C O L L O Q U I U M   M A T H E M A T I C U M

VOL. LXII | 1991 | FASC. 2

A NOTE ON PRIMES p WITH $\sigma(p^m) = z^n$

BY

MAOHUA LE (CHANGSHA)

Let p^m be a power of a prime, and let $\sigma(p^m)$ denote the sum of divisors of p^m. Integer solutions (p, z, m, n) of the equation

$$\sigma(p^m) = z^n, \quad z > 1,\ m > 1,\ n > 1\,, \tag{1}$$

were investigated in many papers. By Nagell [6], $(p, z, m, n) = (7, 20, 3, 2)$ is the only solution of equation (1) with $2 \nmid m$. Takaku [8] proved that if (p, z, m, n) is a solution with $2 \mid n$, then $p < 2^{2^{m+1}}$. Chidambaraswawy and Krishnaiah [1] improved this result to $p < 2^{2^m}$. However, Ljunggren [4] and Rotkiewicz [7] showed that the only solutions (p, z, m, n) with $2 \mid n$ are $(3, 11, 4, 2)$ and $(7, 20, 3, 2)$. Recently, it was proved by Takaku [9] that if (p, z, m, n) is a solution of (1) such that

$$m + 1 = q^r m_1\,,\ q \nmid r\,,\ q \nmid m_1\,,\ q \mid n\,,\ q \text{ is an odd prime,} \tag{2}$$

then $p < mq^2(2q)^{(m-1)q^m}$. In this note we prove the following result.

THEOREM. *Equation* (1) *has no solution* (p, z, m, n) *which satisfies* (2) *with* $q \equiv 3 \pmod 4$.

The proof depends on the next two lemmas, which follow immediately from some old results of Gauss [2; Section 357] and Lucas [5] respectively.

LEMMA 1. *Let q be an odd prime with $q \equiv 3 \pmod 4$, and let x, y be coprime integers. If $q > 3$, then*

$$\frac{x^q - y^q}{x - y} = (A(x, y))^2 + q(B(x, y))^2,$$

where $A(x, y), B(x, y)$ are coprime integers with $2A(x, y) \equiv 0 \pmod{x - y}$ and $2B(x, y) \equiv 0 \pmod{xy(x + y)}$.

LEMMA 2. *Let D be a non-square integer, and let x, y be coprime integers. Further, let $\varepsilon = x + y\sqrt{D}$, $\overline{\varepsilon} = x - y\sqrt{D}$, and let*

$$E(t) = \frac{\varepsilon^t + \overline{\varepsilon}^t}{\varepsilon + \overline{\varepsilon}}, \quad F(t) = \frac{\varepsilon^t - \overline{\varepsilon}^t}{\varepsilon - \overline{\varepsilon}}$$

for any positive integer t with $2 \nmid t$. Then $E(t), F(t)$ are integers. Moreover, if $E(q)F(q) \equiv 0 \pmod p$ for some odd primes p, q, then either $p = q$ or $p \equiv (D/p) \pmod q$, where (D/p) is the Legendre symbol.

Proof of Theorem. (1) can be written as

$$\frac{p^{m+1}-1}{p-1} = z^n, \quad z > 1,\ m > 1,\ n > 1\,. \tag{3}$$

Let (p, z, m, n) be an integer solution of (3) satisfying (2). By Lemma 4 of [3], this is impossible for $q = 3$. Below we assume that $q > 3$.

If $p = q$, then $q \mid n$ implies $p^2 \mid z^n - 1$ (since $p \mid z^n - 1$). So (3) is impossible in this case.

If $p \neq q$ and $p^{m_1} \not\equiv 1 \pmod q$, then from (3) we get

$$\frac{p^{q^{r-1}m_1}-1}{p-1} = z_1^q$$

and

$$\frac{p^{m+1}-1}{p^{q^{r-1}m_1}-1} = p^{q^{r-1}m_1(q-1)} + \ldots + p^{q^{r-1}m_1} + 1 = z_2^q, \tag{4}$$

where z_1, z_2 are positive integers satisfying $z_1 z_2 = z^{n/q}$. Since $p \not\equiv 1 \pmod q$, we have $p \nmid (z_2^q - 1)/(z_2 - 1)$ and $p^{q^{r-1}m_1} \mid z_2 - 1$ by (4). It follows that

$$p^{m+1} - 1 = p^{q^r m_1} - 1 > z_2^q \geq (p^{q^{r-1}m_1} + 1)^q > p^{q^r m_1},$$

a contradiction.

If $p \neq q$, $p^{m_1} \equiv 1 \pmod q$ and $q \equiv 3 \pmod 4$, then $q \nmid r$ implies $r = sq - l$ where s, l are positive integers with $l < q$. From (3) we get

$$\frac{p^{m_1}-1}{p-1} = q^l z_0^q, \quad \frac{p^{q^i m_1}-1}{p^{q^{i-1}m_1}-1} = q z_i^q, \quad i = 1, \ldots, r, \tag{5}$$

where $z_0, z_1, \ldots, z_r$ are positive integers satisfying $q^s z_0 z_1 \ldots z_r = z^{n/q}$, $2 \nmid z_0 z_1 \ldots z_r$ and $q \nmid z_1 \ldots z_r$. We see from (5) that $p \not\equiv \pm 1 \pmod q$. Since $r \geq 1$, by Lemma 1 we have

$$\frac{p^{q m_1}-1}{p^{m_1}-1} = (A(p^{m_1},1))^2 + q(B(p^{m_1},1))^2 = q z_1^q, \tag{6}$$

where $A(p^{m_1}, 1)$, $B(p^{m_1}, 1)$ are coprime integers satisfying

$$\begin{aligned} &2A(p^{m_1},1) \equiv 0 \pmod{p^{m_1}-1},\\ &2B(p^{m_1},1) \equiv 0 \pmod{p^{m_1}(p^{m_1}+1)}\,. \end{aligned} \tag{7}$$

Hence

$$(B(p^{m_1},1))^2 + q\left(\frac{A(p^{m_1},1)}{q}\right)^2 = z_1^q\,,$$

where $B(p^{m_1},1)$, $A(p^{m_1},1)/q$ are coprime integers. Since the class number of $\mathrm{Q}(\sqrt{-q})$ is less than q, it is prime to q. Therefore $B(p^{m_1},1) + (A(p^{m_1},1)/q)\sqrt{-q}$ is the qth power of an algebraic integer of $\mathrm{Q}(\sqrt{-q})$. Recalling that $q > 3$, we have

$$B(p^{m_1},1) + \frac{A(p^{m_1},1)}{q}\sqrt{-q} = (X_1 + Y_1\sqrt{-q})^q\,, \tag{8}$$

where X_1, Y_1 are coprime integers satisfying

$$X_1^2 + qY_1^2 = z_1\,. \tag{9}$$

Let $\varepsilon = X_1 + Y_1\sqrt{-q}$, $\overline{\varepsilon} = X_1 - Y_1\sqrt{-q}$. From (7) and (9) we get

$$B(p^{m_1},1) = X_1\left(\frac{\varepsilon^q + \overline{\varepsilon}^q}{\varepsilon + \overline{\varepsilon}}\right) \equiv 0 \pmod{p^{m_1}}\,. \tag{10}$$

Recalling that $p \not\equiv \pm 1 \pmod q$, by Lemma 2 we see from (10) that $p \nmid (\varepsilon^q + \overline{\varepsilon}^q)/(\varepsilon + \overline{\varepsilon})$ and $p^{m_1} \mid X_1$. If $X_1 = 0$, then $\gcd(X_1, Y_1) = 1$ shows that $Y_1 = \pm 1$ and $z_1 = q$ by (9), which is impossible. Hence $X_1 \neq 0$ and $|X_1| \geq p^{m_1}$. From (6) and (9) we get

$$p^{qm_1} > qz_1^q > X_1^{2q} \geq p^{2qm_1}\,,$$

a contradiction. Thus the theorem is proved.

Acknowledgment. The author would like to thank the referee for his valuable suggestions.

REFERENCES

[1] J. Chidambaraswawy and P. Krishnaiah, *On primes p with* $\sigma(p^\alpha) = m^2$, Proc. Amer. Math. Soc. 101 (1987), 625–628.

[2] C. F. Gauss, *Disquisitiones Arithmeticae*, Fleischer, Leipzig 1801.

[3] K. Inkeri, *On the diophantine equation* $a(x^n - 1)/(x - 1) = y^m$, Acta Arith. 21 (1972), 299–311.

[4] W. Ljunggren, *Some theorems on indeterminate equations of the form* $(x^n - 1)/(x - 1) = y^q$, Norsk. Mat. Tidsskr. 25 (1943), 17–20 (in Norwegian).

[5] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 289–321.

[6] T. Nagell, *Sur l'équation indéterminée* $(x^n - 1)/(x - 1) = y^2$, Norsk Mat. Forenings Skr. (I) No. 3 (1921), 17 pp.

[7] A. Rotkiewicz, *Note on the diophantine equation* $1 + x + x^2 + \ldots + x^n = y^m$, Elemente Math. 42 (1987), 76.

[8] A. Takaku, *Prime numbers such that the sums of the divisors of their powers are perfect squares*, Colloq. Math. 49 (1984), 117–121.

[9] A. Takaku, *Prime numbers such that the sums of the divisors of their powers are perfect power numbers*, Colloq. Math. 52 (1987), 319–323.

RESEARCH DEPARTMENT
CHANGSHA RAILWAY INSTITUTE
CHANGSHA, HUNAN, CHINA

Reçu par la Rédaction le 14.3.1990