J. Austral. Math. Soc. (*Series A*) **29** (1980), 316–321

ON STRONG PSEUDOPRIMES IN ARITHMETIC PROGRESSIONS

A. J. van der POORTEN and A. ROTKIEWICZ

(Received 9 October 1979)

Communicated by J. B. Miller

Abstract

A composite integer N is said to be a strong pseudoprime for the base C if with $N-1=2^s d$, $(2,d)=1$ either

$$C^d \equiv 1, \quad \text{or } C^{2^r} \equiv 1 \pmod{N} \quad \text{some} \quad r, \quad 0 \leqslant r < s.$$

It is shown that every arithmetic progression $ax+b$ $(x=0,1,\ldots)$ where a, b are relatively prime integers contains an infinite number of odd strong pseudoprimes for each base $C \geqslant 2$.

1980 Mathematics subject classification (*Amer. Math. Soc.*): 10 A 15.

1.

A composite integer N is said to be a *pseudoprime* for the base $C \geqslant 2$ if

$$C^{N-1} \equiv 1 \pmod{N}. \tag{1}$$

It is well known that, for each base C, there are infinitely many pseudoprimes. Moreover there are universal pseudoprimes, that is composite integers N that are pseudoprime for all bases C with $(C,N)=1$. Such numbers are called *Carmichael numbers*. It is believed, but not known, that there are infinitely many Carmichael numbers. In fact there is no certain known method for constructing integers that are pseudoprime to more than one base (other than in the trivial case where one base is the power of another).

Lehmer (1976) pointed out that the condition

$$C^{\frac{1}{2}(N-1)} \equiv \left(\frac{C}{N}\right) \pmod{N}, \tag{2}$$

where $\left(\frac{C}{N}\right)$ is the Jacobi symbol, gives a stronger test for primality than does (1);

when N is an odd prime $(N, C) = 1$, (2) is just Euler's criterion. He remarked that (2) is satisfied for fewer C than is (1), and proved that given N, (2) cannot be satisfied for all bases C with $(C, N) = 1$. Lehmer called N satisfying (2) strong pseudoprimes for the base C; thus he showed that there are no strong Carmichael numbers.

Rather appropriately, composite integers satisfying (2) have also recently been called *Euler pseudoprimes* for the base C. The adjective *strong* has been reserved for the following criterion : an odd composite number N is a *strong pseudoprime* for the base C if with $N-1 = 2^s d$, $(2, d) = 1$, either

$$(3) \qquad C^d \equiv 1 \pmod{N} \quad \text{or} \quad C^{2^r d} \equiv 1 \pmod{N} \quad \text{some} \quad r, \quad 0 \leqslant r < s.$$

Any prime p with $(p, C) = 1$ satisfies one or other of these alternatives. Rabin (1976) has shown that no odd composite integer is a strong pseudoprime for more than half the bases relatively prime to it; the same was shown for Euler pseudoprimes by Solovay and Strassen (1977). Indeed Malm (1977) points out that the Euler pseudoprimes $\equiv 3 \pmod 4$ are strong pseudoprimes. Conversely, Pomerance, Selfridge and Wagstaff (1979) show that a strong pseudoprime is always an Euler pseudoprime; so the criterion (3) is indeed stronger than is (2), whilst it coincides with (2) when $N \equiv 3 \pmod 4$. Moreover it is readily seen that an Euler pseudoprime for the base C with $\left(\frac{C}{N}\right) = -1$ is a strong pseudoprime for the base C. The reader will find further detailed discussion, and extensive tables, in the last cited paper.

It was shown by Rotkiewicz (1963), (1967) that every arithmetic progression $ax+b$ $(x = 0, 1, 2, \ldots)$ where $(a, b) = 1$, contains infinitely many pseudoprimes (that is to say, pseudoprimes for the base 2). In the present note we prove that

THEOREM. *Every arithmetic progression* $ax+b$ $(x = 0, 1, 2, \ldots)$, *where* a, b *are relatively prime integers, contains an infinite number of odd* (*composite*) *strong pseudoprimes for each base* $C \geqslant 2$.

One might ask whether the restriction $(a, b) = 1$ is necessary. Our present method certainly does not allow us to nominate a given prime divisor for a strong pseudoprime and it can be shown quite readily (again see Pomerance *et al.* (1979)) that if $(a, b) \neq 1$ then not every such arithmetic progression can contain pseudoprimes.

2.

For each positive integer n we denote by $\Phi_n(X)$ the nth cyclotomic polynomial

$$\Phi_n(X) = \prod_{d \mid n} (X^d - 1)^{\mu(n/d)},$$

https://doi.org/10.1017/S1446788700021315 Published online by Cambridge University Press

where μ is the Möbius function. It will be convenient to write

$$\Phi(C; n) = \Phi_n(C).$$

It is easy to see that $\Phi(C; n) > 1$ for $C \geqslant 2$ and $n > 1$. For we have

$$\Phi(C; n) = \prod_{(m,n)=1} (C - \zeta_n^m)$$

where ζ_n is a primitive nth root of unity and the product is over the $\varphi(n)$ integers m with $1 \leqslant m < n$ and $(m, n) = 1$. But for each such m we have $|C - \zeta_n^m| > 1$ whence our assertion.

A prime factor p of $C^n - 1$ is said to be *primitive* if it does not divide any of the numbers $C^m - 1$, $m = 1, 2, \ldots, n-1$. The following result is well known.

LEMMA 1. *Denote by $r = r(n)$ the largest prime factor of n. If $r \nmid \Phi(C; n)$ then every prime dividing $\Phi(C; n)$ is a primitive prime divisor of $C^n - 1$, and is $\equiv 1 \pmod{n}$. If $r^k \| \Phi(C; n)$, $k \geqslant 1$ (which is to say $r^k \mid \Phi(C; n)$ but $r^{k+1} \nmid \Phi(C; n)$) then r is a primitive prime divisor of $C^{n/r^k} - 1$. If $n > 6$ then $C^n - 1$ has at least one primitive prime divisor.*

PROOF. See the proof of the theorem of Zsigmondy (1892); for example see Kanold (1950).

LEMMA 2. *If q is a prime such that $q^2 \| n$ and a is a natural number such that $a\varphi(a) \mid q - 1$ then $\Phi(C; n) \equiv 1 \pmod{a}$.*

PROOF. We have

$$\Phi(C; n) = \Phi(C; q^2(n/q^2)) = \prod_{d \mid n/q^2} [\Phi(C^d; q^2)]^{\mu(n/q^2 d)}.$$

Hence it certainly suffices to prove that $\Phi(g; q^2) \equiv 1 \pmod{a}$ for natural numbers g. We have

$$\Phi(g; q^2) - 1 = \frac{g^{q^2} - 1}{g^q - 1} - 1 = g^q(g^{q(q-1)} - 1)/(g^q - 1).$$

Suppose $p^m \mid a$ some prime p. If $p^k \mid g^q - 1$ then $p^m \mid q - 1$ implies that $p^{m+k} \mid g^{q(q-1)} - 1$. If $(p, g^q - 1) = 1$ and $(p, g) = 1$ then $\varphi(p^m) \mid q - 1$ and $p^m \mid g^{\varphi(p^m)} - 1$ implies $p^m \mid g^{q(q-1)} - 1$. Finally if $p \mid g$ then $p^m < q$ implies $p^m \mid g^q$. So in each case $p^m \mid (\Phi(g, q^2) - 1)$. This proves the lemma.

3. Proof of the theorem

If for each pair of integers a, b with $(a, b) = 1$ there is at least one strong pseudoprime for the base C of the shape $ax + b$, some natural number x, then there

are infinitely many such pseudoprimes. To see this just notice that we then have such pseudoprimes of the shape $adx+b$ for every natural number d with $(d,b)=1$, and we may choose d as large as we wish. This said, we may also suppose without loss of generality that a is even and b is odd. Thus we prove the theorem if we can produce a strong pseudoprime n for the base C with $n \equiv b \pmod{a}$.

Given a and b as described, with $2^\lambda \| b$, $\lambda \geqslant 1$ we commence our construction by choosing three distinct odd primes p_1, p_2, p_3 that are relatively prime to a. Furthermore we introduce two further primes q, with $q > p_i$ $(i = 1,2,3)$, and p which are to satisfy certain conditions we detail below. Firstly we require that

(a) $$2^\lambda p_1 p_2 p_3 q^2 \| p-1 \quad \text{and} \quad (C,p)=1.$$

Because p is prime it satisfies the condition (3); this is because ± 1 are the only square roots of 1 in a finite field, and $C^{p-1} \equiv 1 \pmod{p}$. So either

(4) $$C^{(p-1)/2^\lambda} \equiv 1 \pmod{p} \quad \text{or} \quad C^{(p-1)/2^\mu} \equiv -1 \pmod{p} \quad \text{some} \quad \mu, \quad 0 < \mu \leqslant \lambda.$$

Slightly different proofs will be required to deal with the two alternatives. However in either case we will construct q and p so that the number

$$n_i = p\Phi(C; (p-1)/2^\lambda p_i) \quad \text{or} \quad p\Phi(C; (p-1)/2^{\mu-1} p_i) \quad (i = 1,2,3)$$

is our required strong pseudoprime; here we take the first choice for n_i if the first alternative in (4) applies, and the second, with the appropriate μ, in the event that the second alternative in (4) applies. It will be convenient to write

$$m_i = n_i/p \quad (i = 1,2,3)$$

and to denote the integer $(p-1)/2^\lambda p_i$, respectively $(p-1)/2^{\mu-1} p_i$ by s_i $(i = 1,2,3)$. We note that by (a) certainly $s_i > 6$. Hence if p divides more than one of the m_i then by Lemma 1 we would have p a primitive prime factor of both $C^{s_i}-1$ and $C^{s_j}-1$ which is absurd if $s_i \neq s_j$. So we may suppose that p divides neither m_1 nor m_2, say. Now let r be the greatest prime factor of $p-1$. By (a) we have $r \geqslant q$ so $r > p_1, p_2$ and thus r *is the greatest prime divisor of both* s_1 and s_2. Again by Lemma 1, if r were to divide both m_1 and m_2 then r would be a primitive prime factor of both $C^{s_1/r^k}-1$ and $C^{s_2/r^k}-1$, where $r^k \| p-1$. But this is absurd, so without loss of generality r does not divide m_1. Then Lemma 1 implies that every prime factor of m_1 is congruent to 1 modulo s_1. So

(5) $$m_1 \equiv 1 \pmod{s_1}.$$

Certainly $q^2 \| s_1$. So if we insist that

(b) $$p_i(p_i-1) \mid q-1 \quad (i = 1,2,3)$$

then by Lemma 2 (recall that $\varphi(p) = p-1$) we have

(6) $$m_1 \equiv 1 \pmod{p_1}.$$

https://doi.org/10.1017/S1446788700021315 Published online by Cambridge University Press

In the same spirit, the requirement on q that

(c) $$2^{2\lambda+1} \mid q-1$$

implies by Lemma 2 (recall that $\varphi(2^{\lambda+1}) = 2^{\lambda}$) that

(7) $$m_1 \equiv 1 \pmod{2^{\lambda+1}}.$$

Recalling that, by (a), both $p_1 \| p-1$ and $2^{\lambda} \| p-1$ we can conclude from (5), (6) and (7) that

$$m_1 \equiv 1 \pmod{2(p-1)},$$

which is to say that

(8) $$n_1 = pm_1 = p(2(p-1)x+1) = (p-1)(2px+1)+1,$$

some positive integer x; x is positive because, with $C \geqslant 2$ and $s > 6$, certainly $\Phi(C; s) > 1$.

Now suppose that the first alternative in (4) applies. We have

$$\frac{n_1-1}{2^{\lambda}} = \frac{p-1}{2^{\lambda}}(2px+1),$$

so $(m_1, p) = 1$ and

$$m_1 = \Phi(C; (p-1)/2^{\lambda}p_1) \mid C^{(p-1)/2^{\lambda}p_1} - 1, \quad p \mid C^{(p-1)/2^{\lambda}} - 1$$

imply that

$$n_1 = p\Phi(C; (p-1)/2^{\lambda}p_1) \mid C^{(n_1-1)2^{\lambda}} - 1.$$

Hence n_1 is a strong pseudoprime for the base C.

If the second alternative in (4) applies we have, as before,

$$\frac{n_1-1}{2^{\mu}} = \frac{p-1}{2^{\mu}}(2px+1)$$

and we note that $2px+1$ is odd. Hence we have

$$m_1 = \Phi(C; (p-1)/2^{\mu-1}p_1) \mid C^{(p-1)/2^{\mu}p_1} + 1, \quad p \mid C^{(p-1)/2^{\mu}} + 1$$

which imply that

$$n_1 = p\Phi(C; (p-1)/2^{\mu-1}p_1) \mid C^{(n_1-1)2^{\mu}} + 1.$$

So also in this case n_1 is a strong pseudoprime for the base C.

It remains for us to show that the conditions (a), (b), (c) can be satisfied and that n_1 lies in the appropriate arithmetic progression. Accordingly apply the Chinese remainder theorem and Dirichlet's theorem on primes in arithmetic progressions to select a prime q with

$$p_1 p_2 p_3 (p_1-1)(p_2-1)(p_3-1) \mid q-1, \quad 2^{2\lambda} a\varphi(a) \mid q-1.$$

https://doi.org/10.1017/S1446788700021315 Published online by Cambridge University Press

This fixes (b) and (c) and automatically yields $q > p_i$ $(i = 1, 2, 3)$. Similarly we select a prime p so that $p > C$ and

$$p \equiv 1 + p_1 p_2 p_3 q^2 \pmod{p_1^2 p_2^2 p_3^2 q^3}, \quad p \equiv b \pmod{2^{\lambda+1} a}.$$

This successfully gives (a) because the moduli are relatively prime. These remarks conclude our proof, for we have $a\varphi(a) \mid q-1$ and $q^2 \| p-1$, so Lemma 2 yields $m_1 \equiv 1 \pmod{a}$. Hence

$$n_1 = pm_1 \equiv b \pmod{a},$$

as required.

References

R. D. Carmichael (1912), 'On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$', *Amer. Math. Monthly* **19**, 22–27.

H. J. Kanold (1950), (Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme', *J. für Math.* **187**, 169–172.

D. H. Lehmer (1976), 'Strong Carmichael numbers', *J. Austral. Math. Soc. Ser. A* **21**, 508–510.

D. E. Malm (1977), 'On Monte-Carlo primality tests', *Notices Amer. Math. Soc.* **24**, A-529, abstract 77T-A222.

Michael O. Rabin (1976), 'Probabilistic algorithms', in *Symposium on new directions and recent results in algorithms and complexity* (editor J. F. Traub) (Academic Press, New York), pp. 21–39.

Carl Pomerance, John L. Selfridge and Samuel S. Wagstaff Jr. (1979), 'The pseudoprimes to 25000000000' (preprint).

A. Rotkiewicz (1963), 'Surles nombres pseudopremiers de la forme $ax+b$', *C. R. Acad. Sci. Paris* **257**, 2601–2604.

A. Rotkiewicz (1967), 'On the pseudoprimes of the form $ax+b$', *Proc. Cambridge Phil. Soc.* **63**, 389–392.

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

A. J. van der Poorten
School of Mathematics and Physics
Macquarie University
North Ryde, N.S.W. 2113
Australia

A. Rotkiewicz
Instytut Matematyczmy PAN
ul. Sniadeckich 8
00-950 Warszawa
Poland

https://doi.org/10.1017/S1446788700021315 Published online by Cambridge University Press