$$\ln|J(\omega)| \geqslant -\lambda^{r-1}(D\ln H(J)+N(J)\ln H)D^{r-2}$$
$$\geqslant -C_{55}\lambda^{r-1}D^{r-1}\mu^{2m}\Omega \geqslant -C_{56}\mu^{(2m+2)r-2}D^{r-1}\Omega.$$

But this contradicts the upper bound for $\ln|J(\omega)|$ as soon as μ is sufficiently large. Hence Theorem 3 is proved.

References

[1] P.-G. Becker-Landeck, *Quantitative Resultate im Zusammenhang mit der Mahlerschen Transzendenzmethode*, Dissertation, Universität zu Köln, 1984.

[2] — *Transcendence measures by Mahler's transcendence method*, Bull. Austral. Math. Soc. 33 (1986), 59–65.

[3] — *Maße für algebraische Unabhängigkeit nach einer Methode von Mahler*, Acta Arith. 50 (1988), 279–293.

[4] A. O. Galochkin, *Transcendence measures of values of functions satisfying certain functional equations*, Mat. Zametki 27 (1980), 175–183; English transl. in Math. Notes 27 (1980), 83–88.

[5] W. Miller, *Transcendence measures by a method of Mahler*, J. Austral. Math. Soc. Ser. A 32 (1982), 68–78.

[6] S. M. Molchanov, *Estimates for the measure of transcendence in the Mahler method* (in Russian), *Diophantine approximations*, Part 1, 56–65, Moskov. Gos. Univ., Mekh.-Mat. Fak., Moscow 1985.

[7] S. M. Molchanov and A. Ya. Yanchenko, *A measure of the algebraic independence of values of functions satisfying certain functional equations* (in Russian), *All-Union Conf. Theory of Transcendental Numbers and its Applications*, Izdat. Moskov. Gos. Univ., Moscow 1983, 98.

[8] Yu. V. Nesterenko, *Estimates for the orders of zeros of functions of a certain class and applications in the theory of transcendental numbers*, Izv. Akad. Nauk. SSSR Ser. Mat. 41 (1977), 235–284; English transl. in Math. USSR-Izv. 11 (1977), 239–270.

[9] — *On algebraic independence of algebraic powers of algebraic numbers*, Mat. Sb. 123 (165) (1984), 435–459; English transl. in Math. USSR-Sb. 51 (1985), 429–454.

[10] — *On a measure of the algebraic independence of the values of certain functions*, Mat. Sb. 128 (170) (1985), 545–568; English transl. in Math. USSR-Sb. 56 (1987), 545–567.

[11] K. Nishioka, *On an estimate for the orders of zeros of Mahler type functions*, Acta Arith. 56 (1990), 249–256.

[12] M. Waldschmidt, *Nombres transcendants*, Lecture Notes in Math. 402, Springer, Berlin 1974.

MATHEMATISCHES INSTITUT
UNIVERSITÄT ZU KÖLN
Weyertal 86-90
D-5000 Köln 41
Germany

Received on 24.4.1989
and in revised form on 4.5.1990 (1928)

ACTA ARITHMETICA
LVIII.3 (1991)

On an irreducibility theorem of I. Schur

by

MICHAEL FILASETA* (Columbia, S.C.)

Dedicated to the memory of Emil Grosswald

1. Introduction. In Grosswald's book *Bessel Polynomials* [7], he investigates various aspects of the Bessel polynomials

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j(n-j)!j!}x^j.$$

In particular, he discusses several results about the irreducibility of $y_n(x)$ over the rationals (also see [8, 9]). He proves that $y_n(x)$ is irreducible if $n = p^m$, $p+1$, or $p-1$ where p is a prime and m is a positive integer. He further shows that the largest degree of an irreducible factor of $y_n(x)$ is asymptotic to n. Later, Grosswald [10] pointed out that if $p_j < n \leqslant p_{j+1}$ where p_j and p_{j+1} are consecutive primes, then $y_n(x)$ is irreducible provided that the product $n(n+1)$ has a prime factor $> \min\{n-p_j+1, p_{j+1}-n\}$. This fact is sufficient enough to establish that $y_n(x)$ is irreducible for every $n \leqslant 10^6$. It may in fact imply that every $y_n(x)$ is irreducible, but to prove so seems to require a much better understanding of gaps between primes than is currently known. On the other hand, with a little work (cf. [5]), one can use Grosswald's observation to show that a positive proportion of the $y_n(x)$ are irreducible. More specifically, if $k_1(t)$ denotes the number of reducible $y_n(x)$ with $n \leqslant t$, then there is a constant $c < 1$ such that $k_1(t) \leqslant ct$ for all t sufficiently large.

Mainly motivated by Grosswald's work and his encouragement, the author pursued the problem of determining when $y_n(x)$ is irreducible. He was able to show [5] that $k_1(t) = o(t)$. Later in Section 4, we will see how work of Lagarias and Odlyzko [11] can aid in establishing that $k_1(t) \ll t/l_3(t)$ where $l_m(t)$ denotes m iterations of $\log t$. Under the assumption of the Generalized Riemann Hypothesis (GRH), the same arguments lead to $k_1(t) \ll t/\log\log t$. On the other hand, we shall see that Grosswald's observation above and the Riemann Hypothesis (RH) imply the better result $k_1(t) \ll t\exp((-1/\sqrt{2}+\varepsilon)\sqrt{\log t \log\log t})$ for any $\varepsilon > 0$.

* Research was supported in part by the NSF under grant number DMS-8903123.

We begin, however, by investigating polynomials of a different form which lend themselves to a similar analysis. In 1929, I. Schur [13] proved that if a_0, $a_1, \ldots, a_n$ are integers with $a_0 = \pm 1$ and $a_n = \pm 1$, then

$$f_n(x) = a_0\frac{x^n}{n!} + a_1\frac{x^{n-1}}{(n-1)!} + \ldots + a_{n-1}x + a_n$$

is irreducible. We shall be interested in investigating polynomials $f_n(x)$ in which the conditions $a_0 = \pm 1$ and $a_n = \pm 1$ may not hold. Clearly, a result as strong as Schur's cannot be true for every such polynomial since every $f(x) \in \mathbf{Z}[x]$ can be expressed in this form. It is our intent to employ Schur's method and a method similar to that used by the author [5] in proving the irreducibility of almost all Bessel polynomials to prove the following result:

THEOREM 1. *Let $B \in \mathbf{Z}^+$. Let $a_0, a_1, \ldots$ be non-zero integers such that*
(i) *each prime divisor of each a_j is $\leqslant B$, and*
(ii) *$|a_j| \leqslant (j/2)^j$ for all j sufficiently large.*
Let

$$f_n(x) = \sum_{j=0}^{n} a_j\frac{x^{n-j}}{(n-j)!} \quad \text{for } n = 1, 2, \ldots$$

Then almost all $f_n(x)$ are irreducible.

We shall furthermore see that as a consequence of Schur's method, each $f_n(x)$ satisfying $p \mid a_0 a_n \Rightarrow p \leqslant B$ has an irreducible factor of degree $> n - B$ (see Lemma 3). From the above theorem we easily get the following:

COROLLARY. *If $a_0, a_1, \ldots$ is a bounded sequence of non-zero integers and*

$$f_n(x) = \sum_{j=0}^{n} a_j\frac{x^{n-j}}{(n-j)!},$$

then almost all $f_n(x)$ are irreducible.

The proof of the theorem appears in the next two sections. We will show in Section 4 that we may obtain that if $a_0, a_1, \ldots$ is a bounded sequence of non-zero integers and $k_2(t)$ denotes the number of reducible polynomials $f_n(x)$ as above with $n \leqslant t$, then $k_2(t) \ll t/l_4(t)$. Under the assumption of the GRH, we get here that $k_2(t) \ll t/l_3(t)$.

2. Preliminaries. Using the notation of Section 1, we define

$$F_n(x) = n!\, f_n(x).$$

Thus, $F_n(x) \in \mathbf{Z}[x]$ and $F_n(x)$ is irreducible over the rationals if and only if $f_n(x)$ is irreducible over the rationals.

LEMMA 1. *Let $F_n(x)$ be as above and suppose $|a_j| \leqslant (n/2)^j$ for $j \geqslant 1$, $a_j \in \mathbf{Z}$ $\forall j$, and $a_0 \neq 0$. If α is a root of $F_n(x)$, then $|\alpha| < n^2$.*

Proof. Assume the lemma does not hold. Then for some root α of $F_n(x)$, $|\alpha| \geqslant n^2$. Thus,

$$0 = \left|\frac{F_n(\alpha)}{\alpha^n}\right| = \left|a_0 + a_1\frac{n}{\alpha} + a_2\frac{n(n-1)}{\alpha^2} + \ldots + a_n\frac{n!}{\alpha^n}\right|$$

$$\geqslant |a_0| - |a_1|\frac{n}{|\alpha|} - |a_2|\frac{n(n-1)}{|\alpha|^2} - \ldots - |a_n|\frac{n!}{|\alpha|^n}$$

$$\geqslant |a_0| - |a_1|\frac{n}{|\alpha|} - |a_2|\frac{n^2}{|\alpha|^2} - \ldots - |a_n|\frac{n^n}{|\alpha|^n}.$$

Now since $|\alpha| \geqslant n^2$, $1/|\alpha| \leqslant 1/n^2$. So

$$\left(\frac{n}{|\alpha|}\right)^j \leqslant \left(\frac{1}{n}\right)^j \quad \text{for all } j \geqslant 1$$

and hence

$$-\left(\frac{n}{|\alpha|}\right)^j \geqslant -\left(\frac{1}{n}\right)^j \quad \text{for all } j \geqslant 1.$$

Thus,

$$\left|\frac{F_n(\alpha)}{\alpha^n}\right| \geqslant |a_0| - |a_1|n^{-1} - \ldots - |a_n|n^{-n} \geqslant 1 - (|a_1|n^{-1} + \ldots + |a_n|n^{-n}).$$

Now $|a_j| \leqslant (n/2)^j$ implies $|a_j|n^{-j} \leqslant (\frac{1}{2})^j$, so

$$|a_1|n^{-1} + \ldots + |a_n|n^{-n} \leqslant \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} < 1.$$

Thus,

$$0 = \left|\frac{F_n(\alpha)}{\alpha^n}\right| > 1 - 1 = 0,$$

which is a contradiction. Hence, $|\alpha| < n^2$ for all roots α of $f_n(x)$, which concludes the proof.

LEMMA 2. *Let n and k be non-negative integers with $k < n$. Suppose $k \equiv n \pmod p$ for some prime p. Then $F_n(x) \equiv x^{n-k}F_k(x) \pmod p$.*

Proof. Assume n, k, and p are as above. Then

$$\begin{aligned} F_n(x) = n!\, f_n(x) &= a_0x^n + a_1nx^{n-1} + \ldots + n!\,a_n \\ &\equiv a_0x^n + a_1nx^{n-1} + \ldots + a_kn(n-1)\ldots(n-k+1)x^{n-k} \pmod p \\ &\equiv x^{n-k}(a_0x^k + a_1kx^{k-1} + \ldots + k!\,a_k) \pmod p \\ &\equiv x^{n-k}F_k(x) \pmod p. \end{aligned}$$

This completes the proof.

Throughout the rest of this paper we shall let $Q(\alpha)$ denote an algebraic extension of Q. Let R denote the ring of algebraic integers in $Q(\alpha)$. Let $N(\beta)$ denote the norm of β where $\beta \in R$. If A is an ideal in R, then $N(A)$ will denote the norm of A.

The next result will play a major role in what follows. We note that it is essentially due to Schur [13]. In fact, the result of Schur mentioned in the Introduction follows from the case $B = 1$ below.

LEMMA 3. *Let n and B be positive integers. Let $a_0, a_1, \ldots, a_n \in Z$ be such that if $p | a_0 a_n$ then $p \leqslant B$. Let $f_n(x)$ be as above. Suppose $f_n(x) = a(x)b(x)$, where $a(x), b(x) \in Q[x]$ and $1 \leqslant \deg a(x) = k \leqslant n/2$. Then $k < B$.*

To prove Lemma 3, we will need the following three lemmas. The first lemma is a nice generalization of Bertrand's Postulate and was originally proved by Sylvester [16]. Schur rediscovered it in obtaining his result mentioned in the Introduction (also see [4]). We omit its proof as well as the proof of the third lemma below which can be found in [1, p. 202].

LEMMA 3.1. *Let k and m be positive integers with $m > k$. Then one of the numbers $m, m+1, \ldots, m+k-1$ is divisible by some prime $p > k$.*

LEMMA 3.2. *Let $\beta \in R$ and suppose p is a rational prime dividing $N(\beta)$. Then there is a prime ideal P dividing (p) such that $P | (\beta)$.*

Proof. It suffices to show that $\mathrm{GCD}((\beta),(p)) \neq (1)$. Assume to the contrary that $\mathrm{GCD}((\beta),(p)) = (1)$. Then $(\beta)+(p) = (1)$ and thus there are λ_1 and λ_2 in R such that $\beta\lambda_1 + p\lambda_2 = 1$. Thus $N(\beta)N(\lambda_1) = N(\beta\lambda_1) = N(1-p\lambda_2)$. Now since p divides $N(\beta)$, we get that $N(1-p\lambda_2) \equiv 0 \pmod p$. Let $\lambda_2^{(1)} = \lambda_2$, $\lambda_2^{(2)}, \ldots, \lambda_2^{(m)}$ be the field conjugates of λ_2. Let $\sigma_1 = \lambda_2^{(1)} + \ldots + \lambda_2^{(m)}, \ldots, \sigma_m = \lambda_2^{(1)} \ldots \lambda_2^{(m)}$ be the elementary symmetric functions for $\lambda_2^{(1)}, \ldots, \lambda_2^{(m)}$. Then $\sigma_1, \ldots, \sigma_m \in Z$, and

$$N(1-p\lambda_2) = \prod_{j=1}^{m} (1-p\lambda_2^{(j)}) = 1 - \sigma_1 p + \sigma_2 p^2 - \ldots + (-1)^m \sigma_m p^m \equiv 1 \pmod p.$$

Hence, we get a contradiction which establishes the lemma.

LEMMA 3.3. *Let k be the degree of the minimal polynomial for α, and let P be a prime ideal dividing (p) where p is a rational prime. Then $N(P) = p^f$ where $1 \leqslant f \leqslant k$.*

Proof of Lemma 3. Suppose $k \geqslant B$. Define

$$F(x) = n! a_0^{n-1} f_n(x)$$
$$= (a_0 x)^n + n a_1 (a_0 x)^{n-1} + \ldots + n! a_{n-1} a_0^{n-2} (a_0 x) + n! a_n a_0^{n-1}.$$

Define

$$G(x) = x^n + n a_1 x^{n-1} + \ldots + n! a_{n-1} a_0^{n-2} x + n! a_n a_0^{n-1}$$

so that

$$G(x) = F\left(\frac{x}{a_0}\right) = a\left(\frac{x}{a_0}\right) b\left(\frac{x}{a_0}\right) n! a_0^{n-1}.$$

So by Gauss' Lemma $G(x) = A(x)B(x)$ where $A(x), B(x) \in Z[x]$ and $\deg A(x) = \deg a(x) = k$. Since $G(x)$ is monic, we may take $A(x)$ to be monic, say $A(x) = x^k + b_{k-1}x^{k-1} + \ldots + b_0$.

Suppose p is a prime such that $p | b_0$. We prove next that $p \leqslant k$. Since $p | b_0$, $p | n! a_n a_0^{n-1}$ and hence $p | a_n a_0^{n-1}$ or $p | n!$. If $p | a_0^{n-1} a_n$ then $p | a_0 a_n$ and hence $p \leqslant B \leqslant k$ by assumption. Thus we may assume $p \nmid a_0^{n-1} a_n$ and hence $p | n!$. Factor $A(x)$ into irreducible polynomials, say $A(x) = A_1(x) \ldots A_{k_0}(x)$ where $A_i(x) \in Z[x]$ for all $i = 1, 2, \ldots, k_0$. Note that since p divides the constant term in $A(x)$, there must be an irreducible factor of $A(x)$ such that p divides its constant term. Let us consider this factor and call it $A_i(x)$. Observe that we may take $A_i(x)$ to be monic since $A(x)$ is. Let $A_i(x) = x^c + d_{c-1}x^{c-1} + \ldots + d_0$ and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_c$ be the roots of $A_i(x)$. Let R denote the ring of algebraic integers in $Q(\alpha)$, and note that since $A_i(x)$ is monic, $\alpha \in R$. Then $d_0 = \pm \prod_{i=1}^{c} \alpha_i$ and hence $N(\alpha) = \pm d_0 \equiv 0 \pmod p$. Hence by Lemma 3.2 there exists a prime ideal P in R such that $P | (\alpha)$ and $P | (p)$. Write $(\alpha) = P^r M$ and $(p) = P^s N$ where $(M, P) = (N, P) = (1)$ and $r \geqslant 1$ and $s \geqslant 1$. Also, by Lemma 3.3, $s \leqslant c \leqslant k$.

Now since $A_i(\alpha) = 0$, $G(\alpha) = 0$ and thus

$$\alpha^n + n a_1 \alpha^{n-1} + \ldots + n! a_n a_0^{n-1} = 0. \tag{1}$$

Let $v \in Z^+$ and $h_v = [v/p] + [v/p^2] + \ldots$, and so $p^{h_v} | v!$ but $p^{h_v+1} \nmid v!$.

Consider the term $(n!/v!) a_{n-v} a_0^{n-v-1} \alpha^v$ in (1) where $v \in \{1, 2, \ldots, n-1\}$. Note that

$$p^{h_n - h_v} \Big| \frac{n!}{v!} \quad \text{and} \quad p^{h_n - h_v + 1} \nmid \frac{n!}{v!}.$$

From the relations $p^{h_n - h_v} | (n!/v!)$ and $P^s | (p)$ we get that $P^{s(h_n - h_v)} | (n!/v!)$. So

$$P^{h_n s + rv - h_v s} \Big| \left(\frac{n!}{v!}\right) (a_{n-v}) (a_0)^{n-v-1} (\alpha)^v.$$

Note also that $P^{h_n s + rn - h_n s} = P^{rn}$ divides $(\alpha)^n$. Suppose there does not exist a $v \in \{1, 2, \ldots, n\}$ such that $rv \leqslant h_v s$. Then for each $v \in \{1, 2, \ldots, n-1\}$, we get that $P^{h_n s + 1}$ divides $(n!/v!)(a_{n-v})(a_0)^{n-v-1}(\alpha)^v$ and $P^{h_n s + 1} | (\alpha)^n$ which implies that $P^{h_n s + 1}$ divides $\mathrm{GCD}((n!)(a_{n-1})(a_0)^{n-2}(\alpha), \ldots, (\alpha)^n)$. Thus, from (1),

$$n! a_n a_0^{n-1} \in (\alpha)^n + \ldots + (n! a_{n-1} a_0^{n-2} \alpha) = \mathrm{GCD}((\alpha)^n, \ldots, (n! a_{n-1} a_0^{n-2} \alpha)) \subseteq P^{h_n s + 1}.$$

Therefore $(n! a_n a_0^{n-1}) \subseteq P^{h_n s + 1}$ and hence $P^{h_n s + 1} | (n! a_n a_0^{n-1})$. But p is a prime such that $p \nmid a_0 a_n$ and $P | (p)$ so that $\mathrm{GCD}(P, (a_n a_0^{n-1})) = (1)$. Thus, we get that $P^{h_n s + 1} | (n!)$. On the other hand, $P^s \| (p)$ and $p^{h_n} \| n!$ imply $P^{h_n s} \| (n!)$ which is

a contradiction. Thus $rv \leqslant h_v s$ for some $v \in \{1, \ldots, n\}$. Fix such a v in $\{1, \ldots, n\}$. Since $h_v < v/p + v/p^2 + \ldots = v/(p-1)$, we get that

$$v \leqslant rv \leqslant h_v s < \frac{vs}{p-1} \leqslant \frac{vk}{p-1}$$

and thus $p-1 < k$. Hence $p \leqslant k$ if p is any prime divisor of b_0.

Now let $m = n-k+1$. Since $k \leqslant n/2$,

$$m = n-k+1 \geqslant k+1 > k$$

so by Lemma 3.1, there is a prime $p > k$ such that $p \mid (n-k+1)\ldots(n-1)n$. But

$$\begin{aligned} G(x) &= A(x)B(x) \\ &= x^n + na_1x^{n-1} + \ldots + n!a_n a_0^{n-1} \\ &\equiv x^n + na_1x^{n-1} + \ldots + n(n-1)\ldots(n-k+2)a_{k-1}a_0^{k-2}x^{n-k+1} \pmod{p} \\ &\equiv x^{n-k+1}(x^{k-1} + na_1x^{k-2} + \ldots + n(n-1)\ldots(n-k+2)a_{k-1}a_0^{k-2}) \pmod{p}. \end{aligned}$$

Now $\deg B(x) = n-k$ and hence $A(x)$ is divisible by x modulo p. Thus $p \mid b_0$ which implies $p \leqslant k$. This contradicts that $p > k$.

Consequently $k < B$, which completes the proof.

We will now explain our strategy behind the proof of the theorem. Fix a non-negative integer n and assume $F_n(x)$ is reducible. Then $F_n(x) = g(x)h(x)$ where

$$g(x) = \sum_{j=0}^{r} b_j x^j \quad \text{and} \quad h(x) = \sum_{j=0}^{s} c_j x^j$$

with b_j, $c_j \in \mathbf{Z}$ for all j and r, $s \geqslant 1$.

Let k be a non-negative integer and p be a prime such that $p > B$ and $n \equiv k \pmod{p}$. Suppose further that $F_k(x)$ is irreducible modulo p. It follows from Lemma 2 that

$$F_n(x) = g(x)h(x) \equiv F_k(x)x^{n-k} \pmod{p}.$$

Now since $F_k(x)$ is irreducible modulo p and polynomials in $\mathbf{Z}_p[x]$ have unique factorization, $F_k(x)$ must divide either $g(x)$ or $h(x)$. Hence, the other factor is a constant times a power of x modulo p.

Now since $p > B$, p does not divide a_0 and hence p divides neither b_r nor c_s. Thus, either $g(x) \equiv b_r x^r$ or $h(x) \equiv c_s x^s \pmod{p}$. Hence, p divides all the coefficients of $g(x)$ or $h(x)$ with the exception of the leading coefficient.

Next we prove that at least one element of $\{b_{r-1}, b_{r-2}, \ldots, b_u\}$ where $u = \max\{0, r-B\}$ is non-zero. By Lemma 3 either $\deg g(x) = r \leqslant B-1$ or $\deg h(x) = s \leqslant B-1$. In the first case where $r \leqslant B-1$, $b_0 c_0 = a_n \neq 0$ and hence $b_0 \neq 0$. Suppose now that $r \geqslant B$. Then $s \leqslant B-1$. Assume each of b_{r-1}, $b_{r-2}, \ldots, b_{r-B}$ is 0. Then

$$g(x) = b_r x^r + b_{r-B-1}x^{r-B-1} + \ldots + b_1 x + b_0;$$

if $r = B$, then we interpret this to mean that $g(x) = b_r x^r$. Thus,

$$\begin{aligned} F_n(x) &= g(x)h(x) \\ &= b_r x^r h(x) + b_{r-B-1}x^{r-B-1}h(x) + \ldots + b_1 x h(x) + b_0 h(x). \end{aligned} \tag{2}$$

Now we observe that all the terms in (2), with the exception of $b_r x^r h(x)$, have degree less than or equal to $r-2$ since $\deg h(x) \leqslant B-1$. Thus, the coefficient of x^{r-1} is 0, which contradicts our original assumption that all the a_j's are non-zero. Hence, one element of $\{b_{r-1}, b_{r-2}, \ldots, b_u\}$ is non-zero. A similar argument shows that one element of $\{c_{s-1}, c_{s-2}, \ldots, c_v\}$ where $v = \max\{0, s-B\}$ is non-zero.

Fix $u_0 \in \{r-1, r-2, \ldots, u\}$ and $v_0 \in \{s-1, s-2, \ldots, v\}$ with $b_{u_0}c_{v_0} \neq 0$. By condition (ii) of the theorem, we have that for all j sufficiently large, $|a_j| \leqslant (j/2)^j$ so that for all n sufficiently large, we get that $|a_j| \leqslant (n/2)^j$ for every $j \in \{1, 2, \ldots, n\}$. Hence, by Lemma 1, each root α of $F_n(x)$ satisfies $|\alpha| < n^2$. Now by considering the elementary symmetric functions for the roots of $g(x)$, we see that

$$\left|\frac{b_{r-1}}{b_r}\right| \leqslant \binom{r}{1}(n^2) \leqslant \binom{n}{1}n^2$$

which implies

$$|b_{r-1}| \leqslant |b_r|\binom{n}{1}n^2 \leqslant |a_0|\binom{n}{1}n^2.$$

Also,

$$\left|\frac{b_{r-2}}{b_r}\right| \leqslant \binom{r}{2}(n^2)^2 \leqslant \binom{n}{2}n^4,$$

and hence,

$$|b_{r-2}| \leqslant |a_0|\binom{n}{2}n^4.$$

Continuing in this manner, and using that $1 \leqslant r-u_0 \leqslant B+1$, we obtain

$$|b_{u_0}| \leqslant |b_r|\binom{r}{r-u_0}(n^2)^{r-u_0} \leqslant |a_0|\binom{n}{r-u_0}n^{2(r-u_0)} \leqslant |a_0|\,n^{B+1}\,n^{2(B+1)}.$$

Similarly,

$$|c_{v_0}| \leqslant |a_0|\binom{n}{s-v_0}n^{2(s-v_0)} \leqslant |a_0|n^{B+1}n^{2(B+1)}.$$

Hence,

$$|b_{u_0}||c_{v_0}| \leqslant |a_0|^2 n^{6(B+1)}. \tag{3}$$

The idea is to show that there are many such k and p as above. Since $b_{u_0}c_{v_0} \neq 0$ and each such p divides $b_{u_0}c_{v_0}$, we will get that $|b_{u_0}c_{v_0}|$ is large. We will, in fact, show that almost always $|b_{u_0}c_{v_0}|$ is too large for (3) to hold. In other words, for almost all n we will get a contradiction to the assumption that $F_n(x)$ is reducible. Hence, our theorem will follow.

3. Proof of the Theorem. Let t be a sufficiently large real number. For each positive integer k, define

$$A_k = \{p \text{ prime: } F_k(x) \text{ is irreducible modulo } p\}$$

and

$$A_k(t) = |A_k \cap (1, t]|.$$

Let m and n denote positive integers with $n \leqslant t$. Also, let p, q, p_1, p_2, q_1, and q_2 denote primes. Define $\theta = 1/4$, $\phi = 1/3$ and

$$\alpha(n) = \alpha_m(n) = \sum_{B<q\leqslant m} \sum_{\substack{t^\theta < p \leqslant t^\phi \\ p\in A_q \\ n\equiv q \pmod p}} 1. \tag{4}$$

Now suppose $m \leqslant t^\theta$ so that if $p \in (t^\theta, t^\phi]$, then $p > m$. Observe that if q_1 and q_2 are distinct primes in $(B, m]$, then since $p > m$, at most one of $n \equiv q_1 \pmod p$ or $n \equiv q_2 \pmod p$ can hold. Thus each prime p in (4) occurs at most once. Now if we can show $\alpha(n) \geqslant 24B+25$, then by Lemma 2 and the discussion at the end of the last section, we get that there are $\geqslant 24B+25$ distinct primes p dividing $b_{u_0}c_{v_0}$ with each $p > t^\theta$. Also, $b_{u_0}c_{v_0} \neq 0$ and $n \leqslant t$ imply that

$$\begin{aligned} |b_{u_0}c_{v_0}| &\geqslant (t^\theta)^{24B+25} = t^{(24B+25)/4} \\ &= t^{1/4}t^{6(B+1)} \geqslant t^{1/4}n^{6(B+1)} > |a_0|^2 n^{6(B+1)} \end{aligned}$$

since t is sufficiently large. As we previously described, this would imply that $F_n(x)$ is irreducible and hence $f_n(x)$ is irreducible. Thus, all that remains to show is that $\alpha(n) \geqslant 24B+25$ for almost all n. We shall prove the stronger result that for any constant C, $\alpha(n) \geqslant C$ for almost all n. We begin with

LEMMA 4. *Let m be a positive integer which is $\leqslant t^\theta$. Define $I = (t^\theta, t^\phi]$. Then*

$$\sum_{n\leqslant t}\left(\alpha(n) - \left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)\right)^2 = t\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p} + E$$

where $E \ll t^{3/4}m^2$.

Proof. We first estimate

$$\sum_{n\leqslant t}\alpha(n) \quad \text{and} \quad \sum_{n\leqslant t}\alpha^2(n).$$

For the first sum, we get

$$\begin{aligned} \sum_{n\leqslant t}\alpha(n) &= \sum_{n\leqslant t}\sum_{B<q\leqslant m}\sum_{\substack{p\in I\cap A_q \\ n\equiv q \pmod p}} 1 = \sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\sum_{\substack{n\leqslant t \\ n\equiv q \pmod p}} 1 \\ &= \sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\left(\frac{t}{p}+O(1)\right) = t\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)+E_1 \end{aligned} \tag{5}$$

where

$$E_1 = \sum_{B<q\leqslant m}\sum_{p\in I\cap A_q} O(1) \ll \sum_{B<q\leqslant m}\sum_{p\in I\cap A_q} 1 \leqslant \sum_{B<q\leqslant m}\sum_{p\leqslant t^\phi} 1 \leqslant \sum_{B<q\leqslant m}\pi(t^\phi),$$

where $\pi(x)$ denotes the number of primes $\leqslant x$. Hence, by the Prime Number Theorem,

$$|E_1| \ll \frac{t^\phi}{\log t}m.$$

For the second sum we get

$$\sum_{n\leqslant t}\alpha^2(n) = \sum_{n\leqslant t}\Big(\sum_{B<q\leqslant m}\sum_{\substack{p\in I\cap A_q \\ n\equiv q \pmod p}} 1\Big)^2 = \sum_1 + \sum_2 + \sum_3 + \sum_4$$

where

$$\sum_1 = \sum_{n\leqslant t}\sum_{B<q\leqslant m}\sum_{\substack{p\in I\cap A_q \\ n\equiv q \pmod p}} 1,$$

$$\sum_2 = \sum_{n\leqslant t}\sum_{B<q\leqslant m}\sum_{\substack{p_1\in I\cap A_q \\ n\equiv q \pmod{p_1}}}\sum_{\substack{p_2\in I\cap A_q\setminus\{p_1\} \\ n\equiv q \pmod{p_2}}} 1,$$

$$\sum_3 = \sum_{n\leqslant t}\sum_{B<q_1\leqslant m}\sum_{\substack{B<q_2\leqslant m \\ q_2\neq q_1}}\sum_{\substack{p\in I\cap A_{q_1}\cap A_{q_2} \\ n\equiv q_1 \pmod p \\ n\equiv q_2 \pmod p}} 1,$$

$$\sum_4 = \sum_{n\leqslant t}\sum_{B<q_1\leqslant m}\sum_{\substack{B<q_2\leqslant m \\ q_2\neq q_1}}\sum_{\substack{p_1\in I\cap A_{q_1} \\ n\equiv q_1 \pmod{p_1}}}\sum_{\substack{p_2\in I\cap A_{q_2}\setminus\{p_1\} \\ n\equiv q_2 \pmod{p_2}}} 1.$$

Next we estimate the above sums. By (5),

$$\sum_1 = \sum_{n\leqslant t}\alpha(n) = t\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)+E_1.$$

Also,

$$\begin{aligned} \sum_2 &= \sum_{n\leqslant t}\sum_{B<q\leqslant m}\sum_{\substack{p_1\in I\cap A_q \\ n\equiv q \pmod{p_1}}}\sum_{\substack{p_2\in I\cap A_q\setminus\{p_1\} \\ n\equiv q \pmod{p_2}}} 1 \\ &= \sum_{n\leqslant t}\sum_{B<q\leqslant m}\Big(\sum_{\substack{p_1,p_2\in I\cap A_q \\ n\equiv q \pmod{p_1p_2}}} 1 - \sum_{\substack{p\in I\cap A_q \\ n\equiv q \pmod{p^2}}} 1\Big) \end{aligned}$$

$$= \sum_{B<q\leqslant m} \sum_{p_1,p_2\in I\cap A_q} \left(\frac{t}{p_1p_2}+O(1)\right) - \sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} \left(\frac{t}{p^2}+O(1)\right)$$

$$= t \sum_{B<q\leqslant m} \left(\sum_{p\in I\cap A_q} \frac{1}{p}\right)^2 + E_2,$$

where

$$E_2 = \sum_{B<q\leqslant m} \sum_{p_1,p_2\in I\cap A_q} O(1) - \sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} \left(\frac{t}{p^2}+O(1)\right)$$

$$\ll \sum_{B<q\leqslant m} \sum_{p_1,p_2\in I\cap A_q} 1 + t \sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} \frac{1}{p^2} + \sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} 1.$$

Now

$$t \sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} \frac{1}{p^2} \leqslant t \sum_{B<q\leqslant m} \sum_{n\geqslant t^\theta} \frac{1}{n^2},$$

but

$$\sum_{n\geqslant z} \frac{1}{n^2} \leqslant \int_{z-1}^{\infty} \frac{1}{y^2}dy = -\frac{1}{y}\Big|_{z-1}^{\infty} = \frac{1}{z-1},$$

and so

$$t \sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} \frac{1}{p^2} \leqslant t \sum_{B<q\leqslant m} \frac{1}{t^\theta-1} \ll t^{1-\theta}m.$$

Hence,

$$E_2 \ll \sum_{B<q\leqslant m} \Big(\sum_{p\in I\cap A_q} 1\Big)^2 + \sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} 1 + t^{1-\theta}m.$$

Therefore, by the Prime Number Theorem,

$$E_2 \ll \left(\frac{t^\phi}{\phi\log t}\right)^2 \Big(\sum_{B<q\leqslant m} 1\Big) + \left(\frac{t^\phi}{\phi\log t}\right) \sum_{B<q\leqslant m} 1 + t^{1-\theta}m,$$

so

$$|E_2| \ll \left(\frac{t^\phi}{\log t}\right)^2 m + \frac{t^\phi}{\log t}m + t^{1-\theta}m.$$

Observe that $\sum_3 = 0$ because $p > t^\theta$ implies $p > m$.

Finally,

$$\sum_4 = \sum_{n\leqslant t} \sum_{B<q_1\leqslant m} \sum_{\substack{B<q_2\leqslant m\\ q_2\neq q_1}} \sum_{\substack{p_1\in I\cap A_{q_1}\\ n\equiv q_1 (\mathrm{mod}\, p_1)}} \sum_{\substack{p_2\in I\cap A_{q_2}\setminus\{p_1\}\\ n\equiv q_2 (\mathrm{mod}\, p_2)}} 1$$

$$= \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{p_1\in I\cap A_{q_1}} \sum_{p_2\in I\cap A_{q_2}\setminus\{p_1\}} \sum_{\substack{n\leqslant t\\ n\equiv q_1 (\mathrm{mod}\, p_1)\\ n\equiv q_2 (\mathrm{mod}\, p_2)}} 1$$

$$= \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{p_1\in I\cap A_{q_1}} \sum_{p_2\in I\cap A_{q_2}\setminus\{p_1\}} \left(\frac{t}{p_1p_2}+O(1)\right)$$

$$= t \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \left[\left(\sum_{p\in I\cap A_{q_1}} \frac{1}{p}\right)\left(\sum_{p\in I\cap A_{q_2}} \frac{1}{p}\right) - \sum_{p\in I\cap A_{q_1}\cap A_{q_2}} \frac{1}{p^2}\right]$$

$$+ \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{\substack{p_1\in I\cap A_{q_1}\\ p_2\in I\cap A_{q_2}\setminus\{p_1\}}} O(1)$$

$$= t \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \left[\left(\sum_{p\in I\cap A_{q_1}} \frac{1}{p}\right)\left(\sum_{p\in I\cap A_{q_2}} \frac{1}{p}\right)\right] + E_4,$$

where

$$E_4 = \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{\substack{p_1\in I\cap A_{q_1}\\ p_2\in I\cap A_{q_2}\setminus\{p_1\}}} O(1) - t \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{p\in I\cap A_{q_1}\cap A_{q_2}} \frac{1}{p^2}.$$

Now

$$t \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{p\in I\cap A_{q_1}\cap A_{q_2}} \frac{1}{p^2} \leqslant t \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{n\geqslant t^\theta} \frac{1}{n^2},$$

which, as before, yields

$$t \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{p\in I\cap A_{q_1}\cap A_{q_2}} \frac{1}{p^2} \leqslant t \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \frac{1}{t^\theta-1} \ll t^{1-\theta}m^2.$$

Hence,

$$E_4 \ll \Big(\sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{\substack{p_1\in I\cap A_{q_1}\\ p_2\in I\cap A_{q_2}\setminus\{p_1\}}} 1\Big) + t^{1-\theta}m^2$$

$$\leqslant \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \sum_{\substack{p_1\in I\cap A_{q_1}\\ p_2\in I\cap A_{q_2}}} 1 + t^{1-\theta}m^2 \ll \sum_{\substack{B<q_1,q_2\leqslant m\\ q_2\neq q_1}} \left(\frac{t^\phi}{\phi\log t}\right)^2 + t^{1-\theta}m^2.$$

Thus

$$|E_4| \ll \left(\frac{t^\phi}{\log t}\right)^2 m^2 + t^{1-\theta}m^2.$$

By combining these estimates for $\sum_1$, $\sum_2$, $\sum_3$, and $\sum_4$, we get

$$(6)\quad \sum_{n\leqslant t} \alpha^2(n) = t\left[\left(\sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} \frac{1}{p}\right) + \left(\sum_{B<q\leqslant m} \sum_{p\in I\cap A_q} \frac{1}{p}\right)^2\right] + E_1 + E_2 + E_4.$$

Now

$$\sum_{n\leqslant t}\left(\alpha(n)-\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)\right)^2$$

$$=\sum_{n\leqslant t}\alpha^2(n)-2\Big(\sum_{n\leqslant t}\alpha(n)\Big)\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)+\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)^2[t].$$

Thus, from (5) and (6) we have

$$\sum_{n\leqslant t}\left(\alpha(n)-\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)\right)^2=t\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}+E,$$

where

$$E\ll E_2+E_4+E_1\left|1-2\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right|+\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)^2$$

$$\ll\left(\frac{t^\phi}{\log t}\right)^2m+\left(\frac{t^\phi}{\log t}\right)m+t^{1-\theta}m+\left(\frac{t^\phi}{\log t}\right)^2m^2+t^{1-\theta}m^2$$

$$+\left(\frac{t^\phi}{\log t}m\right)\left(1+2\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)+\left(\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\right)^2.$$

We note that

$$\sum_{B<q\leqslant m}\sum_{p\in I\cap A_q}\frac{1}{p}\leqslant\sum_{B<q\leqslant m}\sum_{p\leqslant t^\phi}\frac{1}{t^\theta}\leqslant t^{\phi-\theta}m.$$

Now our choices of $\theta=1/4$ and $\phi=1/3$ imply easily that

$$E\ll t^{3/4}m^2.$$

This completes the proof.

To apply Lemma 4, we will make use of the Chebotarev Density Theorem. For q a prime, we view the Galois group G associated with $F_q(x)$ as a subgroup of S_q, the symmetric group on q letters. We will establish that the proportion of q-cycles in G is at least $1/q$. In fact, for any subgroup G of S_n (where n is any positive integer) which contains at least one n-cycle, the proportion of n-cycles in G is at least $1/n$ as we now show. Let C_n denote the set of n-cycles in G. Note that by definition, $|C_n|\geqslant 1$. Fix $g_0\in C_n$. Define $\phi\colon G\to G$ by $\phi(g)=g^{-1}g_0g$.

LEMMA 5. *Let $g_1\in\operatorname{Im}\phi$. Then*

$$|\{g\in G\colon\ \phi(g)=g_0\}|=|\{g\in G\colon\ \phi(g)=g_1\}|.$$

Proof. Define $A=\{g\in G\colon\ \phi(g)=g_0\}$ and $B=\{g\in G\colon\ \phi(g)=g_1\}$. Note that $A, B\neq\emptyset$. Let $h\in B$ and define $\theta(g)=g^{-1}h$ where $g\in A$. We prove first that $|A|\leqslant|B|$ by showing that θ is a one-to-one map from A into B.

Since $h\in B$, $h^{-1}g_0h=g_1$. So $g\in A$ implies

$$(g^{-1}h)^{-1}g_0(g^{-1}h)=h^{-1}g(g^{-1}g_0g)g^{-1}h=h^{-1}g_0h=g_1.$$

Therefore, $g^{-1}h\in B$. Now suppose there are $g_1, g_2\in A$ such that $g_1^{-1}h=g_2^{-1}h$. Then $h=g_1g_2^{-1}h$ which implies $e=g_1g_2^{-1}$ where e is the identity element and hence $g_2=g_1$. So θ is 1-1. Thus $|A|\leqslant|B|$.

Now define $\theta'(g)=hg^{-1}$ where $g, h\in B$. We now show that θ' is a one-to-one map from B into A and hence $|B|\leqslant|A|$. Since $h\in B$ and $g\in B$, $h^{-1}g_0h=g_1$ and $g^{-1}g_0g=g_1$. So

$$(hg^{-1})^{-1}g_0(hg^{-1})=gh^{-1}(hg_1h^{-1})hg^{-1}=gg_1g^{-1}=g_0.$$

Therefore, $hg^{-1}\in A$. The same argument we used to show θ is a 1-1 function also shows that θ' is 1-1 and thus $|B|\leqslant|A|$.

Hence, $|\{g\in G\colon\ \phi(g)=g_0\}|=|\{g\in G\colon\ \phi(g)=g_1\}|$.

LEMMA 6. $|\{g\in G\colon\ \phi(g)=g_0\}|=n$.

Proof. Let $A=\{g\in G\colon\ \phi(g)=g_0\}$ as before. Note that $\phi(g)=g_0$ if and only if $g^{-1}g_0g=g_0$ if and only if $g_0g=gg_0$. Thus, the elements in A are precisely those elements $g\in G$ that commute with g_0. Clearly $\{g_0, g_0^2, \dots, g_0^n\}\subseteq A$. We will show that $A=\{g_0, g_0^2, \dots, g_0^n\}$.

Suppose $g\in A$ and $g_0=(a_1a_2\dots a_n)$. Then $g_0^2(a_1)=a_3$, $g_0^3(a_1)=a_4, \dots$ Hence, $\{g_0(a_1), \dots, g_0^n(a_1)\}=\{a_2, a_3, \dots, a_n, a_1\}$. So $g(a_1)=g_0^j(a_1)$ for some $j=1, 2, \dots, n$. Thus, we have $g(a_k)=g(g_0^{k-1}(a_1))=g_0^{k-1}(g(a_1))=g_0^{k-1}(g_0^j(a_1))=g_0^{k-1+j}(a_1)=g_0^j(g_0^{k-1}(a_1))=g_0^j(a_k)$. Since a_k was arbitrary, $g=g_0^j$. Thus, $A=\{g_0, g_0^2, \dots, g_0^n\}$. Since $g_0(a_1), g_0^2(a_1), \dots, g_0^n(a_1)$ are distinct, so are the elements $g_0, g_0^2, \dots, g_0^n$ of A. Hence, $|A|=n$.

LEMMA 7. *Let G be a subgroup of S_n containing at least one n-cycle. Then the number of n-cycles in G is $\geqslant(1/n)|G|$.*

Proof. Let G, C_n, ϕ, and A be as in the above lemmas, and let $g\in G$. First we note that $g^{-1}g_0g$ is indeed an n-cycle since if $g_0=(a_1a_2\dots a_n)$ then

$$g^{-1}g_0g(g^{-1}(a_j))=g^{-1}g_0(a_j)=g^{-1}(a_{j+1})$$

and so

$$g^{-1}g_0g=(g^{-1}(a_1)\dots g^{-1}(a_n)).$$

Thus,

$$|C_n|\geqslant|\operatorname{Im}\phi|=|G|/|A|.$$

This relation and Lemma 6 imply that $|C_n|/|G|\geqslant 1/n$.

We are now ready to apply the Chebotarev Density Theorem.

LEMMA 8. *If q is prime with $q > B$, then*

$$A_q(t) \sim r_q \frac{t}{\log t}$$

where r_q is independent of t and satisfies $1/q \leqslant r_q \leqslant 1$.

Proof. If q is prime with $q > B$ then $F_q(x) = q! f_q(x) = a_0 x^q + a_1 q x^{q-1} + \ldots + a_q q!$ is such that $q \nmid a_0 a_q$. Thus, $F_q(x)$ is Eisenstein with respect to q and hence is irreducible. Let $r_q = |C_q|/|G|$ where G denotes the Galois group for $F_q(x)$ and C_q denotes the set of q-cycles in G. Clearly, $r_q \leqslant 1$. For any root α of $F_q(x)$, the extension $\boldsymbol{Q}(\alpha)$, which is contained in the splitting field of $F_q(x)$, has dimension q over $\boldsymbol{Q}$ so that q divides $|G|$. Thus, since q is a prime, G must contain at least one q-cycle; hence, by Lemma 7, $r_q \geqslant 1/q$. The Chebotarev Density Theorem (cf. [3], [6]; also see Section 4 of this paper) implies that the proportion of primes p for which $F_q(x)$ is irreducible modulo p is equal to the proportion of q-cycles in G, which implies the desired result.

Observe that by Lemma 8, for a fixed q, we have that

$$\sum_{p \in I \cap A_q} \frac{1}{p} = \int_{t^\theta}^{t^\phi} \frac{1}{y} dA_q(y) = \frac{1}{y} A_q(y)\Big|_{t^\theta}^{t^\phi} + \int_{t^\theta}^{t^\phi} \frac{1}{y^2} A_q(y) dy$$

$$\sim r_q \int_{t^\theta}^{t^\phi} \frac{1}{y^2} \frac{y}{\log y} dy + O\left(\frac{1}{\log t}\right) \sim r_q \log \frac{\phi}{\theta} = r_q \log\left(\frac{4}{3}\right)$$

as $t \to \infty$. Thus, we get

$$\sum_{p \in I \cap A_q} 1/p = r_q \log(4/3) + o(1)$$

as $t \to \infty$.

Recall that we wish to show that $\alpha(n) \geqslant C$ for almost all n. Let $\varepsilon > 0$. Define

$$u(m) = \sum_{B < q \leqslant m} r_q,$$

and note that since $r_q \geqslant 1/q$, $u(m)$ tends to infinity with m. Fix m so that

$$(1/2)\log(4/3)u(m) \geqslant \max\{C, 9/(2\varepsilon)\},$$

and consider t sufficiently large so that $m \leqslant t^\theta$. From Lemma 4, we get that

$$\sum_{n \leqslant t} \left(\alpha(n) - \left(\sum_{B < q \leqslant m} \sum_{p \in I \cap A_q} \frac{1}{p}\right)\right)^2 = t \sum_{B < q \leqslant m} \sum_{p \in I \cap A_q} \frac{1}{p} + E$$

$$= t \sum_{B < q \leqslant m} \left(r_q \log(4/3) + o(1)\right) + E$$

$$= t \log(4/3) u(m) + o(t).$$

For each $n \leqslant t$ such that $\alpha(n) < C \leqslant (\frac{1}{2})\log(\frac{4}{3})u(m)$, we get

$$\left(\alpha(n) - \sum_{B < q \leqslant m} \sum_{p \in I \cap A_q} \frac{1}{p}\right) \leqslant \left(\frac{1}{2}\log\left(\frac{4}{3}\right)u(m) - \sum_{B < q \leqslant m} \sum_{p \in I \cap A_q} \frac{1}{p}\right)$$

$$\leqslant \left(\frac{1}{2}\log\left(\frac{4}{3}\right)u(m) - \log\left(\frac{4}{3}\right)u(m) + o(1)\right)$$

$$\leqslant -\frac{1}{3}\log\left(\frac{4}{3}\right)u(m)$$

for t sufficiently large. Thus, we get a contribution of at least $\{(\frac{1}{3})\log(\frac{4}{3})u(m)\}^2$ in the first summand in Lemma 4. Thus, by Lemma 4, the number of $n \leqslant t$ such that $\alpha(n) < C$ is

$$\leqslant \frac{\log(\frac{4}{3})u(m)}{\{(\frac{1}{3})\log(\frac{4}{3})u(m)\}^2} t + o(t) = \frac{9}{\log(\frac{4}{3})u(m)} t + o(t) \leqslant \varepsilon t + o(t).$$

Since $\varepsilon > 0$ was arbitrary, we get that the number of $n \leqslant t$ for which $\alpha(n) < C$ is $o(t)$. Hence, almost all n satisfy $\alpha(n) \geqslant C$ and the proof is complete.

4. Strengthening the asymptotics. We begin by considering $f_n(x) = \sum_{j=0}^n a_{n-j}(x^j/j!)$ where $a_0, a_1, \ldots$ are non-zero integers with absolute value $\leqslant B$. However, we note that results analogous to those established in this section can be obtained with $a_0, a_1, \ldots$ being non-zero integers satisfying only (i) and (ii) of the Introduction. In the previous section, we showed that $k_2(t) = o(t)$, where $k_2(t)$ denotes the number of reducible $f_n(x)$ with $n \leqslant t$. In this section, we make further improvements on estimating $k_2(t)$. We will then explain how one may similarly improve on the author's previous work with Bessel polynomials by further estimating $k_1(t)$, the number of reducible $y_n(x)$ with $n \leqslant t$.

The main idea is to make use of strong versions of the Chebotarev Density Theorem due to Lagarias and Odlyzko [11]. For a given polynomial $f(x) \in \boldsymbol{Z}[x]$ which is irreducible over $\boldsymbol{Q}$, we define $G = G_f$ to be the Galois group of $f(x)$. Let $C = C_n$ denote the union of the conjugacy classes of G consisting of n-cycles where $n = \deg(f(x))$. Let K denote the splitting field for $f(x)$ and R its ring of integers. Note that $[K : \boldsymbol{Q}] = |G| \leqslant n!$. Let $D = D_K$ represent the absolute value of the discriminant of K. For a rational prime p, we use the Artin symbol $\left[\frac{K/\boldsymbol{Q}}{(p)}\right]$ to denote the conjugacy class of Frobenius automorphisms in G associated with the prime ideals P in R such that $P \mid (p)$.

We will be interested in those p for which $\left[\frac{K/\boldsymbol{Q}}{(p)}\right]$ is a conjugacy class of n-cycles. Let p be such a prime, and let P be a prime ideal in R dividing (p). Then the Frobenius automorphism associated with P is an n-cycle, and

therefore, its powers act transitively on the roots of $f(x)$ modulo p. This implies that $f(x)$ is irreducible modulo p and that (p) is unramified in R.

Now, suppose we are given a prime p, and we know that $f(x)$ is irreducible modulo p. Let P be a prime ideal in R dividing (p). Then one can show again that the powers of the Frobenius automorphism associated with P act transitively on the roots of $f(x)$ modulo p. This implies that the Frobenius automorphism associated with P is an n-cycle in G. Hence, $\left[\frac{K/Q}{(p)}\right]$ is a conjugacy class of n-cycles.

We define

$$\pi_f(t) = \left|\left\{p \leqslant t\colon (p) \text{ is unramified in } K, \left[\frac{K/Q}{(p)}\right] \text{ is a conjugacy class of } n\text{-cycles}\right\}\right|.$$

Then the above arguments imply that

$$\pi_f(t) = \left|\left\{p \leqslant t\colon \left[\frac{K/Q}{(p)}\right] \text{ is a conjugacy class of } n\text{-cycles}\right\}\right| = |\{p \leqslant t\colon f(x) \text{ is irreducible modulo } p\}|$$

(also see [6]). We are now ready to state the results of Lagarias and Odlyzko [11] employing the notation and observations above.

LEMMA 9. *Let $f(x) \in \mathbf{Z}[x]$ be an irreducible polynomial over $\mathbf{Q}$ of degree > 1. Then $\zeta_K(s)$, the Dedekind zeta function for the splitting field K of $f(x)$, has at most one zero in the region defined by*

$$s = \sigma + it, \quad 1 - (4\log D_k)^{-1} \leqslant \sigma \leqslant 1, \quad |t| \leqslant (4\log D_k)^{-1}.$$

If such a zero exists, then it must be real and simple, and we denote it by β_0. Furthermore, there exist absolute positive constants c_1 and c_2 such that if

$$t \geqslant \exp(10|G_f|(\log D_K)^2),$$

then

$$\left|\pi_f(t) - \frac{|C|}{|G_f|}\operatorname{Li}(t)\right| \leqslant \frac{|C|}{|G_f|}\operatorname{Li}(t^{\beta_0}) + c_1 t \exp(-c_2|G_f|^{-1/2}(\log t)^{1/2}),$$

where $\operatorname{Li}(t)$ denotes the logarithmic integral $\int_2^t dt/\log t$ and the term involving β_0 above is present only when β_0 exists.

LEMMA 10. *Let $f(x) \in \mathbf{Z}[x]$ be an irreducible polynomial over $\mathbf{Q}$, and assume that the GRH holds for $\zeta_K(s)$. Then there is an absolute constant c_3 (independent of $f(x)$) such that for every $t > 2$,*

$$\left|\pi_f(t) - \frac{|C|}{|G_f|}\operatorname{Li}(t)\right| \leqslant c_3\left(\frac{|C|}{|G_f|}\, t^{1/2}\log(D_K t^{|G_f|}) + \log D_K\right).$$

It follows from work of Stark [15] that there is an absolute positive constant c_4 such that

$$\beta_0 < \max\{1 - (4\log D_K)^{-1},\ 1 - (c_4 D_K^{1/|G|})^{-1}\}$$

(cf. [11]). Note that $D_K > 1$ (cf. [1, p. 129]) in the above bound. Also, the bounds on σ in Lemma 9 imply that we could omit the quantity $1-(4\log D_K)^{-1}$ above; however, this would not alter our final results. To apply the above lemmas, we need now only to estimate D_K. We will make only a crude estimate for D_K, noting, in particular, that there are exact expressions for the discriminant of Bessel polynomials [7, p. 119].

Write $f(x) = \sum_{j=0}^n a_{n-j}x^j$, and let $\alpha_1, \ldots, \alpha_n$ be any ordering of its roots. Suppose M is such that $|\alpha_j| \leqslant M$ for every $j \in \{1, \ldots, n\}$. One can show that K is spanned by $S = \{\prod_{j=1}^n \alpha_j^{e_j}\colon 0 \leqslant e_j \leqslant j-1\}$ over $\mathbf{Q}$ so that some subset T of S consisting of $[K:\mathbf{Q}] = |G|$ elements forms a basis for K over $\mathbf{Q}$. Note that each element of S and, therefore, T has absolute value $\leqslant M^{n(n-1)/2} \leqslant M^{n^2}$. We next form a basis for K over $\mathbf{Q}$ consisting of elements of R. In fact, since $\beta_j = a_0\alpha_j$ is a root of $x^n + \sum_{i=0}^{n-1} a_{n-i}a_0^{n-1-i}x^i$ for each $j \in \{1, \ldots, n\}$, it follows that

$$T^* = \{a_0^{n(n-1)/2}t\colon t \in T\}$$

is such a basis. Note that $|T^*| = |G|$ and $t^* \in T^* \Rightarrow |t^*| \leqslant (a_0 M)^{n^2}$. It is well known that (cf. [1, p. 403])

$$\Delta = |\det(\sigma_j(t_i^*))|^2,$$

where $G = \{\sigma_1, \ldots, \sigma_{[K:\mathbf{Q}]}\}$, is divisible by the discriminant of K. Hence, $D_K \leqslant \Delta$. Also, from the definition of T^*, one has that each $|\sigma_j(t_i^*)| \leqslant (a_0 M)^{n^2}$. Hence, we get that

$$D_K \leqslant \Delta \leqslant \left(|G|!\,((a_0 M)^{n^2})^{|G|}\right)^2. \tag{7}$$

Recall that Lemma 1 implies that for n sufficiently large, $f(x) = F_n(x)$ and $j \in \{1, \ldots, n\}$ one has that $|\alpha_j| < n^2$. Thus, one can take $M = n^2$. Since $|G| \leqslant n! \leqslant 6n^{n-3}$, we get from (7) that for $f(x) = F_n(x)$,

$$D_K \leqslant n^{n^n} \tag{8}$$

for $n \geqslant n_0$ where $n_0 = n_0(B)$ is sufficiently large. Also, one gets that if $n \geqslant n_0$ and n_0 is sufficiently large, then

$$D_K \leqslant n^{5n^2|G|}. \tag{9}$$

From (8), we get that for $n \geqslant n_0$

$$\exp(10|G|(\log D_K)^2) \leqslant \exp(60n^{3n-3}\log^2 n).$$

We consider now n satisfying

$$n_0 \leqslant n \leqslant \tfrac{1}{2}\sqrt{l_2(t)/l_3(t)} \tag{10}$$

where t is sufficiently large. This easily implies that

$$t \geqslant \exp(10|G|(\log D_K)^2).$$

Hence, Lemma 9 can be applied.

We now turn to our estimate of β_0. We shall assume, henceforth, that t is sufficiently large. If

$$\max\{1-(4\log D_K)^{-1},\ 1-(c_4 D_K^{1/|G|})^{-1}\} = 1-(4\log D_K)^{-1},$$

then (8) and (10) imply easily that $t^{\beta_0} \leqslant t/\log t$. Also, if

$$\max\{1-(4\log D_K)^{-1},\ 1-(c_4 D_K^{1/|G|})^{-1}\} = 1-(c_4 D_K^{1/|G|})^{-1},$$

then (9) and (10) imply that $t^{\beta_0} \leqslant t/\log t$.

Since $|G| \leqslant n! \leqslant n^n$, we get that

$$|G| \leqslant \sqrt{l_2(t)^{\sqrt{l_2(t)}}} \leqslant \sqrt{\log t}.$$

Since $\mathrm{Li}(t^{\beta_0}) \ll t^{\beta_0}/\log t$, we get from Lemma 9 that if $f(x) = F_n(x)$ is irreducible, then

$$\left|\pi_f(t) - \frac{|C|}{|G_f|}\mathrm{Li}(t)\right| \ll \frac{t}{\log^2 t},$$

and hence,

$$\left|\pi_f(t) - \frac{|C|}{|G_f|}\frac{t}{\log t}\right| \ll \frac{t}{\log^2 t}. \tag{11}$$

We are now ready to establish

THEOREM 2. *Let $a_0, a_1, \ldots$ be a bounded sequence of non-zero integers, and let*

$$f_n(x) = a_0\frac{x^n}{n!} + a_1\frac{x^{n-1}}{(n-1)!} + \ldots + a_{n-1}x + a_n.$$

Let $k_2(t)$ denote the number of reducible $f_n(x)$ with $n \leqslant t$. Then $k_2(t) \ll t/l_4(t)$. If the GRH is true for the Dedekind zeta function associated with the splitting field of $f_q(x)$ for each prime q, then this estimate can be improved to $k_2(t) \ll t/l_3(t)$.

The idea is to replace the argument at the end of the previous section with an argument which makes use of (11) with $f(x) = F_q(x)$. To prove the desired result, it suffices to only consider the case when t is sufficiently large and the bound B on the sequence $a_0, a_1, \ldots$ satisfies $B \geqslant n_0$. We want (10) to hold with each $n = q$ so we set $m = \frac{1}{2}\sqrt{l_2(t)/l_3(t)}$ and consider $B < q \leqslant m$. Note that since

t is sufficiently large, $m \leqslant t^{1/9} < t^\theta$. Recall that $F_q(x)$ is Eisenstein with respect to the prime q and, hence, irreducible. Also, $r_q = |C|/|G_{F_q}| \geqslant 1/q$. With A_q and $I = (t^\theta, t^\phi]$ as before, we get that

$$\begin{aligned}\sum_{p\in I\cap A_q}\frac{1}{p} &= \int_{t^\theta}^{t^\phi}\frac{1}{y}d\pi_{F_q}(y)\\ &= r_q\int_{t^\theta}^{t^\phi}\frac{1}{y\log y}dy + O\left(\int_{t^\theta}^{t^\phi}\frac{1}{y\log^2 y}dy\right) + O\left(\frac{1}{\log t}\right)\\ &= r_q\log\left(\frac{4}{3}\right) + O\left(\frac{1}{\log t}\right).\end{aligned}$$

With $u(m) = \sum_{B<q\leqslant m} r_q$, we get that $u(m) \geqslant \sum_{B<q\leqslant m} 1/q \gg \log\log m \gg l_4(t)$. The arguments at the end of Section 3 imply that there is an absolute constant $c_5 > 0$ such that the number of positive integers n with $n_0 \leqslant n \leqslant t$ and $\alpha(n) \leqslant c_5 l_4(t)$ is $\ll t/l_4(t)$. In particular, since t is sufficiently large, $\alpha(n) < 24B+25$ (i.e., $f_n(x)$ is reducible) for $\ll t/l_4(t)$ positive integers $n \leqslant t$, giving the first part of Theorem 2.

If the GRH is true for each $\zeta_K(s)$ where K is the splitting field for $f(x) = F_q(x)$, then one can obtain (11) from Lemma 10 provided only that

$$\log(D_K t^{|G|}) \ll \frac{t^{1/2}}{\log^2 t}. \tag{12}$$

Recall that $D_K \ll q^{q^q}$ and $|G| = |G_{F_q}| \leqslant q! \leqslant q^q$. Take $m = \log t/(3\log\log t)$. Then one easily checks that (12) holds for each q satisfying $B < q \leqslant m$. Here, $u(m) \gg \log\log m \gg l_3(t)$, and we get conditionally that $k_2(t) \ll t/l_3(t)$.

We now turn to the Bessel polynomials. It is more convenient to consider $z_n(x) = x^n y_n(2/x)$ which is irreducible if and only if $y_n(x)$ is. Furthermore, $z_n(x)$ is a monic polynomial in $\boldsymbol{Z}[x]$. The argument for showing that $k_1(t) = o(t)$ in [5] was very similar to the argument given in Sections 2 and 3. In fact, the argument was simpler allowing for $u_0 = r-1$ and $v_0 = s-1$ and, therefore, not needing a result like Lemma 3. Letting A_k now denote the set of primes p for which $z_k(x)$ is irreducible modulo p and setting

$$\alpha(n) = \sum_{B<q\leqslant m}\ \sum_{\substack{p\in I\cap A_q\\ n\equiv q(\mathrm{mod}\ p)}} 1$$

where $I = (t^\theta, t^\phi] = (t^{1/4}, t^{1/3}]$, then the author showed that Lemmas 4 and 8 hold by using arguments similar to those already given here. For Bessel polynomials, one can in fact take $r_q = 1/q$. To prove that $z_n(x)$ is irreducible for almost all n, the author [5] showed that it was sufficient to establish that $\alpha(n) \geqslant 20$. The arguments in this section all carry over to give the same

estimates for $k_1(t)$, the number of reducible $z_n(x)$ with $n \leqslant t$, as we obtained for $k_2(t)$. To further improve on the estimate for $k_1(t)$, we make use of the fact that $k_1(t) = o(t)$ and

LEMMA 11. *If $z_k(x)$ is irreducible, then the Galois group for $z_k(x)$ is S_k.*

The proof of the lemma can be found in [7, p. 116]. In particular, the lemma implies that the proportion of k-cycles in the Galois group for an irreducible $z_k(x)$ is $1/k$. Note that without such a lemma, the Galois group need not have a k-cycle.

We consider now

$$\alpha^*(n) = \sum_{B<k\leqslant m} \sum_{\substack{p\in I\cap A_k \\ n\equiv k(\mathrm{mod}\ p)}} 1,$$

where k represents any integer and not necessarily a prime. Following the proof of Lemma 4, we get

LEMMA 12. *Let m be a positive integer which is $\leqslant t^\theta$. Define $I = (t^\theta, t^\phi]$. Then*

$$\sum_{n\leqslant t}\left(\alpha^*(n) - \left(\sum_{B<k\leqslant m}\sum_{p\in I\cap A_k}\frac{1}{p}\right)\right)^2 = t\sum_{B<k\leqslant m}\sum_{p\in I\cap A_k}\frac{1}{p} + E$$

where

$$E \ll t^{3/4}m^2.$$

Define

$$u^*(m) = \sum_{\substack{k\leqslant m \\ z_k(x)\ \text{irreducible}}} 1/k. \tag{13}$$

Using $u^*(m)$ instead of $u(m)$ in our arguments gives that

$$k_1(t) \ll \frac{t}{u^*(m)} + O\left(\frac{t^{3/4}m^2}{u^*(m)}\right)$$

provided that $m \ll \log t$. Since $z_n(x)$ is monic and its roots have absolute value $\leqslant n(n+1) \leqslant 2n^2$ (cf. [7, p. 82]), we can use the same bounds on the discriminant D_K that we had for $F_n(x)$. As a consequence of (10), we require

$$n_0 \leqslant m \leqslant \tfrac{1}{2}\sqrt{l_2(t)/l_3(t)},$$

where $n_0 = n_0(2)$. The key now is to make use of the already proven result that $z_k(x)$ is irreducible for almost all k so that one can obtain the estimate

$$u^*(m) \gg \log m,$$

thus saving a logarithm factor over the estimate we had for $u(m)$. The end result is the following

THEOREM 3. *Let $k_1(t)$ denote the number of reducible Bessel polynomials $z_n(x)$ of degree $n \leqslant t$. Then $k_1(t) \ll t/l_3(t)$.*

A similar argument works in the case that the GRH holds. We get that if the GRH holds for the Dedekind zeta functions associated with the splitting field of each $z_n(x)$, then $k_1(t) \ll t/\log\log t$. We note that the GRH need only be assumed, in fact, for a positive proportion of such Dedekind zeta functions since $u^*(m) \gg \log m$ will follow even when the $z_k(x)$ in the definition of $u^*(m)$ are further restricted to be from any set which consists of a positive proportion of the $z_k(x)$.

On the other hand, one can get a better conditional result only under the assumption of the RH. Let $y = \exp((1/\sqrt{2})\sqrt{\log t\log\log t})$. It follows from a result of de Bruijn [2] (also see [12, p. 13]) that $\Psi(t, y)$, the number of positive integers $n \leqslant t$ with all the prime factors of n being $\leqslant y$, satisfies

$$\Psi(t, y) \ll t(\log^2 y)\exp(-\alpha\log\alpha),$$

where $\alpha = \log t/\log y$. Hence, one easily gets that

$$\Psi(t, y) \ll t\exp((-1/\sqrt{2}+\varepsilon)\sqrt{\log t\log\log t}),$$

where ε is an arbitrary positive real number. On the other hand, assuming the RH, Selberg [14] has shown that

$$\sum_{p_k\leqslant t}(p_{k+1}-p_k)^2 \ll t(\log t)^3,$$

where p_k denotes the kth prime. Hence,

$$\sum_{\substack{p_k\leqslant t \\ p_{k+1}-p_k>y}}(p_{k+1}-p_k) \ll (t\log^3 t)/y.$$

Thus, the number of positive integers $n \leqslant t$ lying in a gap between consecutive primes of length $> y$ is

$$\ll (t\log^3 t)/y \ll t\exp((-1/\sqrt{2}+\varepsilon)\sqrt{\log t\log\log t}).$$

For $n \geqslant 3$, let $k(n) = \min\{n-p_j+1, p_{j+1}-n\}$ where p_j and p_{j+1} are the consecutive primes such that $n\in(p_j, p_{j+1}]$. Assuming the RH, the above implies that the number of integers $n \geqslant 3$ and $\leqslant t$ for which $k(n) > y$ is $\ll t\exp((-1/\sqrt{2}+\varepsilon)\sqrt{\log t\log\log t})$. On the other hand, at most $\ll t\exp((-1/\sqrt{2}+\varepsilon)\sqrt{\log t\log\log t})$ positive integers $n \leqslant t$ have all their prime factors $\leqslant y$. Thus, assuming the RH, the number of positive integers $n \leqslant t$ for which $n(n+1)$ does not contain a prime factor $> k(n)$ is $\ll t\exp((-1/\sqrt{2}+\varepsilon)\times\sqrt{\log t\log\log t})$. Thus, by the observation of Grosswald mentioned in the Introduction, we get

THEOREM 4. *Let $\varepsilon > 0$. Assuming the RH, we have that*

$$k_1(t) \ll t\exp((-1/\sqrt{2}+\varepsilon)\sqrt{\log t\log\log t}).$$

In closing, the author would like to thank Jacki Pitts for organizing and writing up a good deal of this material as part of a requirement for her M.S. degree at the University of South Carolina. The author further thanks Carl Pomerance for suggesting using reference [14] as in the final part of this paper. In addition, the author is greatly indebted to David Richman for several helpful comments and suggestions including the proof of Lemma 7. Finally, the author is grateful to Emil Grosswald for his constant encouragements through the years knowing well that they will remain with this author in the years to come.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, Orlando 1966.
[2] N. G. de Bruijn, *On the number of positive integers $\leqslant x$ and free of prime factors $> y$*, Nederl. Akad. Wetensch. Proc. Ser. A 54 (= Indag. Math. 13) (1951), 50–60.
[3] N. Chebotarev (N. Tschebotarëw), *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. 95 (1926), 191–228.
[4] P. Erdös, *A theorem of Sylvester and Schur*, J. London Math. Soc. 9 (1934), 282–288.
[5] M. Filaseta, *The irreducibility of almost all Bessel Polynomials*, J. Number Theory 27 (1987), 22–32.
[6] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Sympos. Pure Math. 24, Amer. Math. Soc., Providence, RI, 1973, 91–101.
[7] E. Grosswald, *Bessel Polynomials*, Lecture Notes in Math. 698, Springer-Verlag, Berlin 1978.
[8] –, *On some algebraic properties of the Bessel Polynomials*, Trans. Amer. Math. Soc. 71 (1951), 197–210.
[9] –, *On some algebraic properties of the Bessel Polynomials*, Addendum, ibid. 144 (1969), 569–570.
[10] –, private communication.
[11] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev Density Theorem*, Proceedings of the 1975 Durham Symposium, Academic Press, London and New York 1977, 409–464.
[12] K. K. Norton, *Numbers with small prime factors, and the least k-th power non-residue*, Mem. Amer. Math. Soc. 106 (1971), 1–106.
[13] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I*, Sitzungsber. Preuss. Akad. Wiss. (1929), 125–136; also in *Issai Schur Gesammelte Abhandlungen*, Bd. III, edited by A. Brauer and H. Rohrbach, Springer-Verlag, New York 1973.
[14] A. Selberg, *On the normal density of primes in small intervals, and the difference between consecutive primes*, Arch. Math. Naturvid., no. 6, 47 (1943), 87–105.
[15] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.
[16] J. Sylvester, *On arithmetical series*, Messenger of Math. 21 (1892), 1–19, 87–120.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTH CAROLINA
Columbia, S.C. 29208
U.S.A.

Received on 6.10.1989
and in revised form on 18.4.1990 (1976)

ACTA ARITHMETICA
LVIII.3 (1991)

Norme relative de l'unité fondamentale et 2-rang du groupe des classes d'idéaux de certains corps biquadratiques

par

STÉPHANE LOUBOUTIN (Caen)

Notations. k désigne un corps quadratique imaginaire de nombre de classes d'idéaux $h(k)$ impair, de discriminant $D_{k/Q}$ donc égal à -4, -8 ou égal à p, $p \equiv 1 \pmod 4$ premier, d'anneau des entiers R_k, de groupe des classes d'idéaux $H(k)$ et de groupe (fini) des unités (i.e. de ses racines de l'unité) U_k.

K est une extension quadratique de k, R_K son anneau des entiers, $h(K)$ son nombre de classes d'idéaux et $H(K)$ son groupe des classes d'idéaux (remarquons que K étant totalement complexe, les notions de classe stricte et large coïncident). Nous notons $j_{K/k}$ l'homomorphisme canonique de $H(k)$ dans $H(K)$. Le nombre de classes de k étant supposé impair, cet homomorphisme est ici injectif (car $N_{K/k} \circ j_{K/k}$ n'est autre que l'élévation au carré). Nous notons $D_{K/Q}$ le discriminant absolu de K/Q, $\delta_{K/k}$ l'idéal de R_k égal au discriminant relatif de l'extension K/k et $D_{k/Q}$ le discriminant absolu de k/Q. Nous avons donc $D_{K/Q} = N_{k/Q}(\delta_{K/k})(D_{k/Q})^2$. K étant totalement complexe et de degré quatre, son groupe des unités U_K est de rang 1 et nous notons η_K une unité fondamentale. La norme relative $N_{K/k}(\eta_K)$ de η_K étant une unité de k, elle est une racine de l'unité de k et est égale à ± 1 pour $k \neq Q(i), Q(j)$, elle est égale à $\pm 1, \pm i$ pour $k = Q(i)$, et est finalement égale à $\pm 1, \pm j, \pm j^2$, pour $k = Q(j)$. Il est aisé de voir que pour $k = Q(i)$ on peut se ramener après multiplication éventuelle par i au cas où $N_{K/k}(\eta_K) = +1$ ou i, et que pour $k = Q(j)$ on peut se ramener après multiplication éventuelle par j ou j^2 au cas où $N_{K/k}(\eta_K) = +1$ ou -1. Finalement, nous posons $\varepsilon_k = -1$ lorsque $k \neq Q(i)$, et $\varepsilon_k = i$ lorsque $k = Q(i)$, de sorte que U_k est inclus dans $N_{K/k}(U_K)$ si et seulement si ε_k appartient à $N_{K/k}(U_K)$.

Introduction. Nous déterminons premièrement le 2-rang du groupe des classes d'idéaux de K. L'imparité du nombre de classes de certains de ces corps biquadratiques nous permet de secondement donner au corollaire 6 une preuve rapide, dans notre cas particulier, de la loi de réciprocité établie, par E. Hecke, et au corollaire 11 une preuve de la loi de réciprocité établie par P. G. L. Dirichlet. Nous développons finalement aux propositions 13 et 14 des moyens de calcul de la norme relative de l'unité fondamentale de K. Nous nous astreignons, délibérément, à n'utiliser que les fondements de la théorie