Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 27 (1972)
Heft: 4

Artikel: On a problem of W. Sierpiski
Autor: Rotkiewicz, A.
DOI: https://doi.org/10.5169/seals-28633

10. Gilt in einer euklidischen Ebene E das Axiom Z), so hat E höchstens eine Anordnung. Gelten W) und Z) in E, so lässt sich E auf genau eine Weise anordnen.

Beweis: Ein Positivbereich eines Körpers enthält alle Körperelemente der Form α^2 ($\alpha \neq 0$) und kein Element der Gestalt $-\alpha^2$. Der Koordinatenkörper einer euklidischen Ebene, die Z) erfüllt, kann also wegen 9 keine von der Menge $\{\alpha^2 \mid \alpha \in K^*\}$ verschiedene Teilmenge zum Positivbereich haben.

Der Koordinatenkörper einer stetig angeordneten euklidischen Ebene ist wegen 8 der reelle Zahlkörper. Die reelle euklidische Ebene lässt sich auch kennzeichnen als euklidische Ebene, die die Axiome W) und Z) erfüllt und deren (wegen 10 eindeutig bestimmtes) Halbgeradensystem dem Stetigkeitsaxiom S) genügt.

Alfred Uhl, Universität Karlsruhe

LITERATUR

[1] E. Artin, *Geometric Algebra*, Interscience Tracts in Pure and Applied Mathematics *3* (1957).

[2] F. Bachmann, *Aufbau der Geometrie aus dem Spiegelungsbegriff* (Springer 1959).

[3] D. Hilbert, *Grundlagen der Geometrie*, 8. Aufl. (Teubner 1956).

[4] H. Karzel, E. Ellers, *Grundzüge der Mathematik*, Band II, Teil A (Vandenhoeck und Ruprecht, 1967), Kap. 6.

[5] van der Waerden, *Moderne Algebra*, 3. Aufl. (Springer, 1950).

On a Problem of W. Sierpiński

Let a, b be fixed coprime positive integers and let $p(a, b)$ denote the least prime in an arithmetic progression $\{a x + b\}$. Linnik [3] has proved that there exists an absolute constant L such that $p(a, b) < a^L$. Pan-Cheng-Tun [5] has calculated that $L \leqslant 10^4$.

Let C denote an absolute constant such that $p(a, b) \ll a^C$. Cheng-Jing-Run [1] has proved that $p(a, b) \ll a^{777}$. The best estimate for C to be found in literature is the result $C \leqslant 550$ of Jutila [2]. The Extended Riemann Hypothesis implies that $p(a, b) \ll a^{2+\varepsilon}$.

A positive integer n is called a pseudoprime if $n \mid 2^n - 2$ and n is composite. In [7] (see also [8]) I proved that if a, b are fixed coprime positive integers then there exist infinitely many pseudoprimes of the form $a x + b$ $(x = 0, 1, 2, 3, \ldots)$.

In 1965 (during a seminar which the author attended) W. Sierpiński put forward the following problem: What estimate can we give for the least pseudoprime of the form $a x + b$ $(x = 0, 1, 2, 3, \ldots)$?

Here we shall prove the following.

Theorem. Let $P(a, b)$ denote the least pseudoprime $\equiv b \pmod{a}$ and let L and C be absolute constants such that $p(a, b) < a^L$, $p(a, b) \ll a^C$ respectively; then

1. $\log_2 P(a, b) < a^{6L^2+2L}$ for $a \geqslant 2$,

2. $\log P(a, b) \ll a^{4C^2+C+\varepsilon}$ for $\varepsilon > 0$.

For any positive integer n, let $f_n(x)$ denote the n-th cyclotomic polynomial defined by

$$f_n(x) = \prod_{d/n} (x^d - 1)^{\mu(n/d)},$$

where μ is the Möbius function, and write $f_n = f_n(2)$.

We can assume without any loss of generality that a is even $\geqslant 2$, and hence that b is odd.

The following Lemma holds.

Lemma. Let q, q_1 be any two distinct odd primes satisfying the conditions

$$q_1 \nmid a, \quad q \equiv 1 \pmod{a\, q_1\, \varphi(a\, q_1)},$$

and let m be any (odd) integer such that

$$m \equiv b \pmod{a}, \quad m \equiv 1 + q_1 \pmod{q_1^2}, \quad m \equiv 1 \pmod{q^2}.$$

If $p \equiv m \pmod{a\, q^2\, q_1^2}$, p prime, then one of the numbers

$$p\, f_{p-1}, \quad p\, f_{(p-1)/2}, \quad p\, f_{(p-1)/q}$$

is a pseudoprime $\equiv b \pmod{a}$.

This Lemma was proved in [4].

Proof of the Theorem. Since $L > 1$ we have $4\, L^2 + 2\, L > \log_2 \log_2 10^8$ and for $a \leqslant 30$ our Theorem can easily be verified by using the tables of Poulet [6]. With the help of Dr. Glyn Roberts using the tables of Poulet and computers in Cambridge, I found that for every $a \leqslant 100$ and b coprime with a there exists a pseudoprime $\equiv b \pmod{a}$ ess than 10^8.1

Now let $a > 30$ and let q_1 be the least prime number such that $q_1 \nmid a$. Then $q_1 < \sqrt{a}$ and $q_1 < a^\varepsilon$ for any $\varepsilon > 0$ and sufficiently large a. We have

$$a\, q_1\, \varphi(a\, q_1) < a\sqrt{a}\,(a-1)\sqrt{a} < a^3$$

for $a > 30$ and

$$a\, q_1\, \varphi(a\, q_1) < a \cdot a^\varepsilon \cdot a \cdot a^\varepsilon = a^{2+2\varepsilon}$$

for any $\varepsilon > 0$ and sufficiently large a.

Let q denote the least prime $\equiv 1 \pmod{a\, q_1\, \varphi(a\, q_1)}$. We have

$$q < (a^3)^L = a^{3L}$$

for $a > 30$ and

$$q < (a^{2+2\varepsilon})^C = a^{2C+2C\varepsilon}$$

for any $\varepsilon > 0$ and sufficiently large a, hence

$$a\, q^2\, q_1^2 < a(a^{3L})^2\, a = a^{6L+2}$$

for $a > 30$ and

$$a\, q^2\, q_1^2 < a(a^{2C+2C\varepsilon})^2\, a^{2\varepsilon} = a^{4C+1+4C\varepsilon+2\varepsilon}$$

for $\varepsilon > 0$ and sufficiently large a. Thus we have

$$p = p(a\, q^2\, q_1^2,\, m) < (a^{6L+2})^L = a^{6L^2+2L}$$

for $a > 30$ and

$$p(a\, q^2\, q_1^2,\, m) \ll (a^{4C+1+4C\varepsilon+2\varepsilon})^C = a^{4C^2+C+\varepsilon(4C^2+2C)} .$$

But by our Lemma one of the numbers

$$p\, f_{(p-1)/2}\,,\quad p\, f_{p-1}\,,\quad p\, f_{(p-1)/q_1}$$

is a pseudoprime of the form $a\,x + b$. Denote this number by $P(a, b)$. We have

$$P(a, b) \mid 2^p - 2 = 2\,(2^{p-1} - 1)\,,$$

hence

$$P(a, b) < 2^p\,,\quad \log_2 P(a, b) < p\,.$$

Thus

$$\log_2 P(a, b) < a^{6L^2+2L} \quad \text{for} \quad a \geqslant 2$$

and

$$\log P(a, b) \ll a^{4C^2+C+\bar{\varepsilon}}$$

for any $\bar{\varepsilon} > 0$.

This completes the proof of our Theorem. Thus from the result of Jutila it follows that

$$P(a, b) \ll a^{4(550)^2+550+\varepsilon} = a^{1210550+\varepsilon}$$

and the Extended Riemann Hypothesis implies that $\log P(a, b) \ll a^{18+\varepsilon}$.

A. Rotkiewicz, Warszawa

REFERENCES

[1] Chen-Jing-Run, *On the Least Prime in an Arithmetic Progression*, Scientia sin. *14*, 1868–1871 (1966).

[2] M. Jutila, *A New Estimate for Linnik's Constant*, Ann. Acad. sci. fenn. [Ser. A] *471*, 1–7 (1970).

[3] Y. V. Linnik, *On the Least Prime in an Arithmetic Progression*, I. *The Basic Theorem*, Matem. Sb. *15*, 139–178 (1944); II. *The Deuring-Heilbronn's Phenomenon*, Mat. Sb. *15*, 347–369 (1944).

[4] H. Halberstam, A. Rotkiewicz, *A Gap Theorem for Pseudoprimes in Arithmetic Progressions*, Acta arith. *13*, 395–404 (1968).

[5] Pan-Cheng-Tun, *On the Least Prime in an Arithmetical Progression*, Sci. Rec. N.S. *1*, 311–313 (1957).

[6] P. Poulet, *Tables de nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'a 100000000*, Sphinx *8*, 42–52 (1938).

[7] A. Rotkiewicz, *Sur les nombres pseudopremiers de la forme a x + b*, C. r. hebd. Séanc. Acad. Sci., Paris *257*, 2601–2604 (1963).

[8] A. Rotkiewicz, *On the Pseudoprimes of the Form a x + b*, Proc. Camb. phil. Soc. *63*, 389–392 (1967).