ACTA ARITHMETICA
X(1964)

Almost primes generated by a polynomial*

by

R. J. MIECH (Urbana, Ill.)

Introduction. An almost prime is an integer with a bounded number of prime factors. The concept is a relative one; the bound displayed depends on the problem at hand.

The questions to be discussed in this paper stem from the twin-prime problem, i.e. are there an infinite number of primes p such that $p+2$ is again a prime? The answer is not known but weaker results in this direction are available. V. Brun, [2], for example, proved that there are an infinite number of positive integers m such that the polynomial value $m(m+2)$ has at most 9 prime factors. A. Selberg reduced the bound to 5. Similar statements have been obtained for other polynomials. Y. Wang [11] proved that there are an infinite number of positive integers m such that m^3+2 has at most 4 prime factors; B. V. Levin, [5], has shown that the polynomial n^2+1 will generate an infinite sequence of integers having at most 5 prime factors.

We shall extend this type of result to integral valued polynomials. We shall show that if $G(n)$ is an integral valued polynomial, is of degree h, and has k irreducible factors then there are an infinite number of integers m such that $G(m)$ has, roughly speaking, at most $(9h/5+k\log k)$ prime factors. Our major result, Theorem 1 below, has a slightly different bound, contains information about the manner in which the prime factors of the almost primes are distributed, and is applicable to a fairly large class of polynomials. A result which is applicable to *any* integral valued polynomial will be derived as a corollary to Theorem 1.

Let us be specific. We shall prove:

THEOREM 1. *Let* $G(n)=\prod_{i=1}^{k} G_i(n)$ *where* $G_i(n)$ *is an irreducible polynomial with integral coefficients of degree* h_i; *in addition suppose that no*

---

* This work, which was supported by the Office of Naval Research, is based on a doctoral dissertation that was submitted to the University of Illinois.

one of the irreducible factors is a constant multiple of any other. Suppose that $\omega(p)$, the number of solutions of the congruence

$$G(n) \equiv 0 \pmod{p},$$

is strictly less than p for every prime p. As for notation: let $[x]$ denote the integral part of x, let N be any number greater than N_0, where N_0 is a constant that depends on the polynomial $G(n)$, and let h denote the maximum of the numbers $h_1, h_2, \ldots, h_k$. Then there is a positive constant C, which depends on $G(n)$, such that there are more than $CN/(\log N)^k$ positive integers m not exceeding N for which:

1) *$G(m)$ has no prime factors less than or equal to N^δ, where δ is a positive calculable constant that depends only on k, and at most*

$$\Big[k \sum_{j=1}^{k} 1/j + k \log \tfrac{5}{2}\Big]$$

prime factors less than or equal to N^B, where $B = 2(5h+2)/\{9(2h+1)\}$; none of these prime factors occurs multiply.

2) *Each $G_i(m)$ has at most $[9h_i/5]$ prime factors greater than N^B, multiple prime factors being counted multiply. In brief, there exist more than $CN/(\log N)^k$ integers m not exceeding N such that $G(m)$ has at most*

$$[9h_1/5] + \ldots + [9h_k/5] + \Big[k \sum_{j=1}^{k} 1/j + k \log \tfrac{5}{2}\Big]$$

prime factors.

Thus, each of the polynomials

$$n(n+2), \quad n^2+1, \quad n^3+2, \quad \text{and} \quad (n^2+n+1)(n^2+1)$$

will generate an infinite sequence of almost primes; the bounds will be 6, 4, 6, and 10, respectively.

After Theorem 1 has been proved we shall prove:

COROLLARY 1. *Let $G(n)$ be an integral valued polynomial and suppose that $G(n)$ has k irreducible factors with rational coefficients which are of multiplicity $a_1, a_2, \ldots, a_k$, and of degree $h_1, \ldots, h_k$, respectively. Then there are positive constants C, N_0, C_0, non-negative integers M and l_0, and a positive integer D_0, all of which depend on the polynomial $G(n)$, such that there are more than $CN/(\log N)^k$ integers m of the form $D_0 t + l_0$ not exceeding N, N being any number greater than N_0, for which $G(m)$ has:*

1) *At most M prime factors less than or equal to C_0.*

2) *No prime factors which are greater than C_0 and less than or equal to $(N/D_0)^\delta$.*

3) *At most*

$$(\max_{1 \le i \le k} \{a_i\}) \Big[\Big(k \sum_{j=1}^{k} 1/j + k \log \tfrac{5}{2}\Big)\Big]$$

prime factors greater than $(N/D_0)^\delta$ and less or equal to $(N/D_0)^B$.

4) *At most*

$$a_1[9h_1/5] + a_2[9h_2/5] + \ldots + a_k[9h_k/5]$$

prime factors greater than $(N/D_0)^B$.

All multiple prime factors are counted multiply. The constants δ and B are identical to the constants δ and B of Theorem 1.

Theorem 1 is proved by sieve methods. Its proof is, for the most part, a direct generalization of the method Selberg employed in the twin-prime case. His work is not generally available but the notes of Professors I. Reiner, P. Bateman, and L. Rubel on Selberg's lectures given at the Institute for Advanced Study, in the years 1948, 1950, and 1958, were available to me. (A broad outline of Selberg's method can be found in [9] and [10]; detailed expositions of the way his method can be used to obtain upper bounds can be found in [7] or [8].) The simple transformation used to prove the corollary is explained in Section 7 of this paper.

An upper bound for the numbers of integers m not exceeding N such that $G(m)$ has precisely k prime factors, i.e. such that each irreducible factor $G_1(m), \ldots, G_k(m)$ is prime was presented in a paper by P. Bateman and R. Stemmler [1]. The bound is of order $N/(\log N)^k$.

I would like to take this opportunity to acknowledge my considerable debt to Professor Paul T. Bateman for suggesting this problem to me and for the guidance he gave me during the preparation of this paper.

1. A survey of the proof. Several definitions are needed before we can get started. As usual, let

$$D = \prod_{p \le z, \omega(p) > 0} p$$

where p is a prime and z is a positive number which depends on N. The greatest common divisor of the integers a and b will be denoted by (a, b); $\nu(n)$ will be the number of distinct prime factors of n. The letters T, M_1, $M_2, \ldots$, and $C_1, C_2, \ldots$ will denote absolute constants which depend only on the polynomial $G(n)$.

The first step in the proof of Theorem 1 will consist of defining

a sequence of numbers $\{\varrho_d\colon d = 1, 2, \ldots\}$ having the following property:

$$\sum_{d|(G(n),D)} \varrho_d \leqslant M_1 \quad \text{if} \quad v\big((G(n), D)\big) \leqslant T,$$

$$\sum_{d|(G(n),D)} \varrho_d \leqslant 0 \quad \text{if} \quad v\big((G(n), D)\big) > T.$$

Then, letting $\Phi_0(N)$ denote the number of values of n less than or equal to N such that $G(n)$ has no more than T prime factors less than or equal to z, we shall have

$$M_1\Phi_0(N) \geqslant N\sum_{d|D}\big(\varrho_d/f(d)\big) + O\Big(\sum_{d|D}|\varrho_d R_d|\Big), \tag{1.0.1}$$

where $1/f(d) = \omega(d)/d$ and R is an error term not exceeding $\omega(d)$ in absolute value.

We shall then show that

$$\sum_{d|D}\big(\varrho_d/f(d)\big) \geqslant C/(\log z)^k, \tag{1.0.2}$$

where C is a positive constant that depends on $G(n)$. This inequality is developed in the second and third sections of this chapter.

The next step deals with the error term. Generally speaking, we shall have:

$$\sum_{d|D}|\varrho_d R_d| = O(z^t), \tag{1.0.3}$$

where t is a positive number.

Relations (1.0.1), (1.0.2), and (1.0.3) lead us to the inequality:

$$M_1\Phi_0(N) \geqslant CN/(\log N)^k + O(z^t).$$

After we have reached this point we shall set

$$z = N^{(1-w)/t},$$

where w is a positive number. The interpretation of this inequality will give us the conclusions of Theorem 1.

2. The ϱ's. Following Selberg, we begin by defining the sequence of numbers $\{\varrho_d\colon d = 1, 2, \ldots\}$ in terms of three other sequences of numbers:

$$\{\gamma_a\colon a = 1, 2, \ldots\}, \quad \{\lambda_b\colon b = 1, 2, \ldots\}, \quad \{y_r\colon r = 1, 2, \ldots\}.$$

These three sequences are fairly arbitrary at the moment, but they will have to satisfy the following conditions:

1) $\gamma_a = 0$ if (I) $\mu(a) = 0$ or (II) $a > z$; ($\mu(a)$ is the Möbius function);

2) $\lambda_b = 0$ if (I) $\mu(b) = 0$, or (II) $b > z^\alpha$, where α is a positive number less than 1 that will be determined later;

3) $A = \sum_{r\leqslant z^\alpha} \mu(r)y_r \neq 0$ for any z exceeding 1;

4) (I) $|\lambda_1/A| = 1$, (II) $|\lambda_d/A| \leqslant M_2$ if $v(d)$ is absolutely bounded.

These four conditions will be necessary at various times; they are listed here for convenience.

To get back to the main project at hand, let us insist that:

$$\sum_{\substack{d|D\\ d\leqslant z^{1+2\alpha}}} \varrho_d = \sum_{\substack{a|D\\ a\leqslant z}} \gamma_a\Big(\sum_{\substack{b|a\\ b\leqslant z^\alpha}} (\lambda_b/A)\Big)^2.$$

This leads to the definition

$$\varrho_d = \sum_{[a,b,c]=d} \gamma_a \frac{\lambda_b}{A}\cdot\frac{\lambda_c}{A},$$

where $[a, b, c]$ is the least common multiple of the integers a, b, and c. The ϱ's are defined; we must now show that they behave in a tolerable manner.

If m is any integer then

$$\sum_{d|m}\varrho_d = \sum_{d|m}\sum_{[a,b,c]=d}\gamma_a\frac{\lambda_b}{A}\cdot\frac{\lambda_c}{A} = \sum_{a|m}\gamma_a\Big(\sum_{\substack{b|m\\ c|m}}\frac{\lambda_b}{A}\cdot\frac{\lambda_c}{A}\Big) = \Big(\sum_{a|m}\gamma_a\Big)\Big(\sum_{b|m}\frac{\lambda_b}{A}\Big)^2.$$

Thus, the equality we insisted upon is met.

Now, let:

$\gamma_a = 0$ if a is composite,
$\gamma_1 = T$ (T is a positive fixed number that will be determined later),
$\gamma_p = -T$ if $p \leqslant z^\varepsilon$ (ε, like T, will be chosen later),
$\gamma_p = -1$ if $z^\varepsilon < p \leqslant z$.

Using these definitions we have:

$$\sum_{d|m}\varrho_d = \Big(T - \sum_{\substack{p|m\\ p\leqslant z^\varepsilon}} T - \sum_{\substack{p|m\\ z^\varepsilon<p\leqslant z}} 1\Big)\Big(\sum_{\substack{d|m\\ d\leqslant z^\alpha}}\frac{\lambda_d}{A}\Big)^2.$$

Let $[T]$ be the integral part of T; then the following can be deduced from the above equation:

$$0 \leqslant \sum_{d|m}\varrho_d \leqslant M_3 \tag{1}$$

if the number of prime factors of m between z^r and z is less than or equal to $[T]$ and if m has no prime factors less than or equal to z^r. (Condition 4 is used here.) If this inequality holds for an integer m let us say "$m \in 1$".

$$\sum_{d|m} \varrho_d \leqslant 0 \tag{2}$$

if the number of prime factors of m between z^s and z is strictly greater than $[T]$ or if m has one or more prime factors less than or equal to z^r.

We want to count the number of polynomial values $G(n)$ (with $n \leqslant N$) which have no prime factors less than or equal to z^s and no more than $[T]$ prime factors between z^r and z, i.e. the number of values of n with "$(G(n), D) \in 1$". Letting $\Phi(N)$ denote this number, we have:

$$\begin{aligned} M_3\Phi(N) &\geqslant M_3 \sum_{\substack{n\leqslant N \\ (G(n),D)\in 1}} 1 \geqslant \sum_{n\leqslant N} \sum_{d|(G(n),D)} \varrho_d \\ &= \sum_{d|D} \varrho_d \sum_{\substack{n\leqslant N \\ G(n)\equiv 0 \pmod d}} 1 = \sum_{d|D} \varrho_d [\omega(d)N/d + R_d] \\ &= N \sum_{d|D} (\varrho_d/f(d)) + O\Big(\sum_{d|D} |\varrho_d R_d|\Big), \end{aligned}$$

where $1/f(d) = \omega(d)/d$ and R_d is an error term. Later on we shall need to know that $|R_d| \leqslant \omega(d)$, but this is immediate since

$$\sum_{\substack{n\leqslant N \\ G(n)\equiv 0 \pmod d}} 1 = [N/d]\omega(d) + R'_d,$$

where R'_d is a non-negative integer not exceeding $\omega(d)$.

We have defined the ϱ's in terms of other parameters and have shown that

$$M_3\Phi(N) \geqslant N \sum_{d|D} \varrho_d/f(d) + O\Big(\sum_{d|D} |\varrho_d R_d|\Big).$$

These are the two main results of this section.

3. Some estimates. Several formulas needed to estimate the sum $\sum \varrho_d/f(d)$ will be developed in this section. (See Lemmas 3.9, 3.10, and 3.11.)

A function must be defined before we can continue. Let $1/f(n)$ be defined as in Section 1, $1/f(n) = \omega(n)/n$. Let us restrict the domain of the function to the square free integers n such that $\omega(n)$ is positive; then it is possible to discuss the function $f(n)$ without any difficulties. Define $f'(n)$ by the relation

$$f(n) = \sum_{d|n} f'(n)$$

or, by the Möbius inversion formula,

$$f'(n) = f(n) \prod_{p|n} (1 - 1/f(p)),$$

the domain of $f'(n)$ being the same as that of $f(n)$.

The function $f'(n)$ will appear in a sum of the form

$$\sum_{n\leqslant x}{}' \mu^2(n)/f'(n), \tag{3.0.1}$$

the prime on the summation symbol indicating that the summation is to be taken only on those square free integers n for which $\omega(n)$ is greater than zero. The major purpose of this section is to transform this quantity into a more tractable one. We shall do so by first finding an asymptotic formula for the summatory function of the Dirichlet series

$$\sum_{n=1}^{\infty}{}' \mu^2(n)/(f'(n)n^{s-1}) \qquad (s > 1), \tag{3.0.2}$$

i.e. the sum

$$\sum_{n\leqslant x}{}' \mu^2(n)\cdot n/f'(n). \tag{3.0.3}$$

We can then find an estimate for (3.0.1) from (3.0.3) by partial summation. We shall also estimate sums of the form

$$\sum_{p\leqslant x}{}' \log^j p/f(p)$$

in this section. Most of the lemmas that follow are taken to be known; the details of the proofs are left to the reader.

The estimate to be derived for (3.0.3) is a consequence of

LEMMA 3.1. *Let*

$$\sum_{n=1}^{\infty} a_n/n^s = \sum_{n=1}^{\infty} b_n/n^s \sum_{n=1}^{\infty} c_n/n^s \qquad (s > 1), \tag{3.1.1}$$

and suppose that $\sum b_n/n^s$ converges absolutely for $s > s_0$, where s_0 is such that $0 < s_0 < 1$. In addition suppose that

$$\sum_{n\leqslant x} c_n = Cx + O(x^r) \qquad (s_0 < r < 1)$$

or

$$\sum_{n\leqslant x} c_n = Cx(\log x)^{k-1} + O(x(\log x)^{k-2}) \quad \text{if} \quad k \geqslant 2.$$

Then

$$\sum_{n\leqslant x} a_n = \Big(\sum_{n=1}^{\infty} b_n/n\Big) Cx + O(x^r)$$

or

$$\sum_{n\leqslant x} a_n = \Big(\sum_{n=1}^{\infty} b_n/n\Big) Cx(\log x)^{k-1} + O(x\log^{k-2} x).$$

To prove this lemma in the second case write

$$\sum_{n\leqslant x} a_n = \sum_{n\leqslant x} b_n \sum_{d\leqslant x} c_d = Cx \sum_{n\leqslant x} \frac{b_n}{n}\Big(\log\frac{x}{n}\Big)^{k-1} + O\Big(x\log^{k-2} x \sum_{n=1}^{\infty}\frac{|b_n|}{n}\Big),$$

expand $(\log x - \log n)^{k-1}$ by the binomial theorem, and then use what has been assumed. The proof in the first case is similar.

The first step in passing from the series (3.0.2) to formula (3.1.1) is based on the following property of the quantities involved:

$$(3.1.2)\quad \sum_{n=1}^{\infty}{}' \frac{\mu^2(n)}{n^{s-1}f'(n)} = \prod_p{}'\Big(1+\frac{1}{p^{s-1}f'(p)}\Big)$$

$$= \prod_p\Big(1+\frac{\omega(p)}{p^{s-1}(p-\omega(p))}\Big)\Big(1-\frac{1}{p^s}\Big)^{\omega(p)} \prod_p\Big(1-\frac{1}{p^s}\Big)^{-\omega(p)}.$$

It is not difficult to show that the first of the products in the double product of (3.1.2) is a Dirichlet series which is absolutely convergent for $s > 1/2$. Several facts about congruences are needed before we can deal with the remaining product. The first is:

LEMMA 3.2. *Let* $G(n) = \prod_{i=1}^{k} G_i(n)$ *and* $\omega(p)$ *be defined as in Theorem* 1. *Define* $\omega_i(p)$ *similarly for* $i = 1, 2, \ldots, k$. *Then for all but a finite number of primes* p *we have*:

$$\omega(p) = \omega_1(p) + \ldots + \omega_k(p).$$

This lemma can be proved by contradiction, making use of the fact that if $G_1(x)$ and $G_2(x)$ are relatively prime polynomials then there are polynomials $a(x)$ and $b(x)$ with integral coefficients and an integer C such that $a(x)G_1(x) + b(x)G_2(x) = C$ for every integer x.

The second result about congruences that will be of use is:

LEMMA 3.3. *Let* $g(n)$ *be an irreducible polynomial with integral coefficients and let* $R(\theta)$ *be the field generated by the relation* $g(\theta) = 0$. *Then for all but a finite number of primes* p, $\omega(p)$, *the number of solutions of the congruence* $g(n) \equiv 0 \pmod p$ *is equal to the number of prime ideals of the first degree (in* $R(\theta)$*) containing the prime* p.

See [6], page 63, Theorem 8.1, for the proof. The theorem cited cannot be applied directly unless the leading coefficient of $g(n)$ is 1, but the modifications for the contrary case are minor.

If we apply Lemma 3.3 we shall have:

LEMMA 3.4. *Let* $g(n)$, $\omega(p)$, *and* $R(\theta)$ *be defined as in Lemma* 3.3. *Let* $\zeta(s)$ *be the zeta function of the algebraic number field* $R(\theta)$. *Then*

$$\prod_p (1-1/p^s)^{-\omega(p)} = H_1(s)\zeta(s) \qquad (s > 1),$$

where $H_1(s)$ *is a Dirichlet series that is absolutely convergent for* $s > 1/2$.

If we return to formula (3.1.2), apply Lemma 3.2, and then employ Lemma 3.4 we can assert:

LEMMA 3.5. *Let* $G(n) = \prod_{i=1}^{k} G_i(n)$ *and* $\omega(p)$ *be defined as in Theorem* 1 *and let* $\zeta_i(s)$ *be the zeta function of the field generated by a zero of* $G_i(n)$. *Then*

$$\sum_{n=1}^{\infty}{}' \mu^2(n)/f'(n)n^{s-1} = H_2(s)\prod_{i=1}^{k}\zeta_i(s) \qquad (s > 1),$$

where $H_2(s)$ *is a Dirichlet series which is absolutely convergent for* $s > 1/2$.

The next two lemmas deal with the summatory function of the product of the zeta functions that appears above.

LEMMA 3.6. (Weber). *Let*

$$\zeta_i(s) = \sum_{n=1}^{\infty} a_n/n^s \qquad (s > 1).$$

(Recall that $G_i(n)$ is of degree h_i and that a_n is the number of ideals in the field generated by $G_i(\theta)$ with norm equal to n.) *Then*

$$\sum_{n\leqslant x} a_n = Ax + O(x^v) \qquad (v = 1-1/h_i),$$

where the constant A, *as well as the one implied by the* O*-term, depends on the polynomial* $G_i(n)$.

See [3], page 81.

LEMMA 3.7. *Let* $\zeta_i(s)$ *be defined as in Lemma* 3.5 *and let*

$$\prod_{i=1}^{k}\zeta_i(s) = c_n/n^s \qquad (s > 1).$$

Then

$$\sum_{n\leqslant x} c_n = Cx + O(x^v) \quad \text{if} \quad k = 1 \qquad (v = 1-1/h_1),$$

$$\sum_{n\leqslant x} c_n = Cx(\log x)^{k-1} + O(x(\log x)^{k-2}) \quad \text{if} \quad k \geqslant 2.$$

Proof. The assertion of this lemma is identical to Lemma 3.6 if $k=1$. If $k=2$ use Lemma 3.6 and the fact that

$$\sum_{n\leqslant x} c_n = \sum_{n\leqslant x} a'_n \sum_{nd\leqslant x} a_d = \sum_{n\leqslant x} a'_n \left(Ax/n + O\left((x/n)^v\right)\right),$$

the notation being taken to be obvious. Then use the formula

$$\sum_{n\leqslant x} \frac{a'_n}{n} = \int_1^x \left(\sum_{n\leqslant u} a'_n\right)\frac{1}{u^2}\,du + \left(\sum_{n\leqslant x} a'_n\right)\frac{1}{x}.$$

The general result can be obtained by induction after the result has been proved for $k=2$.

If we employ Lemmas 3.5, 3.7, and 3.1 we shall have the following estimate for the summatory function (3.0.3):

Lemma 3.8. *Using previous notation we have*:

$$\sum_{n\leqslant x}{}' \mu^2(n)\cdot n/f'(n) = Ex + O(x^v)$$

if $k=1$, $v=\max(2/3,\ 1-1/h_1)$, *and*

$$\sum_{n\leqslant x}{}' \mu^2(n)\cdot n/f'(n) = Ex(\log x)^{k-1} + O(x\log^{k-2}x)$$

if $k\geqslant 2$, *where* E *is a positive constant which depends on* $G(n)$.

Using the formula

$$\sum_{n\leqslant x}{}' \frac{\mu^2(n)}{f'(n)} = \int_1^x \left(\sum_{n\leqslant u}{}' \frac{\mu^2(n)\cdot n}{f'(n)}\right)\frac{1}{u^2}\,du + \left(\sum_{n\leqslant x}{}' \frac{\mu^2(n)\cdot n}{f'(n)}\right)\frac{1}{x},$$

we have:

Lemma 3.9. *Suppose that* $x>y\geqslant 1$. *Then*

$$\sum_{y<n\leqslant x}{}' \mu^2(n)/f'(n) = C_1(\log^k x - \log^k y) + O(\log^{k-1}x + \log^{k-1}y)$$

for $k\geqslant 1$. *The positive constant* C_1 *is equal to* E/k.

This is the formula that was sought for (3.0.1).

Let us turn to the sums

$$\sum_{p\leqslant x}{}' (\log p)^j/f(p), \qquad j=0,1,\ldots,k.$$

We shall need a result of Landau's:

$$\sum_{N(P)\leqslant x} 1/N(P) = \log\log x + B + O(1/\log x),$$

where P is a prime ideal in the field generated by a zero of the irreducible polynomial $g(n)$, $N(P)$ is the norm of the ideal P, and B is a constant depending on $g(n)$. See [3], pages 114-115 and pages 149-150, for the proof. If we apply this formula, making use of Lemma 3.2 and 3.3, we shall have:

Lemma 3.10. *Let* $G(n)$ *and* $\omega(p)$ *be defined as in Theorem* 1. *Then*

$$\sum_{p\leqslant x}{}' 1/f(p) = \sum_{p\leqslant x} \omega(p)/p = k\log\log x + B' + O(1/\log x),$$

where B', *as well as the constant in the* O*-term, depends on* $G(n)$. *The number* x *must be greater than* 2.

This lemma gives the estimate desired for the case $j=0$. If $j>0$, we have another exercise in partial summation:

Lemma 3.11. *Let* $1/f(p) = \omega(p)/p$. *Then*

$$\sum_{p\leqslant x}{}' (\log p)/f(p) = k\log x + O(\log\log x),$$

$$\sum_{p\leqslant x}{}' (\log p)^j/f(p) = (k/j)(\log x)^j + O(\log^{j-1}x), \qquad j=2,\ldots,k.$$

The error term of the last two lemmas could be improved by employing the prime ideal theorem ([4], page 113, theorem 191) instead of the result of Landau we have used, but we shall not need such results.

4. An inequality. The aim of this section is to show that

$$\sum_{d\mid D} \varrho_d/f(d) \geqslant C/(\log z)^k,$$

where C is a positive constant which depends on the polynomial $G(n)$.

Several lemmas are needed to obtain this inequality. The first two deal with technical details that arise in the proof of the third.

Lemma 4.1. *Let* $1/f(n) = \omega(n)/n$ *and suppose that* n *is restricted to square free* n *with* $\omega(n)>0$. *Let*

$$f_a(d) = f\left(d/(a,d)\right).$$

Then

$$1/f([a,b,c]) = f_a\left((b,c)\right)/\left(f(a)f_a(b)f_a(c)\right).$$

Proof. Write the equation in the form

$$f(a)f\left(b/(a,b)\right)f\left(c/(a,c)\right) = f([a,b,c])f\left((b,c)/(a,b,c)\right).$$

Since a, b, and c are square free, the result is then immediate.

LEMMA 4.2. *Let $f(n)$ and $f_a(n)$ be defined as in Lemma 4.1, and suppose that the same restrictions regarding the domain of these functions are made. Let the functions $f'(n)$ and $f'_a(n)$ be defined by the relations*

$$f(n) = \sum_{\sigma|n} f'(\sigma), \qquad f_a(n) = \sum_{\sigma|n} f'_a(\sigma).$$

Then

$$f'_a(n) = \begin{cases} f'(n) & \text{if} \quad (n, a) = 1, \\ 0 & \text{if} \quad (n, a) > 1. \end{cases}$$

Proof. The proof is based on the Möbius inversion formula and the fact that the integers involved are square free.

LEMMA 4.3. *Let*

$$y_r = \sum_{\substack{d \leqslant z^a \\ r|d}}{}' \lambda_d / f(d).$$

Recall that $A = \sum_{r \leqslant z^a} \mu(r) y_r$, and let $f'(n)$ be defined as in Lemma 4.2. Then

$$\sum_{d|D} \varrho_d / f(d) = \frac{1}{A^2}\left(\gamma_1 \sum_{r \leqslant z^a}{}' f'(r) y_r^2 + \sum_{p \leqslant z}{}' \frac{\gamma_p}{f(p)} \sum_{\substack{r \leqslant z^a \\ (r,p)=1}}{}' f'(r)\left(y_r + f'(p) y_{pr}\right)^2\right).$$

The prime on the summation symbol ($\sum'$) is used to emphasize the fact that the summation is taken over only those r for which $\omega(r) \neq 0$.

Proof. Let us begin by using the definition of the ϱ's and then applying Lemma 4.1. Doing so we obtain:

$$\sum_{d|D} \varrho_d / f(d) = \frac{1}{A^2} \sum_{\substack{a \leqslant z \\ b,c \leqslant z^a}}{}' \frac{\gamma_a}{f(a)} \cdot \frac{\lambda_b}{f_a(b)} \cdot \frac{\lambda_c}{f_a(c)} f_a\big((b,c)\big).$$

If we now replace $f_a\big((b,c)\big)$ by the sum $\sum_{r|(b,c)}{}' f'(r)$, reverse the order of summation on the resulting sum, and then use the conclusion of Lemma 4.2 we shall find that the last sum is equal to

$$\frac{1}{A^2}\left(\sum_{a \leqslant z}{}' \frac{\gamma_a}{f(a)} \sum_{\substack{r \leqslant z^a \\ (r,a)=1}}{}' f'(r)\left(\sum_{\substack{b \leqslant z^a \\ r|b}}{}' \frac{\lambda_b}{f_a(b)}\right)^2\right).$$

If we apply the same sort of inversion to the squared term in the brackets we get, if $(r, a) = 1$,

$$\sum_{\substack{b \leqslant z^a \\ r|b}}{}' \frac{\lambda_b}{f_a(b)} = \sum_{\sigma|a}{}' f'(\sigma) \sum_{\substack{b \leqslant z^a \\ \sigma r|b}}{}' \frac{\lambda_b}{f(b)} = \sum_{\sigma|a}{}' f'(\sigma) y_{\sigma r}.$$

That is,

$$\sum_{d|D}{}' \frac{\varrho_d}{f(d)} = \frac{1}{A^2} \sum_{a \leqslant z}{}' \frac{\gamma_a}{f(a)} \sum_{\substack{r \leqslant z^a \\ (r,a)=1}}{}' f'(r)\left(\sum_{\sigma|a}{}' f'(\sigma) y_{\sigma r}\right)^2.$$

Since the γ's are zero unless a is 1 or a prime, the conclusion of Lemma 4.3 follows directly.

The next result will be used when the error term is estimated.

LEMMA 4.4. *Let y_r be defined as in Lemma 4.3. Then*

$$\lambda_d / f(d) = \sum_{rd \leqslant z^a} \mu(r) y_{rd}.$$

Conversely, this implies that

$$\sum_{\substack{d \leqslant z \\ r|d}}{}' \lambda_d / f(d) = y_r.$$

Proof.

$$\sum_{rd \leqslant z^a}{}' \mu(r) y_{rd} = \sum_{r \leqslant z^a/d}{}' \mu(r) \sum_{\substack{\sigma \leqslant z^a \\ rd|\sigma}}{}' \lambda_\sigma / f(\sigma) = \sum_{\substack{\sigma \leqslant z^a \\ d|\sigma}}{}' \lambda_\sigma / f(\sigma) \sum_{r|(\sigma/d)}{}' \mu(r) = \lambda_d / f(d).$$

The proof of the converse is similar.

We shall now select the y's which is equivalent to selecting the λ's in view of Lemma 4.4.

Since

$$y_r = \sum_{\substack{d \leqslant z^a \\ r|d}}{}' \lambda_d / f(d),$$

we must have

$$y_r = 0 \quad \text{if} \quad r > z^a.$$

If $r \leqslant z^a$, let

$$y_r = \mu(r)/f'(r) \text{ if } \omega(r) > 0, \quad \text{and} \quad y_r = 0 \text{ if } \omega(r) = 0.$$

According to Lemma 4.3 we need to know the value of

$$y_r + f'(p) y_{rp}$$

when $(r, p) = 1$.

It is easy to calculate:

$$y_r + f'(p)y_{pr} = \frac{\mu(r)}{f'(r)} + f'(p)\frac{\mu(rp)}{f'(rp)} = \begin{cases} 0 & \text{if} \quad rp \leqslant z^\alpha, \\ \dfrac{\mu(r)}{f'(r)} & \text{if} \quad rp > z^\alpha. \end{cases}$$

If we substitute these values in the conclusion of Lemma 4.3 we shall have:

$$\sum_{d|D} \frac{\varrho_d}{f(d)} = \frac{1}{A^2}\left(\gamma_1 \sum_{r \leqslant z^\alpha}{}' \frac{\mu^2(r)}{f'(r)} + \sum_{p \leqslant z}{}' \frac{\gamma_p}{f(p)} \sum_{\substack{z^\alpha/p < r \leqslant z^\alpha \\ (r,p)=1}}{}' \frac{\mu^2(r)}{f'(r)}\right).$$

Since the γ_p's are non-positive the condition $(r, p) = 1$ appearing in the index of summation can be dropped if we replace the equality by an inequality, i.e.

$$\sum_{d|D} \frac{\varrho_d}{f(d)} \geqslant \frac{1}{A^2}\left(\gamma_1 \sum_{r \leqslant z^\alpha}{}' \frac{\mu^2(r)}{f'(r)} + \sum_{p \leqslant z}{}' \frac{\gamma_p}{f(p)} \sum_{z^\alpha/p < r \leqslant z^\alpha}{}' \frac{\mu^2(r)}{f'(r)}\right) = R/A^2,$$

where R is a quantity that is defined by the equation in which it appears. This brings us to

LEMMA 4.5. *Let $\varepsilon = \beta\alpha$ where $0 < \beta < 1$. Then R is equal to*

$$C_1 \alpha^k (\log z)^k \left\{T - (T-1)k\left(\sum_{j=1}^{k} \frac{1-(1-\beta)^j}{j}\right) - k\sum_{j=1}^{k}\frac{1}{j} - k\log\frac{1}{\alpha}\right\} + O\left(\log\log z \cdot (\log z)^{k-1}\right).$$

Proof. If we use the definition of the γ's, employ Lemmas 3.9 and 3.10, expand the quantities $(\log z - \log p)^k$ which then appear by the binomial theorem, reverse the order of summation of several sums, and then gather all the error terms together we shall have

$$R = TC_1(\log z^\alpha)^k + TC_1 \sum_{j=1}^{k} (-1)^j \binom{k}{j} (\log z^\alpha)^{k-j} \left(\sum_{p \leqslant z^\varepsilon}{}' \frac{\log^j p}{f(p)}\right) +$$
$$+ C_1 \sum_{j=1}^{k} (-1)^j \binom{k}{j} (\log z^\alpha)^{k-j} \left(\sum_{z^\varepsilon < p \leqslant z^\alpha}{}' \frac{\log^j p}{f(p)}\right) -$$
$$- C_1 k(\log 1/\alpha)(\log z^\alpha)^k + O\left(\log\log z \cdot (\log z)^{k-1}\right).$$

Now, for the sake of uniformity, replace the quantity $(\log x)^{j-1}$ appearing in the error term of the second formula of Lemma 3.11 by $(\log\log x) \times (\log x)^{j-1}$. Then we shall have

$$R = TC_1(\log z^\alpha)^k +$$
$$+ TC_1 \sum_{j=1}^{k} (-1)^j \binom{k}{j} (\log z^\alpha)^{k-j} \left(\frac{k}{j}(\log z^\varepsilon) + O(\log\log z \log^{j-1} z)\right) +$$
$$+ C_1 \sum_{j=1}^{k} (-1)^j \binom{k}{j} (\log z^\alpha)^{k-j} \left(\frac{k}{j}(\log^j z^\alpha \log^j z^\varepsilon) + O(\log\log z \log^{j-1} z)\right) -$$
$$- C_1 k(\log 1/\alpha)(\log z^\alpha)^k + O(\log\log z \log^{k-1} z).$$

Gathering like terms together, putting $\varepsilon = \beta\alpha$, and letting the constant in the O-term depend on ε, we get

$$R = \alpha^k C_1 (\log z)^k \left\{T + (T-1)k\sum_{j=1}^{k} \frac{(-1)^j}{j}\binom{k}{j}\beta^j + k\sum_{j=1}^{k}\frac{(-1)^j}{j}\binom{k}{j} - k\log\frac{1}{\alpha}\right\} + O(\log\log z \log^{k-1} z).$$

The proof of this lemma will be complete if we establish that

$$S_k = \sum_{j=1}^{k} \frac{(-1)^j}{j}\binom{k}{j}\beta^j = \sum_{j=1}^{k}\frac{(1-\beta)^j - 1}{j} \qquad (0 < \beta \leqslant 1). \tag{4.5.1}$$

But this is a simple matter since

$$S_{k+1} - S_k = \sum_{j=1}^{k+1} \frac{(-1)^j}{j}\left\{\binom{k+1}{j} - \binom{k}{j}\right\}\beta^j = \sum_{j=1}^{k+1}\frac{(-1)^j}{j}\cdot\frac{j}{k+1}\binom{k+1}{j}\beta^j$$
$$= \frac{1}{k+1}\sum_{j=1}^{k+1}(-1)^j\binom{k+1}{j}\beta^j = \frac{(1-\beta)^{k+1}-1}{k+1}.$$

We also have

$$S_1 = -\beta = (1-\beta) - 1.$$

Thus (4.5.1) can be established by induction and, as we have said, it completes the proof of Lemma 4.5.

We now have

$$\sum_{d|D} \varrho_d/R_d \geqslant R/A^2$$
$$= \frac{C_1 \alpha^k (\log z)^k}{A^2}\left\{T - (T-1)k\left(\sum_{j=1}^{k}\frac{1-(1-\beta)^j}{j}\right) - k\sum_{j=1}^{k}\frac{1}{j} - k\log\frac{1}{\alpha}\right\} + O\left(\log\log z \cdot (\log z)^{k-1}/A^2\right).$$

Thus we want to choose the number T so that the coefficient of the main term is positive. Since we shall take α to be rational, we can pick a positive η such that

$$\Big[k\sum_{j=1}^{k}1/j+k\log 1/\alpha+\eta\Big]=\Big[k\sum_{j=1}^{k}1/j+k\log 1/\alpha\Big],$$

where $[x]$ denotes the integral part of x. Having selected η, set

$$T=k\sum_{j=1}^{k}1/j+k\log 1/\alpha+\eta.$$

Then select and fix a sufficiently small value of β so that

$$\left|(T-1)k\sum_{j=1}^{k}\frac{1-(1-\beta)^j}{j}\right|<\eta/2.$$

A particular value of β could be calculated but none will be needed. As for the dependence of β on the other parameters: at this point β depends on α, η, and k. After α has been fixed η will depend only on k; consequently β will depend only on k.

Assuming that η and β have been chosen properly, we have

$$T-(T-1)k\left(\sum_{j=1}^{k}\frac{1-(1-\beta)^j}{j}\right)-k\sum_{j=1}^{k}\frac{1}{j}-k\left(\log\frac{1}{\alpha}\right)>\frac{\eta}{2}.$$

Thus

$$\sum_{d|D}\varrho_d/f(d)\geqslant\frac{C_1\alpha^k(\log z)^k}{A^2}\left(\frac{\eta}{2}+O(\log\log z/\log z)\right).$$

Since

$$A=\sum_{r\leqslant z^\alpha}\mu(r)y_r=\sum_{r\leqslant z^\alpha}\frac{\mu^2(r)}{f'(r)}=C_1\alpha^k(\log z)^k+O(\log^{k-1}z),$$

we can assert that

$$\sum_{d|D}\varrho_d/f(d)\geqslant\frac{C_1\alpha^k(\log z)^k}{C_1^2\alpha^{2k}(\log z)^{2k}}\cdot\frac{(\eta/2+O(\log\log z/\log z))}{(1+O(1/\log z))},$$

i.e. there is a positive constant C such that

$$\sum_{d|D}\varrho_d/f(d)\geqslant C/(\log z)^k.$$

5. The error term. We shall prove:

LEMMA 5.1. *Let ε_1 be any fixed positive number. Then*

$$\sum_{d|D}|\varrho_d R_d|=O(z^{(1+2\alpha)(1+\varepsilon_1)}).$$

Proof. Let us estimate R_d first. Let $Q=h_1+h_2+\ldots+h_k$ and let

$$A_d=\{p\colon p\mid d,\ p^{\varepsilon_1/2}\leqslant Q\},\qquad B_d=\{p\colon p\mid d,\ p^{\varepsilon_1/2}>Q\}.$$

Then, for square free d,

$$|R_d|\leqslant\omega(d)=\left(\prod_{p\in A_d}\frac{\omega(p)}{p^{\varepsilon_1/2}}\right)\left(\prod_{p\in B_d}\frac{\omega(p)}{p^{\varepsilon_1/2}}\right)d^{\varepsilon_1/2}=O(d^{\varepsilon_1/2}),$$

since $\omega(p)\leqslant Q$. Thus

$$\sum_{d|D}|\varrho_d R_d|=O\Big(\sum_{d|D}|\varrho_d|z^{(1+2\alpha)\varepsilon_1/2}\Big),\tag{5.1.1}$$

since $d\leqslant z^{(1+2\alpha)}$.

Now, by definition,

$$\varrho_d=\sum_{[a,b,c]=d}\gamma_a\frac{\lambda_b}{A}\cdot\frac{\lambda_c}{A}.$$

Consequently

$$\sum_{d|D}|\varrho_d|\leqslant\Big(\sum_{a\leqslant z}|\gamma_a|\Big)\Big(\sum_{b\leqslant z^\alpha}\frac{|\lambda_b|}{A}\Big)^2.\tag{5.1.2}$$

The definition of the γ's implies that

$$\sum_{a\leqslant z}|\gamma_a|=O\big(z(\log z)^{-1}\big).\tag{5.1.3}$$

As for the λ's, by Lemma 4.4 and by the definition of y_r, we have

$$\frac{\lambda_d}{f(d)A}=\frac{\sum_{rd\leqslant z^\alpha}\mu(r)y_{rd}}{\sum_{r\leqslant z^\alpha}\mu(r)y_r}=\frac{\mu(d)}{f'(d)}\cdot\frac{\sum_{\substack{rd\leqslant z^\alpha\\(r,d)=1}}(\mu^2(r)/f'(r))}{\sum'_{r\leqslant z^\alpha}(\mu^2(r)/f'(r))}.\tag{5.1.4}$$

Thus, by Lemma 3.10,

$$\left|\frac{\lambda_d}{A}\right|\leqslant\mu^2(d)\frac{f(d)}{f'(d)}=\mu^2(d)\prod_{p\mid d}\left(1-\frac{\omega(p)}{p}\right)^{-1}$$

$$\leqslant\exp\left(-\sum_{p\leqslant z^\alpha}\log\left(1-\frac{\omega(p)}{p}\right)\right)=O(\log^k z).$$

This yields

$$\left(\sum_{b\leqslant z^{\alpha}}\frac{|\lambda_b|}{A}\right)^2 = O(z^{2\alpha}\log^{2k}z). \tag{5.1.5}$$

If we combine (5.1.1), (5.1.2), (5.1.3), and (5.1.5) we shall have

$$\sum_{d|D}|\varrho_d R_d| = O(z^{(1+2\alpha)\varepsilon_1/2}z(\log z)^{-1}z^{2\alpha}\log^{2k}z) = O(z^{(1+2\alpha)(1+\varepsilon_1)}).$$

We use the fact that $(\log z)^{2k-1} = O(z^{(1+2\alpha)\varepsilon_1/2})$ in the last step above.

The proof of Lemma 5.1 is complete.

6. The interpretation. We can now prove Theorem 1. If we combine the results of sections 2, 4, and 5 we shall have

$$\Phi(N) \geqslant CN/(\log z)^k + O(z^{(1+2\alpha)(1+\varepsilon_1)}).$$

Let us set $z = N^B$, where

$$B = \frac{1}{(1+2\alpha)}\cdot\frac{(1-\varepsilon_1)}{(1+\varepsilon_1)}.$$

Then

$$\Phi(N) \geqslant C_2 N/(\log N)^k + O(N^{1-\varepsilon_1}).$$

Since $\Phi(N)$ was defined to be the number of positive integers n for which $G(n)$ has no prime factors less than or equal to z^{ε}, and no more than $[T]$ prime factors less than or equal to z, we can say that there are more than $C_3 N/(\log N)^k$ integers m not exceeding N such that $G(m)$ has no prime factors less than or equal to $N^{B\varepsilon}$ and no more than $[T] = [k\sum_{j=1}^{k}1/j + k\log 1/\alpha]$ of its prime factors less than or equal to N^B.

Let $\alpha = 2/5$ and let $(1-\varepsilon_2) = (1-\varepsilon_1)/(1+\varepsilon_1)$; thus $B = 5(1-\varepsilon_2)/9$. Let $\delta = B\varepsilon$. In addition let us call those primes which are greater than N^{δ} and less than or equal to $N^{5(1-\varepsilon_2)/9}$ "small" primes, and those which are greater than $N^{5(1-\varepsilon_2)/9}$ "large" primes.

We shall now select an ε_2 so that each irreducible factor $G_i(x)$ of $G(x)$ has at most $[9h_i/5]$ large prime factors for $x = m$, where m is one of the integers counted by $\Phi(N)$. Since $G_i(x)$ is of degree h_i there is a constant B_i such that

$$|G_i(x)| \leqslant B_i x^{h_i}; \quad i = 1, 2, \ldots, k; \; x \geqslant 1.$$

Suppose that $G_i(m)$ were to have $([9h_i/5]+1)$ or more large prime factors; we would then have

$$B_i N^{h_i} > |G_i(m)| > N^M$$

or

$$B_i N^{h_i} > N^M, \tag{6.0.1}$$

where

$$M = ([9h_i/5]+1)(5/9)(1-\varepsilon_2).$$

We want to choose ε_2 so that (6.0.1) is false for N sufficiently large, that is we want to have

$$([9h_i/5]+1)(5/9)(1-\varepsilon_2) > h_i. \tag{6.0.2}$$

This last inequality can be written in the form

$$\varepsilon_2 < \frac{1-\{9h_i/5\}}{1+[9h_i/5]}, \tag{6.0.3}$$

where $\{x\}$ denotes the fractional part of x.

If we let h denote the maximum of the degrees of the irreducible factors of $G(x)$ and if we set

$$\varepsilon_2 = \frac{1}{5}\cdot\frac{1}{(2h+1)}$$

we will have a value for ε_2 for which (6.0.3) holds for $i = 1, 2, \ldots, k$. Thus (6.0.1) will be false for N sufficiently large. This, in turn, implies that each irreducible factor of $G_i(x)$ has at most $[9h_i/5]$ large prime factors for $x = m$, where m is an integer counted by $\Phi(N)$ and N is sufficiently large.

It is now possible to calculate B and to specify how to calculate δ. We have

$$B = 5(1-\varepsilon_2)/9 = 2(5h+2)/(9(2h+1)).$$

As for δ,

$$\delta = B\varepsilon = \frac{2}{9}\cdot\frac{(5h+2)}{(2h+1)}\beta^{\alpha} = \frac{4}{45}\cdot\frac{(5h+2)}{(2h+1)}\beta,$$

β being a number which must satisfy conditions that were given in Section 4.

At this point we have proved that there are more than $C_3 N/(\log N)^k$ positive integers m not exceeding N such that $G(m)$ has at most $[k\sum_{j=1}^{k}1/j + k\log\frac{5}{2}]$ small prime factors and such that each $G_i(m)$ has at most $[9h_i/5]$ large prime factors. The large prime factors are counted multiply if they occur multiply; the small ones are not. It would be possible to estimate δ explicitly and obtain a bound on the possible multiplicity of the small prime factors, but it would be fairly large. A better result

can be obtained by discarding those $G(m)$ that are divisible by the square of a small prime.

We need only show that the number of $G(m)$ divisible by the square of a small prime is $O(N^{1-\delta})$. Once we have this bound we can say that there are more than $C_4 N/(\log N)^k$ positive integers m not exceeding N such that $G(m)$ has at most $[k\sum_{j=1}^{k} 1/j + k\log\frac{5}{2}]$ small prime factors, *none of which occurs multiply*, and such that each $G_i(m)$ has at most $[9h_i/5]$ large prime factors multiple prime factors being counted multiply. The proof of the theorem will then be complete.

We shall actually show that the number of positive integers n not exceeding N such that

$$G(n) \equiv 0 \pmod{p^2}, \tag{6.0.4}$$

for some prime p with $N^{\delta} \leqslant p \leqslant N^{B}$, is $O(N^{1-\delta})$.

We will need to know that $\omega(p^2)$, the number of solutions of the congruence above, is absolutely bounded. It is well known that $\omega(p) = \omega(p^2)$ unless the system of equations

$$G(n) \equiv 0 \pmod{p}, \qquad G'(n) \equiv 0 \pmod{p} \qquad (G'(x) = d\big(G(x)\big)/dx)$$

is solvable. Since $\big(G(x), G'(x)\big) = 1$, there are polynomials $a(x)$ and $b(x)$ with integral coefficients and an integer C such that $a(x)G(x) + b(x)G'(x) = C$ for every integer x. Thus the number of primes for which solutions of the system exist is bounded by the number of prime divisors of C, so that $\omega(p^2)$ is bounded.

Now, the number of integers $n \leqslant N$ satisfying (6.0.4) is certainly less than

$$\sum_{N^{\delta} \leqslant p \leqslant N^{B}} \left(\frac{N}{p^2}\,\omega(p^2) + R_{p^2}\right),$$

where R_{p^2} is an error term not exceeding $\omega(p^2)$. This sum in turn is less than

$$2\sum_{N^{\delta} \leqslant p \leqslant N^{1/2}} \left(\frac{N}{p^2}\,\omega(p^2)\right) + O\left(\sum_{N^{1/2} \leqslant p \leqslant N^{B}} 1\right),$$

and this last quantity is

$$O\left(N\int_{N^{\delta}}^{N^{1/2}} \frac{1}{x^2}\,dx\right) + O(N^{5/9}),$$

which is $O(N^{1-\delta})$. Thus the number of $G(m)$ divisible by the square of a small prime is $O(N^{1-\delta})$ and this fact, as we have mentioned, completes the proof of Theorem 1.

7. An extension. The corollary to Theorem 1 can be obtained without any great amount of labor.

Suppose that

$$G(n) = b_0 n^m + b_1 n^{m-1} + \ldots + b_{m-1} n + b_m,$$

where $m = a_1 h_1 + \ldots + a_n h_n$ and b_0 is greater than zero. If b_0 is less than zero $G(n)$ can be replaced by $-G(n)$ in the following argument. Let H_1 denote the least common multiple of the denominators of $b_0, b_1, \ldots, b_m$ and let

$$H_2 = \prod_{p \leqslant m+1} p, \qquad H_3 = H_1 H_2.$$

Let $\{l_1, l_2, \ldots, l_s\}$ be a complete set of residues modulo H_3 and suppose that l_i has been chosen so that $G(l_i) > 0$ for $i = 1, 2, \ldots, s$ $(s = H_3)$. Let $D_i = H_3 G(l_i)$. Let us define the polynomial $F_i(t)$ by the equation:

$$G(D_i t + l_i) = G(l_i) F_i(t).$$

That is,

$$F_i(t) = 1 + b_{i,1} t + b_{i,2} t^2 + \ldots + b_{i,m} t^m,$$

where $b_{i,1}, b_{i,2}, \ldots,$ and $b_{i,m}$ are integers all of which are divisible by H_2. This last property insures that the number of solutions of the congruence $F_i(t) \equiv 0 \pmod{p}$ is always less than p.

Let D_0 and l_0 be any one of the pairs of integers D_i and l_i, and let $F_0(t)$ denote the corresponding polynomial. By the assumptions of the corollary and by a lemma of Gauss we have

$$F_0(t) = \prod_{j=1}^{k} \big(F_{0,j}(t)\big)^{a_j},$$

where $F_{0,j}(t)$ is an irreducible polynomial with integral coefficients. If we apply Theorem 1 to the polynomial

$$\prod_{j=1}^{k} \big(F_{0,j}(t)\big),$$

make allowance for the multiplicity of the irreducible factors, and let M denote the number of prime factors of $G(l_0)$ we shall have corollary 1.

References

[1] P. T. Bateman and R. Stemmler, *Waring's problem for algebraic number fields and primes of the form* $(p^r-1)/(p^a-1)$, Ill. J. Math. 6 (1962), pp. 142-156.

[2] V. Brun, *Le crible d'Eratosthène et le théorème de Goldbach*, Norske Videnskapselskapets Skripter I. Kristiania, 1920, no. 3.

[3] E. Landau, *Über die zu einem algebraischen Zahlkörper gehörige Zetafunction*, J. Reine Angew. Math. 125 (1903), pp. 64-188.

[4] E. Landau, *Einführung in die Elementare und Analytische Theorie der Algebraischen Zahlen und der Ideale*, second edition, Leipzig and Berlin 1927.

[5] B. V. Levin, *Estimates from below for the number of nearly-prime integers belonging to some general sequence*, Vestnik Leningrad Univ. 15, no. 7 (1960), pp. 48-65 (Russian).

[6] H. B. Mann, *Introduction to algebraic number theory*, Columbus, Ohio 1955.

[7] K. Prachar, *Primzahlverteilung*, Berlin-Gottingen-Heidelberg 1957.

[8] A. Selberg, *On an elementary method in the theory of primes*, Norske Vid. Selsk. Forh., Trondheim 19, no. 18 (1947), pp. 64-67.

[9] — *The general sieve-method and its place in prime number theory*, Proceedings of the International Congress of Mathematicians, Cambridge, Mass., 1950, vol. 1, pp. 286-292. Amer. Math. Soc., Providence, R. I., 1952.

[10] — *On elementary methods in prime number-theory and their limitations*, Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, pp. 13-22, Oslo 1952.

[11] Y. Wang, *On sieve methods and some of their applications*, Sci. Record (n. S.) 1 (1957), no. 3, pp. 1-5.

Reçu par la Rédaction le 10.4. 1963

ACTA ARITHMETICA
X(1964)

The general sieve

by

N. C. Ankeny and H. Onishi (Cambridge, Mass.)

Introduction. The sieve is a method used to derive bounds on the number of elements in a set of integers which are not divisible by any prime number in another set.

Let us suppose we are given a set S of integers, a set T of prime numbers, and $M(S, T)$ denotes the number of integers in S not divisible by any prime in T. We would now like to derive bounds on $M(S, T)$. For example, if $S_N = \{m \mid m \leqslant N\}$, $T_{\sqrt{N}} = \{p \mid p \leqslant \sqrt{N}\}$ where p ranges over all primes and N is positive, then $M(S_N, T_{\sqrt{N}})$ equals the number of prime numbers $> \sqrt{N}$ and $\leqslant N$.

To formulate the problem more precisely, define

(i) S_N as a set of N integers, for every positive integer N,

(ii) T as an infinite set of primes, T_Y as the set of primes in T less than a real number Y.

We are prepared now to observe the behavior of the function $M(S_N, T_{N^\lambda})$ for some fixed $\lambda > 0$, as $N \to \infty$. In order to do this we impose restrictions on the sets S_N, T_Y. These restrictions cover not only the classical cases of the sieve, but also several new cases.

Let d denote a square free integer all of whose prime factors are in T. We require the following assumptions:

(A) *For each N, there exists a real valued positive multiplicative function $f_N(d)$ such that*

$$\sum_{m} 1 = N f_N(d)^{-1} + R_d(N), \qquad m \in S_N, \quad d \mid m$$

(i.e. $f(d_1 d_2) = f(d_1) f(d_2)$ when $(d_1, d_2) = 1$).

(B) *There exist positive real numbers α, δ, C_1, C_2 such that $f_N(p)^{-1} < 1 - \delta$ for all $p \in T$,*

$$\sum_{p < X} p f_N(p)^{-1} < C_1 X (\log X)^{-1} \quad \text{for} \quad X \leqslant \log N,$$

$$\left| \sum (p f_N(p)^{-1} - \alpha) \right| < C_2 X (\log X)^{-2} \quad \text{for} \quad \log N < X < Y.$$