Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 20 (1965)
Heft: 5

Artikel: Sur les nombres pseudopremiers de la forme MpMq
Autor: Rotkiewicz, A.
DOI: https://doi.org/10.5169/seals-23932

La solution (optimale) est donc $x_1 = 11/9$, $x_2 = 1/9$, $x_3 = 0$.

La résolution «graphique» de ce problème constitue une application intéressante des éléments de calcul vectoriel. Elle se généralise immédiatement à plus de 3 variables et se prête à des discussions. Enfin, elle a le mérite de montrer à l'élève que des moyens très simples quoique légèrement «détournés» permettent parfois d'obtenir un résultat inaccessible par un procédé direct, celui de la résolution graphique habituelle en l'occurrence; elle peut inciter l'élève à faire preuve d'ingéniosité.

P. BURGAT, Neuchâtel

Sur les nombres pseudopremiers de la forme $M_p M_q$

Je démontrerai ici les deux théorèmes suivants:

Théorème 1. *Le nombre $p q$, où p et $q > p$ sont des nombres premiers, est un nombre pseudopremier*[1]) *dans ce et seulement dans ce cas si le nombre $M_p M_q = (2^p - 1)(2^q - 1)$ est pseudopremier.*

Théorème 2. *Pour tout nombre premier p, où $7 < p \neq 13$, il existe un nombre premier q tel que le nombre $M_p M_q$ est pseudopremier. Pour $p = 2, 3, 5, 7$ et 13 il n'existe aucun nombre premier q pour lequel le nombre $M_p M_q$ soit pseudopremier.*

Démonstration du théorème 1. Supposons que le nombre $p q$, où p et $q > p$ sont des nombres premiers, est pseudopremier. On a alors $p > 2$. En effet, s'il était $2q \mid 2^{2q} - 2$, on aurait $q \mid 2^{2q-1} - 1$, ce qui est impossible, vu que

$$2^{2q-1} - 1 = 2^{2(q-1)}\, 2 - 1 \equiv 1 \pmod{q}$$

(d'après le théorème de FERMAT). Vu que $q > p$, les nombres p et q sont tous les deux impairs et la formule $p q \mid 2^{pq} - 2$ (puisque le nombre $p q$ est pseudopremier) donne $p q \mid 2^{pq-1} - 1$. Or, on a

$$2^{pq-1} - 1 = 2^{(p-1)q}\, 2^{q-1} - 1 \equiv 2^{q-1} - 1 \pmod{p}\,.$$

On a donc $p \mid 2^{q-1} - 1$ et, vu que $q \mid 2^{q-1} - 1$ et $q > p$, on en trouve que

$$p q \mid 2^{q-1} - 1 \mid 2^q - 2.$$

Pareillement on démontre que $p q \mid 2^p - 2$. On a donc $2^p - 1 \equiv 1 \pmod{p q}$ et $2^q - 1 \equiv 1 \pmod{p q}$, d'où $M_p M_q \equiv 1 \pmod{p q}$ et, comme $(2^p - 1,\ 2^q - 1) = 2^{(p,q)} - 1 = 1$, on trouve

$$M_p M_q = (2^p - 1)(2^q - 1) \mid 2^{pq} - 1 \mid 2^{M_p M_q - 1} - 1 \mid 2^{M_p M_q} - 2$$

et le nombre $M_p M_q$ est pseudopremier.

Supposons maintenant que le nombre $M_p M_q$ est pseudopremier. On a donc

$$(2^p - 1)(2^q - 1) \mid 2^{M_p M_q - 1} - 1\,. \tag{1}$$

Le nombre 2 appartenant à l'exposant p modulo 2^p–1, il résulte de (1) que $p \mid M_p M_q$–1.

[1]) C'est-à-dire un nombre composé n qui divise $2^n - 2$.

Pareillement on obtient que $q \mid M_p M_q - 1$. On a donc $p\,q \mid M_p M_q - 1$. Or, on a

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

donc

$$p \mid 2^q - 2\,. \tag{2}$$

Pareillement on trouve

$$q \mid 2^p - 2\,. \tag{3}$$

Il n'est pas $p = 2$, puisqu'alors, d'après (3), on aurait $q = 2$, contrairement à l'hypothèse que $q > p$. Les formules (2) et (3) donnent donc $p \mid 2^{q-1} - 1$ et $q \mid 2^{p-1} - 1$ et, vue que (d'après le théorème de FERMAT) $p \mid 2^{p-1} - 1$ et $q \mid 2^{q-1} - 1$ et que $q > p$, on trouve

$$p\,q \mid 2^{p-1} - 1 \quad \text{et} \quad p\,q \mid 2^{q-1} - 1\,. \tag{4}$$

Vu l'égalité

$$2^{pq-1} - 1 = 2^{p(q-1)+p-1} - 1 = (2^{p(q-1)} - 1)\,2^{p-1} + (2^{p-1} - 1)$$

on obtient de (4) $p\,q \mid 2^{pq-1} - 1 \mid 2^{pq} - 2$, ce qui prouve que le nombre $p\,q$ est pseudopremier. Le théorème 1 est ainsi démontré.

Démonstration du théorème 2. Pour tout nombre premier p, tel que $7 < p \neq 13$ il existe un nombre premier $q > p$, tel que le nombre $p\,q$ est pseudopremier (voir [1]) et, en vertu du théorème 1, le nombre $M_p M_q$ est pseudopremier. Si $p = 2, 3, 5, 7$ ou 13, il n'existe aucun nombre premier q pour lequel le nombre $p\,q$ soit pseudopremier et, en vertu du théorème 1 il n'existe aucun nombre premier q pour lequel le nombre $M_p M_q$ soit pseudopremier.

A. ROTKIEWICZ (Varsovie)

TRAVAIL CITÉ

[1] A. ROTKIEWICZ, *Sur les nombres premiers p et q tels que* $p\,q \mid 2^{pq} - 2$. Rendiconti del Circolo Matematico di Palermo *11*, 280–282 (1962).

Kleine Mitteilungen

Dreiblatt und Brocardsche Punkte

Trifolium, also Dreiblatt, heisst nach einem Vorschlag von Jos. E. HOFMANN die Figur von 3 Kreisen durch einen Punkt S, den Pol des Dreiblatts. Die Punkte A_1, A_2, A_3, in denen sich je 2 der 3 Kreise schneiden, heissen Ecken des Dreiblatts. Herr W. K. B. HOLZ, Ing. für Vermessungstechnik und Stadtarchivar in Hagen (Westfalen) hat zuerst die Frage nach den euklidischen Eigenschaften des Dreiblatts gestellt. In Math. Ann. *130*, 46–86 (1955) habe ich unter anderem die von HOLZ vermuteten Kongruenzsätze des Dreiblatts bewiesen. Ich nannte in dieser Arbeit die Dreiblätter Inversdreiecke, weil ein Dreiblatt durch Inversion aus einem geradlinigen Dreiseit hervorgeht. Nimmt man in der Tat den Einheitskreis $|z| = 1$ einer Gausschen z-Ebene als Umkreis des Dreiblatts – das ist der Kreis durch die 3 Ecken – so führt

$$z' = \frac{S\,\bar{z} - 1}{\bar{z} - \bar{S}} \tag{1}$$

ein Dreiseit mit den Ecken $z' = A_1', A_2', A_3'$ in ein Dreiblatt mit den Ecken $z = A_1, A_2, A_3$ über. Dabei geht $|z| = 1$ in $|z'| = 1$ über und stimmt die Abbildung (1) auf $|z| = 1$ mit