ACTA ARITHMETICA
XLI (1982)

Pseudoprimes and a generalization of Artin's conjecture

by

SAMUEL S. WAGSTAFF, Jr. (Urbana, Ill.)

1. Introduction. One of many generalizations of Artin's conjecture is the following one proved by Lenstra [4], assuming the Generalized Riemann Hypothesis (GRH) to be stated later. If a is a rational number different from $-1, 0, 1$, and t is a positive integer, then the set of primes q for which a has residue index t modulo q has a relative density $A(a, t)$ in the set of all primes. For an integer a other than -1 or a perfect square, Hooley [3] expressed $A(a) = A(a, 1)$ as a product from which it is clear that $A(a) > 0$ for all such a. Lenstra used a clever device to determine when $A(a, t) = 0$ without actually computing product formulas for these densities. The main result of the present paper is a formula for $A(a, t)$ similar to that which Hooley gave for $A(a)$. We express $A(a, t)$ as a rational number times Artin's constant $A = \prod\big(1-1/(q(q-1))\big)$, where the product is over all primes q. See Wrench [7] for A to 45 decimal places.

An odd composite natural number n is a *pseudoprime to base* a if

$$a^{n-1} \equiv 1 \pmod{n}. \tag{1}$$

It is known [2] that for each integer $a > 1$ the pseudoprimes to base a are much rarer than primes, so that a large odd n which satisfies (1) for some $a > 1$ is very likely to be prime. One might expect that n which satisfy (1) for several different bases a are even more likely to be prime. We show that the increase in certainty that n is prime is not so great as one might guess, by deriving from the equation $\sum_{t=1}^{\infty} A(a, t) = 1$ a corollary which implies that pseudoprimes to a given base are more likely to satisfy (1) for many bases than a composite number which is not known to satisfy (1) at all.

A *Carmichael number* is an odd composite number n satisfying (1) for each integer a relatively prime to n. The paper concludes with a heuristic argument connecting the number of pseudoprimes to base a up to x to the number of Carmichael numbers up to x.

The author is indebted to Professors H. W. Lenstra, Jr., C. J. Moreno and C. Pomerance for helpful discussions related to this paper.

2. The main theorem. The letters p and q always represent primes. The greatest common divisor and least common multiple of a and b are written (a, b) and $[a, b]$. For $(a, p) = 1$, let $l_a(p)$ denote the least positive exponent l for which $a^l \equiv 1 \pmod p$. Then $l_a(p)$ divides $p-1$, and $l_a(p) = p-1$ if and only if a is a primitive root modulo p. For positive integers t and real numbers x let $N_{a,t}(x)$ be the number of primes $p \leqslant x$ for which $l_a(p) = (p-1)/t$.

Let φ and μ denote the functions of Euler and Möbius. We use $p^e \| h$ to mean $p^e | h$ but $p^{e+1} \nmid h$. Let $\pi(x)$ be the number of primes $\leqslant x$.

We will determine $A(a, t)$ in terms of a certain sum $S(h, t, m)$. The following lemma, which is proved in Section 4, expresses the sum as a rational number times Artin's constant defined in the Introduction. Define

$$g(t) = \frac{1}{t^2} \prod_{q|t} \frac{q^2-1}{q^2-q-1}.$$

LEMMA 2.1. *Let h, t, and m be positive integers. Write $M = m/(m, t)$ and $H = h/(Mt, h)$. Then*

$$S(h, t, m) \stackrel{\text{def}}{=} \sum_{\substack{k=1 \\ m|kt}}^{\infty} \frac{\mu(k)(kt, h)}{kt\varphi(kt)}$$

$$= \mu(M)(Mt, h)Ag(t) \prod_{q|(M,t)} \frac{1}{q^2-1} \prod_{\substack{q|M \\ q\nmid t}} \frac{1}{q^2-q-1} \prod_{\substack{q|(t,H) \\ q\nmid M}} \frac{q}{q+1} \prod_{\substack{q|H \\ q\nmid Mt}} \frac{q(q-2)}{q^2-q-1}.$$

When a is a non-zero rational, write $a = bc^2$, where c is a rational and b is a squarefree integer. Define $d(a) = b$ if $b \equiv 1 \pmod 4$, and $d(a) = 4b$ if $b \equiv 2$ or 3 (mo d4).

Let Q denote the field of rational numbers and let ζ_n be a primitive nth root of unity. Let GRH(a) be the statement that the Generalized Riemann Hypothesis holds for the Dedekind zeta function over Galois fields of the type $Q(\zeta_k, a^{1/k})$, where k is a positive integer. (Lenstra assumed a slightly weaker GRH.) We can now state our principal result.

THEOREM 2.2. *Let a be a rational $\neq -1, 0, 1$. Assume* GRH(a). *Write $a = \pm a_0^h$, where a_0 is positive and not an exact power of a rational. Let $2^e \| h$. Write $a_0 = a_1 a_2^2$, where a_1 is a squarefree integer and a_2 is a rational. If $a > 0$, set $n = [2^{e+1}, d(a_0)]$. For $a < 0$, define $n = 2a_1$ if $e = 0$ and $a_1 \equiv 3 \pmod 4$, or $e = 1$ and $a_1 \equiv 2 \pmod 4$; let $n = [2^{e+2}, d(a_0)]$ otherwise. Let t be any positive integer. Then $N_{a,t}(x) \sim A(a, t)\pi(x)$ as $x \to \infty$, where*

$$A(a, t) = S(h, t, 1) + S(h, t, n)$$

if $a > 0$ and

$$A(a, t) = S(h, t, 1) - \tfrac{1}{2}S(h, t, 2) + \tfrac{1}{2}S(h, t, 2^{e+1}) + S(h, t, n)$$

if $a < 0$. In particular, if $a > 0$ or $e = 0$, then

$$A(a, t) = (t, h)Ag(t) \prod_{q|(t,H')} \frac{q}{q+1} \prod_{\substack{q|H' \\ q\nmid t}} \frac{q(q-2)}{q^2-q-1} +$$

$$+\mu(M)(Mt, h)Ag(t) \prod_{q|(M,t)} \frac{1}{q^2-1} \prod_{\substack{q|M \\ q\nmid t}} \frac{1}{q^2-q-1} \prod_{\substack{q|(t,H) \\ q\nmid M}} \frac{q}{q+1} \prod_{\substack{q|H \\ q\nmid Mt}} \frac{q(q-2)}{q^2-q-1},$$

where

$$H' = h/(h, t), \quad M = n/(n, t) \quad \text{and} \quad H = h/(Mt, h).$$

Lenstra identified the conditions (8.9)–(8.13) of [4] under which $A(a, t)$ vanishes (assuming GRH(a)). It is easy to verify directly that our expression for $A(a, t)$ vanishes in each of Lenstra's cases, but it is tedious to check that these are the only cases in which it vanishes.

3. Examples. Let us compute $A(2, t)$. We have $a = 2$, $h = 1$, $e = 0$, $a_0 = a_1 = 2$, $d(a_0) = 8$, $n = 8$, and $M = 8/(8, t)$. If $4 \nmid t$, then $\mu(M) = 0$ and $A(2, t) = Ag(t)$. If $4 \| t$, then $\mu(M) = \mu(2) = -1$ and

$$A(2, t) = Ag(t)\big(1 - 1/(2^2-1)\big) = (2/3)Ag(t).$$

Finally, if $8 | t$, then $\mu(M) = \mu(1) = 1$ and $A(2, t) = 2Ag(t)$. We remark that empirical data for the odd primes below 100000 shows close agreement with these formulas. Table 1 gives $N_{2,t}(x)$, $N_{2,t}(x)/\pi(x)$, and $A(2, t)$ for $1 \leqslant t \leqslant 10$ and $x = 100000$.

TABLE 1

$x = 100000$, $\pi(x) = 9592$, $A = 0.3739558136\ldots$ is Artin's constant.

t	$N_{2,t}(x)$	$N_{2,t}(x)/\pi(x)$	$A(2, t)$
1	3603	0.37563	$A = 0.37396$
2	2726	0.28420	$3A/4 = 0.28047$
3	643	0.06704	$8A/45 = 0.06648$
4	460	0.04796	$A/8 = 0.04674$
5	166	0.01731	$24A/475 = 0.01889$
6	482	0.05025	$2A/15 = 0.04986$
7	90	0.00938	$48A/2009 = 0.00893$
8	347	0.03618	$3A/32 = 0.03506$
9	74	0.00771	$8A/405 = 0.00739$
10	118	0.01230	$18A/475 = 0.01417$

To compute $A(3, t)$, we find $M = 12/(12, t)$. If t is odd, then $A(3, t) = Ag(t)$. If $(12, t) = 2$, then $A(3, t) = (16/15)Ag(t)$. If $(12, t) = 4$, then $A(3,t) = (4/5)Ag(t)$. If $(12,t) = 6$, then $A(3,t) = (2/3)Ag(t)$. If $12\,|\,t$, then $A(3,t) = 2Ag(t)$.

The case of $A(4,t)$ is the first one with $h > 1$. We find $A(4,t) = 0$ when t is odd. This occurs because $4^{(p-1)/2} \equiv 2^{p-1} \equiv 1 \pmod p$, so that we cannot have $l_4(p) = (p-1)/t$ with t odd. We also have $A(4,t) = cAg(t)$, where $c = 2, 4/3$, or 4 according as $2\,\|\,t$, $4\,\|\,t$, or $8\,|\,t$.

Finally, we evaluate $A(-3,t)$. It equals $cAg(t)$, where $c = 6/5$, $4/5$, 0, or 2 when $(6,t) = 1, 2, 3$, or 6, respectively. The 0 in the third case is correct, for if $p \equiv 1 \pmod 3$, then the Legendre symbol $(-3\,|\,p) = +1$ and $(-3)^{(p-1)/2} \equiv 1 \pmod p$ by Euler's criterion.

4. Proof of the main theorem. We first prove Lemma 2.1. We will use the elementary fact that

$$\varphi(jk) = \varphi(j)\varphi\left(\frac{k}{(j,k)}\right)(j,k)$$

whenever j and k are positive integers and k is squarefree. Since $M = m/(m,t)$, we have

$$S(h,t,m) = \sum_{\substack{k=1\\ m|kt}}^{\infty} \frac{\mu(k)(kt,h)}{kt\varphi(kt)} = \sum_{k=1}^{\infty} \frac{\mu(Mk)(Mkt,h)}{Mkt\varphi(Mkt)}$$

$$= \frac{\mu(M)(Mt,h)}{Mt\varphi(Mt)} \sum_{\substack{k=1\\ (k,M)=1}}^{\infty} \frac{\mu(k)\left(k, \dfrac{h}{(Mt,h)}\right)}{k\varphi\left(\dfrac{k}{(Mt,k)}\right)(Mt,k)}.$$

Since the summand is a multiplicative function of k we have, using Euler's identity and writing $H = h/(Mt,h)$, that

$$S(h,t,m) = \frac{\mu(M)(Mt,h)}{Mt\varphi(Mt)} \prod_{\substack{q|t\\ q\nmid MH}} \frac{q^2-1}{q^2} \prod_{\substack{q|t\\ q\nmid M\\ q|H}} \frac{q-1}{q} \prod_{q\nmid MtH} \frac{q^2-q-1}{q(q-1)} \prod_{\substack{q|H\\ q\nmid Mt}} \frac{q-2}{q-1}$$

$$= \frac{\mu(M)(Mt,h)A}{Mt\varphi(Mt)} \prod_{\substack{q|t\\ q\nmid MH}} \frac{q^2-1}{q^2} \prod_{\substack{q|(t,H)\\ q\nmid M}} \frac{q-1}{q} \times$$

$$\times \prod_{q|MtH} \frac{q(q-1)}{q^2-q-1} \prod_{\substack{q|H\\ q\nmid Mt}} \frac{q-2}{q-1},$$

since $A = \prod_q (q^2-q-1)/(q^2-q)$. Now $\varphi(Mt) = Mt \prod_{q|Mt} (q-1)/q$. Without loss of generality, we may assume M is squarefree, so that $M^2 = \prod_{q|M} q^2$. Thus we have

$$S(h,t,m) = \frac{\mu(M)(Mt,h)A}{t^2} \prod_{q|t} \frac{q^2-1}{q^2-q-1} \prod_{q|(M,t)} \frac{1}{q^2-1} \times$$

$$\times \prod_{\substack{q|M\\ q\nmid t}} \frac{1}{q^2-q-1} \prod_{\substack{q|(t,H)\\ q\nmid M}} \frac{q}{q+1} \prod_{\substack{q|H\\ q\nmid Mt}} \frac{q(q-2)}{q^2-q-1},$$

which proves Lemma 2.1.

We need the following proposition to compute the degree of a Kummer extension in the proof of Theorem 2.2.

Proposition 4.1. *Let a be a rational $\neq -1, 0, 1$. Write $a = \pm a_0^h$, where a_0 is positive and not an exact power of a rational. Let K be a positive integer. Write $K' = K/(K,h)$ and $[Q(\zeta_K, a^{1/K}) : Q] = \varphi(K)K'/\varepsilon(K)$. If $a > 0$, we have $\varepsilon(K) = 2$ if K' is even and $d(a_0)\,|\,K$; otherwise $\varepsilon(K) = 1$. Now suppose $a < 0$. If K is odd, then $\varepsilon(K) = 1$. If K is even and K' is odd, then $\varepsilon(K) = \frac{1}{2}$. If K is even and $K' \equiv 2 \pmod 4$, then*

$$\varepsilon(K) = \begin{cases} 2 & \text{if } K \equiv 2 \pmod 4 \text{ and } d(-a_0)\,|\,K \\ & \text{or } K \equiv 4 \pmod 8 \text{ and } d(2a_0)\,|\,K, \\ 1 & \text{otherwise.} \end{cases}$$

If K is even and $4\,|\,K'$, then $\varepsilon(K) = 2$ if $d(a_0)\,|\,K$ and $\varepsilon(K) = 1$ if $d(a_0)\nmid K$.

Proof (sketch). From Kummer theory [1] the degree of the extension is $\varphi(K)L$, where L is the least positive integer for which a^L is a Kth power in $Q(\zeta_K)$. One may determine $L = K'/\varepsilon(K)$ in the various cases from Lemmas 3 and 4 of [6].

Proof of Theorem 2.2. Lenstra [4] has proved, assuming GRH(a), that $N_{a,t}(x) \sim A(a,t)\pi(x)$, where

$$A(a,t) = \sum_{k=1}^{\infty} \frac{\mu(k)}{[Q(\zeta_{kt}, a^{1/kt}) : Q]}.$$

A short calculation using Proposition 4.1 shows that if n is defined as in the statement of Theorem 2.2, we have for $a > 0$

$$\varepsilon(K) = \begin{cases} 2 & \text{if } n\,|\,K, \\ 1 & \text{if } n \nmid K \end{cases}$$

and for $a < 0$

$$\varepsilon(K) = \begin{cases} 2 & \text{if } n\,|\,K, \\ \frac{1}{2} & \text{if } 2\,|\,K \text{ and } 2^{e+1} \nmid K, \\ 1 & \text{otherwise.} \end{cases}$$

(There can be no conflict between the first two conditions because $2^{e+1}|n$.) Thus for $a > 0$ we have

$$A(a,t) = \sum_{k=1}^{\infty} \frac{\mu(k)(kt,h)\varepsilon(kt)}{kt\varphi(kt)}$$
$$= \sum_{\substack{k=1\\ n\nmid kt}}^{\infty} \frac{\mu(k)(kt,h)}{kt\varphi(kt)} + 2\sum_{\substack{k=1\\ n|kt}}^{\infty} \frac{\mu(k)(kt,h)}{kt\varphi(kt)}$$
$$= \sum_{k=1}^{\infty} \frac{\mu(k)(kt,h)}{kt\varphi(kt)} + \sum_{\substack{k=1\\ n|kt}}^{\infty} \frac{\mu(k)(kt,h)}{kt\varphi(kt)}$$
$$= S(h,t,1) + S(h,t,n).$$

The equation for $a < 0$ is proved similarly.

5. Pseudoprimes. In the proof of Theorem 5.1 we will need the equality $\sum_{t=1}^{\infty} A(a,t) = 1$ for each $a \neq -1, 0, 1$. For natural numbers t let $\tau(t) = \sum_{d|t} 1$ and $f(t) = [Q(\zeta_t, a^{1/t}):Q]^{-1}$. Then $\tau(t) = O(t^{\varepsilon})$, as $t \to \infty$, for every $\varepsilon > 0$. Also $f(t) \leqslant 2h/(t\varphi(t))$ by Proposition 4.1, so that $f(t) = O(t^{-2+\varepsilon})$. Thus $\sum_{t=1}^{\infty} f(t)\tau(t)$ converges. Therefore

$$\sum_{t=1}^{\infty} A(a,t) = \sum_{t=1}^{\infty}\sum_{k=1}^{\infty} \mu(k) f(kt)$$

is an absolutely convergent double sum which can be rearranged to

$$\sum_{K=1}^{\infty} f(K) \sum_{k|K} \mu(k) = f(1) = 1.$$

This proves the formula $\sum_{t=1}^{\infty} A(a,t) = 1$.

THEOREM 5.1. *For all $\varepsilon > 0$ and all integers a and b with $|a| > 1$ and $|b| > 1$, if GRH(a) and GRH(b) hold, then there is a K such that for all sufficiently large x, at least $(1-\varepsilon)\pi(x)$ primes $p \leqslant x$ satisfy $(l_a(p), l_b(p)) \geqslant (p-1)/K$.*

Proof. Let $\delta = \varepsilon/4$. Choose T so large that $\sum_{t=1}^{T} A(a,t) > 1-\delta$ and $\sum_{t=1}^{T} A(b,t) > 1-\delta$. Let $K = T^2$. Let x_0 be so large that for all $x \geqslant x_0$ we have

$$N_{a,t}(x) > (1-\delta)A(a,t)\pi(x) \quad \text{and} \quad N_{b,t}(x) > (1-\delta)A(b,t)\pi(x)$$

for $t = 1, 2, \ldots, T$. Then for all $x \geqslant x_0$ there are at least $(1-2\delta)\pi(x)$ primes $p \leqslant x$ for which $(p-1)/l_a(p) \leqslant T$ and likewise for $l_b(p)$. Hence, for all $x \geqslant x_0$ there are at least $(1-4\delta)\pi(x) = (1-\varepsilon)\pi(x)$ primes $p \leqslant x$ for which neither $(p-1)/l_a(p)$ nor $(p-1)/l_b(p)$ exceeds T. But for such primes p we must have $(l_a(p), l_b(p)) \geqslant (p-1)/T^2 = (p-1)/K$.

The significance of Theorem 5.1 is explained in [5], where it is noted that the theorem shows that when $l_a(p)|n-1$ is known, it is much easier to have $l_b(p)|n-1$ as well. Hence tests (1) for several bases are not a much more reliable test for the primality of n than a single test (1). Better tests for primality are discussed in [5].

6. The expected value of $(p-1)/l_a(p)$ for fixed a. Let a be a fixed integer with $|a| > 1$. We will show that $\sum_{t=1}^{\infty} tA(a,t)$ diverges, so that $(p-1)/l_a(p)$ does not have a mean value. However, we can estimate the rate at which this sum diverges.

THEOREM 6.1. *For each integer a with $|a| > 1$, there is a positive constant c_a such that $\sum_{t\leqslant T} tA(a,t) \sim c_a \log T$ as $T \to \infty$.*

The proof requires two lemmas. Recall that

$$g(t) = t^{-2}\prod_{q|t}(q^2-1)/(q^2-q-1).$$

LEMMA 6.2. *Let i and N be integers with $0 \leqslant i < N$. There is a positive constant $K(i,N)$ such that*

$$\sum_{\substack{t\leqslant T\\ t\equiv i\,(\mathrm{mod}\,N)}} tg(t) = K(i,N)\log T + O(1) \quad \textit{as } T \to \infty.$$

Proof. Note first that $(q^2-1)/(q^2-q-1) = 1+q/(q^2-q-1)$. Hence,

$$B(T) \stackrel{\text{def}}{=} \sum_{\substack{t\leqslant T\\ t\equiv i\,(\mathrm{mod}\,N)}} t^3 g(t) = \sum_{\substack{t\leqslant T\\ t\equiv i\,(\mathrm{mod}\,N)}} t \sum_{d|t} \frac{\mu^2(d)d}{\prod_{q|d}(q^2-q-1)}$$
$$= \sum_{\substack{cd\leqslant T\\ cd\equiv i\,(\mathrm{mod}\,N)}} \frac{cd^2\mu^2(d)}{\prod_{q|d}(q^2-q-1)} = \sum_{d\leqslant T} \frac{d^2\mu^2(d)}{\prod_{q|d}(q^2-q-1)} \sum_{\substack{c\leqslant T/d\\ cd\equiv i\,(\mathrm{mod}\,N)}} c.$$

Now the inner sum (on c) extends over initial segments of residue classes modulo N. Hence that sum is $K_d(T/d)^2 + O(T/d)$, where $0 \leqslant K_d \leqslant \frac{1}{2}$, K_d depends on N and i as well as on d, and $K_d > 0$ precisely when $(d,N)|i$. The implied constant in $O(T/d)$ does not depend on d. Thus

$$B(T) = T^2 \sum_{d\leqslant T} \frac{\mu^2(d)K_d}{\prod_{q|d}(q^2-q-1)} + O\Big(T\sum_{d\leqslant T} \frac{d\mu^2(d)}{\prod_{q|d}(q^2-q-1)}\Big).$$

For squarefree d we have $d^{1.5}/4 < \prod_{q|d} (q^2-q-1) \leqslant d^2$. Hence for each i and N,

$$\sum_{d=1}^{\infty} \frac{\mu^2(d)K_d}{\prod_{q|d}(q^2-q-1)} \tag{2}$$

converges to a positive number which we write $K(i, N)/2$. Thus

$$B(T) = T^2K(i, N)/2 + O\Big(T^2\sum_{d>T} d^{-1.5}\Big) + O\Big(T\sum_{d\leqslant T} d^{-1}\Big)$$
$$= T^2K(i, N)/2 + D(T),$$

where $D(T) = O(T^{1.5})$. We use a Stieltjes integration to complete the proof. Integration by parts gives

$$\sum_{\substack{t\leqslant T\\ t\equiv i\,(\mathrm{mod}\,N)}} tg(t) = \int_{1-}^{T} u^{-2}dB(u) = \frac{B(T)}{T^2} + 2\int_1^T B(u)u^{-3}du$$
$$= K(i, N)/2 + O(T^{-1/2}) + 2\int_1^T \frac{\big(u^2K(i, N)/2\big) + D(u)}{u^3}du$$
$$= K(i, N)\log T + K(i, N)/2 + 2\int_1^{\infty} D(u)u^{-3}du -$$
$$-2\int_T^{\infty} D(u)u^{-3}du + O(T^{-1/2})$$
$$= K(i, N)\log T + K(i, N)/2 + 2\int_1^{\infty} D(u)u^{-3}du + O(T^{-1/2}).$$

This proves Lemma 6.2.

LEMMA 6.3. *Let N be a positive integer. Let $\{B_i\}_{i=0}^{N-1}$ and $\{C_t\}_{t=1}^{\infty}$ be two sequences of non-negative real numbers. Assume not all B_i vanish. Suppose $C_t = tg(t)B_{t'}$ for every natural number t, where t' denotes the least non-negative residue of $t\,(\mathrm{mod}\,N)$. Then $\sum_{t\leqslant T} C_t \sim K\log T$ as $T\to\infty$, where $K = \sum_{i=0}^{N-1} B_i \times$ $\times K(i, N)$.*

Proof. We have

$$\sum_{t\leqslant T} C_t = \sum_{t\leqslant T} tg(t)B_{t'} = \sum_{i=0}^{N-1} B_i \sum_{\substack{t\leqslant T\\ t\equiv i\,(\mathrm{mod}\,N)}} tg(t)$$
$$= \sum_{i=0}^{N-1} B_i\big(K(i, N)\log T + O(1)\big) = \sum_{i=0}^{N-1} B_iK(i, N)\log T + O(1)$$

by Lemma 6.2. This proves Lemma 6.3.

Proof of Theorem 6.1. By Theorem 2.2 and Lemma 2.1, we know that $A(a, t)$ is a rational number times $Ag(t)$, and the rational number depends only on the residue class of t modulo $N = [n, h]$, with n and h as in Theorem 2.2. Hence there are non-negative constants $B_0, B_1, \ldots, B_{N-1}$, depending only on a, such that $tA(a, t) = tg(t)B_{t'}$, with t' as in Lemma 6.3. By that lemma, we have $\sum_{t\leqslant T} tA(a, t) \sim c_a\log T$ as $T\to\infty$, where $c_a = \sum_{i=0}^{N-1} B_iK(i, N)$. Since the $A(a, t)$ do not all vanish when $|a|>1$, at least one B_i is positive; therefore, c_a is positive. This completes the proof.

In a similar manner one can prove that for each integer a with $|a|>1$, there is a positive constant d_a such that

$$\sum_{t\leqslant T} \varphi(t)A(a, t) \sim d_a\log T \tag{3}$$

as $T\to\infty$. The difference in the proof is that

$$(1-1/q)(q^2-1)/(q^2-q-1) = 1+1/\big(q(q^2-q-1)\big),$$

so that the series replacing (2) converges more swiftly.

7. Speculations on pseudoprimes and Carmichael numbers. Let a be an integer $\neq -1, 0, 1$. We present a heuristic argument connecting the number $P'_a(x)$ of squarefree pseudoprimes to base a up to x to the number $C(x)$ of Carmichael numbers up to x. Every Carmichael number is squarefree.

For odd squarefree n, let $f(n)$ be the least common multiple of the numbers $p-1$ for $p|n$. When $(a, n) = 1$, let $l_a(n)$ be the least positive exponent l for which $a^l \equiv 1\,(\mathrm{mod}\,n)$. Then $l_a(n)|f(n)$. Let $N'_{a,t}(x)$ be the number of odd squarefree $n\leqslant x$ with $l_a(n) = f(n)/t$. By analogy to Theorem 2.2 and (3), suppose there are constants $A'(a, t)$ and $d'_a > 0$ so that $N'_{a,t}(x) \sim A'(a, t)x$ as $x\to\infty$ and $\sum_{t\leqslant T} \varphi(t)A'(a, t) \sim d'_a\log T$ as $T\to\infty$.

For most large n and most small t, t divides $f(n)$. Thus the number $D_t(x)$ of odd composite squarefree $n\leqslant x$ with $t|f(n)$ and $f(n)/t|n-1$ approximately equals the number $E_t(x)$ of odd composite squarefree $n\leqslant x$ with $f(n)|(n-1)t$. Now $D_1(x) = E_1(x) = C(x)$ because Carmichael numbers are odd squarefree n with $f(n)|n-1$. For $t\geqslant 1$ it is plausible that $E_t(x)$ is roughly proportional to t, at least for small t. Thus $D_t(x) \approx E_t(x) \approx tC(x)$. Let $C_t(x)$ be the number of odd composite squarefree $n\leqslant x$ with $t|f(n)$, $f(n)/t|n-1$ and if $1\leqslant s<t$, $s|t$, then $f(n)/s\nmid n-1$. An inclusion-exclusion argument gives $C_t(x) \approx \varphi(t)C(x)$ for small t.

Let $P_{a,t}(x)$ be the number of squarefree pseudoprimes $n\leqslant x$ to base a with $l_a(n) = f(n)/t$. Multiplication of probabilities gives $P_{a,t}(x) \approx C_t(x)N'_{a,t}(x)\pi^2/(4x)$, since $4/\pi^2$ is the density of the odd squarefree numbers. Using the hypothetical analogs of Theorem 2.2 and (3), we find

$$P'_a(x) \approx \sum_{t \leqslant x} P_{a,t}(x) \approx d''_a C(x) \log x \tag{4}$$

for some $d''_a > 0$. Our estimate for $C_t(x)$ should hold only for small t, but presumably the sum in (4) could be cut off at some point much less than x because those n with small $l_a(n)$ can be shown to be negligible. An approximate equality like (4) for $a = 2$ was noticed in [5].

Empirical data in [5] suggests that almost all pseudoprimes to base a are squarefree, that is $P_a(x) \sim P'_a(x)$ as $x \to \infty$, where $P_a(x)$ is the number of pseudoprimes to base a up to x. In a forthcoming paper, Pomerance shows that $P_2(x)/\log x$ is unbounded. From $P_2(x) \sim P'_2(x)$ and (4) it would follow that there are infinitely many Carmichael numbers.

References

[1] B. J. Birch, *Cyclotomic fields and Kummer extensions*, in: *Algebraic Number Theory* (*Proc. Instructional Conf., Brighton*, 1965), Thompson, Washington, D.C., 1967, pp. 85–93.

[2] P. Erdös, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), pp. 201–206.

[3] C. Hooley, *On Artin's Conjecture*, J. Reine Angew. Math. 225 (1967), pp. 209–220.

[4] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. 42 (1977), pp. 201–224.

[5] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. 35 (1980), pp. 1003–1026.

[6] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), pp. 161–168.

[7] J. W. Wrench, Jr., *Evaluation of Artin's constant and the twin-prime constant*, Math. Comp. 15 (1961), pp. 396–398.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
Urbana, Illinois, U.S.A.

Current address:
DEPARTMENT OF STATISTICS AND COMPUTER SCIENCE
UNIVERSITY OF GEORGIA
Athens, Georgia 30602, U.S.A.

Received on 8.11.1979
and in revised form on 30.5.1980 (1181)

ACTA ARITHMETICA
XLI (1982)

On the congruence $f(x^k) \equiv 0 \bmod q$, where q is a prime and f is a k-normal polynomial

by

J. Wójcik (Warszawa)

I proved in [4] the following

THEOREM A. *Let f be a polynomial with rational integral coefficients, irreducible, primitive, with a positive leading coefficient. Assume that f is different from x and is not a cyclotomic polynomial. There exists a positive integer $k_0 = k_0(f)$ such that for every positive integer k divisible by k_0 and for all positive integers D and r, where $(r, D) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many primes q satisfying the following condition: the congruence $f(x^k) \equiv 0 \bmod q$ is soluble, $q \equiv 1 \bmod k$, $q \equiv r \bmod D$. The Dirichlet density σ of this set of primes satisfies the inequality*

$$\frac{c(f)}{C(f) k \varphi([D,k])} \leqslant \sigma \leqslant \frac{n}{\varkappa} \frac{c(f)}{C(f)\varphi([D,k])},$$

where

$$\varkappa = \begin{cases} 1 & \text{if } f \text{ is not reciprocal,} \\ 2 & \text{if } f \text{ is reciprocal,} \end{cases} \qquad n \text{ is the degree of } f,$$

$c(f)$, $C(f)$ denote certain natural numbers depending on f.

The main aim of this paper is to prove a related theorem in the case of what we call a k-normal polynomial. Let K be an arbitrary field. A polynomial $f \in K[x]$ is called *weakly normal over* K if $K(a)$ is the splitting field of f for every root a of f (see [1]).

Let k be any positive integer. The polynomial $f \in K[x]$ is called *k-normal over* K if $f(x)$ is irreducible over K and $f(x^k)$ is weakly normal over $K(\zeta_k)$. Obviously the polynomial f is 1-normal if and only if it is normal. If the field K is fixed, we simply say that f is *k-normal.*

The definitions and notation are taken from [4]. In particular E_k is the group of rationals congruent to 1 mod k. We shall prove the following

THEOREM. *Let f be a polynomial with rational integral coefficients, irreducible, primitive, with a positive leading coefficient. Assume that f is*