Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 21 (1966)
Heft: 6

Artikel: On pseudoprime numbers of the form MpMt
Autor: Makowski, A. / Rotkiewicz, A.
DOI: https://doi.org/10.5169/seals-24655

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 30.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

On Pseudoprime Numbers of the Form $M_p M_t$

In this paper M_k denotes the number $2^k - 1$, $\Delta(s)$ denotes the exponent, to which 2 belongs modulo s.

K. SZYMICZEK ([5], Theorem 4) proved that if p is a prime number $\equiv 7 \pmod 8$ and $t = 2^{\varphi((p-1)/2)}$ then the number $M_p M_t$ is a pseudoprime number (n is pseudoprime iff n is composite and $2^n \equiv 2 \pmod n$). This result can be generalized as follows:

Theorem. *Let p be an odd prime or pseudoprime number such that $\Delta(p)$ is odd, k a positive integer $\leqslant p/\Delta(\Delta(p))$* (e.g. $k = 1$ or 2), $t = 2^{k\Delta(\Delta(p))}$. *Then $M_p M_t$ is a pseudoprime number.*

We must prove that $M_p M_t \mid 2^{M_p M_t} - 2$ which is equivalent to $M_p M_t \mid 2^{M_p M_t} - 1$. Because $(p, t) = 1$ we have $(M_p, M_t) = 1$ and it is sufficient to prove that

$$p \mid M_p M_t - 1\,, \tag{1}$$

$$t \mid M_p M_t - 1\,. \tag{2}$$

We have $\Delta(p) \mid 2^{\Delta(\Delta(p))} - 1 \mid 2^{k\Delta(\Delta(p))} - 1$, hence $p \mid 2^{2^{k\Delta(\Delta(p))}-1} - 1 \mid 2^{2^{k\Delta(\Delta(p))}} - 2 = 2^t - 2 = 2^{t+1} - 2^t - 2$. Because

$$2^{t+1} - 2^t - 2 \equiv 2^{t+p} - 2^t - 2^p \pmod p$$

we get

$$p \mid 2^{t+p} - 2^t - 2^p = M_t M_p - 1$$

and (1) is proved.

We have $k\Delta(\Delta(p)) \leqslant p$, hence $t = 2^{k\Delta(\Delta(p))} \leqslant 2^p$ and $t \mid 2^p$. Because t and 2^t are both powers of 2 and $t < 2^t$ we have $t \mid 2^t$ and $t \mid 2^{t+p}$. Hence $t \mid 2^{t+p} - 2^t - 2^p = M_p M_t - 1$, which completes the proof of the theorem.

We deduce the mentioned above theorem of SZYMICZEK from this theorem. For a prime number $p \equiv 7 \pmod 8$ $\Delta(p)$ is odd. Because for such p $\Delta(p) \mid (p-1)/2$ we have

$$\Delta(\Delta(p)) \,\Big|\, \Delta\left(\frac{p-1}{2}\right) \,\Big|\, \varphi\left(\frac{p-1}{2}\right).$$

Therefore, for some integer k,

$$k\Delta(\Delta(p)) = \varphi\left(\frac{p-1}{2}\right)$$

and evidently

$$\varphi\left(\frac{p-1}{2}\right) < p, \quad \text{hence} \quad k < \frac{p}{\Delta(\Delta(p))}\,.$$

It is known [4] that for $p = 2^q - 1$, where q is an odd prime or pseudoprime number, the number $2^p - 1$ is prime or pseudoprime (because $q \mid 2^q - 2$ implies $2^q - 1 \mid 2^{2^q-2} - 1 \mid 2^{2^q-1} - 2$). Because $\Delta(p) = q$ is odd, we may apply the theorem and we obtain

Corollary 1. The number $M_p M_t$ for $p = 2^q - 1$ (q an odd prime or pseudoprime number) and $t = 2^{k\Delta(q)}$, where

$$k \leqslant \frac{2^q - 1}{\Delta(q)} \left(\text{e.g. } k \leqslant \frac{2^q - 1}{q - 1}\right),$$

is pseudoprime.

Because there exist infinitely many pseudoprime numbers $p_1, p_2, \ldots$ (e.g. those defined by $p_1 = M_{11}$, $p_i = M_{p_{i-1}}$ for $i \geqslant 2$) we obtain

Corollary 2. There exist infinitely many pseudoprime numbers of the form $M_p M_t$, where both p and t are composite numbers.

These are, e.g., the numbers $M_{p_i} M_t$ with $t = 2^{\Delta(p_i)}$ and the numbers $M_p M_t$ for $p = 2^q - 1$, $t = 2^{q-1}$, where q is an odd pseudoprime number (we put in corollary 1 $k = (q-1)/\Delta(q)$ which is evidently $\leqslant (2^q - 1)/\Delta(q)$).

Corollary 2 is a supplement to the results of ROTKIEWICZ [3] and SZYMICZEK ([5], Theorem 4) according to which there exist infinitely many pseudoprime numbers $M_p M_t$ with p and t prime as well as with p prime and t composite.

Corollary 2 can be deduced also from the proof of Theorem 2 in paper [2]. There was proved that there exist infinitely many positive integers n such that n and $2n - 1$ are both pseudoprime (hence composite) and $2n - 1 \mid 2^{n-1} - 1$. We shall prove that for such n the number $M_n M_{2n-1}$ is pseudoprime. Similarly as in the case of the above theorem it is sufficient to prove that

$$n(2n - 1) \mid M_n M_{2n-1} - 1 . \tag{3}$$

Let k denote arbitrary of the numbers n and $2n - 1$. We have

$$M_n M_{2n-1} - 1 = 2^{3n-1} - 2^n - 2^{2n-1} \equiv 2^2 - 2 - 2 = 0 \pmod{k} .$$

Because $(n, 2n - 1) = 1$, we get (3). We may observe that the Theorem 2 of [2] implies the existence of an infinity of pseudoprime numbers which are triangular (cf. [1]). These are the numbers $t_{2n-1} = n(2n - 1)$ for n defined above: we have

$$k \mid 2^{n-1} - 1 \mid 2^{(n-1)(2n+1)} - 1 \mid 2^{(n-1)(2n+1)+1} - 2 = 2^{n(2n-1)} - 2 .$$

A. MAKOWSKI and A. ROTKIEWICZ, Warszawa

REFERENCES

[1] A. ROTKIEWICZ, *Sur les nombres pseudopremiers triangulaires*, El. Math. *19*, 82–83 (1964).

[2] A. ROTKIEWICZ, *Sur les progressions arithmétiques et géométriques formées de trois nombres pseudopremiers distincts*, Acta Arith. *10*, 325–328 (1964).

[3] A. ROTKIEWICZ, *Sur les nombres pseudopremiers de la forme $M_p M_q$*, El. Math. *20*, 108–109 (1965).

[4] W. SIERPIŃSKI, *Remarque sur une hypothèse des Chinois concernant les nombres $(2^n - 2)/n$*, Colloq. Math. *1*, 9 (1947).

[5] K. SZYMICZEK, *On prime numbers p, q and r such that pq, pr, and qr are pseudoprimes*, Colloq. Math. *13*, 259–263 (1965).