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 \( n \mid (2^n - 2) \). 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\(^{(1)} \) \( \log x \) pseudoprimes not exceeding \( x \). In the opposite direction, Erdős [4] has proved that the number of pseudoprimes not exceeding \( x \) is at most \( x \exp\left(-c'(\log x \times x \log \log x)^\theta\right) \), and there is evidence to suggest that Erdős’ 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 \( p(p+1) \) is a pseudoprime; also that there exists a number \( \theta \), \( 0 < \theta < 1 \), such that the interval \( (y, y+\theta y^\theta) \) contains a prime, provided only that \( y \) is large enough. It follows at once that

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

From the work of Ingham [7], \( \theta = \frac{1}{4} \) represents a possible choice of \( \theta \); recent improvements in the estimation of \( \zeta(1/2+it) \) (Hankel [6]) would allow us to take \( \theta \) 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 \( a > \exp \left( \frac{\log a}{\log \log a}^{\frac{1}{2}} \right) \), there exist at least one pseudoprime \( P \) satisfying

\[ P = b(\mod a), \quad x < P < x \exp \left( \frac{\log x}{\log \log x}^{\frac{1}{2}} \right) \]

The condition \( (a, b) = 1 \) is somewhat artificial, because there do exist progressions \( b(\mod a) \) 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 \( b(\mod a) \).

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 \( b(\mod a) \).

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

\[ f_n(x) = \prod_{\mu} (x^{\phi(n)/\mu} - 1) \]

where \( \mu \) is the Möbius function, and write

\[ f_n = f_n(2) \]

It is easy to see that \( f_n > 1 \) if \( n > 1 \). For

\[ f_n = \prod_{\mu|n} (2 - x^{\mu}) \]

where \( f_n \) is a primitive \( \mu \)th root of unity, and for each \( \mu \) occurring in the product \( \prod_{\mu|n} (2 - x^{\mu}) > 1 \) if \( n > 1 \).

A prime factor of \( 2^n - 1 \) is said to be primitive if it does not divide any of the numbers \( 2^{n-1} - 1, \ldots, 2^{n-1} - 1 \).

Denote by \( r(n) \) the greatest primitive 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 divisor of \( f_n(x) \), with the exception of \( x \) when \( \operatorname{rad}(n) \) divides \( f_n(x) \), and is a primitive prime divisor of \( 2^{n-1} - 1 \). If \( \operatorname{rad}(n) \) divides \( f_n(x) \), and \( \operatorname{rad}(n) \) divides \( 2^{n-1} - 1 \), \( \operatorname{rad}(n) \) is a primitive prime divisor of \( 2^{n-1} - 1 \).

\( (\ast) \) \( \operatorname{rad}(n) \) means that \( \operatorname{rad}(n) \) but \( \operatorname{rad}(n) \).

**Lemma 2.** If \( q \) is a prime such that \( q \nmid n \), then \( f_n(2) = f_n(2^q) = 1 \mod(2^q) \); if also \( \operatorname{rad}(q)(q-1), \) then \( f_n = 1 \mod q(\mod 2^q) \).

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

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

**Lemma 3.** Let \( q_1, q_2 \) be any two distinct odd primes satisfying the conditions

\[ q_1, q_2, \quad q = 1 \mod(2q_1q_2) \]

and let \( m \) be any (odd) integer such that

\[ m = b(\mod a), \quad m = q_1(\mod q_2), \quad m = 1(\mod q_2) \]

If \( p = m(\mod 2q_2) \), \( p \) prime, then one of the numbers

\[ \mathcal{P}_{p-1}, \mathcal{P}_{p-\frac{p-1}{2}}, \mathcal{P}_{p-\frac{p-1}{4}} \]

is a pseudoprime \( = b(\mod a) \).

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 \( aq_1q_2 \), so that, by Dirichlet’s Theorem, there exist infinitely many primes \( p = m(\mod 2q_2) \). 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 \( (p-1)/4 \), each of the three numbers \( f_{p-1}, f_{p-\frac{p-1}{2}}, f_{p-\frac{p-1}{4}} \), is \( 1(\mod a) \) and hence each of the numbers (2.4) is \( b(\mod a) \); thus we need prove only that one of them is a pseudoprime.

Denote by \( r \) the largest prime factor of \( (p-1)/2 \). Since \( p = 1(\mod 4) \) by (2.3), we have \( r > g > g_2 > 3 \), so that \( r(p-1) = r(p-1)/2 = r(p-1)/(p)/r = r \). We observe that \( r \) divides at most one of the three numbers \( f_{p-1}, f_{p-\frac{p-1}{2}}, f_{p-\frac{p-1}{4}} \). If \( r \nmid (p-1), \) then also \( r \nmid (p-1)/2 \) and \( r \nmid (p-1)/4 \); and if \( r \mid (p-1)/2, \) \( r \mid (p-1)/4 \), where \( t, t' \) distinct integers from among 1, 2, 4, then \( r \) is, by Lemma 1, a primitive prime factor of both numbers \( 2^{p-1}/r - 1 \) and \( 2^{p-1}/t - 1 \), 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 \( f_{p-1}, f_{p-\frac{p-1}{2}}, f_{p-\frac{p-1}{4}} \).

We now show that at least two of the three numbers \( f_{p-1}, f_{p-\frac{p-1}{2}}, f_{p-\frac{p-1}{4}} \) are \( 1(\mod p-1) \), 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

\[ f_{p-1}/r = 1(\mod p-1)/r \]

\[ r \nmid f_{p-1}/r \]
in particular, taking \( t = 1 \) gives that \( r \not\equiv f_{p - 1} \equiv 1 \pmod{p - 1} \). Next take \( t = q_1 \), and suppose that \( r \not\equiv f_{p - 1} \equiv 1 \pmod{q_1} \). Since \( p = 1 \pmod{q_1^2} \) we may, in view of (2.2), apply the second part of Lemma 2 with \( q_1 \) in place of \( q \) and \( n = (p - 1)/q_1 \) to infer that \( f_{p - 1} \equiv 1 \pmod{q_1} \). From this and (2.5) with \( t = q_1 \), it follows, since \( q_1 \not\equiv (p - 1)/q_1 \pmod{q_1} \), that \( f_{p - 1} \equiv 1 \pmod{p - 1} \).

It remains to consider \( t = 2 \) and here we assume for the time being that

\[
p \not\equiv 1 \pmod{8}.
\]

Then, by the first part of Lemma 2 with \( n = (p - 1)/2 \), \( f_{p - 1} \equiv 1 \pmod{2^b} \) and we note that, of course, \( q \not\equiv 3 \). By (2.5) with \( t = 2 \) and (3.6) it follows that \( f_{p - 1} \equiv 1 \pmod{p - 1} \) if \( r \not\equiv f_{p - 1} \equiv 1 \pmod{p - 1} \) subject to the assumption (3.6).

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

\[
(2.7) \quad \text{at least one of the numbers } f_{p - 1} \text{ is coprime with } p, \quad \text{and } 1 \equiv 1 \pmod{p - 1}.
\]

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

\[
p \equiv (2^{p - 1} - 1),
\]

and therefore, by Lemma 1, \( p \) divides neither of \( f_{p - 1}, f_{p - 2} \). But we showed earlier that \( r \) cannot divide both these numbers, and hence that one of them is, unconditionally, \( 1 \pmod{p - 1} \). Thus (2.7) now holds without any restriction on \( p \) modulo 8.

It is now easy to complete the proof. Let \( f_{p - 1} \) be the number whose existence is asserted in (2.7). Since \( f_{p - 1}(x^2 - 1) \), we see that \( f_{p - 1} \equiv (2^{p - 1} - 1); \) and since \( p \not\equiv f_{p - 1} \equiv 1 \pmod{p - 1} \), we have seen that

\[
f_{p - 1} \equiv (2^{p - 1} - 1).
\]

But clearly \( f_{p - 1} \equiv 1 \pmod{p - 1} \), whence

\[
f_{p - 1} \equiv (2^{p - 1} - 1) \pmod{p - 1} \;
\]

and this shows that \( p \equiv f_{p - 1} \equiv 1 \pmod{p - 1} \).

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 interest.

**Lemma 4.** Let \( D \) be a positive number, and \( h, g \) a pair of coprime natural numbers. If \( x > x_0(D, g) \), there exists a prime \( p \) such that

\[
x \ll p < x(1 + (\log x)^{-D}),
\]

\[
p = h \pmod{p},
\]

\[
(n - 1, P_n(a^{[n]})) = 1, \quad \text{where } P_n(x) = \prod_{p \leq x} p.
\]

The Lemma is a special case of Theorem 1 below. Theorem 1 is a generalisation of the second part of Theorem 5 of Jurkat-Richter [9]; a proof of Theorem 1 and of other sieve results will be given in a forthcoming monograph on "Sieve Methods" by Halberstam and Richert. (Paper [9], by Halberstam, Jurkat and Richert, is a preliminary announcement of these results; see, in particular, [9], Theorem 1.)

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

\[
1 \ll \gamma(p) \ll p,
\]

\[
\sum_{p \leq x} \frac{\gamma(p) - 1}{p} = O \left( \frac{1}{\log x} \right),
\]

\[
\left| \sum_{d \leq x} 1 - \frac{\psi(d)}{d} \right| \leq \eta(X, d) \quad \text{if } (d, k) = 1,
\]

where the error function \( \eta(X, d) \) is small on average, in the following sense: there exists an absolute constant \( \sigma, 0 < \sigma \ll 1 \), and to any given number \( C > 1 \) there corresponds a function \( \rho(X) \) satisfying \( 0 < \rho(X) = O(\log X)^{1/2} \), such that

\[
\sum_{1 \leq c \leq \log X, \rho(X)} \frac{\psi(d)}{d} \eta(X, d) = O \left( \frac{X}{\log X} \right);
\]

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

**Theorem I.** Let

\[
P_k(x) = \prod_{p \leq x} \left( 1 - \frac{\gamma(p)}{p} \right),
\]

and define

\[
f(u) = \phi'(u) - \varphi(u)/u
\]
where \( \gamma \) is Euler’s constant and \( \omega, \varphi \) are solutions of the (well-known) differential-difference equations

\[
\omega(u) = -\frac{1}{u}, \quad \varphi(u) = 1 \quad (0 < u \leq 2),
\]

\[
\{\omega(u)\}' = \omega(u-1), \quad (u-1)\omega'(u) = -\varphi(u-1) \quad (u \geq 2).
\]

If \( s \leq X \) and \( A \) is a sequence of the kind described above, then

\[
S_k(A, s) \geq X \psi(x) \left( \frac{\log x}{\log z} \right) - \epsilon_1 \left( \log \log x \right)^{3k}.
\]

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

\[
f(u) = \begin{cases} 0, & 0 < u \leq 2, \\ \frac{2e}{u} \log(u-1), & 2 < u \leq 4. 
\end{cases}
\]

To apply Theorem I to Lemma 4 we take

\[
A = \left\{ p-1; \ p < p \leq \left( 1 + \frac{1}{(\log p)^{D}} \right), \ p = \lambda \ (\mod g) \right\},
\]

\[
k = 2g, \quad \gamma(d) = d/\varphi(d), \quad s = \varphi^2
\]

and

\[
X = \frac{1}{\psi(x)} \left( \frac{x}{(\log x)^{D}} \right) - \log y;
\]

we may take

\[
\psi(X, z) = 2 \max_{p \leq z} \frac{\max_{m, l} \pi(y; m, l)}{(\log z)^{D-1}},
\]

where \( \pi(y; m, l) \) denotes the number of primes not exceeding \( y \) that are \( = 1 \ (\mod m) \). 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 \( B = B(f) \) such that

\[
\sum_{1 \leqslant n \leqslant M} \max_{1 \leqslant \lambda \leqslant \min} \left| \pi(y; m, l) - \frac{1}{\varphi(m)} \right| = O \left( \frac{Y}{(\log Y)^{D+D+11}} \right)
\]

provided only that

\[
M \leq Y^{1/2} (\log Y)^{-B}.
\]

To apply this result we take \( Y = x + x (\log x)^{-D}, \ a = \frac{1}{2}, \beta(x) = (\log x)^{B}, \)

\[ M = y X^{1/2} (\log X)^{B}, \]

and note that

\[
\frac{1}{\psi(x)} \left( \frac{x}{(\log x)^{D+1}} \right) \leq \frac{1}{\psi(x)} \left( \frac{x}{(\log x)^{D+1}} \right) \leq \frac{1}{\psi(x)} \left( \frac{x}{(\log x)^{D+1}} \right).
\]

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

\[
Y (\log X)^{-2D-11} = O (\log (\log X)^{-2D-11}).
\]

From here on it is an easy calculation, using Cauchy’s inequality, to show that (3.7) is satisfied with \( a = \frac{1}{2} \). It is perhaps worth remarking that our argument can be made uniform with respect to \( g \) if \( g < (\log x)^2 \).

Hence, by Theorem I, the number \( S \) of primes of the kind required in Lemma 4 satisfies

\[
S \geq \frac{1}{\psi(x)} \left( \frac{x}{(\log x)^{D+1}} \right) \times \prod_{p \leq j} \left( 1 - \frac{1}{p-1} \right) \left( f \left( \frac{5}{2} \log X \right) - \frac{1}{\varphi(\log X)} \right)
\]

provided \( s \) is large enough. By (3.9), \( \log X \geq \frac{1}{2} \log s \) and hence

\[
f(\frac{5}{2} \log X) > f(\frac{5}{4} \log X) = \frac{8}{9} e^{-\frac{5}{4} \log X}
\]

if \( s \) is sufficiently large. By the well-known theorem of Mertens

\[
\prod_{p \leq x} \left( 1 - \frac{1}{p-1} \right) > \prod_{p \leq x} \left( 1 - \frac{1}{p} \right) \sim \frac{5e^{-\frac{5}{4} \log s}}{\log s} \quad (s \to \infty).
\]

We may therefore conclude that there exists a constant \( \delta_1(D, g) \) such that

\[
S \geq (4 \log x)^{\frac{1}{2}} \frac{1}{\psi(x)} \left( \frac{x}{(\log x)^{D+1}} \right) \prod_{p \leq j} \left( 1 - \frac{1}{p-1} \right) \sim \delta_1(D, g)
\]

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

**Lemma 5.** Let \( (h, g) = 1 \). For each \( s > \left( \frac{1}{2} \right) g \) there exists a prime \( p \) satisfying (3.1) and (3.2) such that

\[
\left| c_1 (1 - 4s^{-11}) \right| < \frac{\sigma(g-1)}{p-1} < c_2,
\]

where \( c_1 \) and \( c_2 \) are positive constants.

**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 \( 2g \), since \( p-1 = \lambda-1 \ (\mod g) \); 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 \(\varepsilon^2\), and there are clearly at most four such prime factors. Hence

\[
\frac{\varphi(p-1)}{p-1} = \frac{\varphi(2(g, h-1))}{2(g, h-1)} \prod_{p|\varphi(p-1)} \left(1 - \frac{1}{p}\right) \geq c_4(1-\varepsilon^{-2}) > c_4(1-4\varepsilon^{-2}),
\]

and

\[
\frac{\varphi(p-1)}{p-1} \leq c_4
\]

follows trivially.

**Lemma 6.** If \((h, g) = 1\) and \(x \geq x_1(D, g)\) there exists a prime \(p = h \pmod{g}\) such that

\[
x \leq \varphi(p-1) \leq x \left(1 + \frac{2}{(\log x)^2}\right).
\]

**Proof.** Let \(p\) be a prime whose existence was established in Lemma 5. Then

\[
ce_4(x-1)(1-4\varepsilon^{-2}) \leq \varphi(p-1) \leq c_4 \left(1 + \frac{1}{(\log x)^2}\right).
\]

We let \(y = c_4(x-1)(1-4\varepsilon^{-2})\), so that \(y < x\), and obtain

\[
y \leq \varphi(p-1) \leq y \left(1 + \frac{2}{(\log y)^2}\right);
\]

the result follows on replacing \(y\) by \(x\).

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

\[
x \leq \varphi\left(\frac{p-1}{q'}\right) \leq x \left(1 + \frac{2}{(\log x)^2}\right).
\]

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

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

the result follows, by the argument used in the proof of Lemma 6, on taking \(y = x/q'\) or \(y/(q'-1)\) 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 \(\varphi(n) = k\),

\[
2^{(n+1)\varepsilon^{-2}} < n < 2^{(n+1)\varepsilon^{-1}}.
\]

**Proof.** Since \(n > 1\), \(\sum_{d|n} \varphi(d)/d = 0\), whence

\[
\sum_{x \geq x_1} 1 = \sum_{x \geq x_1} \frac{1}{x} = \frac{1}{4} \cdot 2^{4n_0}.
\]

It follows that

\[
f_n = \prod_{d|n} (2d-1)^{\varphi(d)/d} = \frac{\prod_{d|n} (2d-1)}{\prod_{d|n} (2d-1)} > \frac{\prod_{d|n} (2d-1)}{\prod_{d|n} (2d-1)^{\varphi(d)/d}} = 2^{4n_0} - 1
\]

on writing \(\varphi(n) = k\). 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 \(q, g\) 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 \(p = m \pmod{aq^2g^2}\) is such that one of the integers \(p^{(n-1)/\varphi}\) or \(p^{(\varepsilon^{-2})}\) is a pseudoprime \(= h \pmod{a}\). If now we choose \(\varepsilon\) large enough, Lemma 6 and Lemma 7 (with \(q' = 2\) or \(q_2\)) imply that \(p\) can been chosen to satisfy also each of the three pairs of inequalities

\[
\varepsilon \leq \varphi\left(\frac{p-1}{t}\right) \leq \varepsilon \left(1 + \frac{2}{(\log t)^2}\right) \quad (t = 1, 2, q_2);
\]

we have to take \(g = aq^2g_2\) in Lemma 6 (the case \(t = 1\)) or we take \(g = aq^2g_1\) in Lemma 7 when \(t = q_1\) and \(g = aq^2g_2\) when \(t = 2\). In fact, we shall choose \(x_1 = x_1(D, a, q, g)\) so large that for \(x \geq x_1\), \(p\) satisfies in addition the two conditions

\[
p < 2^{4\varepsilon^{-2}} \quad \text{and} \quad \varphi(p-1) < \frac{x}{(\log x)^2}.
\]

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

Thus in particular, \(2^{4\varepsilon^{-2}} = O(p^{(n-1)/\varphi}) = O(p^{a^{-1} \log \log x})\).

We now suppose that \(x \geq x_1\) and apply Lemma 8 with \(n = (p-1)/\varphi\), where \(t_0 = 1, 2, q_1\) is such that \(p^{(n-1)/\varphi}\) is a pseudoprime. Then, by (4.1) and (4.2),

\[
p^{(n-1)/\varphi} > 2^{(p-1)/\varphi} \cdot 2^{\varepsilon^{-1}} > 2^{p^{-1} \log \log x^{-1}}
\]

and

\[
p^{(\varepsilon^{-2})} < 2^{(1+4\varepsilon^{-2})} \cdot 2^{4\varepsilon^{-1} \log \log x^{-2}} < 2^{(1+4\varepsilon^{-2})}\).
\]

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

\[
y < p^{(n-1)/\varphi} < 2^{(1+4\varepsilon^{-2})}\).
\]

this completes the proof of Theorem 1.
Zur Anzahl Abelscher Gruppen gegebener Ordnung II
von
PETER GEORG SCHMIDT (Marburg)

Einführung. $A(x)$ sei die Anzahl der wesentlich verschiedenen Abelschen Gruppen, deren Ordnung $x$ nicht übersteigt, und $A(x)$ das Restglied in der asymptotischen Entwicklung

$$A(x) = A_1 x + A_2 x^{12} + A_3 x^{18} + A(x)$$

mit

$$A_\mu := \int_0^x \frac{y^{\mu}}{\mu!} \, dy \quad (\mu = 1, 2, 3).$$

 Ist $\theta$ die untere Grenze aller $\theta$, für die

$$A(x) < x^{\theta^2} \quad (x \rightarrow \infty)$$

gilt, so zeigten (1) P. Erdős und G. Szekeres, D. G. Kendall und R. A. Rankin, H. E. Bichert, W. Schwarz, der Verfasser

$$\theta < 1/2, 3/4, 3/10, 20/60 \approx 0.33, 5/18 = 0.27...$$

In dieser Arbeit soll $\theta < 7/27 = 0.259...$ oder genauer

(1) $$A(x) < x^{2/3} \log^2 x \quad (x \rightarrow \infty)$$

bewiesen werden.

Nach Hilfssatz 1 genügt es, letztere Ungleichung für das dort erklärte Restglied $A_1(x)$ zu zeigen. Ausgangspunkt sei daher unsere in [3], § 1 gegebene Darstellung der Funktion $A_1(x)$ durch gewisse Doppelsummen (Hilfssätze 2), zu deren Abschätzung die von van der Corput- Methode (Hilfssätze 3-6) heranzogen wird. In unserem Falle berührt die van der Corput Methode vornehmlich auf der wiederholt Transformation gewisser Exponentialdoppelsummen vermöge „Weylischer“ und „van der Corputischer Schritte“ (Hilfssätze 4 und 5), wobei sowohl die Schrittfolge

(1) Ausführlicheres, insbesondere weitere Literatur, findet sich in [3], Einführung.