A NOTE ON A NUMBER THEORETICAL PAPER OF SIERPINSKI

ALFRED BRAUER

W. Sierpinski [5] has just published the following theorem:

"The set A of all primes which are divisors of integers of form 2^r+1 contains all primes of the form $8n\pm 3$ and infinitely many primes of the form $8n+1$. The set B of all primes which are divisors of integers of the form $2^{2s+1}-1$ contains all primes of the form $8n+7$ and some primes of the form $8n+1$. Every prime of form $8n+1$ belongs either to A or to B. The question whether the set B contains infinitely many primes of form $8n+1$ is raised, but remains open."

In this note a simple proof of this result will be given. Moreover, it will be shown that B contains infinitely many primes of form $8n+1$. More exactly, we prove a little more.

THEOREM 1. *Let a be a given positive integer. An odd prime p is a divisor of an integer of form a^r+1 if and only if a belongs to an even exponent* mod p. *The odd prime q is a divisor of an integer of form $a^{2s+1}-1$ if and only if a belongs to an odd exponent* mod q.

PROOF. If a belongs to an even exponent $2k$ (mod p), then

$$a^{2k} \equiv 1 \pmod{p},$$

hence

$$(a^k + 1)(a^k - 1) \equiv 0 \pmod{p},$$

$$a^k + 1 \equiv 0 \pmod{p}$$

since otherwise $2k$ would not be the exponent to which a belongs (mod p). Conversely, if p divides a^r+1, then

$$a^r \equiv -1 \pmod{p},$$

$$a^{2r} \equiv 1 \pmod{p}.$$

The exponent to which a belongs must be a divisor of $2r$, but not of r, and is therefore even.

If a belongs to the odd exponent $2k+1$ (mod q), then

$$a^{2k+1} \equiv 1 \pmod{q},$$

hence q is a divisor of $a^{2k+1}-1$. Conversely, if q is a divisor of $a^{2s+1}-1$, then

Presented to the Society, November 20, 1959; received by the editors August 7, 1959.

$$a^{2s+1} \equiv 1 \pmod{q}.$$

The exponent of a (mod q) must be a divisor of $2s+1$, and is therefore odd.

It follows that each odd prime which is relatively prime to a is either a divisor of an integer of form a^r+1 or of an integer of form $a^{2s+1}-1$.

If, in particular, $a=2$, then the primes for which 2 belongs to an even exponent form the set A of Sierpinski, the other odd primes the set B. Now 2 is a quadratic nonresidue for the primes p of form $8n\pm 3$, hence by Euler's criterion

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

and 2 belongs to an even exponent. Moreover, 2 is a quadratic residue for the primes q of form $8n+7$, hence

$$2^{4n+3} \equiv 1 \pmod{q},$$

and the exponent of 2 is odd. Finally, for $p=8n+1$ we have

$$2^{4n} \equiv 1 \pmod{p},$$

and the exponent to which 2 belongs can be even or odd.

B. M. A. Makowski (see [5]) proved that there are infinitely many primes of form $8n+1$ which belong to A namely the prime divisors of $2^{2^m}+1$. This result follows here at once from Theorem 1 since 2 belongs to an even exponent for all these prime divisors. There exist infinitely many such primes since $2^{2^m}+1$ and $2^{2^k}+1$ are relatively prime for $m\neq k$. Finally all these prime divisors for $m>1$ are of form $8n+1$ since the odd prime divisors of the 2^{m+1}st cyclotomic polynomial have the form $2^{m+1}z+1$.

This is a special case of the following theorem.

THEOREM 2. *Let p be a prime of form $8n+1$. We set*

$$p-1 = 2^e u \qquad (u \text{ odd}).$$

If 2 is a 2^eth power residue mod p, *then p belongs to the set B, otherwise to A.*

PROOF. If 2 is a 2^eth power residue, then by Euler's criterion

$$2^{(p-1)/2^e} \equiv 2^u \equiv 1 \pmod{p},$$

hence p belongs to B. Otherwise 2 belongs to an even exponent mod p, and p is an element of A by Theorem 1.

We shall use the following theorems on the biquadratic and octavic character of 2. (See, for instance, the paper of A. L. Whiteman [7].)

If p is a prime of form $8n+1$, then 2 is a biquadratic residue mod p if and only if p can be represented as x^2+64y^2. If p is of form $16n+1$, then 2 is an octavic residue if and only if p can be represented as x^2+256y^2. If p is of form $16n+9$, then 2 is an octavic residue if and only if p can be represented as x^2+64y^2, but not as x^2+256y^2.

THEOREM 3. *The number* 2 *is a biquadratic nonresidue for the infinitely many primes which can be represented as*

$$17x^2 + 64xy + 64y^2.$$

It is an octavic nonresidue for the infinitely many primes of form $16n+1$ *which can be represented as*

$$65x^2 + 256xy + 256y^2$$

and for the infinitely many primes of form $16n+9$ *which can be represented as* x^2+256y^2.

All these primes belong to the set A.

PROOF. Assume that the prime p can be represented by the positive properly primitive quadratic form

$$(1) \quad 17x^2 + 64xy + 64y^2 = x^2 + (4x + 8y)^2 = x^2 + 16(x + 2y)^2.$$

Then x must be odd and $4x+8y\equiv 4 \pmod 8$. Hence in the representation of p as sum of two squares one of the squares is odd and the other divisible by 16, but not by 64. Since this representation is unique, p cannot be represented as x^2+64y^2. Hence 2 is a biquadratic nonresidue mod p, and consequently a 2^eth power nonresidue, so that p belongs to A. It was proved by H. Weber [6] that every positive properly primitive quadratic form represents infinitely many primes. (See also E. Schering [4], P. Bernays [1], W. E. Briggs [2].) Therefore infinitely many primes are represented by (1) and all of them belong to A.

Suppose that p is a prime of form $16n+1$ and can be represented by the form

$$(2) \quad 65x^2 + 256xy + 256y^2 = x^2 + (8x + 16y)^2 = x^2 + 64(x + 2y)^2.$$

Then p is a biquadratic residue, but an octavic nonresidue since it is representable as x^2+64y^2 but not as x^2+256y^2 because $x+2y$ is odd. It was proved by A. Meyer [3] that any positive properly primitive quadratic form represents infinitely many primes which belong to a given linear form if at least one such prime exists. Since the prime 577 is represented by the quadratic form (2) for $x=y=1$ and is of form $16n+1$, infinitely many primes of form $16n+1$ are represented by (2) and all of them belong to A.

Suppose that p can be represented as x^2+256y^2 and is of form $16n+9$. Since $p=281=5^2+256$ is such a prime, infinitely many such primes exist. They belong to A since 2 is an octavic nonresidue for each of them.

THEOREM 4. *The number 2 is an octavic residue for every prime of form $16n+9$ which can be represented as $65x^2+256xy+256y^2$. All these infinitely many primes belong to the set B.*

PROOF. Let q be such a prime. It follows from (2) that 2 is an octavic residue mod q. Hence q belongs to the set B by Theorem 2. Since 73 is of form $16n+9$ and represented by (2) for $x=3$, $y=-1$, it follows from the theorem of Meyer that there exist infinitely many such primes q. This proves the theorem.

BIBLIOGRAPHY

1. Paul Bernays, *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht-quadratischen Diskriminante,* Dissertation, Göttingen, 1912.

2. W. E. Briggs, *An elementary proof of a theorem about the representation of primes by quadratic forms,* Canad. J. Math. vol. 6 (1954) pp. 353–363.

3. Arnold Meyer, *Über einen Satz von Dirichlet,* J. Reine Angew. Math. vol. 103 (1888) pp. 98–117.

4. Ernst Schering, *Beweis des Dirichletschen Satzes, dass durch jede eigentlich primitive quadratische Form unendlich viele Primzahlen dargestellt werden,* Gesammelte Mathematische Werke vol. 2 (1856) pp. 357–365.

5. Waclaw Sierpinski, *Sur une décomposition des nombres premiers en deux classes,* Collect. Math. vol. 10 (1958) pp. 81–83.

6. Heinrich Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist,* Math. Ann. vol. 20 (1882) pp. 301–329.

7. A. L. Whiteman, *The sixteenth power residue character of* 2, Canad. J. Math. vol. 6 (1954) pp. 364–373.

UNIVERSITY OF NORTH CAROLINA