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 $\mathbb{Q}[\sqrt{p}]$.

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 $s$, $(\frac{x^r + 1}{x^s + 1}) = 1$, where here and elsewhere $(a|b)$ denotes the Legendre-Jacobi symbol.

Proof of the Lemma. Fix $x \equiv 0 \pmod{4}$ and let $f(r, s) = (\frac{x^r + 1}{x^s + 1})$. 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 $f(r, s) = f(2s - r, s)(\frac{x^{s+1}}{x^{s+1}})$ and, since $4|x$, $(\frac{x^{s+1}}{x^{s+1}}) = (x|x^{s-1} - x^{s-2} - \ldots - x + 1) = (x|1) = 1$, completing the induction.

Proof of Theorem 1. From the equation we obtain $x + 1 \equiv 0 \pmod{p}$, and so $p | x^{p+1} + 1$. 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
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
\[1 = \left(\frac{x^p + 1}{x + 1}\right) \left(\frac{x^r + 1}{x + 1}\right) = \left(\frac{x^{r-1} - x^{r-2} + \ldots - x + 1}{x + 1}\right) = (r|p),\]
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 $\pi$. Let $h$ denote the class number of the field. Then $h < p$ and so $(h, p) = 1$. Since $\pi^h$ is a principal ideal, it then follows that $1 + y\sqrt{p}$ is an associate of the $p$th power of an element of the field. Thus without loss of generality $1 + y\sqrt{p} = (\frac{u^2 + v^2\sqrt{p}}{2})^p$ for some integers $a = b \pmod{2}$ and $0 \leq r < p$. 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 $2^{r+1}(1 + y\sqrt{p}) = (v + u\sqrt{p})^r(a + b\sqrt{p})^p$ and then, since $p|y$, $2^{r+1} \equiv \sqrt{r} - 1(v + ru\sqrt{p})a^p \pmod{p}$. In particular we must have $p|\sqrt{r} - 1 ru a^p$. But $p$ cannot divide $u$ by hypothesis, nor $a$, since $(-x)^p = (1 + y\sqrt{p})(1 - y\sqrt{p}) = \pm(\frac{x^2 + y^2}{2})^p$, 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 $2^p = a \sum_{i=0}^{(p-1)/2} \left(\frac{p}{2i}\right) a^{p-2i-1}b^{2i}p^r$ whence $a = 1$ and then
\[2^{p+1} = 2 \sum_{i=0}^{(p-1)/2} \left(\frac{p}{2i}\right) b^{2i} p^r \geq (1 + \sqrt{5})^p + (1 - \sqrt{5})^p\]
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
\[1 = A \sum_{i=0}^{(p-1)/2} \left(\frac{p}{2i}\right) A^{p-2i-1}(pB^2)^i,\]
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 
[11] can also be generalised very simply to cover the case $p \equiv 3 \pmod{4}$.

Theorem 2. The equation $x^p + 2^{2m} = p^3 y^2$ has no solution in odd positive integers $x$ and $y$ for any odd prime $p$ satisfying Condition [\[12\]]

Proof. Exactly as above we obtain $2^{2m} + py\sqrt{p} = (A + B\sqrt{p})^p$ and $x = pB^2 - A^2$, whence $A$ and $B$ have opposite parity. Then, since
\[2^{2m} = A \sum_{i=0}^{(p-1)/2} \left(\frac{p}{2i}\right) A^{p-2i-1}(pB^2)^i,\]
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.
THE DIOPHANTINE EQUATION \( x^p + 1 = py^2 \)

REFERENCES


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

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use