Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 59 (2004)

Artikel: Two conjectures on primes dividing [Formel]
Autor: Skalba, Marius
DOI: https://doi.org/10.5169/seals-9319

Elem. Math. 59 (2004) 171 – 173
0013-6018/04/040171-3
DOI 10.1007/s00017-004-0211-x

Elemente der Mathematik

Two conjectures on primes dividing $2^a + 2^b + 1$

Mariusz Skałba

M. Skałba promovierte im Jahr 1992 an der Universität Warschau. Danach verbrachte er einen zweijährigen Forschungsaufenthalt an der Technischen Universität in Wien. Gegenwärtig arbeitet er am mathematischen Institut der Universität Warschau und am mathematischen Institut der Polnischen Akademie der Wissenschaften. Sein mathematisches Hauptinteresse gilt der Zahlentheorie.

The starting point is the celebrated theorem of H. Hasse stating that the set of primes p which divide a number of the form $2^a + 1$ has the natural density $17/24$ ([2]).

What about the primes dividing some number of the form $2^a + 2^b + 1$?

Let $\mathrm{ord}_p(2)$ denote the multiplicative order of 2 mod p.

Theorem 1 *If a prime number p satisfies*

$$\mathrm{ord}_p(2) \geq p^{0.8}$$

then it divides some number of the form $2^a + 2^b + 1$.

Proof. Let us take a prime p satisfying

$$\mathrm{ord}_p(2) \geq p^{0.8}.$$

For such a prime p the powers of 2 mod p are exactly the non-zero power residues of dth degree, where

$$d = \frac{p-1}{\mathrm{ord}_p(2)} \leq p^{0.2}.$$

Üblicherweise wird die Anzahl der Primzahlen kleiner gleich x mit $\pi(x)$ bezeichnet. Der Primzahlsatz besagt, dass sich $\pi(x)$ asymptotisch wie $x/\log(x)$ verhält. Bezeichnet $H(x)$ die Anzahl der Primzahlen kleiner gleich x, die eine Zahl der Form $2^a + 1$ teilen, so hat H. Hasse gezeigt, dass der Grenzwert $\lim_{x\to\infty} H(x)/\pi(x)$ existiert und gleich $17/24$ ist. In der vorliegenden Arbeit wird nun die Anzahl $T(x)$ der Primzahlen kleiner gleich x untersucht, die eine Zahl der Form $2^a + 2^b + 1$ teilen. Unter Verwendung einer Vermutung von P. Erdös wird $\lim_{x\to\infty} T(x)/\pi(x) = 1$ gezeigt.

Now, let us consider the Fermat curve

$$x^d + y^d = -1 \quad \text{over} \quad \mathbb{F}_p\,.$$

By the Hasse-Weil theorem (for instance [3], Proposition 8.4.1) the number N_p of its points in $\mathbb{F}_p$ satisfies the inequality

$$N_p \geq p - d^2\sqrt{p} > 0\,.$$

This means exactly what we want:

$$\exists a, b \geq 0: \quad 2^a + 2^b \equiv -1 \pmod{p}. \qquad \square$$

Now, let $A(x,c)$ denote the number of primes p below x with $\operatorname{ord}_p(2) < p^c$ (Erdös [1]). At the bottom of the first page of [1] Erdös states the conjecture:
For each $c < 1$

$$A(x,c) = o\left(\frac{x}{\log x}\right).$$

So, having the above conjecture of Erdös proved for $c = 0.8$ we would obtain from Theorem 1

Conjecture 1 *Let $T(x)$ denote the number of primes p below x which divide some number of the form $2^a + 2^b + 1$. Then*

$$T(x) = (1 + o(1))\frac{x}{\log x}\,.$$

Theorem 2 *Assume that a natural number m satisfies the inequality*

$$\Omega(2^m - 1) \leq c \log m \quad \textit{with} \quad c = \frac{1}{\log 3},$$

where $\Omega(n)$ is the number of prime factors of n counted with multiplicities. Then, there exists a prime number q, dividing $2^m - 1$ and such that q does not divide any number of the form $2^a + 2^b + 1$.

Proof. Let us assume to the contrary that for each prime divisor q of $2^m - 1$ there exist non-negative integers a_q, b_q such that $q \mid (2^{a_q} + 2^{b_q} + 1)$. Taking into account the canonical decomposition of

$$2^m - 1 = \prod_{j=1}^{k} q_j^{n_j} \quad \text{(where } q_j \text{ are distinct and } n_j > 0),$$

let us consider the number

$$M = \prod_{j=1}^{k} (2^{a_{q_j}} + 2^{b_{q_j}} + 1)^{n_j}\,.$$

On the one hand, M is divisible by $2^m - 1$. However, on the other hand, it is a sum of (not necessarily distinct) $3^{\Omega(2^m-1)} < m$ powers of 2. But this contradicts the fact, that a number which is a sum of less than m powers of 2 is not divisible by $2^m - 1$. $\square$

One may expect that there are infinitely many m's coprime in pairs satisfying the assumptions of Theorem 2 (obviously the m's giving Mersenne primes $2^m - 1$ do satisfy!). This leads to the conjecture

Conjecture 2 *There are infinitely many primes q such that q does not divide any number of the form $2^a + 2^b + 1$.*

We hope that our two conjectures are more tractable than, say, the conjecture on infinitude of Mersenne primes, and are interesting enough to stimulate some further investigations.

Acknowledgements. I would like to thank Prof. J. Browkin and Prof. A. Schinzel for their kind attention and remarks improving presentation.

References

[1] Erdös, P.: Bemerkungen zu einer Aufgabe in den Elementen. *Arch. Math.* 27 (1976), 159–163.

[2] Hasse, H.: Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist. *Math. Ann.* 168 (1966), 19–23.

[3] Ireland, K.; Rosen, M.: *A classical introduction to modern number theory*. Second ed., Graduate Texts in Math. 84, Springer-Verlag, 1990.

Mariusz Skałba
Department of Mathematics,
Computer Science and Mechanics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
e-mail: skalba@mimuw.edu.pl