (1) we see that $(-C)^{(p-1)/2} \equiv \pm 1 \pmod{q^2}$. If now $q^\gamma \,\|(p-1)$ with $\gamma \ge 0$, let $p - 1 = Hq^\gamma$. Then every term except the last on the right of (1) is divisible by $q^{\gamma+2}$, and so $C^{p-1} \equiv 1 \pmod{q^{\gamma+2}}$, whence $C^H \equiv 1 \pmod{q^2}$. But by Fermat's theorem $C^{q-1} \equiv 1 \pmod q$ and thus if $K = (H, q-1)$ then $C^K \equiv 1 \pmod q$. But $C^H \equiv 1 \pmod{q^2}$ and since H is a multiple of K, but not of q, it follows that $C^K \equiv 1 \pmod{q^2}$. Since $q - 1$ is also a multiple of K, $C^{q-1} \equiv 1 \pmod{q^2}$.

Finally, unless $p = q = 3$ we find if $q^\alpha \,\|\, a$ that $(-C)^{(p-1)/2} \mp 1$ is divisible by $q^{2\alpha+\gamma}$ and by no higher power of q, and then repeating the above argument yields $q^{2\alpha} \,\|(C^{q-1} - 1)$ without difficulty.

Lemma 4. *The minus sign in* (1) *can occur only if* $p \equiv 3 \pmod 4$, *and the following conditions are both satisfied*:

1. *either*
   (a) $C \equiv 1$ *or* $13 \pmod{16}$, *or*

   (b) $C \equiv 0 \pmod 8$, *and* $p \equiv 7 \pmod 8$, *or*

   (c) $C \equiv 4 \pmod 8$, *and* $p \equiv 3 \pmod 8$;
2. *either*
   (a) $C \equiv 1 \pmod 9$, *or*

   (b) $C \equiv 0 \pmod 3$ *and* $p \equiv 2 \pmod 3$, *or*

   (c) $C \equiv 4$ *or* $7 \pmod 9$, *and* $p \equiv 3 \pmod 8$.

Proof. If C is odd, then a is even, and $-1 \equiv (-C)^{(p-1)/2} \pmod{a^2}$. So $C \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$. If $4 \mid a$, then $C \equiv 1 \pmod{16}$. If $2 \,\|\, a$, then we find with $p = 4k + 3$ that $\binom{p}{2} \equiv 2k + 3 \pmod 8$ and so $C^{2k+1} \equiv 1 + 4(2k+3) \pmod{16}$, whence $C \equiv 13 \pmod{16}$.

If C is even then a is odd. If $8 \mid C$ then $p \equiv 7 \pmod 8$; if $2^2 \,\|\, C$ then $p \equiv 3 \pmod 4$ and so $\binom{p}{3}$ is odd, whence $-1 \equiv p + 4 \pmod 8$, i.e. $p \equiv 3 \pmod 8$. Finally, $2 \,\|\, C$ would imply $-1 \equiv p + 2\binom{p}{3} \pmod 4$ or $p + 1 \equiv p(p-1)(p-2) \pmod 4$, which is impossible.

Next if $3 \mid a$ then $-1 \equiv (-C)^{(p-1)/2} \pmod 9$, and so $C \equiv 1 \pmod 3$ since $p \equiv 3 \pmod 4$. Then by Lemma 3, $C \equiv 1 \pmod 9$.

If $3 \nmid a$ then $a^2 \equiv 1 \pmod 3$ and $C \equiv -1 \pmod 3$ is impossible since it would imply

$$-1 \equiv \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} = 2^{p-1} \pmod 3\,;$$

$C \equiv 0 \pmod 3$ yields $-1 \equiv pa^{p-1} \equiv p \pmod 3$ and $C \equiv 1 \pmod 3$ gives $-1 \equiv \{(1+i)^p - (1-i)^p\}/(2i) \pmod 3$, which implies $p \equiv 3$ or $5 \pmod 8$, the latter of which we have already seen to be impossible. This concludes the proof.

Lemma 5. *The plus sign in* (1) *can occur only if the following conditions are both satisfied*:

1. *either*
   (a) $C \equiv 3 \pmod 4$, *or*

   (b) $C \equiv 1 \pmod 4$, $2^{2\gamma} \,\|(C-1)$ *and* $p \equiv 1 \pmod 4$, *or*

   (c) $C \equiv 2 \pmod 8$, *and* $p \equiv 3 \pmod 8$, *or*

   (d) $C \equiv 6 \pmod 8$, *and* $p \equiv 7 \pmod 8$;

2. *either*
   (a) $C \equiv 2 \pmod 3$, *or*

   (b) $C \equiv 4$ *or* $7 \pmod 9$, *and* $p \equiv 1$ *or* $7 \pmod 8$, *or*

   (c) $C \equiv 1 \pmod 9$, *and* $p \not\equiv 3 \pmod 8$, *or*

   (d) $C \equiv 21 \pmod{27}$, *and* $p \equiv 1 \pmod 3$.

Proof. If $4 \mid C$ then a is odd and $1 \equiv pa^{p-1} \equiv p \pmod 4$. Let $2^{\varrho} \,\|(p-1)$. Then

$$1 = pa^{p-1} - \binom{p}{3} Ca^{p-3} + \binom{p}{5} C^2 a^{p-5} + \ldots \equiv pa^{p-1} \pmod{2^{\varrho+1}}\,.$$

But now $1 \equiv (p-1)a^{p-1} + a^{p-1} \pmod{2^{\varrho+1}}$, and so $2^{\varrho} \,\|(a^{p-1} - 1)$, while since $2^{\varrho+2} \mid (a^{2^{\varrho}} - 1)$, $2^{\varrho+2} \mid (a^{p-1} - 1)$, which is impossible.

If $2 \,\|\, C$, then a is odd, and so

$$1 \equiv p - C\binom{p}{3} + 4\binom{p}{5} \pmod 8\,.$$

If $C \equiv 2 \pmod 8$ this gives

$$\begin{aligned} 0 &\equiv (p-1)\{1 - (p^2 - 2p)/3 + (p^2 - 2p)(p^2 - 7p + 12)/30\} \pmod 8 \\ &\equiv (p-1)\{1 + 1 - 2p + (1 - 2p)(p-3)/30\} \pmod 8 \\ &\equiv (p-1)(p-3)(1-2p)/30 \pmod 8 \end{aligned}$$

and so $p \equiv 1$ or $3 \pmod 8$. In exactly the same way we find that if $C \equiv 6 \pmod 8$, then $p \equiv 1$ or $7 \pmod 8$. However, in either case we now show that $p \equiv 1 \pmod 8$ is impossible. For if $2^\varrho \,\|\, (p-1)$ with $\varrho \geq 3$ then $2^\varrho \,\|\, Ca^{p-3}\binom{p}{3}$ and $2^\varrho \,\|\, C^2a^{p-3}\binom{p}{5}$ whereas $2^{\varrho+1}$ divides all subsequent terms. Thus again $1 \equiv pa^{p-1} \equiv (p-1)a^{p-1} + a^{p-1} \pmod{2^{\varrho+1}}$, which is impossible as before.

If $C \equiv 1 \pmod 4$ then a is even, and $1 \equiv (-C)^{(p-1)/2} \pmod 4$ yields $p \equiv 1 \pmod 4$. Suppose that $2^\varrho \,\|\, (p-1)$ where $\varrho \geq 2$, that $2^\alpha \,\|\, a$ with $\alpha > 0$ and that $C = 1 + k \cdot 2^{2\gamma+3}$ where k is odd and $\gamma \geq 0$. Then (1) would give

$$1 - (-C)^{(p-1)/2} = (-C)^{(p-3)/2}\binom{p}{2}a^2 + \ldots$$

and here the left is divisible by precisely $2^{\varrho+2\gamma+2}$ whereas the right is divisible by precisely $2^{\varrho+2\alpha-1}$, which is clearly impossible.

Next consider the equation modulo powers of 3. If $3 \mid a$ then by Lemma 3, $C^2 \equiv 1 \pmod 9$; if here $C \equiv 1 \pmod 9$, we see from (1) that $(p-1)/2$ must be even, i.e. $p \equiv 1$ or $5 \pmod 8$. Otherwise $3 \nmid a$ and $1 \equiv \sum_{r=0}^{(p-1)/2}\binom{p}{2r+1}(-C)^r \pmod 3$. If $C \equiv 1 \pmod 3$, then $1 \equiv \{(1+i)^p - (1-i)^p\}/(2i) \pmod 3$ whence $p \equiv \pm 1 \pmod 8$.

Finally, if $3 \mid C$, then $3 \nmid a$ and so $1 \equiv pa^{p-1} \pmod 3$. Thus $p \equiv 1 \pmod 3$, and so $a^{p-1} \equiv 1 \pmod 9$. Then $9 \mid C$ is impossible, since it would imply $p \equiv 1 \pmod 9$, and then if $3^\varrho \,\|\, (p-1)$ that $1 \equiv pa^{p-1} \equiv (p-1)a^{p-1} + a^{p-1} \pmod{3^{\varrho+1}}$, whence $3^\varrho \,\|\, (a^{p-1}-1)$, which is impossible. Next if $C \equiv 6 \pmod 9$, then $1 \equiv p - 6\binom{p}{3} \pmod 9$. Thus 9 divides $(p-1)\{1 - p(p-2)\} = (p-1)\{2 - (p-1)^2\}$, and so $p \equiv 1 \pmod 9$. Let $p - 1 = 3^\varrho\lambda$, where $3 \nmid \lambda$. Then $C\binom{p}{3} \equiv -3^\varrho\lambda \equiv 1 - p \pmod{3^{\varrho+1}}$ and so (1) yields

$$1 \equiv pa^{p-1} + p - 1 \equiv (p-1)(a^{p-1}+1) + a^{p-1} \pmod{3^{\varrho+1}},$$

which is impossible as before. The last case is $C \equiv 3 \pmod 9$; suppose here that $3^\varrho \,\|\, (p-1)$. Then we use an identity proved in [10],

$$\sum_{r=0}^{(p-1)/2}\binom{p}{2r+1}a^{p-2r-1}(-3)^r = 2^{p-1} + \sum_{r=2}^{(p-1)/2} A_r(a^2-1)^r$$

where for each r, A_r is divisible by $3^{\varrho+2-r}$. Inserting this into (1) we obtain

$$2^{p-1} - 1 \equiv \sum_{r=0}^{(p-1)/2}\binom{p}{2r+1}a^{p-2r-1}(-1)^{r-1}\{C^r - 3^r\} \pmod{3^{\varrho+2}}.$$

On the right hand side of this congruence, the term with $r = 0$ disappears and so $2^{p-1} - 1 \equiv \binom{p}{3}a^{p-3}(C-3) \pmod{3^{\varrho+2}}$, since as is easily seen, all the terms with $r \geq 2$ are divisible by $3^{\varrho+2}$. Now let $p - 1 = 2k \cdot 3^\varrho$ where $3 \nmid k$. Then $\binom{p}{3} \equiv -k \cdot 3^{\varrho-1} \pmod{3^\varrho}$, $(C-3)$ is divisible by 9, $a^{p-3} \equiv 1 \pmod 3$ and $2^{p-1} = (1+3)^{k \cdot 3^\varrho} \equiv 1 + k \cdot 3^{\varrho+1} \pmod{3^{\varrho+2}}$. Substituting these yields

$k \cdot 3^{\varrho+1} \equiv -k \cdot 3^{\varrho-1}(C-3) \pmod{3^{\varrho+2}}$ whence cancelling $k \cdot 3^{\varrho-1}$ yields $C \equiv 21 \pmod{27}$ as required, concluding the proof.

LEMMA 6. *Let P denote any odd prime dividing C. Then the plus sign in* (1) *implies $pa^{p-1} \equiv 1 \pmod P$, $(p \mid P) = 1$ and if $P \neq 3$ then $p \not\equiv 1$* $\pmod P$), *whereas the minus sign implies $pa^{p-1} \equiv -1 \pmod P$, $(-p \mid P) = 1$, and $p \not\equiv 1 \pmod P$.*

Proof. We have $\pm 1 \equiv pa^{p-1} \pmod P$.

Then the upper sign gives $(p \mid P) = 1$. Also if $P > 3$ and $p \equiv 1 \pmod P$, suppose that $P^\varrho \,\|\, (p-1)$; then P^ϱ divides $\binom{p}{3}$. Thus $1 \equiv pa^{p-1} \equiv (p-1)a^{p-1} + a^{p-1} \pmod{P^{\varrho+1}}$ and so $P^\varrho \,\|\, (a^{p-1}-1)$. But this is impossible since as is easily seen if $a^{p-1}-1$ is divisible by P at all, it is divisible by $P^{\varrho+1}$.

The lower sign gives $(-p \mid P) = 1$. The last part follows as above, except that the condition $P > 3$ can be eliminated in view of Lemma 4.

LEMMA 7. *In* (1), *$p = 3$ if and only if $C = 3a^2 \mp 1$, $x = 8a^3 \mp 3a$, $p = 5$ if and only if $C = 19$, $x = 22{,}434$ or $C = 341$ and $x = 2{,}759{,}646$ and $p = 7$ does not occur.*

Proof. If $p = 3$ then $\pm 1 = 3a^2 - C$, yielding $C = 3a^2 \mp 1$, $y = 4a^2 \mp 1$ and then $x = 8a^3 \mp 3a$.

The result for $p = 5$ is due to Wren [37], but a very simple proof is available. From (1) we obtain $(C - 5a^2)^2 = 20a^4 \pm 1$. The lower sign is impossible, and it is shown in [13] that the upper sign occurs only for $a = 6$, yielding the result.

The result for $p = 7$ is due to Blass and Steiner [3].

Although the results proved to date are useful, only occasionally, e.g. if $C = 6$, do they suffice to dismiss both cases of (1). We now consider how we might treat other cases. As will be seen, a fair amount of computation is often involved, and there seems no *a priori* guarantee of success in any particular example. Nevertheless, the technique does seem to work with sufficient perseverence.

Define for integers a and $m \geq 0$ the integer function

$$f_m(a) = \frac{(a+\sqrt{-C})^m - (a-\sqrt{-C})^m}{2\sqrt{-C}}. \tag{2}$$

Then (1) takes the form $f_p(a) = \pm 1$. We consider one odd prime q not dividing C at a time, and shall attempt to locate any possible solutions or to prove that there are none, by showing (2) to be impossible modulo q for some values of p not already excluded by one of the lemmas above. We first observe that as a function of m, the sequence $\{f_m(a)\}$ is periodic modulo q, the period being a factor of Q where $Q = q-1$ or q^2-1 according as

$(-C \mid q) = 1$ or -1. For,

$$(a+\sqrt{-C})^q \equiv a^q + (-C)^{(q-1)/2}\sqrt{-C} \equiv a + (-C \mid q)\sqrt{-C} \pmod q,$$

and similarly for the complex conjugate; if $(-C \mid q) = -1$ then repeating the process gives $(a+\sqrt{-C})^{q^2} \equiv (a-\sqrt{-C})^q \equiv (a+\sqrt{-C}) \pmod q$, and so $f_{m+Q}(a) \equiv f_m(a) \pmod q$ in either case.

From (2) we see that $f_0(a) = 0$, $f_1(a) = 1$ and for $m \geq 0$,

$$f_{m+2}(a) = 2af_{m+1}(a) - (a^2 + C)f_m(a) \tag{3}$$

and so as a function of a, $f_m(a)$ is a polynomial and contains only even powers of a if m is odd. Thus to solve $f_p(a) \equiv \pm 1 \pmod q$ it suffices to consider only $p \equiv m \pmod Q$ with $1 \leq m \leq Q-1$ and values of a satisfying $0 \leq a < q/2$. Using Lemma 3, the value $a = 0$ can be excluded, provided we check that $q^2 \nmid (C^{q-1} - 1)$. It is a routine computation to check that this does not occur for any of the primes q we wish to use. Of course, this condition is occasionally violated, and in such cases we have to select other primes q.

The procedure therefore is as follows. For a given C, we select some odd primes $q \nmid C$ such that Lemma 3 ensures that $q \nmid a$. For each one of these, we calculate the residue of $f_m(a)$ modulo q using (3) for each a in the range $1 \leq a < q/2$ and each odd m in the range $1 \leq m \leq Q-1$. In this way, we compile a list of all those m in the range for which the congruence can hold for *any* a, and so prove a result which forces p to belong to one of a set of residue classes modulo Q. From this list we may delete any possible residue which would prevent p being a prime; thus the value 15 can be removed from the list if $Q = 66$. All this is easily automated. The object of the exercise is to find sufficiently many such congruence conditions, together with any information available from Lemmas 4 or 5 to complete a proof. It may appear surprising that this should *ever* work, but it often does.

In the case of the plus sign in (1), it might be objected that the above method can never succeed, for since $f_1(a) = 1$, it follows that the possibility $p \equiv 1 \pmod Q$ can never be excluded by the reasoning of the previous paragraph, and accordingly, unless $p \equiv 1 \pmod 4$ be excluded by Lemma 5, no matter for how many different primes q the method be repeated, all that will be achieved will be to show that $p-1$ must have a very large number of different factors. However, if C has any prime factor $P \geq 5$, then choosing some suitable q with P dividing Q, there remains the prospect of proving that $p \equiv 1 \pmod P$, and this is excluded by Lemma 6. This can sometimes be done directly; sometimes, for example if $C = 21$, the plus sign can be eliminated by proving that $p-1$ is divisible by $P-1$, where P is a prime exceeding 3 which divides C and the conclusion then follows by Lemma 6; occasionally, for example if $C = 17$, a combination of these two ideas is required. A few examples may make all this much clearer. The plus sign in cases in which C has only prime factors 2 or 3 does not arise in view of Lemma 5.

4. Some examples

Result 1. *There are no solutions when $C = 6$.*

For, in this case there are no solutions with n even, since 6 is not the difference of two squares. So $n = p$, and $(x, 6) = 1$. The principal ideals generated by $\pm x + \sqrt{-6}$ are coprime, and since the class number of the field is 2, it follows that we need only consider (A). But now by Lemmas 4 and 5, both signs are impossible.

Result 2. *There are no solutions when $C = 5$.*

Again, we see without difficulty that we cannot have n even, and as again $h = 2$, we obtain only (A). This time the minus sign in (1) is again excluded by Lemma 4, but with the plus sign, the only information provided by Lemma 5 is $p \equiv 1 \pmod 4$. Then by Lemma 6, $(p \mid 5) = 1$, $p \not\equiv 1 \pmod 5$ gives $p \equiv 4 \pmod 5$ and combining these yields $p \equiv 9 \pmod{20}$.

Now consider $q = 61$ and 601 in turn, for each of which it is easily seen that $5^{q-1} \not\equiv 1 \pmod{q^2}$, for $5^{60} \equiv 1 + 38 \cdot 61 \pmod{61^2}$ and $5^{600} \equiv 1 + 405 \cdot 601 \pmod{601^2}$. Since $(-5 \mid 61) = 1$ we obtain $Q = 60$ and find only $p \equiv 49 \pmod{60}$, and in particular $p \equiv 1 \pmod 3$. Then with $q = 601$, we obtain $Q = 600$ and we find that modulo Q all the possible residues have $p \equiv 2 \pmod 3$ which is impossible.

Result 3. *When $C = 11$, the only solutions are $x = 4$ or 58.*

Again, n cannot be even. Here $h = 1$, and we obtain case (A) or case (B), the latter of which gives just $x = 4$, by Lemma 1. By Lemma 4, the minus sign does not occur, but Lemma 5 gives no information about (1) with the plus sign. By Lemma 7, when $p = 3$ we get just one more solution $x = 58$, and so we may assume that $p \geq 5$. By Lemma 3, we then find that none of the primes $q = 23,\ 67,\ 89$ or 397 divides a, since a calculation reveals the residues of 11^{q-1} modulo q^2 to be respectively $1 + 7q$, $1 + 43q$, $1 + 72q$ and $1 + 82q$. We then apply the procedure outlined above, and obtain from $q = 23$, $p \equiv 3$ or $15 \pmod{22}$. Using this with results from $q = 67$ then gives $p \equiv 25$ or $37 \pmod{66}$, since we can now reject $p \equiv 3 \pmod{66}$. Similarly, from $q = 89$ we obtain $p \equiv 3,\ 15,\ 47$ or $59 \pmod{88}$, and so certainly $p \equiv 3 \pmod 4$. But the result from $q = 397$ taken together with the one modulo 66 then gives $p \equiv 37$ or $289 \pmod{396}$ each of which implies $p \equiv 1 \pmod 4$, and so there is no further solution.

It may be observed that this result generalizes [8] which proves that $x = 4$ is the sole solution of $x^2 + 11 = 3^n$.

Result 4. *There are no solutions when* $C = 21$.

Here if n were even, $y^{n/2} = (21+1)/2$ or $(7+3)/2$ neither of which gives a solution. Thus assume $n = p$. Since $h = 4$, we need only consider case (A). Then the minus sign is impossible by Lemma 4, and for the plus sign Lemma 5 yields both $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$. Thus $p \equiv 1 \pmod 6$, and this is impossible by Lemma 6 with $P = 7$.

Result 5. *When* $C = 17$, *the only solution is* $x = 8$.

Here we find for n even $y^{n/2} = 9$, yielding the solution $x = 8$. For n odd we need only consider (A) since $h = 4$, and exclude the minus sign by Lemma 4. By Lemma 5, the plus sign would imply $p \equiv 1 \pmod 4$, and then by Lemma 6, p must be a quartic residue, but not $\equiv 1 \pmod{17}$. Thus $p \equiv -1,\ 4$, or $-4 \pmod{17}$.

Now with $q = 7,\ 137$ and 409 we obtain respectively $Q = 6,\ 136$ and 408 and in each case $q \nmid a$ by Lemma 3. Then we obtain $p \equiv 1 \pmod 6$ from $q = 7$, and $p \equiv 101 \pmod{136}$ using $p \equiv -1,\ 4$ or $-4 \pmod{17}$ from $q = 137$. Finally, using $q = 409$ and all the above congruences, we find no possible residue modulo 408.

Result 6. *When* $C = 40$, *the only solution is* $x = 52$.

Here we find no solution for n even. Suppose first that x is odd. Then since $h = 2$, we have $\pm x + 2\sqrt{-10} = (a + b\sqrt{-10})^p$, as in (D), where a must be odd. But now

$$2 = b \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} a^{p-2r-1}(-10b^2)^r$$

and since the second factor is odd, $b = \pm 2$. Thus we arrive at (1), and now both sings can be eliminated by Lemmas 4 and 5. It follows therefore that x must be even. Then $2 \parallel x$ is impossible since it would imply $2^2 \parallel y^p$ and if $4 \mid x$ then $2^3 \parallel y^p$, whence $p = 3$. We then obtain only $x = 52$ as in [33].

5. Statement of results. We have considered in detail all values of $C \le 100$, and have completed the solution for 77 of these values, quoting the known results for $p = 3$ [7] in a few cases, as follows:

There are no solutions at all for 46 values of C, viz.: 1, 3, 5, 6, 8, 9, 10, 14, 21, 22, 24, 27, 29, 30, 33, 34, 36, 37, 38, 41, 42, 43, 46, 50, 51, 52, 57, 58, 59, 62, 66, 68, 69, 70, 73, 75, 78, 82, 84, 85, 88, 90, 91, 93, 94, and 98.

For the following 31 values of C, the only solutions for x are:

C	x	C	x	C	x	C	x
2	5	20	14	53	26, 156	77	2
4	2, 11	26	1, 207	54	17	80	1
11	4, 58	32	7, 88	56	5, 76	81	46
12	2	35	36	61	8	83	140
13	70	40	52	64	8	89	6
16	4	44	9	65	4	96	23
17	8	48	4, 148	67	110	97	48
19	18, 22434	49	24, 524	76	7, 1015		

Two values $C = 74$ and 86 for which the class number is divisible by 5 may have other solutions with $p = 5$ but none with $p \neq 5$, apart from the known solutions $x = 13, 985$ when $C = 74$.

The remaining 21 cases seem to be very difficult indeed because the ideals $\pi = [x + \sqrt{-C}]$ and π' can have common factors; these values are the twelve for which $C \equiv 7 \pmod 8$ and nine others, viz., 18, 25, 28, 45, 60, 72, 92, 99 and 100. In some cases there are partial results which avoid the difficulties, e.g. that there are no solutions with x even if $C = 7$, nor with x odd if $C = 28$.

As mentioned in Section 1, by no means all of the above results are new. We are aware of previous results, explicit or implicit, for each of the following 33 values of C for which a complete solution, in some cases in conjunction with [7], has been obtained previously, although in the case of $C = 40$, the solution $x = 52$ is inadvertently omitted. We hope that the list is complete and that in each case the reference is to the first such solution:

1	[14]	14	[16]	56	[15]
2	[20]	19	[11]	57	[21]
3	[29]	20	[1]	58	[16]
4	[32]	21	[22]	73	[21]
5	[29]	32	[12]	76	[1]
6	[16]	33	[21]	78	[16]
8	[33]	34	[16]	82	[16]
9	[19]	40	[15]	88	[15]
10	[16]	41	[21]	89	[21]
12	[26]	42	[16]	94	[16]
13	[22]	44	[1]	97	[21]

6. Conclusion. As indicated, there are a number of open questions, principally that of dealing with the difficult cases, exemplified by $C = 7$. The author would like to throw out a challenge to prove the

Conjecture. *The equation* $x^2 + 7 = y^n$ *has only the solutions given by* $x = 1, 3, 5, 11$ *and* 181.

or, if it be false, to solve it completely. What is known about this equation is that there are no other solutions if y is odd [25], nor if n is even nor if $3 \mid n$ [24] nor if y is a power of 2 [30].

Secondly, it would be of interest to complete the solution for the values 74 and 86. These may be considerably less difficult questions.

Finally, Lemma 7 leads to a rather peculiar result, capable of various extensions, but which we state in its simplest form as

Theorem 2. *For any positive integers* A, B *with* A *odd*, *with* $C = A^7 - B^2$ *positive and square-free*, *the class number of the imaginary quadratic field* $\mathbb{Q}[\sqrt{-C}]$ *is divisible by* 7.

A similar result applies with 7 *replaced by* 5 *throughout with two exceptions* $C = 19$ *and* 341, *and with* 7 *replaced by* 3 *if we exclude the cases in which* $C \pm 1$ *or* $C \pm 8$ *is of the form* $3a^2$.

References

[1] A. Aigner, *Die diophantische Gleichung* $x^2 + 4D = y^p$ *im Zusammenhang mit Klassenzahlen*, Monatsh. Math. 72 (1968), 1–5.

[2] J. Blass, *A note on diophantine equation* $Y^2 + k = X^5$, Math. Comp. 30 (1976), 638–640.

[3] J. Blass and R. Steiner, *On the equation* $y^2 + k = x^7$, Utilitas Math. 13 (1978), 293–297.

[4] E. Brown, *Diophantine equations of the form* $x^2 + D = y^n$, J. Reine Angew. Math. 274/275 (1975), 385–389.

[5] —, *Diophantine equations of the form* $ax^2 + Db^2 = y^p$, ibid. 291 (1977), 118–127.

[6] K. Chao, *On the diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica (Notes) 14 (1964), 457–460.

[7] F. B. Coghlan and N. M. Stephens, *The diophantine equation* $x^3 - y^2 = k$, in: Computers in Number Theory, Academic Press, London, 1971, 199–205.

[8] E. L. Cohen, *Sur l'équation diophantienne* $x^2 + 11 = 3^k$, C. R. Acad. Sci. Paris Sér. A 275 (1972), 5–7.

[9] —, *On the Ramanujan–Nagell equation and its generalizations*, in: Proc. First Conference of the Canadian Number Theory Association, Banff, Alberta, 1988, de Gruyter, 1990, 81–92.

[10] J. H. E. Cohn, *The Diophantine equation* $x^2 + 3 = y^n$, Glasgow Math. J. 35 (1993), 203–206.

[11] —, *The diophantine equation* $x^2 + 19 = y^n$, Acta Arith. 61 (1992), 193–197.

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

[13] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. 7 (1965), 24–28.

[14] L. Euler, *Algebra*, Vol. 2.

[15] O. Korhonen, *On the Diophantine equation $Ax^2 + 8B = y^n$*, Acta Univ. Oulu. Ser. A Sci. Rerum Natur. Math. 16 (1979).

[16] —, *On the Diophantine equation $Ax^2 + 2B = y^n$*, ibid. 17 (1979).

[17] —, *On the Diophantine equation $Cx^2 + D = y^n$*, ibid. 25 (1981).

[18] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$*, Nouvelles Annales des Mathématiques (1) 9 (1850), 178–181.

[19] W. Ljunggren, *On the diophantine equation $x^2 + p^2 = y^n$*, Norske Vid. Selsk. Forh. Trondheim 16 (8) (1943), 27–30.

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

[21] —, *On the diophantine equation $x^2 + D = y^n$*, Norske Vid. Selsk. Forh. Trondheim 17 (23) (1944), 93–96.

[22] —, *On a diophantine equation*, ibid. 18 (32) (1945), 125–128.

[23] —, *New theorems concerning the diophantine equation $Cx^2 + D = y^n$*, ibid. 29 (1) (1956), 1–4.

[24] —, *On the diophantine equation $y^2 - k = x^3$*, Acta Arith. 8 (1963), 451–463.

[25] —, *On the diophantine equation $Cx^2+D = y^n$*, Pacific J. Math. 14 (1964), 585–596.

[26] —, *On the diophantine equation $Cx^2 + D = 2y^n$*, Math. Scand. 18 (1966), 69–86.

[27] —, *New theorems concerning the diophantine equation $x^2 + D = 4y^q$*, Acta Arith. 21 (1972), 183–191.

[28] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.

[29] T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk. Mat. Forensings Skrifter No. 13 (1923), 65–82.

[30] —, *Løsning til oppgave nr 2, 1943, s. 29*, Norske Mat. Tidsskrift 30 (1948), 62–64.

[31] —, *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. (Basel) 5 (1954), 153–159.

[32] —, *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*, Nova Acta Regiae Soc. Sci. Upsaliensis (4) 16 (2) (1955).

[33] —, *On the Diophantine equation $x^2 + 8D = y^n$*, Ark. Mat. 3 (1954), 103–112.

[34] S. Ramanujan, *Question 464*, J. Indian Math. Soc. 5 (1913), 120.

[35] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, *Applications of the Gel'fond–Baker method to diophantine equations*, in: Transcendence Theory: Advances and Applications, Academic Press, London, 1977, 59–77.

[36] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.

[37] B. M. E. Wren, $y^2 + D = x^5$, Eureka 36 (1973), 37–38.

DEPARTMENT OF MATHEMATICS
ROYAL HOLLOWAY AND BEDFORD NEW COLLEGE
EGHAM, SURREY TW20 OEX, ENGLAND
E-mail: UHAH206@UK.AC.RHBNC

Received on 27.11.1992
and in revised form on 25.6.1993 (2347)