ACTA ARITHMETICA
LXI.2 (1992)

The diophantine equation $x^2 + 19 = y^n$

by

J. H. E. Cohn (London)

We prove that the equation of the title has only the solutions $x = 18$, $y = 7$, $n = 3$ and $x = 22434$, $y = 55$, $n = 5$ in positive integers x, y and $n \geq 3$.

Results are known for certain *fixed* values of n. Thus the impossibility of other solutions when $n = 3$ is classical, when $n = 5$ was proved in [1] and [3] and when $n = 7$ in [2]. The case n even is easily dismissed, since then 19 is to be expressed as the difference of two integer squares; this would imply $x = 9$, giving no solution with $n \geq 3$. Thus there is no loss of generality in considering only $n = p$, an odd prime. For x odd, $x^2+19 \equiv 4 \pmod 8$, yielding no solution. Thus x is even, y odd and

$$(x + \sqrt{-19})(x - \sqrt{-19}) = y^p\,,$$

where in the field $\mathbb{Q}[\sqrt{-19}]$ with unique prime factorisation the factors on the left hand side have no common factor. Thus for some rational integers A and B with the same parity

$$x + \sqrt{-19} = (\tfrac{1}{2}(A + B\sqrt{-19}))^p \quad \text{and} \quad y = \tfrac{1}{4}(A^2 + 19B^2)\,,$$

since the only units of the field, ± 1, can be absorbed into the power. Thus

$$2^p = B \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} A^{p-2r-1}(-19B^2)^r\,.$$

If B is odd, then $B = \pm 1$, and then modulo p, we find

$$2 \equiv 2^p \equiv B(-19B^2)^{(p-1)/2} \equiv B\,(-19\,|\,p) \pmod p\,,$$

which is impossible unless $p = 3$. This then gives $8 = B(3A^2 - 19B^2)$, whence $A = 3$, $B = 1$ and then $x = 18$, $y = 7$, $n = 3$.

Otherwise, A and B are both even, and substituting $A = 2a$, $B = 2b$

gives

$$1 = b \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} a^{p-2r-1}(-19b^2)^r ,$$

and so $b = \pm 1$, $y = a^2 + 19$. Since y is odd, a is even and

$$\pm 1 = \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} a^{p-2r-1}(-19)^r ,$$

and we may reject the lower sign modulo 4. Hence

$$1 = \sum_{r=0}^{(p-1)/2} \binom{p}{2r+1} a^{p-2r-1}(-19)^r . \tag{1}$$

Lemma 1. *Let q be any odd prime dividing a, satisfying* (1). *Then*

$$19^{q-1} \equiv 1 \pmod{q^2} .$$

Proof. From (1) we see that $(-19)^{(p-1)/2} \equiv 1 \pmod{q^2}$, and in particular $q \neq 19$. If now $q^\gamma \parallel (p-1)$ with $\gamma \geq 0$, then every term except the last on the right of (1) is divisible by $q^{\gamma+2}$, and so $q^{\gamma+2}$ divides $19^{p-1} - 1$. Let $p - 1 = Hq^\gamma$. Then $19^{Hq^\gamma} \equiv 1 \pmod{q^{\gamma+2}}$, which implies $19^H \equiv 1 \pmod{q^2}$. But by Fermat's Theorem, $19^{q-1} \equiv 1 \pmod{q}$ and then if $K = (H, q-1)$, $19^K \equiv 1 \pmod{q}$. But $19^H \equiv 1 \pmod{q^2}$ and as H is a multiple of K, but not of q, it follows that $19^K \equiv 1 \pmod{q^2}$. Since $q-1$ is a multiple of K, the result follows.

A simple calculation shows that the only primes under 30000 which satisfy the condition of the lemma are 3, 7, 13 and 43. In particular, none of the primes 191, 229, 457 and 761 can divide a for any solution of (1).

Lemma 2. *For any solution of* (1), $(p \mid 19) = 1$, $p \not\equiv 1 \pmod{19}$.

Proof. From (1), $pa^{p-1} \equiv 1 \pmod{19}$, and so p is certainly a quadratic residue modulo 19. Now suppose that $19^\varrho \parallel (p-1)$, say $p - 1 = 19^\varrho H$. Then (1) gives

$$1 \equiv pa^{p-1} \equiv (p-1)a^{p-1} + a^{p-1} \pmod{19^{\varrho+1}}$$

and the first term on the right is divisible by precisely 19^ϱ, and so $19^\varrho \parallel (a^{p-1} - 1)$. But this is impossible, since unless $a^H - 1$ is divisible by 19 neither is $a^{p-1} - 1$, and if it is then $p^{\varrho+1} \mid (a^{p-1} - 1)$.

Lemma 3. *For any solution of* (1), $2 \parallel a$ *and* $p \equiv 5 \pmod{8}$.

Proof. We have already seen that a must be even. Suppose if possible that $4 \mid a$. Then (1) would imply $(-19)^{(p-1)/2} \equiv 1 \pmod{16}$, whence $8 \mid (p-1)$. Suppose that $2^\alpha \parallel a$ and $2^\beta \parallel (p-1)$ where $\alpha \geq 2$ and $\beta \geq 3$.

Then

$$(2)\quad -(-19)^{(p-1)/2} + 1 = a^2(-19)^{(p-3)/2}\binom{p}{2} + a^4(-19)^{(p-5)/2}\binom{p}{4} + \ldots$$

Now on the right hand side, every term is divisible by $2^{\beta+3}$. However, $19^2 \equiv 1 + 8 \pmod{16}$ and we find easily by induction that

$$19^{2^{\beta-1}} \equiv 1 + 2^{\beta+1} \pmod{2^{\beta+2}},$$

and so $2^{\beta+1}$ and no higher power of 2 divides the left hand side. Thus $2 \parallel a$. Then $p \equiv 1 \pmod 4$, otherwise $(p-1)/2$ is odd, and $a^2 \equiv 4 \pmod{16}$ whence from (1),

$$1 \equiv -19^{(p-1)/2} + 4\binom{p}{2} \pmod{16},$$

and it is easily seen that whether $p \equiv 3$ or $7 \pmod 8$, the right hand side is congruent to 9 modulo 16.

Now suppose that $p \equiv 1 \pmod 8$; then in the above $\beta \geq 3$. Now $19^4 \equiv 1 + 2^4 \pmod{2^7}$ and we find easily by induction that for $\sigma \geq 2$, $19^{2^\sigma} \equiv 1 + 2^{\sigma+2} \pmod{2^{\sigma+5}}$. Hence we find (where $p - 1 = 2^\beta \cdot k$)

$$\begin{aligned}
(-19)^{(p-1)/2} &\equiv (1 + 2^{\beta+1})^k \equiv 1 + k \cdot 2^{\beta+1} \pmod{2^{\beta+4}}, \\
a^2(-19)^{(p-3)/2}\binom{p}{2} &= 2^{\beta+1}k(2^\beta k + 1)(a/2)^2(-19)^{(p-3)/2} \\
&\equiv -3k \cdot 2^{\beta+1} \pmod{2^{\beta+4}}, \\
a^4(-19)^{(p-5)/2}\binom{p}{4} &= \tfrac{1}{3}2^{\beta+2}k(2^{2\beta}k^2 - 1)(2^{\beta-1}k - 1)(a/2)^4(-19)^{(p-5)/2} \\
&\equiv -k \cdot 2^{\beta+2} \pmod{2^{\beta+4}}
\end{aligned}$$

and all the other terms on the right hand side of (2) are multiples of $2^{\beta+4}$. Thus substituting into (2) gives

$$-k \cdot 2^{\beta+1} \equiv -3k \cdot 2^{\beta+1} - k \cdot 2^{\beta+2} \equiv -5k \cdot 2^{\beta+1} \pmod{2^{\beta+4}},$$

which is impossible. This concludes the proof.

Next for $p = 5$ we find $1 = 5a^4 - 190a^2 + 361$ yielding only $a = 6$, whence $x = 22434$, $y = 55$ and $n = 5$. We now complete the proof that there are no solutions when $p \neq 5$. Define the function

$$(3)\qquad f_m(a) = \frac{(a + \sqrt{-19})^m - (a - \sqrt{-19})^m}{2\sqrt{-19}}.$$

Then (1) takes the form $f_p(a) = 1$ and we shall show that this cannot occur, by showing it to be impossible modulo q for at least one prime q for any particular a and p not already excluded by one of the lemmas above. If

$q \equiv 1 \pmod{19}$ is a prime we find modulo q that

$$f_{m+q}(a) \equiv f_{m+1}(a)\,, \qquad \text{for } (-19)^{(q-1)/2} \equiv (-19 \mid q) = (q \mid 19) = +1$$

and so

$$(a+\sqrt{-19})^q \equiv a^q + (-19)^{(q-1)/2}\sqrt{-19} \equiv a+\sqrt{-19}\,,$$

and similarly for the complex conjugate. Thus for fixed a, the sequence $\{f_m(a)\}$ is periodic modulo q with period $q-1$ or a factor thereof. Also since $f_m(-a) = f_m(a)$ for odd m and since $f_m(a+q) \equiv f_m(a) \pmod{q}$, in deciding whether $f_m(a) \equiv 1 \pmod{q}$ is possible, it suffices to consider only odd values of m in the range 1 to $q-2$ and values of a satisfying $0 \le a \le (q-1)/2$. In addition, if q is one of the primes which is known not to divide a by virtue of the corollary to Lemma 1, we may exclude $a = 0$. This finite set $\{f_m(a)\}$ of residues is most easily calculated from $f_0(a) = 0$, $f_1(a) = 1$ and the recurrence relation

$$f_{m+2}(a) = 2af_{m+1}(a) - (a^2+19)f_m(a)$$

all of which follow from (3). For each such q, this gives a list of possible residues $\{m\}$ modulo $(q-1)$ for p. From this list we may delete any possible residue which would prevent p being a prime > 3. It will be obvious that $m = 1$ always appears in the list, since $f_1(a) = 1$, but if $q \equiv 1 \pmod{19}$, in view of Lemma 2, this and any other $m \equiv 1 \pmod{19}$ can also be deleted. Again $m = 5$ will always appear, since 5 is a solution, but whenever $5 \mid (q-1)$ we can remove any other multiples of 5. Using the fact that $p \equiv 5 \pmod{8}$ we find the following results from the primes mentioned above:

q	modulo	p is congruent to one of:
191	760	5, 61, 149, 197, 277, 309, 397, 453, 461, 541, 557, 653, 669, 693, 701, 709 or 733
229	456	5, 61, 101, 149, 157, 277, 349 or 365
457	456	5, 61, 85, 125, 157, 197, 365 or 397
761	760	5, 93, 157, 197, 213, 237, 277, 349, 429, 501, 517, 541, 581, 613, 653, 701 or 733.

Combining the results from 229 and 457, we find that we must have $p \equiv 5$, 61, 157 or 365 $\pmod{456}$, and so in particular $p \equiv 4$ or $5 \pmod{19}$. From the other two we find that $p \equiv 5$, 197, 277, 541, 653, 701 or 733 $\pmod{760}$, and of these $p \equiv 5 \pmod{760}$ is the only one which also satisfies $p \equiv 4$ or $5 \pmod{19}$. But the only prime which satisfies $p \equiv 5 \pmod{760}$ is $p = 5$, which concludes the proof.

References

[1] J. Blass, *A note on Diophantine equation* $Y^2 + k = X^5$, Math. Comp. 30 (1976), 638–640.
[2] J. Blass and R. Steiner, *On the equation* $y^2 + k = x^7$, Utilitas Math. 13 (1978), 293–297.
[3] 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 0EX, ENGLAND
E-mail: UHAH206@UK.AC.RHBNC.VAX

Received on 17.6.1991
and in revised form on 15.10.1991 (2149)