ON DIOPHANTINE EQUATIONS OF THE FORM $x^n + y^n = hp^m$

ALFRED BRAUER AND JAMES E. SHOCKLEY

E. Catalan [3] conjectured the following theorem: The square of a prime can be the sum of two cubes only if the prime $p=3$. This conjecture was proved by L. Gegenbauer [4] as a special case of the following theorem:

Let p be a prime and n an integer which is not a power of 2. Then the Diophantine equation $x^n + y^n = p^m$ has no solution in relatively prime positive integers x and y unless $p=3$, $m=2$, $x=2$, $y=1$.

W. S. Baer [2] proved that for a given positive integer h there exists at most a finite number of pairs of relatively prime positive integers x, y where $(x^3 + y^3)/h$ is a power of a prime.

In this paper we will generalize these results by proving the following theorem:

THEOREM. *Let n and h be given positive integers where n is not a power of 2. There exist at most a finite number of relatively prime positive integers x and y , of primes p and of integers m such that*

$$x^n + y^n = hp^m.$$

The proof will give a method to find all possible solutions for given n and h . The mentioned results of Gegenbauer and Baer follow as special cases.

For completeness we will prove the following well-known lemma.

LEMMA. (See, for instance [1, p. 13].) *Let x and y be relatively prime positive integers and q an odd prime. We set $g(x, y) = (x^q + y^q)/(x + y)$ and denote the greatest common divisor of $g(x, y)$ and $(x + y)$ by d . Then*

$$(1) \quad d = (x + y, g(x, y)) = 1 \text{ or } q.$$

Moreover, in both cases $g(x, y) \not\equiv 0 \pmod{q^2}$.

PROOF. We set $x + y = s$. Then

$$(2) \quad \begin{aligned} g(x, y) &= \frac{(s - y)^q + y^q}{s} \\ &= s^{q-1} - \binom{q}{1} s^{q-2} y + \cdots + \binom{q}{q-1} y^{q-1}. \end{aligned}$$

Received by the editors December 22, 1960.

Hence d must divide qy^{q-1} and since $(s, y) = 1$ we have that d divides q . Thus (1) is proved. Moreover, if $s \equiv 0 \pmod{q}$ all terms of the right-hand side of (2) except the last one are divisible by q^2 . If $s \not\equiv 0 \pmod{q}$, all terms except the first are divisible by q .

We now prove the theorem. It is sufficient to prove the theorem for the case that n is an odd prime q and $x > y$. Assume

$$(3) \quad x^q + y^q = hp^m.$$

For $m=0$ the theorem is trivial. For $m=1$ we obtain

$$x^q + y^q = (x + y) \cdot g(x, y) = hp.$$

Hence either $x+y$ or $g(x, y)$ is a divisor of h . Since

$$(4) \quad g(x, y) \geq x^{q-2}(x - y) + y^{q-1} \geq x^{q-2} + y^{q-1} \geq x + y$$

we have in either case that $x+y \leq h$ and we obtain at most a finite number of solutions.

For $m > 1$ we have to consider the finite number of factorizations of h in the form $h = h_1 h_2$. It follows from (3) that

$$\begin{aligned} x + y &= h_1 p^k, & 0 \leq k \leq m, \\ g(x, y) &= h_2 p^{m-k}. \end{aligned}$$

The case $k=0$ is trivial. If $k=m$, then by (4) $h_2 = g(x, y) \geq x+y$ so there are at most a finite number of x and y which satisfy (3). If $1 \leq k \leq m-1$, then $(x+y, g(x, y)) = p$. Thus by the lemma $q=p$ and

$$(5) \quad x + y = h_1 q^{m-1},$$

$$(6) \quad g(x, y) = h_2 q.$$

Thus by (4)

$$(7) \quad x + y \leq g(x, y) = h_2 q,$$

and since h and q are given we obtain at most a finite number of solutions.

For the proof of the result of Gegenbauer we take $h=1$. It is obvious that the cases $m=0$ and $m=1$ cannot occur. By (5), (6) and (7) we obtain $q^{m-1} \leq q$. Hence $m=2$. Moreover, in (4) we only have equality if $q=3$.

When finding all solutions of $x^q + y^q = hp^m$ we have only to consider those factorizations of h for which h_2 contains only q and primes of form $2qz+1$. For suppose t is a prime divisor of h_2 . Then $g(x, y) \equiv 0 \pmod{t}$. Since $(x, y) = 1$ it follows that $(x, t) = (y, t) = 1$, so there is a positive integer s such that $y \equiv sx \pmod{t}$. Hence

$$g(x, y) \equiv g(x, sx) \equiv x^{q-1}g(s, 1) \equiv 0 \pmod{t},$$

which implies that $g(s, 1) \equiv 0 \pmod{t}$. Since q is a prime, $g(x, 1)$ is the $2q$ th cyclotomic polynomial. It follows from the well-known theorem on cyclotomic polynomials that either $t=q$ or t is of the form $2qz+1$.

REFERENCES

1. P. Bachmann, *Das Fermatproblem in seiner bisherigen Entwicklung*, Berlin, de Gruyter, 1919.
2. W. S. Baer, *Sur les entiers qui peuvent être représentés sous la forme de la somme de deux valeurs entières d'un polynôme cubique à nombres entiers*, Tôhoku Math. J. vol. 12 (1917) pp. 181-189.
3. E. Catalan, *Quelques théorèmes empiriques* (1842-43), Mem. Soc. Roy. Sci. Liège vol. 12 (1885) pp. 42-43.
4. L. Gegenbauer, *Notiz über gewisse binäre Formen, durch welche sich keine Potenzen von Primzahlen darstellen lassen*, S.-B. Akad. Wiss. Wien, Math.- Nat. Kl. vol. 97 Abt. IIa (1888) pp. 368-373.

UNIVERSITY OF NORTH CAROLINA