References

[1] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8 (1960), pp. 65-70.

[2] J. Mikusiński et A. Schinzel, *Sur la réductibilité de certains trinômes*, Acta Arith. 9 (1964), pp. 91-96.

[3] A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives des nombres irrationnels*, Colloq. Math. 9 (1962), pp. 291-296, *Correction*, ibid.. 12 (1964), p. 289.

[4] A. Schinzel, *Some unsolved problems on polynomials*, Matematička Biblioteka 25 (1963), pp. 63-70.

[5] N. Tschebotaröw und H. Schwerdtfeger, *Grundzüge der Galoischen Theorie*, Groningen-Djakarta 1950.

Reçu par la Rédaction le 21. 2. 1964

ACTA ARITHMETICA
XI (1965)

Primes, polynomials and almost primes

by

R. J. Miech (Urbana, Ill.)

A set of almost primes is a set of integers each of which contains no more than a fixed number of prime factors. An integral valued polynomial $F(n)$ which is of degree h and which has k irreducible factors, for example, will generate a sequence of almost primes, the bound being approximately $(9h/5+k\log k)$, [3]. I propose to show that the sequence $\{F(p)\}$, where p is a prime, contains an infinite subsequence of almost primes. To be specific, I shall prove:

Theorem. *Let $F(n)$ be an integral valued polynomial. Let K be any integer and let c be any integer which is relatively prime to K. Then there is a constant A which depends on the polynomial $F(n)$ such that there are an infinite number of primes p congruent to c modulo K for which $F(p)$ has at most A prime factors, multiple prime factors being counted multiply.*

The constant A of the conclusion of the theorem is not readily computable.

Several comments regarding assumptions and notational devices are in order. First of all, we shall assume without loss of generality that $F(n)$ has a non-zero constant term, for if n^L is the highest power of n dividing $F(n)$ we can apply our theorem to the polynomial $F(n)/n^L$ and replace A by $A+L$ to get the same general result. Secondly, we shall suppose that $F(n)$ has k distinct irreducible factors. Finally, the letter p will always denote a prime.

The Theorem will be proved by a main-term versus remainder-term type of argument. We shall actually prove that there is an integer H which is a multiple of K and a positive constant B which depends on the polynomial $F(n)$ and the integers H and c such that there are

$$Bx(\log x)^{-k-2}+O\big(x(\log x)^{-k-3}\big)$$

primes p congruent to c modulo H which do not exceed x for which $F(p)$ has at most A prime factors. We shall use Brun's method [1] to obtain the main teim and then use of result of Renyi's [5] on the distribution of the zeros of the L-series to evaluate the error term. This paper is accordingly divided into three sections: the main term is developed in the first, the second contains the results we shall need to evaluate the error term, and the third deals with the estimation of the error.

I would like to express my thanks to Professor Paul T. Bateman for suggesting this problem to me and for the advice he gave me during the preparation of this paper.

1. The main term. We shall begin by defining the integer H mentioned in the introduction. Let H_1 be the least common multiple of the denominators of the coefficients of $F(n)$ and let H_2 be the product of all the primes less than or equal to $m+1$, where m is the degree of $F(n)$. Let $H_3 = H_1H_2F(0)K$. We can suppose without loss of generality that $(c, H_3) = 1$ and that $F(c) \neq 0$, for if c does not satisfy these conditions we can replace it by a sufficiently large prime of the form $c+tK$ which does. Since $\big(c, F(0)\big) = 1$ we have $\big(c, F(c)\big) = 1$. Thus $\big(c, H_3F(c)\big) = 1$. Now let $H = \big(H_3F(c)\big)^2$ and let $G_c(t)$ be the polynomial defined by the equation $F(tH+c) = F(c)G_c(t)$. That is

$$G_c(t) = 1+b_1t+\ldots+b_mt^m,$$

where $b_1, b_2, \ldots,$ and b_m are integers, all of which are divisible by $\big(H_3F(c)\big)$. This last divisibility property implies that the congruence $G_c(t)\equiv 0 \bmod p$ has no solutions if p divides H; thus if p does not divide H then $p-2 \geqslant m$ and the number of solutions of this congruence does not exceed $p-2$ for any prime p. We can also assert that if the congruence $G_c(t)\equiv 0 \bmod d$ does have solutions then $(d, H) = 1$. These facts will be of importance later. We shall also assume that the polynomial $G_c(t)$ has no repeated irreducible factors; if it does replace it by its square free kernel in the following argument.

We have to prove that there are an infinite number of positive integers t such that $tH+c$ is prime and such that $G_c(t)$ has a bounded number of prime factors. We shall fix c and drop the subscript c appearing in the expression $G_c(t)$ at this point.

Several other notational devices will be used throughout this paper: $\mu(n)$ will denote the Möbius function, $\varphi(n)$ will denote Euler's function, x will be a positive number, z will be a positive number which depends on x, D will represent the product of the primes not exceeding z, and a_p will be equal to $(\log p)\exp(-p\log x/x)$. $\Phi(x)$ will denote the number of elements in the set

$$\big\{t\colon\ 0<tH+c\leqslant x;\ tH+c \text{ is prime};\ \big(G(t), D\big)=1\big\}.$$

We are now in a position to outline the method that will be used to obtain the main term. We shall begin with the definitions and get

(1.0.1) $$\Phi(x)\log x \geqslant \sum_{\substack{tH+c=p\leqslant x\\ (G(t),D)=1}} a_p.$$

Then, following Brun, we shall introduce a set of square free integers E such that

(1.0.2) $$\sum_{\substack{d|(G(t),D)\\ d\in E}} \mu(d)\begin{cases} =1 & \text{if}\quad \big(G(t), D\big)=1,\\ \leqslant 0 & \text{if}\quad \big(G(t), D\big)>1.\end{cases}$$

If we put (1.0.2) in (1.0.1) and reverse the order of summation of the resulting double sum we shall have

(1.0.3) $$\Phi(x)\log x \geqslant \sum_{\substack{d|D\\ d\in E}}\mu(d)\sum_{\substack{tH+c=p\leqslant x\\ G(t)\equiv 0 \bmod d}} a_p.$$

We shall then show, roughly speaking, that

(1.0.4) $$\sum_{\substack{tH+c=p\leqslant x\\ G(t)\equiv 0 \bmod d}} a_p = \omega(d)\sum_{\substack{p\leqslant x\\ p\equiv w \bmod dH}} a_p,$$

where $\omega(d)$ is a certain multiplicative function and w is an integer such that $(w, dH) = 1$. At this point we shall assume the results of the second and third sections of this paper, i.e.

(1.0.5) $$\sum_{\substack{p\leqslant x\\ p\equiv w \bmod dH}} a_p = \frac{1}{\varphi(dH)}\cdot\frac{x}{\log x}+\text{an Error}.$$

Relations (1.0.3), (1.0.4), and (1.0.5) lead us to the inequality:

(1.0.6) $$\Phi(x)\log x \geqslant \frac{1}{\varphi(H)}\sum_{\substack{d|D\\ d\in E}}\frac{\mu(d)\omega(d)}{\varphi(d)}\cdot\frac{x}{\log x}+\text{an Error}.$$

After reaching this point we shall employ Brun's method to show that the coefficient of $x(\log x)^{-1}$ above is greater than $C_1(\log z)^{-k}$, where C_1 is a positive constant. Thus, assuming we have set z equal to a fractional power of x, we shall have

(1.0.7) $$\Phi(x)\log x \geqslant C_2x(\log x)^{-k-1}+\text{an Error},$$

where C_2 is a positive constant.

Let us turn to the details, the first being:

LEMMA 1.1. *Using previously introduced notation, we have*

$$\Phi(x)\log x \geqslant \sum_{\substack{tH+c=p\leqslant x\\ (G(t),D)=1}} a_p.$$

Proof. This is immediate since

$$a_p = (\log p)\exp(-p\log x/x) \leqslant \log x.$$

We shall now define the set of integers E mentioned earlier. Let q_0 be a fixed prime greater than 3; the only other conditions q_0 must meet will be given in Lemma 1.4. Let Q be the product of all the primes less than or equal to q_0. Let $\exp(y;a) = y^a$. (We shall also continue to use the notation $\exp a = e^a$.) Let h be a fixed number greater than 1 and let $z(h,i) = \exp(z; h^{-[i/2]})$, where i is an integer and $[y]$ denotes the integral part of y. By definition, E will be the set of integers $\{d\}$ such that d divides Q or $d = d^* p_1 \ldots p_r$ where d^* divides Q, $p_1 > p_2 > \ldots > p_r > q_0$ and $p_i \leqslant z(h,i)$ for $i = 1, 2, \ldots, r$. Note, first of all, that if b is the integer defined by the inequalities $z(h, 2b+2) \leqslant q_0 < z(h, 2b+1)$ it follows that $r \leqslant 2b+1$ since we must have $q_0 < p_r \leqslant z(h,r)$. Secondly, if d is in E then d divides D since D is the product of the primes not exceeding z.

We must now prove

LEMMA 1.2. *Let E be defined as above. Then*

$$\sum_{\substack{d \mid (G(t),D) \\ d \in E}} \mu(d) \begin{cases} = 1 & \textit{if} \quad (G(t), D) = 1, \\ \leqslant 0 & \textit{if} \quad (G(t), D) > 1. \end{cases}$$

Proof. The proof is immediate if $(G(t), D) = 1$. If the square-free part of $(G(t), D)$ is equal to $d^* p_1 \ldots p_r$ where $d^* \mid Q$, $d^* > 1$, and $p_1 > \ldots > p_r > q_0$ then, since all of the divisors of d^* are in E,

$$\sum_{\substack{d \mid d^* p_1 \ldots p_r \\ d \in E}} \mu(d) = \sum_{\substack{d \mid p_1 \ldots p_r \\ d \in E}} \mu(d) \sum_{a \mid d^*} \mu(a) = 0.$$

If the square-free part of $(G(t), D)$ is equal to $p_1 \ldots p_r$ where $p_1 > \ldots > p_r > q_0$, then

$$\sum_{\substack{d \mid p_1 \ldots p_r \\ d \in E}} \mu(d) = \sum_{\substack{d \mid p_1 \ldots p_{r-1} \\ d \in E}} \mu(d) - \sum_{\substack{d \mid p_1 \ldots p_{r-1} \\ d \in E}} \mu(d) + \sum_{\substack{d \mid p_1 \ldots p_{r-1} \\ d \in E, dp_r \notin E}} \mu(d).$$

If the last sum on the right is empty we are done. If it is not it is not difficult, using the properties of the set E, to show that if $d \mid p_1 \ldots p_{r-1}$, $d \in E$, and $dp_r \notin E$ then d has an odd number of prime factors, i.e. $\mu(d) = -1$. This will complete the proof of the lemma.

The first two lemmas can be summarized as:

$$\Phi(x) \log x \geqslant \sum_{d \in E} \mu(d) \sum_{\substack{tH+c=p \leqslant x \\ G(t) \equiv 0 \bmod d}} a_p. \tag{1.2.1}$$

See formulas (1.0.1), (1.0.2) and (1.0.3) for the proof of this inequality.

The next step in our argument consists of proving:

LEMMA 1.3. *Let $u_1, \ldots, u_s$ denote the solutions of the congruence $G(t) \equiv 0$ $\bmod d$ such that $(dH, c+u_iH) = 1$; let $\omega(d) = s$. Let $\omega_1(d)$ denote the number of solutions of this congruence. Then*

$$\sum_{\substack{tH+c=p \leqslant x \\ G(t) \equiv 0 \bmod d}} a_p = \sum_{i=1}^{\omega(d)} \sum_{\substack{p \leqslant x \\ p \equiv c+u_iH \bmod dH}} a_p + \theta\big(\omega_1(d) \log x\big), \tag{1.3.1}$$

where $0 \leqslant \theta < 1$. In addition, $\omega(d)$ is a multiplicative function and $\omega(p) = \omega_1(p)$ for all but a finite number of primes p.

Proof. Let r be any solution of the congruence $G(t) = 0 \bmod d$. We are interested in those $t = r + jd$ such that $tH + c = (c+rH) + j(dH) = p$. Since the left hand side of (1.3.1) is equal to

$$\sum_{\substack{r \\ (dH, c+rH)=1}} \sum_{\substack{tH+c=p \leqslant x \\ t \equiv r \bmod d}} a_p + \sum_{\substack{r \\ (dH, c+rH)>1}} \sum_{\substack{tH+c=p \leqslant x \\ t \equiv r \bmod d}} a_p,$$

equation (1.3.1) follows easily.

The fact that $\omega(d)$ is multiplicative follows from the Chinese Remainder Theorem.

If $\omega(p) \neq \omega_1(p)$ for some prime p then there is an integer r such that $G(r) \equiv 0 \bmod p$ and $(pH, c+rH) > 1$, i.e. the system of equations

$$G(t) \equiv 0 \bmod p,$$
$$c + tH \equiv 0 \bmod p$$

is solvable. Since $F(c+tH) = F(c)G(t)$ and $F(0) \neq 0$, $G(t)$ and $c+tH$ are relatively prime polynomials. Consequently there are polynomials $a(t)$ and $b(t)$ with integral coefficients and an integer B such that $a(t)G(t) + b(t)(c+tH) = B$ for every integer t. Thus the number of primes p for which the above system is solvable does not exceed the number of prime divisors of B. This in turn implies that $\omega(p) = \omega_1(p)$ for all but a finite number of primes p. The proof of Lemma 1.3 is complete.

Later on we shall show that if $(d, H) = 1$ and if $(w, dH) = 1$ then

$$\sum_{\substack{p \leqslant x \\ p \equiv w \bmod dH}} a_p = \frac{1}{\varphi(dH)} \cdot \frac{x}{\log x} + R(dH, w), \tag{1.3.2}$$

where $R(dH, w)$ is an error term. We shall also show that if d is in E then $d \leqslant x^{1/2}(2QH)^{-1}$. Since $\omega_1(d) = \theta(d^\eta)$ where η is a fixed positive number (see [3], proof of Lemma 5.1), we have

$$\sum_{d \in E} \omega_1(d) \log x = O(x^{1/2+\eta} \log x). \tag{1.3.3}$$

Thus formulas (1.2.1), (1.3.1), (1.3.2) and (1.3.3) imply that

$$(1.3.4)\qquad \Phi(x)\log x$$

$$\geqslant \frac{1}{\varphi(H)}\Bigl[\sum_{d\epsilon E}\frac{\mu(d)\omega(d)}{\varphi(d)}\Bigr]\frac{x}{\log x}+O\Bigl[\sum_{d\epsilon E}\sum_{i=1}^{\omega(d)}|R(dH, c+u_iH)|+x^{1/2+\eta}\log x\Bigr].$$

Let us turn our attention to the sum $\sum\mu(d)\omega(d)/\varphi(d)$. We want to show that this quantity is greater than $C_3(\log z)^{-k}$, where C_3 is a positive constant. The first lemma we shall need to accomplish this is:

LEMMA 1.4. *Let h and h_0 be fixed numbers with $1 < h < h_0$. Then for any $y > q_0$, where q_0 is a sufficiently large fixed prime, we have*

$$(1.4.1)\qquad \sum_{y<p\leqslant y^h}\omega(p)/\varphi(p) < k\log h_0,$$

$$(1.4.2)\qquad \prod_{y<p\leqslant y^h}\Bigl[1-\frac{\omega(p)}{\varphi(p)}\Bigr] > h_0^{-k}.$$

Proof. These two inequalities can be proved by making use of the formula of Landau:

$$\sum_{p\leqslant x}\omega_i(p)/p = \log\log x+B_i+O[(\log x)^{-1}],$$

where $\omega_i(p)$ is the number of solutions of the congruence $G_i(t)\equiv 0 \bmod p$, $G_i(t)$ is an irreducible factor of $G(t)$ and B_i is a constant which depends on $G_i(t)$. (See [3], Lemma 3.10).

To be specific, the relations

$$\sum_{y<p\leqslant y^h}\frac{\omega_i(p)}{p} = \log h+O\bigl((\log y)^{-1}\bigr),$$

$$\sum_{y<p\leqslant y^h}\frac{\omega_i(p)}{\varphi(p)}-\sum_{y<p\leqslant y^h}\frac{\omega_i(p)}{p} = O\Bigl[\sum_{y<n\leqslant y^h}\frac{1}{(n-1)(n-1)}\Bigr] = O\Bigl[\frac{1}{y}\Bigr]$$

imply that

$$\sum_{y<p\leqslant y^h}\frac{\omega_i(p)}{\varphi(p)} = \log h+O\Bigl(\frac{1}{\log y}\Bigr).$$

Since $\omega(p) = \omega_1(p)+\omega_2(p)+\ldots+\omega_k(p)$ for all but a finite number of primes (see [3], Lemma 3.2), we can choose q_0 sufficiently large so that this equation holds for all primes $p\geqslant y > q_0$. Thus

$$\sum_{y<p\leqslant y^h}\frac{\omega(p)}{\varphi(p)} = k\log h_0+k\log(h/h_0)+O\bigl(k(\log y)^{-1}\bigr).$$

Since $h < h_0$ the quantity $k\log(h/h_0)+O\bigl(k(\log y)^{-1}\bigr)$ will be less than zero if q_0 is sufficiently large. Hence

$$\sum_{y<p\leqslant y^h}\omega(p)/\varphi(p) < k\log h_0,$$

as asserted. Equation (1.4.2) can be established by writing the product as

$$\exp\sum_{y<p\leqslant y^h}\log\Bigl(1-\frac{\omega(p)}{\varphi(p)}\Bigr),$$

expanding the logarithmic function as a power series and using what has been proved; q_0 may have to be increased.

We shall also need:

LEMMA 1.5. *Suppose that $y' > y > q_0$ and suppose that h_0 has been chosen so that $k\log h_0 < 1$. Let*

$$I(j; y, y') = \{d:\ d = p_1\ldots p_j,\ y < p_j < p_{j-1} < \ldots < p_1 \leqslant y'\}.$$

Let

$$T(j; y, y') = \sum_{d\epsilon I(j;y,y')}\omega(d)/\varphi(d).$$

Then $T(j; y, y^h)$ and $T\bigl(j; q_0+1, z(h, 2b)\bigr)$ are decreasing functions of j for $j = 1, 2, \ldots$ We also have

$$(1.5.1)\qquad T\bigl(2f; y, \exp(y; h^f)\bigr) \leqslant (\tfrac{1}{2}ek\log h_0)^{2f},\qquad f = 1, 2, \ldots;$$

$$(1.5.2)\qquad T\bigl(2b+2; q_0+1, z(h, 1)\bigr) \leqslant (\tfrac{1}{2}ek\log h_0)^{2b+2}.$$

Proof. The definition of $T(j; y, y')$ implies that

$$(1.5.3)\qquad T(1; y, y')T(j-1; y, y') \geqslant jT(j; y, y').$$

Thus, if we set $y' = y^h$ (or $y = q_0+1$ and $y' = z(h, 2b)$) and then use (1.4.1) the first assertion of the lemma follows. Repeated applications of (1.5.3) will yield

$$(1.5.4)\qquad T(j; y, y') \leqslant \bigl(T(1; y, y')\bigr)^j/j!.$$

Inequality (1.5.1) (or (1.5.2)) is a consequence of (1.5.4), the inequality $j! > (j/e)^j$, and (1.4.1).

We are now in a position to prove:

LEMMA 1.6. *There is a positive constant C_4 such that*

$$(1.6.1)\qquad \sum_{\substack{d\epsilon E\\(d,Q)=1}}\frac{\mu(d)\omega(d)}{\varphi(d)} \geqslant C_4\prod_{q_0<p\leqslant z}\Bigl(1-\frac{\omega(p)}{\varphi(p)}\Bigr).$$

Proof. Let us call the left hand side of (1.6.1) S; let $z'(h, i) = z(h, i)$ for $i = 1, 2, \ldots, 2b+1$ and let $z'(h, 2b+2) = q_0+1$. Let $g(d) = \mu(d)\omega(d)/\varphi(d)$ and let

$$E(f) = \sum_{j=0}^{2f-1} \sum_{d \epsilon E}^{(j,f)} g(d), \qquad f = 1, 2, \ldots, b+1, \tag{1.6.2}$$

where the superscript (j, f) means that the summation is to be restricted to those d having precisely j prime factors all of which are greater than $z'(h, 2f)$; the sum corresponding to $j = 0$ is equal to 1. Note that $E(b+1) = S$. Let

$$J(f) = \prod_{z'(h,2f) < p \leqslant z'(h,2f-1)} \left(1 - \frac{\omega(p)}{\varphi(p)}\right). \tag{1.6.3}$$

We want to show that, for $f = 1, 2, \ldots, b$,

$$E(f+1) \geqslant J(f+1)E(f) - \left(ek(\log h_0)/2\right)^{2f+2}. \tag{1.6.4}$$

Once we have the inequality (1.6.1) will be easy to prove.

Let us turn to the details. Let

$$T(i, f) = \sum_{d}{}_{(i,f)} g(d), \qquad i = 1, 2, \ldots, m_f,$$

where the subscript (i, f) is used to indicate that the summation is restricted to those d having i prime factors, all of which are greater than $z'(h, 2f+2)$ and less than or equal to $z(h, 2f)$, and m_f is the number of primes in this range.

Note that $|T(i, f)|$ is equal to the quantity $\left|T\left(i; z'(h, 2f+2), z'(h, 2f)\right)\right|$ of Lemma 1.5. Note also that the terms of $T(i, f)$ are terms of S if i does not exceed $2f+1$, for if all the prime factors of $d = p_1 \ldots p_i$ are less than or equal to $z'(h, 2f)$ then

$$p_1 \leqslant z'(h, 2f) \leqslant z'(h, 1), \quad \ldots, \quad p_i \leqslant z'(h, 2f) \leqslant z'(h, i),$$

i.e. $p_1 \ldots p_i$ is in E. Let $T(0, f) = 1$.

If we refer to the definitions of the quantities involved we see that

$$E(f+1) = \sum_{i=0}^{2f+1} \sum_{j=0}^{i} \sum_{d}{}_{(i-j,f)} g(d) \sum_{d \epsilon E}^{(j,f)} g(d), \tag{1.6.5}$$

where $\sum\limits_{d \epsilon E}^{(j,f)} g(d) = 0$ if $j \geqslant 2f$. If we set

$$S(j, f) = \sum_{d \epsilon E}^{(j,f)} g(d) \tag{1.6.6}$$

equation (1.6.5) can be written as

$$E(f+1) = \sum_{i=0}^{2f+1} \sum_{j=0}^{i} T(i-j, f) S(j, f).$$

Now, (1.6.3), (1.6.2), and (1.6.6) imply that

$$J(f+1)E(f) = \left(\sum_{i=0}^{\infty} T(i, f)\right)\left(\sum_{j=0}^{\infty} S(j, f)\right)$$

$$= E(f+1) + \sum_{i=0}^{2f-1} T(2f+2-i, f) S(i, f) + \sum_{j=0}^{2f-1} S(j, f) \sum_{i=0}^{\infty} T(2f+3-j+i, f).$$

The quantity

$$\sum_{i=0}^{2f-1} T(2f+2-i, f) S(i, f)$$

is, by definition, made up to terms $g(d)g(d')$ where dd' has precisely $2f+2$ prime factors, all of which are greater than $z'(h, 2f+2)$. Consequently it is less than or equal to $T\left(2f+2; z'(h, 2f+2), z'(h, 1)\right)$ which, by Lemma 1.5, is less than or equal to $\left(ek(\log h_0)/2\right)^{2f+2}$. Since $S(j, f) = (-1)^j |S(j, f)|$, $T(i, f) = (-1)^i |T(i, f)|$, and $|T(i, f)|$ is a decreasing function of i, we also have

$$\sum_{j=0}^{2f-1} S(j, f) \sum_{i=0}^{\infty} T(2f+3-j+i, f) \leqslant 0.$$

Therefore

$$E(f)J(f+1) \leqslant E(f+1) + \left(ek(\log h_0)/2\right)^{2f+2},$$

i.e. formula (1.6.4) holds.

Since

$$E(1) = 1 - \sum_{z'(h,2) < p \leqslant z'(h,1)} \frac{\omega(p)}{\varphi(p)} \geqslant 1 - k\log h_0,$$

the inequality being a consequence of Lemma 1.4, repeated applications of formulas (1.6.4) and (1.4.2) will lead us to the inequality

$$E(f+1) \geqslant J(f+1) \ldots J(2)\left[1 - k\log h_0 - \frac{h_0^k\left(ek(\log h_0)/2\right)^4}{1 - h_0^k\left(ek(\log h_0)/2\right)^2}\right],$$

provided that h_0 has been chosen so that $h_0^k\left(ek(\log h_0)/2\right)^2 < 1$. If we set $h_0 = \exp\left((3k)^{-1}\right)$, let $f = b$, and make use of the fact that $1 \geqslant J(1)$ we shall have

$$S = E(b+1) \geqslant C_4 J(1) \ldots J(b+1) = C_4 \prod_{q_0 < p \leqslant z} \left(1 - \frac{\omega(p)}{\varphi(p)}\right),$$

where C_4 is a positive constant. This completes the proof of Lemma 1.6.

We now have:

$$\sum_{d \in E} \frac{\mu(d)\omega(d)}{\varphi(d)} = \Big[\prod_{q \leqslant q_0}\Big(1-\frac{\omega(q)}{\varphi(q)}\Big)\Big] \sum_{\substack{d \in E\\ (d,Q)=1}} \frac{\mu(d)\omega(d)}{\varphi(d)}$$

$$\geqslant C_4 \prod_{p \leqslant z}\Big(1-\frac{\omega(p)}{\varphi(p)}\Big) = C_4 \exp\Big[\sum_{p \leqslant z} \log\Big(1-\frac{\omega(p)}{\varphi(p)}\Big)\Big]$$

$$\geqslant C_5 (\log z)^{-k}.$$

The first equality follows from the definitions; the first inequality is a consequence of Lemma 1.6, and the last inequality can be obtained by making use of the formula quoted in the proof of Lemma 1.4. Thus, (see (1.3.4))

$$(1.6.7) \qquad \Phi(x)\log x$$

$$\geqslant \frac{C_5}{\varphi(H)} \cdot \frac{1}{(\log z)^k} \cdot \frac{x}{\log x} + O\Big[\Big(\sum_{d \in E} \sum_{i=1}^{\omega(d)} |R(dH,\, c+u_i H)|\Big)\Big] + O(x^{1/2+\eta}\log x).$$

2. Some estimates. In this section we shall bring together the results which are needed to estimate the sum

$$P(x;\, d,\, w) = \sum_{\substack{p \leqslant x\\ p \equiv w \bmod d}} a_p,$$

where $d = d'H$, d' is in E, $(d', H) = 1$, and $(w, d) = 1$. The lemmas that follow are, for the most part, modifications of statements which can be found in Renyi's paper [5]; outlines of the proofs are included for the sake of convenience.

LEMMA 2.1. *Let d_1 be the primitive modulus not exceeding $\exp[c_1(\log x)^{1/2}]$, which is unique if it exists, for which an L-series $L(s, \chi)$, formed with a real character modulo d_1, has a zero β on the real line with $\beta > 1-c_2(\log x)^{-1/2}$. Then for $d \leqslant \exp[c_1(\log x)^{1/2}]$ we have*

$$(2.1.1) \quad P(x;\, d,\, w) = \frac{1}{\varphi(d)} \cdot \frac{x}{\log x} + O\big(x\exp\{-c_3(\log x)^{1/2}\}\big) + O(x^F),$$

where $F = 1-c(\varepsilon)d_1^{-\varepsilon}$. The last O-term appears iff d_1 divides d; ε is a fixed positive number, and $c(\varepsilon)$ is a constant that depends only on ε. The O-estimates hold uniformly for $d \leqslant \exp\{c_1(\log x)^{1/2}\}$.

The numbers $c_1, \ldots$ appearing in this section will denote positive constants.

Lemma 2.1 can be proved by means of the classical result of Page

$$\pi(u;\, d,\, w) = \frac{1}{\varphi(d)}\operatorname{Li}(u) + \Delta(u;\, d,\, w),$$

where $\pi(u;\, d,\, w)$ is the number of primes of the form $dt+w$ which are less than or equal to u,

$$\operatorname{Li}(u) = \lim_{\varepsilon -> 0}\Big(\int_0^{1-\varepsilon} + \int_{\dot 0}^{1+\varepsilon}\Big)\frac{dt}{\log t},$$

and

$$\Delta(u;\, d,\, w) = O\Big(\frac{1}{\varphi(d)}u^F + u\exp\big(-c_4(\log u)^{1/2}\big)\Big).$$

These relations are proved in [4]; see chapter IV, Theorems (6.7), (7.4), and (8.2).

To obtain (2.1.1) note, first of all, that

$$\sum_{\substack{p \leqslant x\\ p \equiv w \bmod d}} a_p = \int_{2-}^{x} (\log u)\exp(-u\log x/x)\, d[\pi(u;\, d,\, w)]$$

$$= \int_2^x \frac{\exp(-u\log x/x)}{\varphi(d)}\, du + \int_{2-}^{x} (\log u)\exp(-u\log x/x)\, d\big(\Delta(u;\, d,\, w)\big).$$

Then integrate the last integral by parts.

LEMMA 2.2. *There is a positive constant c_5 such that $P(x;\, d,\, w) \leqslant c_5 x/\varphi(d)$ uniformly for $d \leqslant x^{1/2}$, where $x \geqslant 2$.*

Proof. Make use of the formula ([4], Chapter 2, Th. (4.1))

$$\sum_{\substack{p \leqslant x\\ p \equiv w \bmod d}} 1 \leqslant \frac{c_6}{\varphi(d)} \cdot \frac{x}{\log x/d}.$$

Most of the sums $P(x;\, d,\, w)$, where d is "large", will be reduced to a sum to which Lemma 2.1 can be applied. The reduction will be an interative one and it will be done in terms of the sums $K(x;\, \chi)$, where

$$K(x;\, \chi) = \sum_{p \leqslant x} \chi(p)a_p.$$

The next lemma will deal with these sums, but we need one more definition before stating it. Suppose that $d = p \cdot q$, where $(p, q) = 1$, p is a prime, $q = q'H$, $(q', H) = 1$, and q' is square free. Let χ_d be a character mod d. From the theory of characters we can write

$$\chi_d = \chi_p \chi_q$$

where X_p (X_q) is a character modulo p (modulo q). (See [2], exercise 4 for Chapter III, page 244.) If in this decomposition X_p is not the principal character modulo p we shall say that χ_d *is primitive with respect to p.*

LEMMA 2.3 (Renyi). *Let $q = q'H$, where $(q', H) = 1$ and q' is square free. Let x be a sufficiently large number, and let A be a number such that $\exp(\log x)^{2/5} < Aq \leqslant x^{1/2}/2$. Let p be a prime such that $(p, q) = 1$ and such that $A \leqslant p < 2A$. Suppose, in addition, that*

$$k_1 = (\log q)\big(\log(p/2)\big)^{-1}+1 \leqslant \log^3 A.$$

Then for almost all primes p under consideration, i.e., with the possible exception of at most $A^{3/4}$ exceptional primes, and for all characters χ which belong to the modulus $p\cdot q$ and which are primitive with respect to p, the following inequality holds:

$$|K(x;\chi)| \leqslant c_7 X^P,$$

where $P = 1-a(k_1+1)^{-1}$, c_7 and a are absolute positive constants, and a is less than 1.

This lemma is almost identical to Lemma 4 of [5], the chief difference being that the q of Lemma 4 must be square free. Lemma 2.3, however, can be proved by the same method that was used to prove Lemma 4; small changes have to be made in the proofs of Lemmas 1 and 2 and Theorem 3 of [5].

Let

$$E_1 = \{d\colon\ d = d'H,\ d'\,\epsilon\, E,\ (d', H) = 1\}.$$

We shall also use the following notation. If d is in E_1 then $d = d'H = p_1 \ldots p_r d^* H$. Set $d = p_1 b_1$, $b_1 = p_2 b_2, \ldots, b_{r-1} = p_r b_r$, $b_r = d^* H$. The numbers $b_1, \ldots, b_r$ will be called the *diagonal divisors of* d; it follows directly from the definitions that they are in E_1. The next few lemmas will deal with the properties of the set E_1.

LEMMA 2.4. *If d is in E_1, if $z = x^{1/R}$, where R is a constant greater than 2, and if $v(d)$ denotes the number of prime factors of d, where the multiple prime factors of H are counted multiply, then $v(d) \leqslant B\log\log x$, where B is a constant which depends on h, q_0, and R.*

Proof. Make use of the facts: $d = p_1 \ldots p_r d^* H$, $r \leqslant 2b+1$, and $q_0 < z(h, 2b)$.

LEMMA 2.5. *If d is in E_1 and if $p_1 \leqslant \exp(z; h^{-n})$, where n is a non-negative integer, then*

$$d \leqslant QH\exp\big[z; h^{-n}\big(2n+1+2(h-1)^{-1}\big)\big].$$

Proof. By our assumptions we have for $i = 1, 2, \ldots, 2n+1$,

$$p_i \leqslant p_1 \leqslant \exp(z; h^{-n}),$$

while for $j = 2, 3, \ldots$

$$p_{2n+j} \leqslant z(h, 2n+j) = \exp\{z; h^{-n-[j/2]}\}.$$

Therefore,

$$d \leqslant QH\exp\big\{z; h^{-n}\big(2n+1+2(h-1)^{-1}\big)\big\},$$

and the conclusion of the lemma follows.

COROLLARY 1. *If d is in E_1, then*

$$d \leqslant Q\cdot H\exp\left\{x; \frac{1}{R}\cdot\frac{h+1}{h-1}\right\}.$$

Proof. Let $n = 0$, where $z = x^{1/R}$, in Lemma 2.5.

COROLLARY 2. *If q_0 is the λ-th prime then the set E has at most $2^{\lambda}H\exp\left\{x; \frac{1}{R}\cdot\frac{h+1}{h-1}\right\}$ elements.*

LEMMA 2.6. *If $d = p_1 b_1$ is in E_1 and if $p_1 < (b_1)^{1/t}$, where t is a positive integer, then $d < \exp(z; c_8 t h^{-t/2})$, where c_8 is a constant that depends on q_0 and h.*

Proof. Suppose that q_0 is the λth prime and that

$$\exp(z; h^{-n-1}) < p_1 \leqslant \exp(z; h^{-n}),$$

where n is a non-negative integer. Proceeding as in Lemma 2.5 we have

$$b_1 \leqslant p_2 \ldots p_{2n+1} \ldots p_r QH \leqslant p_1^{2n+\lambda'}\exp[z; 2h^{-n}(h-1)^{-1}],$$

where $\lambda' = \lambda + v(h)$. Thus

$$d = p_1 b_1 \leqslant \exp\big[z; h^{-n}\big(2n+\lambda'+1+2(h-1)^{-1}\big)\big]$$
$$< \exp\big[z; h^{-n}\big(2n+\lambda'+2h(h-1)^{-1}\big)\big].$$

We also have

$$p_1^t < b_1 < \exp[p_1; 2n+\lambda'+2h(h-1)^{-1}],$$

i.e.

$$t < 2n+\lambda'+2h(h-1)^{-1}.$$

For convenience, let $\lambda'+2h(h-1)^{-1} = M$.

Since $h^{t/2}t^{-1}$ takes on its maximum value at $t = 1$ or $t = 2n+M$ for $1 \leqslant t \leqslant 2n+M$, we have

$$\begin{aligned}\frac{(2n+M)}{h^n}\cdot\frac{h^{t/2}}{t} &\leqslant \max\left\{\frac{2n+M}{h^n}h^{1/2}, \frac{2n+M}{h^n}\cdot\frac{h^{(2n+M)/2}}{2n+M}\right\}\\ &\leqslant \max\left\{\left\{\max_{n\geqslant 0}\frac{2n+M}{h^{n-1/2}}\right\}, \exp(h; M/2)\right\}\\ &= c_8.\end{aligned}$$

Consequently,

$$d = p_1 b_1 < \exp[z; h^{-n}(2n+M)] < \exp[z; c_8 t h^{-t/2}],$$

which is the inequality we set out to prove.

LEMMA 2.7. *Let $\{p'\}$ be a sequence of primes with the property that no interval $(A, 2A)$ contains more than $A^{3/4}$ terms of the sequence $\{p'\}$. Then for any number $M_1 > 2$,*

$$\sum_{p'>M_1} \frac{1}{p'-1} < c_9 (M_1)^{-1/4},$$

where c_9 is an absolute positive constant.

Proof.

$$\sum_{p'>M_1} \frac{1}{p'-1} = \sum_{j=0}^{\infty} \sum_{2^j M_1 < p' \leqslant 2^{j+1} M_1} \frac{1}{p'-1} < \sum_{j=0}^{\infty} \frac{(2^j M_1)^{3/4}}{2^j M_1 - 1} < c_9 (M_1)^{-1/4}.$$

LEMMA 2.8. *There is a positive constant c_{10}, which depends on the polynomial $G(n)$, such that*

$$\sum_{n\leqslant x} \frac{\mu^2(n)\omega(n)}{\varphi(n)} \leqslant c_{10} (\log x)^k.$$

To obtain this inequality first obtain the summatory function of the series

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{\varphi(n)} \cdot \frac{\omega(n)}{n^{s-1}}$$

by comparing the series with the product of the zeta functions of the fields associated with the polynomials $G_i(t)$, where $G_i(t)$ is an irreducible factor of $G(n)$. Then proceed by partial summation (see [3], section 3).

3. The error term. We are now in a position to estimate the sum

$$P(x; d, w) = \sum_{\substack{p\leqslant x \\ p\equiv w \bmod d}} a_p$$

where d is in E_1. If d is small, i.e. if $1 \leqslant d \leqslant 2\exp(\log x)^{2/5}$, the sum in question can be evaluated by means of Lemma 2.1. The approach to the problem is less direct if $2\exp(\log x)^{2/5} < d \leqslant x^{1/2}/2$.

Suppose that d is large, fixed, and in E_1. Let $b_1, \ldots,$ and b_r be the diagonal divisors of d. Let χ_d denote a character formed to the modulus d. Let

$$A(d) = \{\chi_d\colon\ \chi_d = \chi_{p_1}\chi_{b_1},\ \chi_{p_1} \text{ is principal}\},$$
$$B(d) = \{\chi_d\colon\ \chi_d = \chi_{p_1}\chi_{b_1},\ \chi_{p_1} \text{ is not principal}\}.$$

Now,

$$P(x; d, w) = \sum_{p\leqslant x} a_p \frac{1}{\varphi(d)} \sum_{\chi_d} \overline{\chi_d(w)}\,\chi_d(p) = \frac{1}{\varphi(d)} \sum_{\chi_d} \overline{\chi_d(w)} \sum_{p\leqslant x} \chi_d(p)\,a_p$$
$$= \frac{1}{\varphi(d)} \sum_{\chi_d \in A(d)} \overline{\chi_{b_1}(w)}\,\overline{\chi_{p_1}(w)} \sum_{p\leqslant x} \chi_{b_1}(p)\chi_{p_1}(p)\,a_p +$$
$$+ \frac{1}{\varphi(d)} \sum_{\chi_d \in B(d)} \overline{\chi_d(w)} \sum_{p\leqslant x} \chi_d(p)\,a_p$$
$$= \frac{1}{\varphi(p_1)} \left[\frac{1}{\varphi(b_1)} \sum_{\chi_{b_1}} \overline{\chi_{b_1}(w)} \sum_{p\leqslant x} \chi_{b_1}(p)\,a_p\right] -$$
$$- \frac{1}{\varphi(d)} \left[\sum_{\chi_{b_1}} \overline{\chi_{b_1}(w)}\,\chi_{b_1}(p_1)\right] a_{p_1} + \frac{1}{\varphi(d)} \sum_{\chi_d \in B(d)} \overline{\chi_d(w)}\,K(x; \chi_d).$$

That is,

(3.0.1) $P(x; d, w)$

$$= \frac{1}{\varphi(p_1)} P(x; b_1, w) - C(p_1, b_1) \frac{a_{p_1}}{\varphi(p_1)} + \frac{1}{\varphi(d)} \sum_{\chi_d \in B(d)} \overline{\chi_d(w)}\,K(x; \chi_d),$$

where $C(p_1, b_1) = 1$ if $p_1 \equiv w \bmod b_1$ and is 0 otherwise. If p_1 is not exceptional with respect to b_1 in the sense of Lemma 2.3 we can estimate the last sum on the right hand side of (3.0.1); to do this we must define the number A and check out the assumptions of that lemma.

As for the number A, since

$$p_1 > d^{1/v(d)} > \exp[(\log x)^{2/5}/v(d)] > \exp[(\log x)^{2/5}/B\log\log x]$$
$$> \exp(\log x)^{1/3}$$

for x sufficiently large (see Lemma 2.4), we shall set $A = 2^l M_1$ where $M_1 = \exp(\log x)^{1/3}$ and l is a non-negative integer; we will not need to know the exact value of l. The assumption (of Lemma 2.3) that

$$\exp(\log x)^{2/5} \leqslant Ab_1 < x^{1/2}/2$$

follows since:

(1) $Ab_1 < p_1 b_1 = d \leqslant x^{1/2}/2$,

(2) $Ab_1 > (p_1/2) b_1 = d/2 > \exp(\log x)^{2/5}$.

The character χ_d will be primitive with respect to p_1 since χ_d is in $B(d)$. The fact that $k_1 \leqslant \log^3 A$ follows from the definition of k_1 and the inequalities

$$b_1 < p_1^{v(d)} < p_1^{B\log\log x}.$$

Thus the assumptions of Lemma 2.3 hold. Since we have also assumed that p_1 is not exceptional with respect to b_1 we can apply Renyi's lemma to get

$$\frac{1}{\varphi(d)} \sum_{\chi_d \epsilon B(d)} |\chi_d(w) K(x; \chi_d)| < c_7 x^P, \tag{3.0.2}$$

where c_7 is an absolute constant. Relations (3.0.1) and (3.0.2) and the fact that $a_{p_1}/\varphi(p_1) = O(1)$ imply that

$$P(x; d, w) = \frac{1}{\varphi(p_1)} P(x; b_1, w) + O(x^P), \tag{3.0.3}$$

provided that $2\exp(\log x)^{2/5} < d \leqslant x^{1/2}$ and that p_1 is not exceptional with respect to b_1.

Suppose that $b_i > 2\exp(\log x)^{2/5}$ for $i = 1, 2, \dots, s-1$ $(s \geqslant 2)$ and that p_i is not exceptional with respect to b_i for $i = 1, 2, \dots, s$, and suppose that $b_s \leqslant 2\exp(\log x)^{2/5}$ or p_{s+1} is exceptional with respect to b_{s+1}. Applying (3.0.3) s times we have

$$P(x; d, w) = \frac{1}{\varphi(p_1 \dots p_s)} P(x; b_s, w) + O\left[\sum_{i=1}^{s} \frac{x^{P(i)}}{\varphi(p_0 \dots p_{i-1})}\right],$$

where $d = p_1 \dots p_s b_s$, $p_0 = 1$, $P(i) = 1 - a(k_i+1)^{-1}$, and $k_i = (\log b_i) \times \times (\log(p_i/2))^{-1} + 1$. If $b_s \leqslant 2\exp(\log x)^{2/5}$ we can apply Lemma 2.1 to get

$$P(x; d, w) = \frac{1}{\varphi(d)} \cdot \frac{x}{\log x} + O\left[\frac{x\exp[-c_3(\log x)^{1/2}]}{\varphi(p_1 \dots p_s)}\right] + \\ + O\left[\frac{x^F}{\varphi(d)}\right] + O\left[\sum_{i=1}^{s} \frac{x^{P(i)}}{\varphi(p_0 \dots p_{i-1})}\right],$$

the second O-term appearing iff d_1 divides d. If p_{s+1} is exceptional with respect to b_{s+1} we would have, by Lemma 2.2

$$P(x; d, w) = \frac{1}{\varphi(d)} \cdot \frac{x}{\log x} + O\left(\frac{x}{\varphi(d)}\right) + O\left[\sum_{i=1}^{s} \frac{x^{P(i)}}{\varphi(p_0 \dots p_{i-1})}\right].$$

We would also employ Lemma 2.2 if p_1 were exceptional to b_1.

The last two equations show that we have four types of error terms to evaluate when we estimate the error. Keeping in mind that we are working with the sum

$$\sum_{i=1}^{\omega(d')} \sum_{\substack{p \leqslant x \\ p \equiv w_i \bmod d}} a_p = \sum_{i=1}^{\omega(d')} \left[\frac{1}{\varphi(d)} \cdot \frac{x}{\log x} + \text{an Error}\right],$$

where $d = d'H$, we see that they are terms of the form:

$$(1) \quad \frac{\omega(d')}{\varphi(d)} x; \qquad (2) \quad \frac{\omega(d') x \exp[-c_3(\log x)^{1/2}]}{\varphi(p_1 \dots p_s)};$$

$$(3) \quad \frac{\omega(d')}{\varphi(d)} x^F; \qquad (4) \quad \omega(d') \frac{x^{P(i)}}{\varphi(p_0 \dots p_{i-1})}.$$

Let $R(1)$ denote the sum of the error terms of the first type, the summation being extended over all those d in E_1 for which terms of the first form exist; define $R(2)$, $R(3)$, and $R(4)$ similarly.

$R(1)$ is made up of terms of the form

$$\frac{\omega(d')}{\varphi(d)} x$$

where $d = d'H$, $d = p_1 \dots p_s p_{s+1} b_{s-1}$, and p_{s+1} is exceptional with respect to b_{s+1}. That part of $R(1)$ arising from those $d = p_1 \dots p_s p_{s+1} b_{s+1}$ where both $p_1 \dots p_s$ and b_{s+1} are fixed is

$$O\left[\frac{\omega(p_1 \dots p_s b'_{s+1})}{\varphi(p_1 \dots p_s b_{s+1})} x \sum_{p_{s+1} > \exp(\log x)^{1/3}} \frac{\omega(p_{s+1})}{(p_{s+1}-1)}\right],$$

where $b'_{s+1} = b_{s+1}/H$. This last quantity is, by Lemma 2.7,

$$O\left[\frac{\omega(p_1 \dots p_s b'_{s+1})}{\varphi(p_1 \dots p_s b_{s+1})} \exp\left\{-\frac{1}{4}(\log x)^{1/3}\right\} x\right].$$

If we now sum on the $p_1 \dots p_s b_{s+1}$ we have, according to Lemma 2.8.

$$R(1) = O\left(\sum_{d \epsilon E_1} \frac{\omega(d')}{\varphi(d)} \exp\left\{-\frac{1}{4}(\log x)^{1/3}\right\} x\right)$$
$$= O\left((\log x)^k \exp\left\{-\frac{1}{4}(\log x)^{1/3}\right\} x\right)$$
$$= O\left(x(\log x)^{-k-2}\right).$$

The constant in the O-term will depend on the polynomial $G(n)$.

Let us turn to $R(2)$. We are dealing with terms of the form

$$\frac{\omega(p_1\dots p_s)}{\varphi(p_1\dots p_s)}\,\omega(b_s')x\exp[-c_3(\log x)^{1/2}],$$

where $b_s' = b_s/H \leqslant 2\exp(\log x)^{2/5}$. Since $\omega(b_s') = O\big((b_s')^{\varepsilon}\big)$ and since there are at most $2\exp(\log x)^{2/5}$ numbers b_s' associated with each fixed $p_1\dots p_s$ it follows that that part of $R(2)$ arising from each fixed $p_1\dots p_s$ is

$$O\left(\frac{\omega(p_1\dots p_s)}{\varphi(p_1\dots p_s)}x\exp[-C_3(\log x)^{1/2}]\exp[(1+\varepsilon)(\log x)^{2/5}]\right).$$

If we now sum on the $p_1\dots p_s$ and apply Lemma 2.8 we shall have

$$R(2) = O[x(\log x)^{-k-2}].$$

The terms of $R(3)$ are of the form

$$\frac{\omega(p_1\dots p_s)}{\varphi(p_1\dots p_s)}\cdot\frac{\omega(b_s')}{\varphi(b_s)}x^F,$$

where $F = 1-c(\varepsilon)d_1^{-\varepsilon}$, d_1 divides b_s, d_1 is a unique fixed integer depending on x, and $b_s \leqslant 2\exp(\log x)^{2/5}$. Thus that part of $R(3)$ stemming from a fixed $p_1\dots p_s$ is, with $d_2 = d_1/(d_1, H)$,

$$O\left[\frac{\omega(p_1\dots p_s)}{\varphi(p_1\dots p_s)}\sum_{\substack{n\leqslant 2\exp(\log x)^{2/5}\\ d_2|n}}\frac{\mu^2(n)\,\omega(n)}{\varphi(nH)}x^F\right],$$

which, by Lemma 2.8, is

$$O\left(\frac{\omega(p_1\dots p_s)}{\varphi(p_1\dots p_s)}x^F\frac{\omega(d_2)}{\varphi(d_1)}(\log x)^{2k/5}\right).$$

If we now sum on $p_1\dots p_s$ we shall have

$$R(3) = O\left(\frac{\omega(d_2)}{\varphi(d_1)}(\log x)^{7k/5}x^F\right).$$

But $1/\varphi(d_1) < C_{11}\log d_1/d_1$, $\omega(d_2) < C_{12}d_1^{\varepsilon}$, and $d_1 < x$ imply that $\omega(d_1)/\varphi(d_1) < C_{11}C_{12}(\log d_1)d_1^{-1+\varepsilon} < C_{11}C_{12}(\log x)d_1^{-1+\varepsilon}$. Consequently,

$$\begin{aligned}R(3) &= O\big((\log x)^{7k/5+1}d_1^{-1+\varepsilon}x^F\big)\\ &= O\left[x(\log x)^{3k}\exp\left(\frac{-C(\varepsilon)}{d_1^{\varepsilon}}\log x-(1-\varepsilon)\log d_1\right)\right].\end{aligned}$$

The function

$$f(d_1) = \frac{c(\varepsilon)}{d_1^{\varepsilon}}\log x+(1-\varepsilon)\log d_1$$

has a minimum value of

$$\left(\frac{1-\varepsilon}{\varepsilon}\right)\log\log x+\left(\frac{1-\varepsilon}{\varepsilon}\right)\log\left(\frac{ec(\varepsilon)\varepsilon}{1-\varepsilon}\right)$$

at the point

$$d_1 = \left(\frac{\varepsilon c(\varepsilon)\log x}{1-\varepsilon}\right)^{1/\varepsilon}.$$

If, therefore, we set $\varepsilon = 1/(4k+3)$ we shall have

$$R(3) = O\big(x(\log x)^{-k-2}\big).$$

$R(4)$ remains. We are dealing with terms of the form

$$\frac{\omega(d')}{\varphi(p_0\dots p_{i-1})}x^{P(i)}$$

where $d = d'H = p_0p_1\dots p_{i-1}p_ib_i$, $P(i) = 1-a(k_i+1)^{-1}$, and $k_i = \log b_i\big(\log(p_i/2)\big)^{-1}+1$. Split $R(4)$ into two sums, $R(4;1)$ and $R(4;2)$; the first is to contain those terms for which $k_i < 4$, the second those for which $k_i \geqslant 4$.

Now,

$$R(4;1) = O\left[\sum_{i\geqslant 1}\sum_{\substack{p_0\dots p_{i-1}\\ p_0\dots p_{i-1}\epsilon E}}\frac{\omega(p_0\dots p_{i-1})}{\varphi(p_0\dots p_{i-1})}\sum_{\substack{p_ib_i\\ k_i<4,p_0\dots p_{i-1}p_ib_i\epsilon E_1}}\omega(p_ib_i')x^{P(i)}\right].$$

We have: $P(i) < 1-a/5$, since $k_i < 4$; $\omega(p_ib_i') = (x^{\delta\cdot\varepsilon})$ by Corollary 1 of Lemma 2.5, where $\delta = (h+1)\big(R(h-1)\big)^{-1}$, and the number of $\omega(p_ib_i')$ entering our calculations is $O(x^{\delta})$, by the second corollary of Lemma 2.5. Thus, the inner sum above is $O\big(\exp(x; 1-a/5+\delta+\delta\cdot\varepsilon)\big)$. If now we sum on the i and the $p_0\dots p_{i-1}$ we shall have

$$R(4;1) = O\big((\log x)^k\exp(x; 1-a/5+\delta+\delta\cdot\varepsilon)\big).$$

We shall want to have

$$1-\tfrac{1}{5}a+\delta+\delta\cdot\varepsilon < 1-\tfrac{1}{10}a.$$

Since $\delta = (h+1)R^{-1}(h-1)^{-1}$ and $\varepsilon = (4k+3)^{-1}$ this is equivalent to demanding that

$$R > \frac{10}{a}\cdot\frac{4k+4}{4k+3}\left(\frac{h+1}{h-1}\right).$$

Thus, supposing we have selected R properly, we have

$$R(4;1) = O[x(\log x)^{-k-2}].$$

icm©

We shall now estimate $R(4;2)$. Note that $R(4;2)$ is made up of terms for which

$$2v \leqslant k_i < 2v+2, \qquad v = 2, \ldots, [(B+1)(\log\log x)/2] = B(x).$$

This observation is a consequence of the facts that:

(1) $k_i = (\log b_i)\big(\log(p_i/2)\big)^{-1}+1$;

(2) If $d = p_i b_i$ then $b_i < p_i^{\tau(d)} < p_i^{B\log\log x}$.

Note also that if $2v \leqslant k_i$ then $p_i < (b_i)^{1/v}$. This follows for if

$$k_i = (\log b_i)\big(\log(p_i/2)\big)^{-1}+1 \geqslant 2v$$

then

$$p_i < 2\exp[b_i;\,(2v-1)^{-1}].$$

If we assume that $2\exp[b_i;\,(2v-1)^{-1}] > b_i^{1/v}$ then

$$\log b_i < v\left(\frac{2v-1}{v-1}\right)\log 2 < (2v+2)\log 2 < \big((B+1)\log\log x+2\big)\log 2.$$

Since

$$(p_i/2) > \big(\exp(\log x)^{1/3}\big)/2 > \exp(\log x)^{3/10}$$

we have

$$k_i = \frac{\log b_i}{\log(p_i/2)}+1 < \frac{\big((B+1)\log\log x+2\big)\log 2}{(\log x)^{3/10}}+1 < 4,$$

for x sufficiently large. But we are assuming that $k_i \geqslant 2v \geqslant 4$. Thus $2\exp[b_i;\,(2v-1)^{-1}] \leqslant b_i^{1/v}$, or $p_i \leqslant (b_i)^{1/v}$.

We have

$$R(4;2) = O\Bigg[\sum_{v=2}^{B(x)}\sum_{i\geqslant 1}\sum_{p_0\ldots p_{i-1}\epsilon E}\frac{w(p_0\ldots p_{i-1})}{\varphi(p_1\ldots p_{i-1})}\sum_{\substack{p_0\ldots p_{i-1}p_ib_i\epsilon E_1\\ 2v\leqslant k_i<2v+2}} w(p_ib_i')x^{P(i)}\Bigg].$$

Let us hold v, i, and $p_0\ldots p_{i-1}$ fixed. Then, since $k_i < 2v+2$, $P(i) < 1-\alpha(2v+3)^{-1}$. Since $p_i < (b_i)^{1/v}$, we have by Lemma 2.6,

$$\omega(p_ib_i') = O\left(\exp\left(x;\,\frac{C_8}{R}\cdot\frac{v}{h^{v/2}}\,\varepsilon\right)\right);$$

one more application of Lemma 2.6 yields the equation

$$\sum_{\substack{p_ib_i\\ 2v\leqslant k_i<2v+2}}\omega(p_ib_i')x^{P(i)} = O\left[\exp\left(x;\,1-\frac{a}{2v+3}+\frac{c_8}{R}\cdot\frac{v}{h^{v/2}}(1+\varepsilon)\right)\right].$$

When we select R we shall insist that

$$R > \frac{2c_8}{a}\left(\frac{4k+4}{4k+3}\right)(2r+3)\frac{r}{h^{r/2}}.$$

i.e.,

$$1-\frac{a}{2r+3}+\frac{c_8}{R}\cdot\frac{r}{h^{r/2}}(1+\varepsilon) < 1-\frac{a}{2(2r+3)}.$$

Assuming that R has been chosen with care, we have:

$$R(4,2) = O\Bigg[\sum_{r=2}^{B(x)}\sum_{i\geqslant 1}\sum_{p_0\ldots p_{i-1}\epsilon E}\frac{\omega(p_0\ldots p_{i-1})}{\varphi(p_0\ldots p_{i-1})}\exp\left(x;\,1-\frac{a}{2(2r+3)}\right)\Bigg].$$

If, now, we sum on the i's and the $p_0\ldots p_{i-1}$'s, and then sum on the r's we shall have

$$R(4;2) = O\left[B(x)(\log x)^k\exp\left(x;\,1-\frac{a}{2(2B(x)+3)}\right)\right] = O\big(x(\log x)^{-k-2}\big).$$

The constant R has to satisfy three conditions:

(1) $$R > 2(h+1)(h-1)^{-1} = J_1.$$

This inequality must be satisfied because we insisted that if d is in E_1 then $d \leqslant x^{1/2}/2$. (See the comments preceeding formula (1.3.3) and Corollary 1 of Lemma 2.5).

(2) $$R > \frac{10}{a}\left(\frac{4k+4}{4k+3}\right)\frac{h+1}{h-1} = J_2.$$

This inequality was used in the estimate of $R(4;1)$. The inequality

(3) $$R > \frac{2c_8}{a}\left(\frac{4k+4}{4k+3}\right)\left(\max_{v\geqslant 2}(2v+2)\frac{v}{h^{v/2}}\right) = J_3$$

was used in the estimate of $R(4;2)$. We also had $1 < h < h_0$, where $h_0 = \exp\big((3k)^{-1}\big)$. Let $h = \exp\big((4k)^{-1}\big)$ and $R = [2+\max\{J_1, J_2, J_3\}]$. Then R will be large enough for our requirements.

We can now prove Theorem 1. If we turn to formula (1.6.7) set $z = x^{1/R}$, fix R, set $\eta = 1/4$, and then use the results of this section we shall have

$$\Phi(x) \geqslant C_6x(\log x)^{-k-2}+O[x(\log x)^{-k-3}],$$

where C_6 in a constant which depends on the polynomial $G(n)$ and the integer H. In words, there are more than $C_7x(\log x)^{-k-2}$ primes p congruent to c modulo H which are less than x for which $G(t)$ has all of its prime factors greater than $x^{1/R}$, i.e., $G(t)$ has at most $R\cdot m$ prime factors, m being the degree of the polynomial. Since the polynomial $F(n)$ of Theorem 1 is equal to $F(c)G(t)$, the theorem follows if we set

$$A = Rm+A_1,$$

where A_1 is the number of prime factors of $F(c)$.

References

[1] V. Brun, *Le crible d'Eratosthene et le theoreme de Goldbach*, Norske Videnskapselskapets Skripter I. Kristiania, 3 (1920).

[2] E. Landau, *Elementary Number Theory*, Chelsea, New York, 1958.

[3] R. Miech, *Almost primes generated by a polynomial*, Acta Arith. 10 (1964), pp. 11-32.

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

[5] A. Renyi, *On the representation of an even number as the sum of a prime and of an almost prime*. American Mathematical Society Translations, Ser. 2, Vol. 19, Amer. Math. Soc., Providence, R. I., 1962. (English). Izvestiya Akad. Nauk SSSR. Ser. Mat. 12 (1948), pp. 57-78 (Russian).

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS

Reçu par la Rédaction le 20. 3. 1964

ACTA ARITHMETICA
XI (1965)

On Mordell's theorem

by

I. SH. SLAVUTSKY (Leningrad)

1. Suppose that $R(\sqrt{d})$ is a real quadratic field with fundamental discriminant d, main unit $E_1 = T_1+U_1\sqrt{d}$ and class number $h(d)$. Following Berger and Leopoldt ([6], [21]), we introduce the generalized Bernoulli numbers B_χ^k belonging to a primitive residue character χ modulo $f \geqslant 1$ by the relation[1]

$$\sum_{r=1}^{f} \frac{\chi(r)te^{rt}}{e^{ft}-1} = \sum_{k=0}^{\infty} B_\chi^k \frac{t^k}{k!}, \qquad |t| < \frac{2\pi}{f}.$$

Then the results we find in some Mordell's articles ([24]-[27]), and in the article by Ankeny and Chowla ([4]) demonstrate the equivalence of two facts

$$U_1 \equiv 0 (\mathrm{mod}\, p),$$

$$B_\chi^{(p-1)/2} \equiv 0 \ (\mathrm{mod}\, p),$$

where $f = 1$ for $d = p \equiv 1 (\mathrm{mod}\, 4)$, and $f = 4$ for $d = 4p$, $p \equiv 3 (\mathrm{mod}\, 4)$.

This fact was first stated by Kiselev ([15], [16]) and later independently by Ankeny, Artin and Chowla ([1], [2], [4]), but Mordell succeeded without Dirichlet's formulae which have not up to now been proved with the help of elementary methods.

In this note, by extending Mordell's method of p-adic logarithm, there is demonstrated the

THEOREM. *Let $R(\sqrt{d})$ be a real quadratic field with fundamental discriminant $d = np$, $p > 3$, an odd prime number and $1 \leqslant n < p$. The congruence*

$$U_1 \equiv 0 (\mathrm{mod}\, p^l) \tag{1}$$

[1] As for arithmetical properties of B_χ^k, see articles [9], [18], [19], [21], [29]. We remark also that for $f = 1$ and $f = 4$, generalized Bernoulli numbers correspond to usual Bernoulli and Euler numbers.