On pseudoprime numbers

By ANDRZEJ ROTKIEWICZ (Cambridge)

A composite number n is called a pseudoprime if $n|2^n-2$. The first proof of the existence of infinitely many pseudoprimes was given by M. CIPOLLA in 1904 ([2]). He proved the following theorem:

The number $F_m \cdot F_n \ldots F_s$, *where* $F_i=2^{2^i}+1$, $m<\ldots<s$ *is a pseudoprime if and only if* $2^m>s$. If follows at once from this theorem that every number F_mF_{m+1}, $m=2, 3, \ldots$ is a pseudoprime. Cipolla's results remained long unnoticed by later writers on the subject. In the thirties D. H. LEHMER ([6]) and P. POULET ([8]) tabulated all odd pseudoprimes $<10^8$, and in 1949 D. H. Lehmer ([7]) gave a list of all odd pseudoprimes n with $10^8<n<2\cdot10^8$, and all of whose factors exceed 313.

The distribution of pseudoprimes is very irregular. The only pair of consecutive pseudoprimes below 10^8 with difference 2 is the pair $17\cdot257$, $17\cdot257+2$. I do not know, whether there exist two or three consecutive natural numbers each of which is a pseudoprime. It is a surprising fact that more than one half of all odd pseudoprimes $<10^8$ end in the digit 1 (when represented on the decimal scale) and approximately 10% end in the digit 3, 5, 7 or 9.

In 1936 D. H. Lehmer ([6]) showed that there are infinitely many pseudoprimes which are products of two primes and in 1949 he proved that this is true also for product of three primes (see [7]).

In 1949 P. ERDŐS ([3]) generalizing a method due to Lehmer proved that for any $k\geqq2$ there are infinitely many pseudoprimes which are products of exactly k different primes.

1947 W. SIERPIŃSKI ([22]) gave a very simple proof that there are infinitely many pseudoprimes by proving that if n is a pseudoprime then 2^n-1 is also pseudoprime. The same result was found later by R. STEURWALD ([23]).

Until 1950 only odd pseudoprimes were known. D. H. Lehmer was the first to find an even pseudoprime, namely $=161038$.

In 1951 N. G. W. H. BEEGER ([1]) proved that there exist infinitely many even pseudoprimes. We give now the proof, that there exist infinitely many squarefree pseudoprimes divisible by an arbitrary given prime p (cf. [9]).

We begin with a definition. A prime p which divides 2^n-1 and does not divide 2^k-1 for $k=1, 2, \ldots, n-1$ is called a primitive prime factor of 2^n-1. That such a prime p exists for $n>6$ follows from a theorem of K. ZSIGMONDY ([25]). It is enough to prove that for a given prime p there exists at least one pseudoprime with the required property. For suppose that $2^{pn}\equiv2 \pmod{pn}$ and let q be a primitive prime factor of $2^{pn-1}-1$. Then $pn-1$ divides $q-1$, thus $pqn|2(2^{pn-1}-1)|2(2^{q-1}-1)=$

$=2^q-2$, and since $2^{pqn}\equiv 2^q \pmod{pqn}$ it follows that $pqn|2^{pqn}-2$. It remains to find one pseudoprime with required property. For $p=2, 3, 5, 7, 11, 13$ such numbers are given by $\mathbf{2}\cdot 73\cdot 1103$, $\mathbf{3}\cdot 11\cdot 17$, $\mathbf{5}\cdot 13\cdot 17$, $\mathbf{7}\cdot 13\cdot 19$, $\mathbf{11}\cdot 31$, $\mathbf{13}\cdot 7\cdot 19$ respectively.

It is easy to prove that

1. for $p=8k\pm 1>13$ a suitable pseudoprime is pq where q is a primitive prime factor of $2^{p-1}-1$.

2. for $p=8k+3>13$ a suitable pseudoprime is pq where q is a primitive prime factor of $2^{p-1/2}-1$.

Finally for $p=8k+5>13$ a suitable pseudoprime is pq where $q\neq p$ is a primitive prime factor of $2^{p-1}-1$. Such a factor exists by virtue of a theorem of A. SCHINZEL ([20]) to the effect that the number $2^{4n}-1$ for n odd >5 has at least two primitive prime factors.

Let $P(x)$ denote the number of pseudoprimes $\leqq x$. P. ERDŐS ([4]) proved in 1955 that

$$P(x)<x\exp\{-c(\log x\log\log x)^{\frac{1}{2}}\},$$

where c is a positive constant.

On the other hand it follows from the construction of Lehmer that $P(x)>\frac{1}{4}\log x$ for $x\geqq 2^{22}-1$. No estimation for $P(x)$ better than $P(x)>c\log x$ is known. In [19] I proved, that for every integer $n\geqq 19$, there is a pseudoprime between n and n^2 and that for every $\varepsilon>0$ and all $x>x_0(\varepsilon)=4^{\exp\left(\frac{2}{\varepsilon}+\frac{5}{2}\right)}$ there is a pseudoprime between x and $x^{1+\varepsilon}$.

The tables suggest that for $x>170$ there is a pseudoprime between x and $2x$, but this cannot be proved from the constructions of pseudoprimes given so far. Since the number of primes $\leqq x$ is asymptotic to $x/\log x$, it follows from the results of Erdős that there are considerably fewer pseudoprimes than primes. It would therefore, seem that a problem of the distribution of pseudoprimes in arithmetical progression would present much greater difficulties than the analogous problem, settled by the theorem of Lejeune—Dirichlet. The condition $(a, b)=1$ necessary in the theorem of Lejeune—Dirichlet is no longer necessary here. There exist arithmetical progressions $ax+b$, where $(a, b)>1$ containing infinitely many pseudoprimes, e.g. $4x+2$, or px, where p is a prime. It would not be reasonable, however to replace the condition $(a, b)=1$, for example by the condition $(a, b)|p$ where p is a prime, since there are progressions $ax+b$ satisfying the latter and not containing any pseudoprime. Indeed, let $a=p(p-1)$, $b=3p$, where p is a prime $\equiv 5 \pmod 6$, so that $(a, b)=p$. If we had for some $n=ax+b$, $n|2^n-2$, then p would divide 2^n-2 and since $2^{ax+b}=2^{p(p-1)x+3(p-1)+3}\equiv 2^3 \pmod p$ we should get $p|2^3-2$ which is impossible. Similarly, it is easy to prove that a progression pqx $(x=0, 1, 2, \ldots)$, where $q|2^p-1$ does not contain any pseudoprime.

It seems noteworthy that there are arithmetical progressions for which it is easier to prove that they contain infinitely many pseudoprimes than that they contain infinitely many primes. For instance, as observed by. A. Schinzel the existence of infinitely many pseudoprimes in the progression $7x+3$ follows from an analogous property of the progression $3x+2$. Indeed, suppose that there are infi-

nitel many pseudoprimes of the from $3x+2$ and let n be any one of them. Then 2^n-1 is also a pseudoprime and since $2^{3x+2}-1\equiv 2^2-1\equiv 3 \pmod 7$ it belongs to the progression $7x+3$.

There is no similar deduction for the distribution of primes. Since pseudoprimes of the form $3x+2$ can be found from the formula $F_nF_{n+1}F_{n+2}$ $(n=3, 4, \ldots)$ it follows that the progression $7x+3$ contains an infinity of pseudoprimes.

The proof that every arithmetical progression $ax+b$ $(x=0, 1, 2)$ where a and b are relatively prime positive integers contains an infinity of pseudoprimes is much more difficult ([10]). It is achieved by showing that the progression $ax+b$ where $(a, b)=1$ contains a pseudoprime

$$P=\begin{cases} p f_{\frac{p-1}{2}}(2) & \text{if 2 is a primitive root of } p \\ p f_{p-1}(2) & \text{if 2 is not a primitive root of } p \end{cases}$$

where $f_n(x)$ is the n-th cyclotomic polynomial and p is a prime $\equiv b \pmod a$ satisfying certain conditions. The Brun—Titchmarch estimate for the number of primes $\equiv 1 \pmod k$ and not exceeding x is used in the proof of the following lemma:

In every arithmetical progression $ax+b$, where $(a, b)=1$ there exists a prime p such that

$$\frac{p-1}{2}=2^{\alpha-1}p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}}p_k^{\alpha_k}\quad,\qquad 2<p_1<\ldots<p_k,$$

$$2^{\alpha-1}p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}}\nmid p_k-1.$$

In a note ([19]) joint with Schinzel we proved also, that every quadratic form (positive or indefinite) with fundamental discriminant and belonging to the principal genus represents infinitely many pseudoprimes. The theorem about pseudoprimes in an arithmetic progression has the following consequences ([12]):

1. For an arbitrary finite sequence $c_1, c_2, \ldots, c_m$ of digits where $c_m=1, 3, 7, 9$ there exists an infinity of pseudoprimes whose last m digits are $c_1, c_2, \ldots, c_m$.
2. There exist pseudoprimes arbitrarily distant from others on both sides, i.e. for every k there exists a pseudoprime $p>k$ such that none of the numbers $p\pm i$ $(i=1, 2, \ldots, k)$ is a pseudoprime.
3. For every even integer $2k$ and every modulus m there exist pseudoprimes p and q arbitrarily large such that $2k\equiv p\pm q \pmod m$.

In particular every integer divides a sum of two pseudoprimes. Professor Sierpiński raised the questions, whether there exist arithmetic progressions formed from three different pseudoprimes and whether there exist pseudoprimes which are at the same time triangular. In [15], [16] I proved that the answer to these questions is in the affirmative. Here I give another proof begining by the following.

Lemma. *There exist infinitely many positive integers n such that the numbers $6n+1$, $12n+1$, $18n+1$ are composite and*

$$6n+1,\ 12n+1,\ 18n+1 \mid 2^{6n}-1. \tag{1}$$

PROOF. It can be verified that for $n=\frac{2^{36}-1}{9}$ the numbers $6n+1=\frac{2^{37}+1}{3}$, $12n+1=\frac{2^{38}-1}{3}$ and $18n+1=2^{37}-1$ are composite and (1) holds. Now, we notice that if $6n+1$, $12n+1$, and $18n+1$ are composite and satisfy (1), then the numbers $6N+1$, $12N+1$ and $18N+1$, for $N=\frac{2^{12n}-1}{9}$ have the same property. Indeed, we have $6N=\frac{2(2^{12n}-1)}{3}$, whence by (1) it follows that $2(6n+1)(12n+1)|6N$. Thus

$$6N+1 = \frac{2^{12n+1}+1}{3} \mid 2^{2(12n+1)}-1 \mid 2^{6N}-1,$$

$$12N+1 = \frac{2^{2(6n+1)}-1}{3} \mid 2^{2(6n+1)}-1 \mid 2^{6N}-1,$$

$$18N+1 = 2^{12n+1}-1 \mid 2^{6N}-1$$

Since the numbers $6N+1$, $12N+1$, $18N+1$ are composite, as is easily proved and $N=\frac{2^{12n}-1}{9} > n$ for $n \geqq 1$, the lemma follows.

As consequence we obtain:

I. *There exist infinitely many triplets of pseudoprimes, which are in A. P.* [15].

II. *There exist infinitely many triangular pseudoprimes* ([16]).

III. *There exist infinitely many pentagonal pseudoprimes* ([11]).

(A pentagonal number is one of the form $\frac{1}{2}k(3k-1)$).

PROOF OF I. If the composite number $6n+1$, $12n+1$ and $18n+1$ satisfy (1) then:

$$6n+1 \mid 2^{6n}-1 \mid 2^{6n+1}-2, \quad 12n+1 \mid 2^{6n}-1 \mid 2^{12n+1}-2,$$

$$18n+1 \mid 2^{6n}-1 \mid 2^{18n}-1 \mid 2^{18n+1}-2.$$

Hence $6n+1$, $12n+1$ and $18n+1$ are pseudoprimes. They form an arithmetic progression with the difference $6n$. Another arithmetic progression formed of three pseudoprimes is given by $\frac{2^{26}+1}{5}$, $\frac{2^{28}-1}{18}$, $\frac{2^{26}-1}{3}$.

PROOF OF II. It follows from (1) that

$$t_{12n+1} = (6n+1)(12n+1) \mid 2^{6n}-1 \mid 2^{t_{12n+1}-1}-1 \mid 2^{t_{12n+1}}-2.$$

PROOF OF III.

$$\omega_{12n+1} = (12n+1)(18n+1) \mid 2^{6n}-1 \mid 2^{\omega_{12n+1}-1}-1 \mid 2^{\omega_{12n+1}}-2.$$

There exist only 6 triangular pseudoprimes $\leqq 20000$ and only one pentagonal pseudoprime $\leqq 60000$. The least triangular pseudoprime is the number $t_{33}=561$. I do not know any arithmetic progression formed by six pseudoprimes. I cannot prove the existence of infinitely many pseudoprimes which are at the same time tetrahedral. Also I do not know whether for every n, there exist a pseudoprime which

is at the same time n-gonal number (i.e. number of the form $\frac{k}{2}[(n-2)(k-1)+2]$, $k=1, 2, \ldots$). As far as geometric progressions formed by pseudoprimes are concerned, one can give examples of such progressions with three terms ([15]).

However, the existence of infinitely many such progressions as well as the existence of pseudoprime squaress would imply the existence of infinitely many primes such that $p^2|2^{q-1}-1$ ([17]), [18]). The last problem seems very far from solution, since it is known that there are only two primes $p<10^6$ satisfying $p^2|2^{p-1}-1$ ([5]) and we cannot prove that there exists infinitely many primes p such that $p^2|2^{p-1}-1$. We also do not know whether there exists an integer k such that for every prime p the number 2^p-2 is not divisible by p^k.

One can show that there exist only two square pseudoprimes $<10^{12}$ ([17]).

The existence of geometric progressions formed by k different pseudoprimes implies the existence of a prime p such that $p^{k-1}|2^{p-1}-1$ ([18]); conversely the existence of a prime p such that $p^k|2^{p-1}-1$ implies the existence of a geometric progression formed by k different pseudoprimes ([18]). If $p^k|2^{p-1}-1$, then $p^2, p^3, \ldots, p^k$ are pseudoprimes ([18]). It follows from the formual (1) that there exist infinitely many integers x such that $x, 2x-1, 3x-2|2^{x-1}-1$, whence one can easily conclude that there exist infinitely many integers x such that all the numners $x, 2x-1$, $3x-2, x(2x-1), x(3x-2), (2x-1)(3x-2), x(2x-1)(3x-2)$ are pseudoprimes.

We do not know any polynomial of degree >1 in *a* variable x about which we could prove that it takes primes values for infinitely many values of x. On the other hand for every integer $n>1$ there exists a polynomial of degree n which represents infinitely many pseudoprimes ([13]). One such polynomial is given for instance, by $f(x)=2^m x^n-1$, where $(m, n)=1$.

Indeed, if $nk+m$ is a pseudoprime, then $2^{nk+m}-1=2^m(2^k)^n-1$ is also pseudoprime, and we see that the value of the polynomial $f(x)$ for $x=2^k$ is a pseudoprime.

I do not know any example of an irreducible polynomial of the degree >1 representing infinitely many pseudoprimes and not representing ± 1.

If n and kn are pseudoprimes then $n|2^k-2$ ([14]). The least positive integer k for which there exist a pseudoprime n such that nk is also a pseudoprime is $k=23$ ([14]).

If n and $n(n+k)$ are pseudoprimes then $n|2^{k+1}-2$ ([14]), and hence it follows inter alia that there is no number x for which x and $x(x+4)$ are both pseudoprimes.

I conjecture that the following hypothesis H_1 ([13]), holds for pseudoprimes analogous to the hypothesis H ([21]) of A. Schinzel concerning primes.

H_1: If s is a natural number and $f_1(x), \ldots f_s(x)$ are polynomial with integral coefficients, with the leading coefficients positive, relatively prime in pairs and satisfying the property S given below, then there exist infinitely many natural numbers x for which each of the number $f_1(x), f_2(x), \ldots, f_s(x)$ is a pseudoprime.

S: There is no natural number >1 which is a divisor of the product $f_1(x)f_2(x) \ldots \ldots f_s(x)$ for every integral value of x.

References

[1] N. G. W. H. Beeger, On even numbers m dividing 2^m-2, *Amer. Math. Monthly* **58** (1951), 553—555.

[2] M. Cipolla, Sui numeri composti P che verificiano la congruenca di Fermat $a^{P-1}\equiv 1 \pmod P$, Annali di Matematica **9** (1904), 139—160.

[3] P. Erdős, On the converse of Fermat's theorem, *Amer. Math. Monthly* **56** (1949), 623—624.

[4] P. Erdős, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen* **4** (1955), 201—206.

[5] M. Hausner and D. Sachs, On the congruence $2^p \equiv 2 \pmod{p^2}$ *Amer. Math. Monthly* **70** (1963), 996.

[6] D. H. Lehmer, On the converse on Fermat's theorem, *Amer. Math. Monthly* **43** (1936), 347—354.

[7] D. H. Lehmer, On the converse of Fermat's theorem 11, *ibidem* **56** (1949), 300—309.

[8] P. Poulet, Table de nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'a 100 000 000, *Sphinx* **8** (1938), 42—52.

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

[10] A. Rotkiewicz, Sur les nombres pseudoprimes de la forme $ax+b$, *C. R. Acad. Sci. Paris* **257** (1963), 2601—2604.

[11] A. Rotkiewicz, Sur les nombres pseudopremiers pentagonaux, *Bull, Soc. Roy. Sci. Liège* **33** (1964), 261—263.

[12] A. Rotkiewicz, Quelques conséquences de l'existence infinite des nombres pseudopremiers de la forme $ax+b$, *Publ, Inst. Math. (Beograd)* **4** (1964), 139—140.

[13] A. Rotkiewicz, Sur les polynômes en x qui pour infinité des nombres naturels x donnent des nombres pseudopremiers, *Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* **36** (1964), 136—140.

[14] A. Rotkiewicz, Sur les nombres naturels n et k tels que les nombres n et nk sont à la fois pseudopremiers, *ibidem* **36** (1964), 816—818.

[15] A. Rotkiewicz, Sur les progressions arithmétiques et géométriques formees de trois nombres pseudopremiers distincts, *Acta Arith.* **10** (1964), 325—328.

[16] A. Rotkiewicz, Sur les nombres pseudopremiers triangulaires, *Elem. Math.* **19** (1964), 82—83.

[17] A. Rotkiewicz, Sur les nombres pseudopremiers carrés, *ibidem* **20** (1965), 39—40.

[18] A. Rotkiewicz, Sur les progressions géometriques formées de k nombre pseudopremiers distincts, *Rend. Circ. Mat. Palermo* **13** (1964), 369—372.

[19] A. Rotkiewicz, Les intervalles contenants les nombres pseudopremiers, *ibidem* **14** (1965), 278—280.

[20] A. Rotkiewicz et A. Schinzel, Sur les nombres pseudopremiers de la forme $ax^2+bxy+cy^2$, *C. R. Acad. Sci. Paris* **258** (1964), 3617—3620.

[21] A. Schinzel, On primitive prime factors of a^n-b^n, *Proc. Cambridge Philos. Soc.* **58** (1962), 555—562.

[22] A. Schinzel et W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185—208.

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

[24] R. Steuerwald, Über, die Kongruenz $2^{n-1}\equiv 1 \pmod n$, *S.—B. Math. Natur. Kl. Bayer. Akad. Wiss. München* (1947), 177.

[25] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265—284.

(Received March 28, 1966.)