ON THE PRIME FACTORS OF THE NUMBER $2^{p-1}-1$

by A. ROTKIEWICZ

(Received 6 April, 1967)

From the proof of Theorem 2 of **[5]** it follows that for every positive integer k there exist infinitely many primes p in the arithmetical progression $ax+b$ ($x = 0, 1, 2, \ldots$), where a and b are relatively prime positive integers, such that the number $2^{p-1}-1$ has at least k composite factors of the form $(p-1)x+1$. The following question arises:

For any given natural number k, do there exist infinitely many primes p such that the number $2^{p-1}-1$ *has k prime factors of the form* $(p-1)x+1$ *and* $p \equiv b \pmod{a}$, *where a and b are coprime positive integers?*

For $k = 2$ the answer to this question is in the affirmative because in the paper **[5]** we proved that for every prime number $p \neq 2, 3, 5, 7, 13$ there exists a prime $q > p$ such that $q \equiv 1 \pmod{p-1}$ and $q \mid 2^{p-1}-1$.

Here we prove the following

THEOREM 1. *In every arithmetical progression* $ax+b$, *where a and b are relatively prime positive integers* (*excluding the case* $a \equiv 0 \pmod{16}$, $b \equiv 9 \pmod{16}$), *there exist infinitely many primes p such that the number* $2^{p-1}-1$ *has at least three distinct prime factors of the form* $(p-1)x+1$.

LEMMA. *For every natural number c there exist infinitely many primes p in every arithmetical progression* $ax+b$ ($x = 0, 1, 2, \ldots$), *where a and bc are relatively prime positive integers such that*

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

Proof. Let Q denote the field of rational numbers and ζ_n be a primitive nth root of unity. Let

$$K = Q(\zeta_a), \qquad L = Q(\zeta_c), \qquad M = Q(2^{1/c}).$$

If $c \equiv 0 \pmod 2$, then $a \not\equiv 0 \pmod 2$ and the discriminants of the fields K and LM are coprime. Hence we have

$$K \cap LM = Q, \tag{1}$$

where LM denotes the union of L and M, and $K \cap LM$ the intersection of K and LM.

If $c \not\equiv 0 \pmod 2$, then by Nagell's theorem **[4]** for every prime divisor $q > 1$ of the number c the number $2^{1/q}$ does not belong to the field $Q(\zeta_{ac}) = KL$. Thus by a theorem of Capelli **[1]** the polynomial x^c-2 is irreducible in KL. Hence

$$|KLM| = |KL|\,|M|,$$

where $|F|$ denotes the degree of the field F. On the other hand, in view of $(a, c) = 1$, we have $|KL| = |K||L|$. Thus

$$|KLM| = |K||L||M|.$$

Hence we again get formula (1).

It now follows from a theorem of Hasse [3, p. 144] that for every class Σ of conjugate elements of the Galois group of the field K there exist infinitely many primes p such that

$$\left(\frac{K}{p}\right) = \Sigma \tag{2}$$

and

$$p \text{ is divisible by a prime ideal of the first degree in } LM. \tag{3}$$

Since $(b, c) = 1$ we may assume $\Sigma = \{\tau\}$, where $\zeta_a^{(\tau)} = \zeta_a^b$. From (2) it follows that $\zeta_a^b \equiv \zeta_a^p \pmod{\mathfrak{p}}$ where $\mathfrak{p}$ is a prime ideal in K which divides p. Hence $\zeta_a^b = \zeta_a^p$ and $p \equiv b \pmod a$.

On the other hand, from (3) and a theorem of Dedekind [2, Satz I, pp. 15–16], it follows that the congruence $x^c - 2 \equiv 0 \pmod p$ has c solutions, and then by Euler's criterion we have

$$2^{(p-1)/c} \equiv 1 \pmod p.$$

Proof of Theorem 1. Let a and b be relatively prime positive integers. We exclude the case $a \equiv 0 \pmod{16}$, $b \equiv 9 \pmod{16}$. Let q be a prime number such that $q \nmid 2a$. If $2 \mid a$, and $b \not\equiv 9 \pmod{16}$, then there exists a positive integer x_0 such that $ax_0 + b \not\equiv 9 \pmod{16}$. If $2 \nmid a$ then there exists a positive integer x_0 such that $ax_0 + b \equiv 1 \pmod{16}$.

In both cases $16ax + ax_0 + b \not\equiv 9 \pmod{16}$, and $(16a, ax_0 + b) = 1$ for every x. By the Lemma, there exist infinitely many primes p such that $p \not\equiv 9 \pmod{16}$, $p \equiv a \pmod b$ and

$$p \mid 2^{(p-1)/q} - 1. \tag{4}$$

Let $p > 20$ be a prime number possessing the above properties. We first consider the case when $p \equiv 3 \pmod 4$. Since $p > 20$ we have $\frac{1}{2}(p-1) \geqq 10$ and, by a theorem of Zsigmondy [9], the number $2^{\frac{1}{2}(p-1)} - 1$ has a primitive prime factor q of the form $\frac{1}{2}(p-1)l + 1$. (A prime p is called a primitive prime factor of the number $2^n - 1$ if $p \mid 2^n - 1$ and $p \nmid 2^x - 1$ for $0 < x < n$.)

Since $p \equiv 3 \pmod 4$ we have $2 \nmid \frac{1}{2}(p-1)$. Thus $2 \mid l$ and $q \equiv 1 \pmod{p-1}$. The primitive prime factor of the number $2^{p-1} - 1$ is the second prime factor of the form $(p-1)x + 1$. The prime p which divided $2^{(p-1)/q} - 1$ is the third prime factor of the form $(p-1)x + 1$.

Now suppose that $p \equiv 5 \pmod 8$. In view of a theorem of A. Schinzel [8], there exist two primitive prime factors q and r of the number $2^{p-1} - 1$ such that $q \equiv 1 \pmod{p-1}$, $r \equiv 1 \pmod{p-1}$. The prime p is the third prime factor of the form $(p-1)x + 1$.

Finally we consider the case $16 \mid p - 1$. From a theorem of Zsigmondy [9], there exists a primitive prime factor q of the number $2^{\frac{1}{2}(p-1)} - 1$. We prove that this prime factor q is of the form $(p-1)x + 1$. Indeed, since q is a primitive prime factor of the number $2^{\frac{1}{2}(p-1)} - 1$, we have $q \equiv 1 \pmod{\frac{1}{2}(p-1)}$.

Since $16 \mid p - 1$ we have $q \equiv 1 \pmod 8$, and the number 2 is a quadratic residue modulo q. Thus $q \mid 2^{\frac{1}{2}(q-1)} - 1$. Since q is a primitive prime factor of the number $2^{\frac{1}{2}(p-1)} - 1$, we have $\frac{1}{2}(p-1) \mid \frac{1}{2}(q-1)$; hence $q \equiv 1 \pmod{p-1}$.

The primitive prime factor of the number $2^{p-1}-1$ is the second prime factor of the form $(p-1)x+1$. The prime p is the third prime factor of the form $(p-1)x+1$. This completes the proof of Theorem 1.

A number m is called a pseudoprime if it is composite and $m \mid 2^m-2$. K. Szymiczek proved in [7] that for infinitely many primes p of the form $8k+1$ there exist primes q and r (distinct from each other and from p) such that all the numbers pq, pr and qr are pseudoprimes.

From the Lemma we obtain

THEOREM 2. *For infinitely many primes p of the form $ax+b$, where $(a, b) = 1$ there exist primes q and r (distinct from each other and from p) such that all the numbers pq, qr and pr are pseudoprimes.*

Proof. Let $(a, b) = 1$ and let q be a prime number such that $q \nmid 2a$. By the Lemma, there exist infinitely many primes p such that

$$p \mid 2^{(p-1)/q}-1, \qquad p \equiv b \pmod a.$$

The rest of the proof runs completely parallel to the proof of Theorem 2 given in [7].

A number each of whose divisors d satisfies the relation $d \mid 2^d-2$ *is called a super-pseudoprime number.*

THEOREM 3. *For infinitely many primes p of the form $ax+b$, where $(a, b) = 1$, (excluding the case $a \equiv 0 \pmod{16}$, $b \equiv 9 \pmod{16}$) there exist primes q and r such that the number pqr is a super-pseudoprime number.*

Proof. Let $a \not\equiv 0 \pmod{16}$ or $b \not\equiv 9 \pmod{16}$. It follows from Theorem 1 that there exist distinct prime numbers p, q and r such that $q, r \equiv 1 \pmod{p-1}$ and

$$pqr \mid 2^{p-1}-1. \tag{6}$$

Let d be any divisor of the number pqr. From (6) it follows that $d \mid 2^{p-1}-1$. We have also $d \equiv 1 \pmod{p-1}$. Hence

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

Theorem 3 is thus proved.

REFERENCES

1. A. Capelli, Sulla reduttibilita della funzione x^n-A in un campo qualunque di razionalità, *Math. Ann.* **54** (1901), 602–603.

2. R. Dedekind, *Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen* (Göttingen, 1878).

3. H. Hasse, *Bericht über neuere Untersuchungen and Probleme aus der Theorie der algebraischen Zahlen*, Teil II, *Reziprozitätsgesetze* (Berlin, 1930).

4. T. Nagell, Contributions à la théorie des corps et des polynômes cyclotomiques, *Ark. Mat.* **5** (1965), 153–192.

5. A. Rotkiewicz, Sur les nombres naturels n et k tels que les nombres n et nk sont a la fois pseudoprimes, *Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fiz. Mat. Nat.* (8) **36** (1964), 816–818.

6. A. Rotkiewicz, Sur les nombres premiers p et q tels que $pq \mid 2^{pq}-2$, *Rend. Circ. Mat. Palermo* **11** (1962), 280–282.

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

8. A. Schinzel. On primitive factors of $a^n - b^n$, *Proc. Cambridge Philos. Soc.* (4), **58** (1962), 555–562.

9. K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265–284.

DEPARTMENT OF PURE MATHEMATICS
CAMBRIDGE UNIVERSITY

Permanent address: Institute of Mathematics, ul. Śniadeckich 8, Warsaw, Poland.

https://doi.org/10.1017/S0017089500000331 Published online by Cambridge University Press