ACTA ARITHMETICA
XIII (1968)

A gap theorem for pseudoprimes in arithmetic progressions

by

H. HALBERSTAM (Nottingham) and A. ROTKIEWICZ (Warszawa)

1. A composite natural number n is said to be a *pseudoprime* if $n|(2^n-2)$. There exist several ways of constructing such numbers, and from these it is possible to show that there exist infinitely many pseudoprimes; more precisely, that there exist at least[1] $c\log x$ pseudoprimes not exceeding x. In the opposite direction, Erdös [4] has proved that the number of pseudoprimes not exceeding x is at most $x\exp\{-c'(\log x \times \times \log\log x)^{1/2}\}$, and there is evidence to suggest that Erdös' estimate is much closer to the true order of magnitude. The tables suggest also that if $x > 170$, there is always a pseudoprime between x and $2x$; but at present all that is known is (Rotkiewicz [10]) that

(i) if m is an integer and $m > 19$, there is a pseudoprime between m and m^2;

(ii) given $\varepsilon > 0$, there is a pseudoprime between x and $x^{1+\varepsilon}$ provided $x > x_0(\varepsilon)$.

Actually one can do a little better than (ii) by using deep information about gaps between consecutive primes. For it is known that if $p > 5$, p prime, then $\frac{1}{3}(4^p-1)$ is a pseudoprime; also that there exists a number θ, $0 < \theta < 1$, such that the interval $(y, y+y^\theta)$ contains a prime, provided only that y is large enough. It follows at once that

there exists a pseudoprime between x and $x\exp\{c''(\log x)^\theta\}$ provided only that x is sufficiently large.

From the work of Ingham [7], $\theta = \frac{5}{8}$ represents a possible choice of θ; recent improvements in the estimation of $\zeta(\frac{1}{2}+it)$ (Haneke [6]) would allow us to take θ a little smaller.

Even less is known about the distribution of pseudoprimes in arithmetic progressions. Let a, b denote (here and throughout the rest of this paper) any fixed pair of coprime positive integers. Then Rotkiewicz ([11], [12]) has shown that the arithmetic progression $am+b$ $(m = 0, 1, 2, \ldots)$

[1] Throughout the paper $c, c', \ldots, c_1, c_2, \ldots$ denote positive constants.

contains an infinity of pseudoprimes. We now take matters a little further and establish the following gap result.

THEOREM 1. *Let a, b be fixed coprime positive integers. If $D>0$ is given and $x>x_0(a,D)$, there exists at least one pseudoprime P satisfying*

$$P\equiv b\pmod a,\qquad x<P<x\exp\left\{\frac{\log x}{(\log\log x)^D}\right\}.$$

The condition $(a,b)=1$ is somewhat artificial, because there do exist progressions $b\pmod a$ with $(a,b)>1$ that contain infinitely many pseudoprimes; for example, the fact that there exist infinitely many even pseudoprimes demonstrates this assertion for the progression $2\pmod 4$. Unfortunately it appears very difficult to formulate a more general condition on (a,b) which is likely to be sufficient to ensure an infinity of pseudoprimes $\equiv b\pmod a$.

The proof will be based on a combination of cyclotomy and sieve methods.

2. In this section cyclotomy is used to locate an infinite class of convenient pseudoprimes in the progression $b\pmod a$.

For any positive integer n, let $f_n(x)$ denote the nth cyclotomic polynomial defined by

$$f_n(x)=\prod_{d\mid n}(x^d-1)^{\mu(n/d)},\tag{2.1}$$

where μ is the Möbius function, and write

$$f_n=f_n(2).$$

It is easy to see that $f_n>1$ if $n>1$. For

$$f_n=\prod_{\substack{m=1\\(m,n)=1}}^{n}(2-\xi_n^m)$$

where ξ_n is a primitive nth root of unity, and for each m occuring in the product $|2-\xi_n^m|>1$ if $n>1$.

A prime factor of 2^n-1 is said to be *primitive* if it does not divide any of the numbers 2^m-1, $m=1,2,\dots,n-1$.

Denote by $r(n)$ the greatest prime factor of n. From the theorem of K. Zsigmondy (see [1], [2], [9], [13], [14], [15]) we have at once the following result.

LEMMA 1. *Every prime divisor of f_n, with the exception of $r(n)$ when $r(n)\mid f_n$, is $\equiv 1\pmod n$, and is a primitive prime divisor of 2^n-1. If $r(n)\mid f_n$ and* (2) *$r(n)^\alpha\| n$, then $r(n)$ is a primitive prime divisor of $2^{n/r(n)^\alpha}-1$.*

(2) $r^\alpha\| m$ means that $r^\alpha\mid m$ but $r^{\alpha+1}\nmid m$.

LEMMA 2. *If q is a prime such that $q^2\mid n$, then $f_n(2)=f_{n/q}(2^q)\equiv 1\pmod{2^q}$; if also $aq(a)\mid(q-1)$, then $f_n\equiv 1\pmod a$.*

This result was proved in [11] and [12].

We come to the main result of this section. We can assume without any loss of generality that a is even, and hence that b is odd.

LEMMA 3. *Let q, q_1 be any two distinct odd primes satisfying the conditions*

$$q_1\nmid a,\qquad q\equiv 1\pmod{aq_1\varphi(aq_1)},\tag{2.2}$$

and let m be any (odd) integer such that

$$m\equiv b\pmod a,\qquad m\equiv 1+q_1\pmod{q_1^2},\qquad m\equiv 1\pmod{q^2}.\tag{2.3}$$

If $p\equiv m\pmod{aq^2q_1^2}$, p prime, then one of the numbers

$$pf_{p-1},\ pf_{(p-1)/2},\ pf_{(p-1)/q_1}\tag{2.4}$$

is a pseudoprime $\equiv b\pmod a$.

Proof. It is clear from (2.2) that $(a,q_1)=(q_1,q)=(q,a)=1$, so that there does exist, by the Chinese Remainder Theorem, an integer m satisfying simultaneously the three congruences (2.3). Furthermore, such an integer m is necessarily coprime with $aq^2q_1^2$, so that, by Dirichlet's Theorem, there exist infinitely many primes $p\equiv m\pmod{aq^2q_1^2}$. Let p be such a prime.

We remark at the outset that, by (2.2), (2.3) and the second part of Lemma 2 applied in turn to $n=p-1,(p-1)/2$ and $(p-1)/q_1$, each of the three numbers $f_{p-1},f_{(p-1)/2},f_{(p-1)/q_1}$, is $\equiv 1\pmod a$ and hence each of the numbers (2.4) is $\equiv b\pmod a$; thus we need prove only that one of them is a pseudoprime.

Denote by r the largest prime factor $r(p-1)$ of $p-1$. Since $p\equiv 1\pmod{qq_1}$ by (2.3), we have $r\geqslant q>q_1\geqslant 3$, so that $r(p-1)=r\big((p-1)/2\big)=r\big((p-1)/q_1\big)=r$. We observe that r divides at most one of the three numbers $f_{(p-1)/t}$ ($t=1,2$ or q_1). For if $r^\alpha\|(p-1)$, then also $r^\alpha\|(p-1)/2$ and $r^\alpha\|(p-1)/q_1$; and if $r\mid f_{(p-1)/t}$, $r\mid f_{(p-1)/t'}$, where t, t' are distinct integers from among $1,2,q_1$, then r is, by Lemma 1, a *primitive* prime factor of both numbers $2^{(p-1)/(tr^\alpha)}-1$ and $2^{(p-1)/(t'r^\alpha)}-1$, a contradiction.

A similar (but simpler) argument based on Lemma 1 shows that any other prime, and p in particular, divides at most one of the three numbers $f_{(p-1)/t}$ ($t=1,2$ or q_1).

We now show that at least two of the three numbers $f_{(p-1)/t}$ ($t=1,2,q_1$) are $\equiv 1\pmod{p-1}$, and we use here the fact that at least two of these numbers are not divisible by r. If follows at once from Lemma 1 that

$$f_{(p-1)/t}\equiv 1\left(\mathrm{mod}\,\frac{p-1}{t}\right)\quad\text{if}\quad r\nmid f_{(p-1)/t};\tag{2.5}$$

in particular, taking $t=1$ gives that if $r \nmid f_{p-1}, f_{p-1} \equiv 1 \pmod{p-1}$. Next take $t = q_1$, and suppose that $r \nmid f_{(p-1)/q_1}$. Since $p \equiv 1 \pmod{q^2}$ we may, in view of (2.2), apply the second part of Lemma 2 with q_1 in place of a and $n = (p-1)/q_1$ to infer that $f_{(p-1)/q_1} \equiv 1 \pmod{q_1}$. From this and (2.5) with $t = q_1$ it follows, since $q_1 \nmid (p-1)/q_1$, that $f_{(p-1)/q_1} \equiv 1 \pmod{p-1}$.

It remains to consider $t = 2$, and here we assume for the time being that

$$p \not\equiv 1 \pmod 8. \tag{2.6}$$

Then, by the first part of Lemma 2 with $n = (p-1)/2$, $f_{(p-1)/2} \equiv 1 \pmod{2^q}$ and we note that, of course, $q \geqslant 3$. By (2.5) with $t = 2$ and (2.6) it follows that $f_{(p-1)/2} \equiv 1 \pmod{p-1}$ if $r \nmid f_{(p-1)/2}$, subject to the assumption (2.6).

We sum up this part of the argument: we have shown, subject to (2.6), that at least two of the numbers $f_{(p-1)/t}$ ($t = 1, 2$ or q_1) are $\equiv 1 \pmod{p-1}$. In view of an earlier remark about the divisibility of such numbers by p, it follows further that, subject to (2.6),

(2.7) *at least one of the numbers* $f_{(p-1)/t}$ $(t = 1, 2, q_1)$ *is coprime with* p *and* $\equiv 1 \pmod{p-1}$.

We may now remove the restriction (2.6). For if $p \equiv 1 \pmod 8$ then

$$p \mid (2^{\frac{1}{4}(p-1)} - 1),$$

and therefore, by Lemma 1, p divides neither of $f_{p-1}, f_{(p-1)/q_1}$. But we showed earlier that r cannot divide both these numbers, and hence that one of them is, unconditionally, $\equiv 1 \pmod{p-1}$. Thus (2.7) now holds without any restriction on p modulo 8.

It is now easy to complete the proof. Let $f_{(p-1)/t}$ be the number whose existence is asserted in (2.7). Since $f_n(x) \mid (x^n - 1)$, we see that $f_{(p-1)/t} \mid (2^{p-1} - 1)$; and since $p \nmid f_{(p-1)/t}$, we have seen that

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

But clearly $pf_{(p-1)/t} \equiv 1 \pmod{p-1}$, whence

$$pf_{(p-1)/t} \mid (2^{pf_{(p-1)/t}-1} - 1);$$

and this shows that $pf_{(p-1)/t}$ is a pseudoprime.

3. It is now necessary to appeal to sieve theory. The principal result of the section is Lemma 5 below, which appears to be of some independent interes.

LEMMA 4. *Let D be a positive number, and h, g a pair of coprime natural numbers. If $x > x_1(D, g)$, there exists a prime p such that*

$$x \leqslant p < x\bigl(1 + (\log x)^{-D}\bigr), \tag{3.1}$$

$$p \equiv h \pmod g, \tag{3.2}$$

$$\bigl(p-1, P_{2g}(x^{1/5})\bigr) = 1, \quad \text{where} \quad P_k(z) = \prod_{\substack{p<z \\ p \nmid k}} p. \tag{3.3}$$

The Lemma is a special case of Theorem I below. Theorem I is a generalization of the second part of Theorem 5 of Jurkat-Richert [8]; a proof of Theorem I and of other sieve results will be given in a forthcoming monograph on 'Sieve Methods' by Halberstam and Richert. (Paper [5], by Halberstam, Jurkat and Richert, is a preliminary announcement of these results; see, in particular, [5], Theorem 1.)

Theorem I relates to the following sieve problem: Let $\mathcal{A} = \{a_1, a_2, \ldots, a_N\}$ be a set of N natural numbers, k a natural number and z a real number $\geqslant 2$. Let $S_k(\mathcal{A}, z)$ denote the number of elements in $\mathcal{A}$ coprime with $P_k(z)$ (cf. (3.3)). Suppose there exist a multiplicative arithmetic function $\gamma(p)$ and a number $X > 1$ such that

$$1 \leqslant \gamma(p) < p, \tag{3.4}$$

$$\sum_{p \geqslant z} \frac{\gamma(p)-1}{p} = O\Bigl(\frac{1}{\log z}\Bigr), \tag{3.5}$$

$$\Bigl|\sum_{\substack{a \in \mathcal{A} \\ d \mid a}} 1 - \frac{\gamma(d)}{d} X\Bigr| \leqslant \eta(X, d) \quad \text{if} \quad (d, k) = 1, \tag{3.6}$$

where the error function $\eta(X, d)$ is small on average, in the following sense: there exists an absolute constant α, $0 < \alpha \leqslant 1$, and to any given number $C > \frac{15}{14}$ there corresponds a function $\beta(X)$ satisfying $0 < \beta(X) = O\bigl((\log X)^{1/2}\bigr)$, such that

$$\sum_{1 \leqslant d \leqslant X^{\alpha}/\beta(X)} \mu^2(d) 3^{\nu(d)} \eta(X, d) = O\Bigl(\frac{X}{(\log X)^C}\Bigr); \tag{3.7}$$

here $\nu(d)$ denotes the number of distinct prime factors of d. Then we have

THEOREM I. *Let*

$$\Gamma_k(z) = \prod_{\substack{p \nmid k \\ p < z}} \Bigl(1 - \frac{\gamma(p)}{p}\Bigr),$$

and define

$$f(u) = e^{\gamma}\{\omega(u) - \varrho(u)/u\}$$

where γ is Euler's constant and ω, ϱ are solutions of the (well-known) differential-difference equations

$$\omega(u) = \frac{1}{u}, \quad \varrho(u) = 1 \quad (0 < u \leqslant 2),$$

$$\{u\omega(u)\}' = \omega(u-1), \quad (u-1)\varrho'(u) = -\varrho(u-1) \quad (u \geqslant 2).$$

If $z \leqslant X$ and A is a sequence of the kind described above, then

$$S_k(A, z) \geqslant X\Gamma_k(z)\left\{f\left(\alpha\frac{\log X}{\log z}\right) - c_1\frac{\log\log 3k}{(\log X)^{1/14}}\right\}.$$

We shall need also the additional remark that f is monotonic increasing with u and that

$$f(u) = \begin{cases} 0, & 0 < u \leqslant 2, \\ \dfrac{2e^{\gamma}}{u}\log(u-1), & 2 \leqslant u \leqslant 4. \end{cases}$$

To apply Theorem I to Lemma 4 we take

$$A = \left\{p-1;\ x < p \leqslant x\left(1+\frac{1}{(\log x)^D}\right),\ p \equiv h \pmod g\right\},$$

$$k = 2g, \quad \gamma(d) = d/\varphi(d), \quad z = x^{1/5}$$

and

$$X = \frac{1}{\varphi(g)}\left\{\mathrm{li}\left(x+\frac{x}{(\log x)^D}\right) - \mathrm{li}\,x\right\};$$

we may take

$$\eta(X, d) = 2\max_{y \leqslant x+x(\log x)^{-D}} \max_{\substack{1 \leqslant l \leqslant dg \\ (l, dg)=1}} \left|\pi(y; dg, l) - \frac{\mathrm{li}\,y}{\varphi(dg)}\right|,$$

where $\pi(y; m, l)$ denotes the number of primes not exceeding y that are $\equiv l \pmod m$. With these choices, conditions (3.4), (3.5) and (3.6) are satisfied. It remains to check (3.7). By Bombieri's Theorem ([3], theorem 4) there exists a positive constant $B = B(C)$ such that

$$\sum_{1 \leqslant m \leqslant M} \max_{y \leqslant Y} \max_{\substack{1 \leqslant l \leqslant m \\ (l, m)=1}} \left|\pi(y; m, l) - \frac{\mathrm{li}\,y}{\varphi(m)}\right| = O\left(\frac{Y}{(\log Y)^{2C+D+11}}\right)$$

provided only that

$$M \leqslant Y^{1/2}(\log Y)^{-B}. \tag{3.8}$$

To apply this result we take $Y = x + x(\log x)^{-D}$, $\alpha = \frac{1}{2}$, $\beta(X) = (\log X)^B$, $M = gX^{1/2}(\log X)^{-B}$, and note that

$$\frac{1}{\varphi(g)} \cdot \frac{x}{(\log x)^{D+1}}\left(1 - \frac{1}{\log x}\right) \leqslant X \leqslant \frac{1}{\varphi(g)} \cdot \frac{x}{(\log x)^{D+1}}. \tag{3.9}$$

By (3.9), M satisfies (3.8), and

$$Y(\log Y)^{-2C-D-11} = O\left(X(\log X)^{-2C-10}\right).$$

From here on it is an easy calculation, using Cauchy's inequality, to show that (3.7) is satisfied with $\alpha = \frac{1}{2}$. (It is perhaps worth remarking that our argument can be made uniform with respect to g if $g < (\log x)^{c_2}$.) Hence, by Theorem I, the number S of primes of the kind required in Lemma 4 satisfies

$$S \geqslant \frac{1}{\varphi(g)} \cdot \frac{x}{(\log x)^{D+1}}\left(1 - \frac{1}{\log x}\right) \times \\ \times \prod_{\substack{p \nmid 2g \\ p < x^{1/5}}} \left(1 - \frac{1}{p-1}\right)\left\{f\left(\frac{5}{2} \cdot \frac{\log X}{\log x}\right) - c_1\frac{\log\log 6g}{(\log X)^{1/14}}\right\}$$

provided x is large enough. By (3.9), $\log X \geqslant \frac{9}{10}\log x$ and hence

$$f\left(\frac{5}{2} \cdot \frac{\log X}{\log x}\right) > f\left(\frac{9}{4}\right) = \frac{8}{9}e^{\gamma}\log\frac{5}{4}$$

if x is sufficiently large. By the well-known theorem of Mertens

$$\prod_{p < x^{1/5}}\left(1 - \frac{1}{p-1}\right) > \prod_{p < x^{1/5}}\left(1 - \frac{1}{p}\right) \sim \frac{5e^{-\gamma}}{\log x} \quad (x \to \infty).$$

We may therefore conclude that there exists a constant $x_1(D, g)$ such that

$$S \geqslant (4\log\tfrac{5}{4})\frac{1}{\varphi(g)} \prod_{\substack{p \mid g \\ p > 2}} \frac{p-1}{p-2} \cdot \frac{x}{(\log x)^{D+2}}, \quad x \geqslant x_1; \tag{3.10}$$

and this is much more than was required to prove Lemma 4.

Lemma 5. *Let $(h, g) = 1$. For each $x > x_1(D, g)$ there exists a prime p satisfying* (3.1) *and* (3.2) *such that*

$$c_3(1 - 4x^{-1/5}) \leqslant \frac{\varphi(p-1)}{p-1} \leqslant c_3, \quad c_3 = \frac{\varphi\big(2(g, h-1)\big)}{2(g, h-1)}.$$

Proof. Let p be a prime of the kind described in Lemma 4; by (3.10) there are many such primes. Any prime dividing both $2g$ and $p-1$ also divides $2(g, h-1)$, since $p-1 \equiv h-1 \pmod g$; conversely, any prime

factor of $2(g, h-1)$ divides $p-1$. Thus every prime factor of $p-1$ that does not divide $2(g, h-1)$ is at least $x^{1/5}$, and there are clearly at most *four* such prime factors. Hence

$$\frac{\varphi(p-1)}{p-1} = \frac{\varphi(2(g,h-1))}{2(g,h-1)} \prod_{\substack{p' \mid (p-1) \\ p' \geqslant x^{1/5}}} \left(1-\frac{1}{p'}\right) \geqslant c_3(1-x^{-1/5})^4 > c_3(1-4x^{-1/5}),$$

and

$$\frac{\varphi(p-1)}{p-1} \leqslant c_3$$

follows trivially.

LEMMA 6. *If* $(h, g) = 1$ *and* $x \geqslant x_1(D, g)$ *there exists a prime* $p \equiv h \pmod g$ *such that*

$$x \leqslant \varphi(p-1) \leqslant x\left(1+\frac{2}{(\log x)^D}\right).$$

Proof. Let p be a prime whose existence was established in Lemma 5. Then

$$c_3(x-1)(1-4x^{-1/5}) \leqslant \varphi(p-1) \leqslant c_3 x\left(1+\frac{1}{(\log x)^D}\right).$$

We let $y = c_3(x-1)(1-4x^{-1/5})$, so that $y < x$, and obtain

$$y \leqslant \varphi(p-1) \leqslant y\left(1+\frac{2}{(\log y)^D}\right);$$

the result follows on replacing y by x.

LEMMA 7. *Let* q' *be a fixed prime, and* h *an integer such that* $(h, q'g) = 1$ *and* $h \equiv 1 \pmod{q'}$. *If* x *is large enough, there exists a prime* p *such that* $p \equiv h \pmod{q'g}$ *and*

$$x \leqslant \varphi\left(\frac{p-1}{q'}\right) \leqslant x\left(1+\frac{2}{(\log x)^D}\right).$$

Proof. Apply Lemma 6 with gq' in place of g to obtain inequalities for $\varphi(p-1)$. Since

$$\varphi\left(\frac{p-1}{q'}\right) = \frac{\varphi(p-1)}{q'} \quad \text{or} \quad \frac{\varphi(p-1)}{q'-1},$$

the result follows, by the argument used in the proof of Lemma 6, on taking $y = x/q'$ or $x/(q'-1)$ respectively.

4. We combine the results of sections 2 and 3 by means of the following simple remark.

LEMMA 8. *If* n *is a natural number* >1 *and* $\nu(n) = k$,

$$2^{\varphi(n)-2^{k-1}} < f_n < 2^{\varphi(n)+2^{k-1}}.$$

Proof. Since $n > 1$, $\sum_{d \mid n} \mu(n/d) = 0$, whence

$$\sum_{\substack{d \mid n \\ \mu(n/d)=1}} 1 = \sum_{\substack{d \mid n \\ \mu(n/d)=-1}} 1 = \tfrac{1}{2} \cdot 2^{\nu(n)}.$$

It follows that

$$f_n = \prod_{d \mid n} (2^d-1)^{\mu(n/d)} = \frac{\prod_{d \mid n, \mu(n/d)=1} (2^d-1)}{\prod_{d \mid n, \mu(n/d)=-1} (2^d-1)} > \frac{\prod_{d \mid n, \mu(n/d)=1} \frac{1}{2} \cdot 2^d}{\prod_{d \mid n, \mu(n/d)=-1} 2^d} = 2^{\varphi(n)-2^{k-1}}$$

on writing $\nu(n) = k$. This proves the left hand inequality, and the right hand inequality is derived in the same manner.

It is now clear what we have to do to complete the proof of Theorem 1. Let q, q_1 be two odd, distinct primes satisfying (2.2), and m an integer satisfying (2.3); we keep these three numbers fixed. By Lemma 3 any prime $p \equiv m \pmod{aq^2q_1^2}$ is such that one of the integers pf_{p-1}, $pf_{(p-1)/2}$, $pf_{(p-1)/q_1}$ is a pseudoprime $\equiv b \pmod a$. If now we choose x large enough, Lemma 6 and Lemma 7 (with $q' = 2$ or q_1) imply that p can be chosen to satisfy also each of the three pairs of inequalities

$$x \leqslant \varphi\left(\frac{p-1}{t}\right) \leqslant x\left(1+\frac{2}{(\log x)^D}\right) \quad (t = 1, 2, q_1); \tag{4.1}$$

we have to take $g = aq^2q_1^2$ in Lemma 6 (the case $t = 1$) or we take $g = aq^2q_1$ in Lemma 7 when $t = q_1$ and $g = \frac{1}{2}aq^2q_1^2$ when $t = 2$. In fact, we shall choose $x_2 = x_2(D, a, q, q_1)$ so large that for $x \geqslant x_2$, p satisfies in addition the two conditions

$$p < 2^{\frac{1}{2}x(\log x)^{-D}}, \quad 2^{\nu(p-1)} < \frac{x}{(\log x)^D}. \tag{4.2}$$

Actually, $\varphi(p-1) < 2x$ implies that $p = O(x \log\log x)$, so that the first of these conditions is easily satisfied; and the second follows at once from the well-known fact that $2^{\nu(n)} = O(n^{1/2})$ for every natural number n. Thus in particular, $2^{\nu(p-1)} = O(p^{1/2}) = O\{x^{1/2}(\log\log x)^{1/2}\}$.

We now suppose that $x \geqslant x_2$ and apply Lemma 8 with $n = (p-1)/t_0$, where t_0 $(= 1, 2$ or $q_1)$ is such that $pf_{(p-1)/t_0}$ is a pseudoprime. Then, by (4.1) and (4.2),

$$pf_{(p-1)/t_0} > 2^{\varphi((p-1)/t_0)-2^{k-1}} > 2^{x-\frac{1}{2}x(\log x)^{-D}}$$

and

$$pf_{(p-1)/t_0} < p2^{x(1+2(\log x)^{-D})+\frac{1}{2}x(\log x)^{-D}} < 2^{x(1+3(\log x)^{-D})}.$$

If now we set $y = 2^{x-\frac{1}{2}x(\log x)^{-D}}$, so that $y < e^x$ and therefore $\log x > \log\log y$, we obtain easily that

$$y < pf_{(p-1)/t_0} < y^{1+5(\log\log y)^{-D}};$$

this completes the proof of Theorem 1.

References

[1] A. S. Bang, *Taltheoretiske Undersogelser*, Tidsskrift for Math. 4 (1886), pp. 70-80, 130-137.

[2] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* a^n-b^n, Ann. of Math. (2), 5 (1904), pp. 173-180.

[3] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), pp. 201-225.

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

[5] H. Halberstam, W. B. Jurkat and H.-E. Richert, *Un nouveau résultat de la méthode du crible*, C. R. Acad. Sci. Paris, 264 (1967), pp. 920-923.

[6] W. Haneke, *Verschärfung der Abschätzung von* $\zeta(\frac{1}{2}+it)$, Acta Arith. 8 (1962/63), pp. 357-430.

[7] A. E. Ingham, *On the difference between consecutive primes*, Quart. J. Math. 8 (1937), pp. 255-266.

[8] W. B. Jurkat and H.-E. Richert, *An improvement of Selberg's sieve method I*, Acta Arith. 11 (1965), pp. 215-240.

[9] H. J. Kanold, *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme*, Journal für Math. 187 (1950), pp. 169-172.

[10] A. Rotkiewicz, *Les intervalles contenants les nombres pseudopremiers*, Rend. Circ. Mat. Palermo 14 (1965), pp. 278-280.

[11] — *Sur les nombres pseudopremiers de la forme* $ax+b$, C. R. Acad. Sci. Paris 257 (1963), 2601-2604.

[12] — *On the pseudoprimes of the form* $ax+b$, Proc. Cambridge Phil. Soc. 63 (1967), pp. 389-392.

[13] — *Elementarny dowód istnienia dzielnika pierwszego pierwolnego liczby* a^n-b^n, Prace Mat. 4 (1960), pp. 21-28.

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

[15] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), pp. 265-284.

UNIVERSITY OF NOTTINGHAM
INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES
UNIVERSITY OF CAMBRIDGE

Reçu par la Rédaction le 8. 3. 1967

ACTA ARITHMETICA
XIII (1968)

Zur Anzahl Abelscher Gruppen gegebener Ordnung II

von

PETER GEORG SCHMIDT (Marburg)

Einleitung[1]. $A(x)$ sei die Anzahl der wesentlich verschiedenen Abelschen Gruppen, deren Ordnung x nicht übersteigt, und $\Delta(x)$ das Restglied in der asymptotischen Entwicklung

$$A(x) = A_1 x + A_2 x^{1/2} + A_3 x^{1/3} + \Delta(x)$$

mit

$$A_\mu := \prod_{\substack{\nu=1 \\ \nu \neq \mu}}^{\infty} \zeta\left(\frac{\nu}{\mu}\right) \qquad (\mu = 1, 2, 3).$$

Ist ϑ die untere Grenze aller θ, für die

$$\Delta(x) \ll x^\theta \qquad (x \to \infty)$$

gilt, so zeigten[1] P. Erdös und G. Szekeres, D. G. Kendall und R. A. Rankin, H. E. Richert, W. Schwarz, der Verfasser

$$\vartheta \leqslant 1/2,\ 1/3,\ 3/10,\ 20/69 \approx 0.29, \qquad 5/18 = 0.2\dot{7}\ldots$$

In dieser Arbeit soll $\vartheta \leqslant 7/27 = 0.\overline{259}\ldots$ oder genauer

$$\Delta(x) \ll x^{7/27}\log^2 x \qquad (x \to \infty) \tag{1}$$

bewiesen werden.

Nach Hilfssatz 1 genügt es, letztere Ungleichung für das dort erklärte Restglied $\Delta_3(x)$ zu zeigen. Ausgangspunkt sei daher unsere in [3], § 1 gegebene Darstellung der Funktion $\Delta_3(x)$ durch gewisse Doppelsummen (Hilfssatz 2), zu deren Abschätzung die van der Corput-Methode (Hilfssätze 3-6) herangezogen wird. In unserem Falle beruht die van der Corput-Methode vornehmlich auf der wiederholten Transformation gewisser Exponentialdoppelsummen vermöge „Weylscher" und „van der Corputscher Schritte" (Hilfssätze 4 und 5), wobei sowohl die Schrittfolge

---

[1] Ausführlicheres, insbesondere weitere Literatur, findet sich in [3], Einleitung.