PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 1, Pages 13–15
S 0002-9939(02)06732-1
Article electronically published on August 19, 2002

THE DIOPHANTINE EQUATION $x^p + 1 = py^2$

J. H. E. COHN

(Communicated by David E. Rohrlich)

ABSTRACT. Cao has recently proved that, subject to a certain condition on the odd prime p, the equation $x^p+1 = py^2$ has no solutions in positive integers x and y, provided also that $p \equiv 1 \pmod 4$. It is the object of this note to remove this restriction, and to provide a simple self-contained proof.

The condition referred to in the abstract is:

Condition A. An odd prime p is said to satisfy Condition A if $p \nmid u$ where $\frac{1}{2}(v + u\sqrt{p})$ is the fundamental unit in the field $Q[\sqrt{p}]$.

Here u and v have like parity, and this must be even if $p \equiv 3 \pmod 4$. The condition can be expressed in terms of the Bernoulli coefficients if $p \equiv 1 \pmod 4$ as was done in [1], or the Euler coefficients if $p \equiv 3 \pmod 4$. It is conjectured that Condition A holds for all primes p, and it has recently [2] been verified for all $p < 10^{11}$.

We prove

Theorem 1. *The equation $x^p + 1 = py^2$ has no solution in positive integers x and y for any odd prime p satisfying Condition A,*

which generalises the main result of [1] which required also that $p \equiv 1 \pmod 4$.

Lemma. *For each positive integer $x \equiv 0 \pmod 4$ and each pair of relatively prime odd positive integers r and s, $(\frac{x^r+1}{x+1}|\frac{x^s+1}{x+1}) = 1$, where here and elsewhere $(a|b)$ denotes the Legendre-Jacobi symbol.*

Proof of the Lemma. Fix $x \equiv 0 \pmod 4$ and let $f(r,s) = (\frac{x^r+1}{x+1}|\frac{x^s+1}{x+1})$. We use induction on the quantity $r+s$, the result being trivial if $r+s = 2$. Let $r+s = k$, and suppose the result holds for all values of $r+s < k$. For all n, $\frac{x^n+1}{x+1} \equiv 1 \pmod 4$ and so there is no loss of generality in assuming that $r > s$. Now if $r > 2s$, the identity $x^r + 1 = x^{r-2s}(x^{2s} - 1) + (x^{r-2s} + 1)$ yields $f(r,s) = f(r-2s, s)$, whereas if $2s > r > s$, then $x^r(x^{2s-r} + 1) - (x^r + 1) = (x^{2s} - 1)$ gives $f(r,s) = f(2s-r, s)(x|\frac{x^s+1}{x+1})$ and, since $4|x$, $(x|\frac{x^s+1}{x+1}) = (x|x^{s-1} - x^{s-2} + \ldots - x + 1) = (x|1) = 1$, completing the induction.

Proof of Theorem 1. From the equation we obtain $x + 1 \equiv 0 \pmod p$, and so $p\|\frac{x^p+1}{x+1}$. Thus we must have $x + 1 = p^2y_1^2$, $\frac{x^p+1}{x+1} = py_2^2$ with $y = py_1y_2$. We now

Received by the editors July 13, 2001.
2000 *Mathematics Subject Classification.* Primary 11D61.

see that x even is impossible for the former would then imply that $8|x$ and then for any odd r not divisible by p the lemma would give

$$1 = \left(\frac{x^p+1}{x+1}\middle|\frac{x^r+1}{x+1}\right) = \left(py_2^2\middle|\frac{x^r+1}{x+1}\right) = (x^{r-1}-x^{r-2}+\ldots-x+1|p) = (r|p),$$

and this is impossible on taking r to be an odd quadratic non-residue modulo p.

So now suppose that x is odd, and hence that y is even. Then factorising in the field $Q[\sqrt{p}]$ we obtain $(-x)^p = (1+y\sqrt{p})(1-y\sqrt{p})$ where the principal ideals $[1+y\sqrt{p}]$ and $[1-y\sqrt{p}]$ are coprime. Thus $[1+y\sqrt{p}] = \pi^p$ for some ideal π. Let h denote the class number of the field. Then $h < p$ and so $(h,p) = 1$. Since π^h is a principal ideal, it then follows that $1+y\sqrt{p}$ is an associate of the pth power of an element of the field. Thus without loss of generality $1+y\sqrt{p} = (\frac{v+u\sqrt{p}}{2})^r(\frac{a+b\sqrt{p}}{2})^p$ for some integers $a = b \pmod 2$ and $0 \le r < p$. Of course in the case that $p \equiv 3 \pmod 4$, all of u, v, a and b will be even, but in any case we obtain $2^{r+p}(1+y\sqrt{p}) = (v+u\sqrt{p})^r(a+b\sqrt{p})^p$ and then, since $p|y$, $2^{r+p} \equiv v^{r-1}(v+ru\sqrt{p})a^p \pmod p$. In particular we must have $p|v^{r-1}rua^p$. But p cannot divide u by hypothesis, nor a, since $(-x)^p = (1+y\sqrt{p})(1-y\sqrt{p}) = \pm(\frac{a^2-pb^2}{4})^p$, and x is not divisible by p nor v since $v^2 - pu^2 = \pm 4$. Hence $p|r$ which implies $r = 0$.

Thus $1+y\sqrt{p} = (\frac{a+b\sqrt{p}}{2})^p$. We show first that a and b cannot both be odd, for then taking rational parts would give $2^p = a\sum_{i=0}^{(p-1)/2}\binom{p}{2i}a^{p-2r-1}b^{2r}p^r$ whence $a = 1$ and then

$$2^{p+1} = 2\sum_{i=0}^{(p-1)/2}\binom{p}{2i}b^{2r}p^r \ge (1+\sqrt{5})^p + (1-\sqrt{5})^p$$

which would imply that $2 > (\frac{1+\sqrt{5}}{2})^p - 1$, which is impossible. So with $a = 2A$, $b = 2B$, $1+y\sqrt{p} = (A+B\sqrt{p})^p$, and then taking rational parts gives

$$1 = A\sum_{i=0}^{(p-1)/2}\binom{p}{2i}A^{p-2i-1}(pB^2)^i,$$

which is impossible unless $A = 1$ and $B = 0$. But this gives only $y = 0$, concluding the proof.

The second part of the theorem of [1] can also be generalised very simply to cover the case $p \equiv 3 \pmod 4$.

Theorem 2. *The equation $x^p + 2^{2m} = p^3y^2$ has no solution in odd positive integers x and y for any odd prime p satisfying Condition A.*

Proof. Exactly as above we obtain $2^m + py\sqrt{p} = (A+B\sqrt{p})^p$ and $x = pB^2 - A^2$, whence A and B have opposite parity. Then, since

$$2^m = A\sum_{i=0}^{(p-1)/2}\binom{p}{2i}A^{p-2i-1}(pB^2)^i,$$

the second factor must be odd and hence equal to 1, which is impossible.

The author wishes to thank the referee most sincerely for making a number of suggestions, resulting in a much clearer exposition.

References

[1] Z. Cao, *On the Diophantine equation* $x^p + 2^{2m} = py^2$, Proc. Amer. Math. Soc. **128** (2000), 1927–1931. MR **2000m:**11028

[2] A. J. van Poorten, H. J. te Riele and H. C. Williams, *Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than* 100 000 000 000, Math. Comp. **70** (2001), 1311–1328. MR **2001j:**11125

Department of Mathematics, Royal Holloway University of London, Egham, Surrey TW20 0EX, United Kingdom

E-mail address: j.cohn@rhul.ac.uk