COLLOQUIUM MATHEMATICUM

VOL. XX 1969 FASC. 2

ON PSEUDOPRIME NUMBERS OF SPECIAL FORM

BY

A. MĄKOWSKI AND A. ROTKIEWICZ (WARSZAWA)

Rotkiewicz [1] proved that the numbers $(2^{2p}+1)/5$ are pseudoprime (p is a prime number >5).

We prove the following

THEOREM. *Let n be a positive integer >1 and p a prime number satisfying the following condition: if $n = n_1 p^k$, where $p \nmid n_1$, then* 1° $p \nmid 2(2^{2n}+1)$, 2° $n_1 | 2^{n_1}+1$. *Then the numbers $(2^{2np}+1)/(2^{2n}+1)$ are pseudoprime.*

First we observe that there are infinitely many integers m such that $m | 2^m+1$, e.g. $m = 3^t$. The hypothesis $n > 1$ is unessential in view of the result of Rotkiewicz, but the case $n = 1$ needs some additional consideration to exclude the case $p = 3$.

Proof of the theorem. Let $n = n_1 p^k$, $p \nmid n_1$. Because

$$n_1 | 2^{n_1}+1 | 2^{2n_1}-1 | 2^{2n}-1, \tag{1}$$

$p^{k+1} | 2^{(p-1)p^k}-1$ and $(p, n_1) = 1$, we get $np = n_1 p^{k+1} | 2^{2(n-1)}(2^{2n_1(p-1)p^k}-1) = 2^{2(n-1)}(2^{2n(p-1)}-1)$ and

$$4np | 2^{2n}(2^{2n(p-1)}-1) = 2^{2np}-2^{2n}. \tag{2}$$

We have $(4, 2^{2n}+1) = 1$ and $(n, 2^{2n}+1) = 1$ (because if $d|n$ and $d|2^{2n}+1$, then $p \nmid d$, as $p \nmid 2^{2n}+1$, and by (1) $d|2^{2n}-1$, whence $d|(2^{2n}+1)-(2^{2n}-1) = 2$, but d is odd, thus $d = 1$), and by hypothesis, $(p, 2^{2n}+1) = 1$. From these relations it follows that

$$(4np, 2^{2n}+1) = 1. \tag{3}$$

From (2) and (3) we conclude that $4np \Big| \dfrac{2^{2np}-2^{2n}}{2^{2n}+1}$. The last number is evidently an integer. Further,

$$\frac{2^{2np}+1}{2^{2n}+1} \Big| 2^{2np}+1 | 2^{4np}-1 | 2^{\frac{2^{2np}-2^{2n}}{2^{2n}+1}}-1 = 2^{\frac{2^{2np}+1}{2^{2n}+1}-1}-1 | 2^{\frac{2^{2np}+1}{2^{2n}+1}}-2.$$

Let $n = 2r+1, p = 2s+1$. We have

$$N = \frac{2^{2np}+1}{2^{2n}+1} = \frac{\prod_{u=0}^{1}\left(2^{4rs+2r+2s+1}+(-1)^u 2^{2rs+r+s+1}+1\right)}{2^{2(2r+1)}+1}.$$

For positive integers r and s the inequality

$$2^{4rs+2r+2s+1} \pm 2^{2rs+r+s+1}+1 > 2^{2(2r+1)}+1$$

holds, because $2^{2rs+r+s} > 2^{2r+1}$, whence $2^{2rs+r+s} \pm 1 \geqslant 2^{2r+1}$ and $2^{2rs+r+s+1}(2^{2rs+r+s} \pm 1)+1 > 2^{2(2r+1)}+1$. Thus N is represented as a product of two factors both >1. Therefore N is composite.

This completes the proof of the theorem.

Observe that we may put $n = p^k$ (p is an odd prime $\neq 5$, k a positive integer) in the theorem. Indeed, in this case we have $n_1 = 1, 1 \mid 2^1+1$, and

$$p \nmid 2(2^{2p^k}+1). \tag{4}$$

Proof of (4). It is sufficient to prove that $p \nmid 2^{2p^k}+1$. We have $p \mid 2^{p-1}-1 \mid 2^{p^k-1}-1 \mid 2^{2p^k-2}-1 \mid 2^{2p^k}-4$. If $p \mid 2^{2p^k}+1$, then $p \mid (2^{2p^k}+1)-(2^{2p^k}-4) = 5$, which is impossible.

COROLLARY 1. *The numbers* $\dfrac{4^{p^{k+1}}+1}{4^{p^k}+1}$ ($k = 1, 2, \ldots$ *and* p *is an odd prime* $\neq 5$) *are pseudoprime.*

COROLLARY 2. *If* $n\varphi(n) \mid p-1$ *and* p *is an odd prime* $\neq 5$, *then the number* $N = \dfrac{4^{p^2}+1}{4^p+1}$ *is a pseudoprime number of the form* $kn+1$.

Proof. We may suppose $n > 2$ (for $n \leqslant 2$ the result is trivial). Let $n = 2^a \nu$, where $2 \nmid \nu$. We have then $n\varphi(n) \mid p-1$, $2 \mid \varphi(n), \varphi(\nu) \mid \varphi(n)$, $4^{p\varphi(n)} \equiv 1 \pmod{\nu}$ and (because $4^p+1 \mid 4^{p\varphi(n)}-1$) the number

$$N-1 = \frac{4^p(4^{p(p-1)}-1)}{4^p+1}$$

is divisible by

$$\frac{4^{pn\varphi(n)}-1}{4^{p\varphi(n)}-1} = \sum_{k=0}^{n-1} (4^{p\varphi(n)})^k \equiv n \equiv 0 \pmod{\nu},$$

hence $N \equiv 1 \pmod{\nu}$. Because $p > n > a$, we have $2^a \mid 4^p$, and therefore $N \equiv 1 \pmod{2^a}$. The last two congruences imply that $N \equiv 1 \pmod{n}$.

In [2] it was shown that the number

$$\prod_{k=1}^{\varphi(b)} F_{3n+(k-1)\varphi(\varphi(b))}$$

is a pseudoprime number $\equiv 1 \pmod{n}$ (F_s is the Fermat number and $3n = 2^\beta b$, where $2 \nmid b$). The formula given in corollary 2 is simpler, but for the existence of numbers p the theorem on arithmetical progression is needed.

REFERENCES

[1] A. Rotkiewicz, *Sur les formules donnant des nombres pseudopremiers*, Colloquium Mathematicum 12 (1964), p. 69-72.

[2] — *Sur les nombres pseudopremiers de la forme* $nk+1$, Elemente der Mathematik 21 (1966), p. 32-33.

Reçu par la Rédaction le 10. 6. 1968