COLLOQUIUM MATHEMATICUM

VOL. XIII 1965 FASC. 2

ON PRIME NUMBERS p, q, AND r SUCH THAT pq, pr, AND qr ARE PSEUDOPRIMES

BY

K. SZYMICZEK (KATOWICE)

Rotkiewicz [5] has shown that for every prime number $p \neq 2, 3, 5, 7, 13$ there exists a prime $q > p$ such that pq is a pseudoprime (1). This theorem implies that there exist infinitely many pseudoprimes of the form $M_p M_q$, where $M_n = 2^n - 1$ and p, q are distinct primes (cf. [6]).

The purpose of this paper is to prove that for infinitely many primes p of the form $8k+1$ there exist primes q and r such that pq, pr and qr are all pseudoprimes. The proof of this theorem is based on deep results concerning fourth power residues [2], quadratic forms [10] and the existence of two prime primitive divisors of the number $a^n - b^n$ [7].

From our theorem we conclude that there exists an infinity of pseudoprimes of the form $M_p M_q M_r$, where p, q and r are distinct primes. We also remark that there is an infinity of pseudoprimes $M_p M_t$, where t is a composed number.

The following notation is used: $\varphi(n)$ is Euler's totient function; $[m, n, l]$ — the least common multiple of m, n, l; $\Delta(m)$ — the least natural number Δ such that $m \mid 2^\Delta - 1$.

It may be easily seen that an odd composed number m is pseudoprime if and only if $\Delta(m) \mid m-1$.

LEMMA 1. *If m, n, l are pairwise relatively prime, then $\Delta(mnl) = [\Delta(m), \Delta(n), \Delta(l)]$.*

LEMMA 2. *$\Delta(M_n) = n$. If $(m, n) = 1$, then $\Delta(M_n M_m) = mn$.*

LEMMA 3. *If p, q are primes and $p < q$, then the following conditions are equivalent:*

(a) $pq \mid 2^{pq} - 2$,

(b) $p \mid 2^q - 2$ *and* $q \mid 2^p - 2$,

(c) $pq \mid 2^{q-p} - 1$.

(1) A number m is said to be a *pseudoprime* if it is composed and $m \mid 2^m - 2$.

Lemma 1 is known (cf. [1], p. 144, or [9], lemma 4). Lemma 2 results from the definition of $\Delta(m)$ and from Lemma 1.

Proof of Lemma 3. The equivalence of (a) and (b) was proved by Jeans [3] (see also [4]). In order to prove that (b) implies (c) we observe that if $\Delta(p)|q-1$ and $\Delta(q)|p-1$, then $\Delta(p)$ and $\Delta(q)$ are divisors of $q-p=(q-1)-(p-1)$, because $\Delta(p)|p-1$ and $\Delta(q)|q-1$ in view of Fermat's little theorem. Thus $pq|2^{q-p}-1$. On the other hand, if (c) holds, then $\Delta(p)|q-p=(q-1)-(p-1)$ and $\Delta(p)|p-1$, hence $\Delta(p)|q-1$. Similarly $\Delta(q)|p-1$ and we obtain (b).

THEOREM 1. *Let p be a prime number of the form $8k+1$. If the number 2 is a fourth power residue* mod p, *then there exist prime numbers q and r $(p \neq q \neq r \neq p)$ such that all the numbers pq, pr and qr are pseudoprimes.*

Remarks. 1. The assumption that 2 is a fourth power residue mod p may be replaced by the equivalent condition $p|2^{(p-1)/4}-1$.

2. Gauss [2] has proved that 2 is a fourth power residue mod p if and only if p is of the form x^2+64y^2.

3. From a theorem of Dirichlet and Weber [10] we conclude that there is an infinity of primes of the form x^2+64y^2. All these numbers are clearly of the form $8k+1$.

Hence from Theorem 1 follows

THEOREM 2. *For infinitely many primes p of the form $8k+1$ there exist primes q and r $(p \neq q \neq r \neq p)$ such that all the numbers pq, pr and qr are pseudoprimes.*

Proof of Theorem 1. Let $p=8k+1$ be a prime. According to the first remark we may suppose that $p|2^{(p-1)/4}-1$.

We first consider the case when p is of the form $16k+1$. In view of a theorem of Zsigmondy [11] there exist primes q and r such that $\Delta(q)=(p-1)/2$, $\Delta(r)=p-1$ and $(p-1)/2|q-1$, $p-1|r-1$. We shall prove that $p-1|q-1$. Contrary to this let us suppose that

$$q-1=\frac{p-1}{2}(2t+1).$$

Then $q=8k(2t+1)+1$ and the number 2 is a quadratic residue mod q. Thus

$$q|2^{(q-1)/2}-1=2^{(p-1)(2t+1)/4}-1$$

and we obtain

$$\Delta(q)=\frac{p-1}{2}\,\Big|\,\frac{p-1}{4}(2t+1)$$

which is impossible. Thus $p-1|q-1$ and $p-1|r-1$ and we have $p|2^{q-1}-1$, $p|2^{r-1}-1$. We have also $\Delta(q)|p-1$, $\Delta(r)|p-1$ which implies $q|2^{p-1}-1$, $r|2^{p-1}-1$. On account of Lemma 3 the numbers pq, pr are pseudoprimes. Similarly $q|2^{p-1}-1|2^{r-1}-1$ and $r|2^{p-1}-1|2^{q-1}-1$ implies that qr is a pseudoprime.

Now suppose that p is of the form $16k+9$. If $p = 16k+9$ and $p|2^{(p-1)/4}-1$, then $(p-1)/2 = 8k+4$; here $k \geqslant 4$, for 41 is not a divisor of $2^{(p-1)/4}-1$. In view of a theorem of Schinzel [7] there exist two distinct primes q and r such that $\Delta(q) = \Delta(r) = (p-1)/2$. Hence

$$p|2^{(p-1)/4}-1|2^{(p-1)/2}-1 = 2^{\Delta(q)}-1|2^{q-1}-1,$$

and similarly $p|2^{r-1}-1$. Moreover,

$$q|2^{(p-1)/2}-1|2^{p-1}-1 \quad \text{and} \quad q|2^{(p-1)/2}-1 = 2^{\Delta(r)}-1|2^{r-1}-1,$$

and similarly $r|2^{p-1}-1$, $r|2^{q-1}-1$. On account of Lemma 3 the numbers pq, pr and qr are all pseudoprimes, which completes the proof of Theorem 1.

There is a simple characteristic of pseudoprimes of the form M_pM_q, where p, q are distinct primes, namely M_pM_q is a pseudoprime if and only if pq is a pseudoprime (cf. [6]). But if pqr is a pseudoprime, $M_pM_qM_r$ is not necessary a pseudoprime, e. g. in the case when $p = 3$, $q = 5$, $r = 43$. In this connection we shall prove

THEOREM 3. *If p, q and r are distinct primes and the numbers pq, pr and qr are all pseudoprimes, then the number $M_pM_qM_r$ is a pseudoprime.*

Proof. First we remark that if u, v, w are distinct primes, then $u|M_uM_vM_w-1$ if and only if $u|M_vM_w-1$. This follows from $u|M_u-1$ and $M_uM_vM_w-1 = M_vM_w(M_u-1)+M_vM_w-1$.

Now let u denote one of the primes p, q, r and v, w $(v > w)$ denote the remaining primes. By our assumption the numbers uv, uw are pseudoprimes, thus Lemma 3 implies $u|2^v-2$, $u|2^w-2$ and we obtain $\Delta(u)|v-1$, $\Delta(u)|w-1$. Thus $\Delta(u)|v-w$ and $u|2^{v-w}-1$. Hence $u|2^v-2-(2^{v-w}-1) = 2^v-2^{v-w}-1|2^w(2^v-2^{v-w}-1) = M_vM_w-1$. Because $u|M_vM_w-1$ implies $u|M_uM_vM_w-1$, we obtain $pqr|M_pM_qM_r-1$. Thus

$$M_pM_qM_r|2^{pqr}-1|2^{M_pM_qM_r-1}-1|2^{M_pM_qM_r}-2,$$

which completes the proof.

From Theorems 1, 2 and 3 we obtain the following

COROLLARY 1. *There exist infinitely many triplets of distinct primes p, q, r such that the number $M_pM_qM_r$ is a pseudoprime.*

Thus e. g. the numbers $M_{37}M_{73}M_{109}$, $M_{23}M_{89}M_{683}$, $M_{31}M_{151}M_{331}$ are pseudoprimes.

We may also state the following

COROLLARY 2. *There exist infinitely many triplets of distinct primes* p, q, r *such that all the numbers* $pq, pr, qr, pqr, M_pM_q, M_pM_r, M_qM_r, M_{pq}, M_{pr}, M_{qr}, M_{pq}M_r, M_{pr}M_q, M_{qr}M_p, M_{pqr}, M_pM_qM_r$ *are pseudoprimes.*

Proof. Let us suppose that p, q, r are distinct primes and the numbers pq, pr, qr are pseudoprimes. Thus $\Delta(p)|q-1$ and $\Delta(p)|r-1$, which simultaneously with $\Delta(p)|p-1$ yields $\Delta(p)|pqr-1$. Similarly $\Delta(q)$ and $\Delta(r)$ are divisors of $pqr-1$. Hence, by Lemma 1, $\Delta(pqr) = [\Delta(p), \Delta(q), \Delta(r)]|pqr-1$ and pqr is a pseudoprime. The numbers M_pM_q, M_pM_r, M_qM_r are pseudoprimes in view of [6]. It is known that if m is a pseudoprime, then M_m is also a pseudoprime (see [8]), thus the numbers $M_{pq}, M_{pr}, M_{qr}, M_{pqr}$ are pseudoprimes. In view of Theorem 3 the number $M_pM_qM_r$ is a pseudoprime and it remains to prove that $M_{pq}M_r$ is a pseudoprime. By our assumption $p|M_r-1$ and $q|M_r-1$, thus $pq|M_r-1$. The number M_{pq} is a pseudoprime, so $pq|M_{pq}-1$. Thus $pq|M_{pq}M_r-1$. In an analogous way we obtain $r|M_{pq}M_r-1$. Since $(pq, r) = 1$ we have $(M_{pq}, M_r) = 1$ and so, by Lemma 1, $\Delta(M_{pq}M_r) = [\Delta(M_{pq}), \Delta(M_r)] = pqr$. Finally we have $pqr|M_{pq}M_r-1$ and $M_{pq}M_r$ is a pseudoprime. By the symmetry $M_{pr}M_q$ and $M_{qr}M_p$ are also pseudoprimes, which completes the proof.

We also remark that if $p = 43$, $q = 127$, $r = 337$, $s = 5419$, then all the numbers pq, pr, ps, qr, qs, rs are pseudoprimes.

Corollary 2 implies that there exist pseudoprimes of the form M_pM_t, where t is a composed number. In this connection we shall prove

THEOREM 4. *If* $p = 8k+7$ *is a prime and* $t = 2^{\varphi((p-1)/2)}$, *then the number* M_pM_t *is a pseudoprime.*

Proof. It is known that 2 is a quadratic residue of primes p of the form $8k+7$. According to Euler's criterion we have $p|2^{(p-1)/2}-1$. Putting $m = \max(p, t)$, $n = \min(p, t)$ we get $m \neq n$ and $(m, n) = 1$.

Since $m-n = \pm[(2^{\varphi((p-1)/2)}-1)-(p-1)]$, we can write $(p-1)/2|m-n$. Then $p|2^{m-n}-1$, and either $p|2^m-2$ or $p|2^n-2$, and so, by $2^m-2^{m-n}-1 = 2^m-2-(2^{m-n}-1) = 2^{m-n}(2^n-2)+2^{m-n}-1$, we have

$$p|2^m-2^{m-n}-1.$$

Because $\varphi\big((p-1)/2\big) < n$ we obtain $mn|2^n(2^m-2^{m-n}-1)$, which gives $mn|M_mM_n-1$. By Lemma 2 we have $\Delta(M_mM_n) = mn$, and thus M_mM_n is a pseudoprime, which completes the proof.

For example, $(2^7-1)(2^4-1)$, $(2^{23}-1)(2^{2^{10}}-1)$, $(2^{31}-1)(2^{2^8}-1)$ are pseudoprimes.

REFERENCES

[1] M. Cipolla, *Sui numeri composti P che verificano la congruenza di Fermat* $a^{P-1} \equiv 1 \pmod{P}$, Annali di Matematica 9 (1904), p. 139-160.

[2] C. F. Gauss, *Theoria residuorum biquadraticorum*, Commentatio prima, Werke, Band II, Göttingen 1863, p. 65-92.

[3] J. H. Jeans, *The converse of Fermat's theorem*, Messenger of Mathematics 27 (1897-1898), p. 174.

[4] D. H. Lehmer, *On the converse of Fermat's theorem*, American Mathematical Monthly 43 (1936), p. 347-354.

[5] A. Rotkiewicz, *Sur les nombres premiers p et q tels que* $pq \mid 2^{pq}-2$, Rendiconti del Circolo Matematico di Palermo 9 (1962), p. 280-282.

[6] — *Sur les nombres pseudopremiers de la forme* $M_p M_q$, Elemente der Mathematik 20 (1965) (in press).

[7] A. Schinzel, *On primitive prime factors of* $a^n - b^n$, Proceedings of the Cambridge Philosophical Society (4) 58 (1962), p. 555-562.

[8] W. Sierpiński, *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n-2)/n$, Colloquium Mathematicum 1 (1947), p. 9.

[9] K. Szymiczek, *A few theorems on pseudoprimes*, Zeszyty Naukowe Wyższej Szkoły Pedagogicznej w Katowicach 5 (1965) (in press).

[10] H. Weber, *Beweis des Satzes, daß jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Mathematische Annalen 20 (1882), p. 301-329.

[11] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatshefte für Mathematik und Physik 3 (1892), p. 265-284.

Reçu par la Rédaction le 22. 8. 1964