PACIFIC JOURNAL OF MATHEMATICS
Vol 118, No. 2, 1985

INFINITELY INTEGER-VALUED POLYNOMIALS OVER AN ALGEBRAIC NUMBER FIELD

KENNETH ROGERS AND E. G. STRAUS

In memory of Ernst Straus

Let K be an algebraic number field and R its ring of integers. A polynomial f over K is integer-valued iff $f(R) \subseteq R$: it is infinitely integer-valued, written $f \in D^{\infty}(R)$, iff f and all its derivatives are integer-valued. For each K we construct a sequence of ideals A_k of R, and a sequence of polynomials $H_k(x)$ over R, such that a polynomial f of degree n lies in $D^{\infty}(R)$ if and only if it is of the form $a_0 H_0(x)/0! + \cdots + a_n H_n(x)/n!$, with a_k in A_k, $k = 0, 1, \ldots, n$.

1. Introduction. It is well-known that $\binom{x}{n}$, $n = 0, 1, 2, \ldots$ is a basis for the integer-valued polynomials over $\mathbf{Z}$: for any polynomial of degree n over a field of characteristic zero can be written as

$$f(x) = f(0)\binom{x}{0} + \Delta f(0)\binom{x}{1} + \cdots + \Delta^n f(0)\binom{x}{n} \tag{1.1}$$

where $\Delta g(x) = g(x+1) - g(x)$. Let $\mathbf{D}_n$ denote the $\mathbf{R}$-module of all polynomials of degree at most n that lie in $\mathbf{D}^{\infty}(\mathbf{R})$:

$$g(x) \in \mathbf{D}_n \quad \text{iff} \quad \deg g \leq n \text{ and } g^{(k)}(\mathbf{R}) \subseteq \mathbf{R}, \qquad k = 0, 1, 2, \ldots.$$

Note that $n!\mathbf{D}_n \subseteq \mathbf{R}[x]$, by (1.1). In 1919, Polya [**2**] found a basis for the integer-valued polynomials over $\mathbf{R}$ when $\mathbf{R}$ is principal, analogous to $\binom{x}{n}$ for $\mathbf{Z}$. Then Ostrowski [**1**] found a condition on $\mathbf{K}$ for such a basis to exist even in cases of non-principal $\mathbf{R}$. In 1951, Straus [**3**] showed that

$$f \in D^{\infty}(\mathbf{Z}) \quad \text{iff} \quad \exists\, a_k \in \mathbf{Z}, f(x) = \sum_{k=0}^{n} a_k \binom{x}{k} \prod_p p^{[k/p]}$$

where p always denotes primes.

To state our results we need some standard notation: for each prime ideal $\mathbf{P}$ of $\mathbf{R}$, the quotient field is finite, so we write

$$\mathbf{R}/\mathbf{P} = GF[N], \qquad N = \operatorname{Norm} \mathbf{P} = p^f. \tag{1.2}$$

Since p is the rational prime in $\mathbf{P}$, there is a positive integer e such that

$$e = e_{\mathbf{P}} = \max\{\, s \mid p \in \mathbf{P}^s \,\}. \tag{1.3}$$

As we shall see, the real difficulties arise when $e \geq p$.

THEOREM 1. *Let* $\mathbf{K}$ *be an algebraic number field,* $\mathbf{R}$ *its ring of integers, and* $\mathbf{D}_n(\mathbf{R})$ *the set of polynomials* f *of degree at most* n*, such that* $f^{(k)}(\mathbf{R})$ *lies in* $\mathbf{R}$ *for all* k*. Let*

$$I_n = \{ \delta | \delta f \in \mathbf{R}[x], \forall f \in \mathbf{D}_n(\mathbf{R}) \}. \tag{1.4}$$

Then $\mathbf{I}_n$ *is an ideal of* $\mathbf{R}$*, contains* $n!$*, and hence there is an ideal* $\mathbf{A}_n$ *of* $\mathbf{R}$ *such that*

$$\mathbf{A}_n \mathbf{I}_n = n!\mathbf{R}. \tag{1.5}$$

There exists a sequence β_n *in* $\mathbf{R}$ *such that*

$$f \in \mathbf{D}_n \quad \textit{iff} \quad \exists\, a_k \in \mathbf{A}_k, 0 \leq k \leq n,$$

$$n!f(x) = a_0 + \sum_{k=1}^{n} a_k (x - \beta_0) \cdots (x - \beta_{k-1}).$$

Furthermore

$$\mathbf{I}_n = \prod_{\mathbf{P},\, \mathrm{Norm}\, \mathbf{P} \leq n} \mathbf{P}^{\psi_n(\mathbf{P})} \tag{1.6}$$

where

$$\psi_n(\mathbf{P}) \leq e_{\mathbf{P}} \sum_{k=1}^{\infty} \left[\frac{n}{p^k N} \right]. \tag{1.7}$$

If $e < p$*, then* (1.7) *holds with equality.*

REMARKS. At most finitely many $\mathbf{P}$ have $e \geq p$, since then p divides the discriminant of $\mathbf{K}$. Both the formula for $\psi_n(\mathbf{P})$ and the construction of the sequence β_n are greatly complicated by these few $\mathbf{P}$.

2. The local ring $\mathbf{R}_\mathbf{P}$. We denote by $\mathbf{R}_\mathbf{P}$, $\mathbf{U}_\mathbf{P}$ the ring of $\mathbf{P}$-adic integers in $\mathbf{K}$ and its group of units:

$$\mathbf{R}_\mathbf{P} = \{ \alpha/\beta | \alpha \in \mathbf{R}, \beta \in \mathbf{R}, \beta \notin \mathbf{P} \}$$

$$\mathbf{U}_\mathbf{P} = \{ \theta | \theta \in \mathbf{R}_\mathbf{P}, \theta^{-1} \in \mathbf{R}_\mathbf{P} \}.$$

Let π denote an element of $\mathbf{P}$ that is not in $\mathbf{P}^2$: with it we can write each nonzero element of $\mathbf{K}$ in the form $\pi^\nu \theta$ with a uniquely determined integer ν and a unit θ. This exponent is the same for all choices of π: it is the *additive valuation*, defined as

$$\mathrm{ord}_\mathbf{P} \alpha = \max \{ \nu | \alpha \in \mathbf{P}^\nu \mathbf{R}_\mathbf{P} = \pi^\nu \mathbf{R}_\mathbf{P} \}. \tag{2.1}$$

In particular, $\operatorname{ord}_{\mathbf{P}} 0 = \infty$. We frequently use the properties:

$$\operatorname{ord}_{\mathbf{P}} \alpha\beta = \operatorname{ord}_{\mathbf{P}} \alpha + \operatorname{ord}_{\mathbf{P}} \beta \tag{2.2}$$

$$\operatorname{ord}_{\mathbf{P}}(\alpha + \beta) \geq \min(\operatorname{ord}_{\mathbf{P}} \alpha, \operatorname{ord}_{\mathbf{P}} \beta) \tag{2.3}$$

with equality if $\operatorname{ord}_{\mathbf{P}} \alpha \neq \operatorname{ord}_{\mathbf{P}} \beta$. Since e is the exact power of $\mathbf{P}$ dividing p, we have for all m in $\mathbf{Z}$:

$$\operatorname{ord}_{\mathbf{P}} m = e_{\mathbf{P}} \operatorname{ord}_p m \tag{2.4}$$

where $\operatorname{ord}_p m$ is the exact power of p dividing m. Since we are concerned with how highly divisible the values of a polynomial and all its derivatives can be, we define a $\mathbf{P}$ valuation on polynomials: for nonzero f in $\mathbf{K}[x]$

$$\operatorname{ord}_{\mathbf{P}} f(x) = \min\{\operatorname{ord}_{\mathbf{P}} f^{(k)}(\alpha), \forall\, \alpha \in R, \forall\, k \geq 0\}. \tag{2.5}$$

This minimum does exist: there is a δ in $\mathbf{R}$ such that $\delta f(x) \in \mathbf{R}[x]$, $\delta \neq 0$, so $\operatorname{ord}_{\mathbf{P}} f(x) \geq -\operatorname{ord}_{\mathbf{P}} \delta$. By Leibnitz' rule,

$$(fg)^{(m)} = \sum_{k=0}^{m} \binom{m}{k} f^{(k)} g^{(m-k)}$$

we have an analog of (2.2):

$$\operatorname{ord}_{\mathbf{P}} f(x)g(x) \geq \operatorname{ord}_{\mathbf{P}} f(x) + \operatorname{ord}_{\mathbf{P}} g(x). \tag{2.6}$$

The analog of (2.3) holds unchanged:

$$\operatorname{ord}_{\mathbf{P}}(f(x) + g(x)) \geq \min(\operatorname{ord}_{\mathbf{P}} f(x), \operatorname{ord}_{\mathbf{P}} g(x)) \tag{2.7}$$

with equality if $\operatorname{ord}_{\mathbf{P}} f \neq \operatorname{ord}_{\mathbf{P}} g$.

LEMMA 2.1. *If $f(x)$ is in $\mathbf{R}_{\mathbf{P}}[x]$ and some coefficient is a unit, then*

$$\operatorname{ord}_{\mathbf{P}} f(x) \leq e_P \sum_{k=1}^{\infty} \left[\frac{\deg f}{p^k N} \right]. \tag{2.8}$$

Proof. Let $\alpha_0, \ldots, \alpha_{N-1}$ be elements of $\mathbf{R}$ forming a complete set of residues mod $\mathbf{P}$:

$$\{\bar{\alpha}_0, \ldots, \bar{\alpha}_{N-1}\} = \mathbf{R}/\mathbf{P} = \mathbf{R}_{\mathbf{P}}/\mathbf{P}\mathbf{R}_{\mathbf{P}} = \bar{\mathbf{R}}$$

the bar denoting the image under the mod $\mathbf{P}$ mapping. There is nothing to prove if $\operatorname{ord} f \leq 0$, so we may assume that $\operatorname{ord}_{\mathbf{P}} f > 0$ and hence $f^{(k)}(\alpha)$ lies in $\mathbf{P}\mathbf{R}_{\mathbf{P}}$ for all $k \geq 0$, all α in $\mathbf{R}$. Therefore, in $\bar{\mathbf{R}}[x]$

$$\bar{f}(x) = (x - \bar{\alpha}_0)^{s_0} \cdots (x - \bar{\alpha}_{N-1})^{s_{N-1}} \bar{h}(x)$$

say, where each $s_i > 0$ and $\bar{h}(x)$ has no roots in $\bar{\mathbf{R}}$. Since $\deg \bar{f}$ is at most $\deg f$, we have

$$\min s_i \leq [(\deg f)/N].$$

Let $h(x)$ be in $\mathbf{R}_{\mathbf{P}}[x]$ such that $\bar{h}$ is its mod $\mathbf{P}$ image: then

$$f(x) = (x - \alpha_0)^{s_0} \cdots (x - \alpha_{N-1})^{s_{N-1}} h(x) + \pi j(x)$$

where $j(x) \in \mathbf{R}_{\mathbf{P}}[x]$ and $h(\alpha) \in U_P$ for all α in $\mathbf{R}$. Hence

$$f^{(s_i)}(\alpha_i) = s_i! h(\alpha_i) \prod_{k \neq i} (\alpha_i - \alpha_k)^{s_k} + \pi s_i! j^{(s_i)}(\alpha_i)/s_i!.$$

Now both $h(\alpha_i)$ and the factors $\alpha_i - \alpha_k$ are units, and $j^{(s_i)}(\alpha_i)/s_i!$ lies in $\mathbf{R}_{\mathbf{P}}$ because $j^{(s)}(x)/s! \in \mathbf{R}_{\mathbf{P}}[x]$. Hence

$$\operatorname{ord}_{\mathbf{P}} f^{(s_i)}(\alpha_i) = \operatorname{ord}_{\mathbf{P}} s_i!$$

and thus, using the i minimizing s_i, we deduce that

$$\operatorname{ord}_{\mathbf{P}} f(x) \leq \min_i \operatorname{ord}_{\mathbf{P}} s_i! \leq e_{\mathbf{P}} \operatorname{ord}_p([(\deg f)/N]!).$$

The proof is complete, since $\operatorname{ord}_p[x]! = [x/p] + [x/p^2] + \cdots$.

LEMMA 2.2. *Let* $\beta_{i+kN} = \alpha_i$, *for* $i = 0, \ldots, N-1$, *all* $k \geq 0$, *where* α_i, $i = 0, \ldots, N-1$ *is a complete set of residues* mod $\mathbf{P}$ *in* $\mathbf{R}$. *Set* $f_n = (x - \beta_0) \cdots (x - \beta_{n-1})$ *and* $f_0(x) = 1$. *If* $e_{\mathbf{P}} < p$ *then*

$$\operatorname{ord}_{\mathbf{P}} f_n(x) = e_{\mathbf{P}} \operatorname{ord}_p([n/N]!).$$

Proof. If $n = i + kN$, $k = [n/N]$, then

$$f_n = (x - \alpha_0)^{\nu_0} \cdots (x - \alpha_{N-1})^{\nu_{N-1}}$$

where $\nu_j = k + 1$ if $j < i$, but $\nu_j = k$ if $i \leq j$. Using the formula

$$f_n^{(l)}(\xi) = \sum_{l_0 + \cdots + l_{N-1} = l} \binom{l}{l_0, \ldots, l_{N-1}} \times \left\{ \left((x - \alpha_0)^{\nu_0} \right)^{(l_0)} \cdots \left((x - \alpha_{N-1})^{\nu_{N-1}} \right)^{(l_{N-1})} \right\}_{x=\xi}$$

we shall show that, for ξ in $\mathbf{R}$, each summand has $\operatorname{ord}_{\mathbf{P}} \geq e_{\mathbf{P}} \operatorname{ord}_p k!$, and that equality holds when $l = k$ and $\xi = \beta_n$. For any summand, consider the factor for which $\xi \equiv \alpha_j \bmod \mathbf{P}$. If $\xi = \alpha_j$ then that factor contributes either infinity or $\operatorname{ord}_{\mathbf{P}} \nu_j!$, which is at least $\operatorname{ord}_{\mathbf{P}} k!$. There remain the cases with $1 \leq \operatorname{ord}_{\mathbf{P}}(\xi - \alpha) < \infty$ and $l \leq \nu$:

$$\operatorname{ord}_{\mathbf{P}} \left[\left((x - \alpha)^{\nu} \right)^{(l)} \right]_{x=\xi} = \operatorname{ord}_{\mathbf{P}} \frac{\nu!}{(\nu - l)!} (\xi - \alpha)^{\nu - l}$$

$$= \operatorname{ord}_{\mathbf{P}} \nu! + \{ (\nu - l) \operatorname{ord}_{\mathbf{P}}(\xi - \alpha) - \operatorname{ord}_{\mathbf{P}}(\nu - l)! \}.$$

Here v is fixed and $0 \le l \le v$: so we are to minimize $\lambda m - e \operatorname{ord}_p m!$ over the range $0 \le m \le v$, where $\lambda = \operatorname{ord}_{\mathbf{P}}(\xi - \alpha)$ and so $\lambda \ge 1$. Using the hypothesis that $e \le p - 1$, we have

$$\begin{aligned}\lambda m - e \operatorname{ord}_p m! &\ge m - e \operatorname{ord}_p m! \\ &\ge m - (p-1)\left([m/p] + [m/p^2] + \cdots\right) \\ &\ge m - (p-1)(m/p + m/p^2 + \cdots) \ge 0.\end{aligned}$$

Hence $\operatorname{ord}_{\mathbf{P}} f_n^{(l)}(\xi) \ge \operatorname{ord}_{\mathbf{P}} v_j! \ge \operatorname{ord}_{\mathbf{P}} k! = e_{\mathbf{P}} \operatorname{ord}_p [n/N]!$. This shows that $\operatorname{ord}_{\mathbf{P}} f_n(x) \ge e_{\mathbf{P}} \operatorname{ord}_p [n/N]!$. To show that equality holds, it is not necessary to apply Lemma 2.1, because

$$\operatorname{ord}_{\mathbf{P}} f_n^{(k)}(\beta_n) = \operatorname{ord}_{\mathbf{P}}\left(\prod_{j \ne i} (\alpha_i - \alpha_j)^{v_j}\right) k! = e_{\mathbf{P}} \operatorname{ord}_p k!.$$

We have constructed monic polynomials for each degree that maximize $\operatorname{ord}_{\mathbf{P}}$, but only when $e_{\mathbf{P}} < p$. We cannot yet prove Theorem 1 constructively. Applying (2.8) to monic polynomials in $\mathbf{R}[x]$, we know there exists for each degree n a monic polynomial in $\mathbf{R}[x]$ of that degree and of largest possible $\operatorname{ord}_{\mathbf{P}}$ among such $f(x)$: x^n will do for $n < pN$.

LEMMA 2.3. *For each n, let f_n denote a a monic polynomial of degree n in $\mathbf{R}[x]$ and of maximum $\operatorname{ord}_{\mathbf{P}}$ among such monic polynomials. If $f \in \mathbf{R}_{\mathbf{P}}[x]$, $\deg f = n$, and if $\operatorname{ord}_{\mathbf{P}} f > \operatorname{ord}_{\mathbf{P}} f_n$, then $f \in \mathbf{PR}_{\mathbf{P}}[x]$.*

Proof. Since $\operatorname{ord}_{\mathbf{P}} f_n \ge \operatorname{ord}_{\mathbf{P}} x f_{n-1} \ge \operatorname{ord}_{\mathbf{P}} f_{n-1}$, we know that $\operatorname{ord}_{\mathbf{P}} f_n$ increases with n. We need this for induction. By (2.8), $\operatorname{ord}_{\mathbf{P}} f = 0$ for degree $n < pN$ unless all coefficients lie in $\mathbf{PR}_{\mathbf{P}}$: so induction can start. Since the f_k are monic, we can write $f(x) = a_0 f_0 + \cdots + a_n f_n$ with coefficients a_i from $\mathbf{R}_{\mathbf{P}}$. We assert that if $\operatorname{ord}_{\mathbf{P}} f > \operatorname{ord}_{\mathbf{P}} f_n$, then $\operatorname{ord}_{\mathbf{P}} a_n > 0$. Assume that on the contrary a_n is a unit. There exists a δ in $\mathbf{R}$, not in $\mathbf{P}$, such that $\delta f(x) \in \mathbf{R}[x]$, and hence δa_n is a unit. Choosing a large enough integer M so that $M > \operatorname{ord}_{\mathbf{P}} f$, there exists θ in $\mathbf{R}$ such that $\theta \delta a_n \equiv 1 \bmod \mathbf{P}^M$. Hence the polynomial obtained from $\theta \delta f(x)$ by replacing the coefficient of x^n by 1 is of degree n, over $\mathbf{R}$, monic, but of the same $\operatorname{ord}_{\mathbf{P}}$ as f. This is a contradiction, since such polynomials have ord at most that of f_n. Knowing thar ord $a_n > 0$, we can apply the induction hypothesis to $f - a_n f_n$: it has smaller degree than n but its $\operatorname{ord}_{\mathbf{P}}$ exceeds $\operatorname{ord}_{\mathbf{P}} f_n$ and hence exceeds $\operatorname{ord}_{\mathbf{P}} f_{n-1}$. All the coefficients of $f - a_n f_n$ must lie in $\mathbf{PR}_{\mathbf{P}}$, so the same holds for f.

COROLLARY. *Let f_n be as in Lemma* 2.3: *if $f \in \mathbf{R}_{\mathbf{P}}[x]$, $\deg f = n$, and if $\operatorname{ord}_{\mathbf{P}} f - \operatorname{ord}_{\mathbf{P}} f_n = k > 0$, then $f \in \mathbf{P}^k \mathbf{R}_{\mathbf{P}}[x]$.*

Proof. Since $\mathbf{P}\mathbf{R}_{\mathbf{P}} = \pi\mathbf{R}_{\mathbf{P}}$, we know from the hypothesis and Lemma 2.3 that $f = \pi f_1$, with f_1 in $\mathbf{R}_{\mathbf{P}}[x]$. But then $\operatorname{ord} f_1 = \operatorname{ord} f - 1$, so an induction process works.

REMARK. We can express Lemma 2.3 as saying that, among all f in $\mathbf{R}_{\mathbf{P}}[x]$ of degree n and with some coefficient a unit, there is at least one of largest $\operatorname{ord}_{\mathbf{P}}$ and it can be taken to lie in $\mathbf{R}[x]$ and be monic.

3. Proof of Theorem 1. Let $\psi_n(\mathbf{P})$ denote $\max \operatorname{ord}_{\mathbf{P}} f$, taken over all f of degree n in $\mathbf{R}_{\mathbf{P}}[x]$ with some coefficient a unit. We've seen that this is the same as the maximum taken over all monic f of degree n in $\mathbf{R}[x]$. Let f_n be such a polynomial, as in Lemma 2.3, so

$$\operatorname{ord}_{\mathbf{P}} f_n(x) = \psi_n(\mathbf{P}). \tag{3.1}$$

Let $H_n(x)$ denote a monic polynomial in $\mathbf{R}[x\mathrm{c}]$ and of degree n, such that

$$H_n(x) \equiv f_n(x) \qquad (\operatorname{mod} \mathbf{P}^{\psi_n(\mathbf{P})}) \tag{3.2}$$

for all prime ideals $\mathbf{P}$ and associated polynomials $f_n = f_{n,\mathbf{P}}$. By Lemma 2.1, only the primes p with $pN \leq n$ can give an actual constraint (3.2) on H_n for the finite number of primes $\mathbf{P}$ dividing p. By the Chinese Remainder Theorem, H_n therefore exists. Define the ideal $\mathbf{J}_n$ as the product

$$\mathbf{J}_n = \prod \mathbf{P}^{\psi_n(\mathbf{P})}. \tag{3.3}$$

We know by Lemma 2.1 that (1.7) holds, so the product in (3.3) is finite. Ultimately we must show that $\mathbf{J}_n$ is the same as the $\mathbf{I}_n$ of (1.4). The crucial step is to show that

$$\sum_{k=0}^{n} b_k H_k(x) \in \mathbf{D}_n(\mathbf{R}) \quad \text{iff all } b_k H_k \in \mathbf{D}_n \quad \text{iff all } b_k \mathbf{J}_k \subseteq \mathbf{R}. \tag{3.4}$$

For $j = 0, 1, 2, \ldots$ and all α in $\mathbf{R}$, $H_k^{(j)}(\alpha) \in \mathbf{J}_k$: so if $b_k \mathbf{J}_k \subseteq \mathbf{R}$ then $b_k \mathbf{H}_k \in \mathbf{D}^{\infty}(\mathbf{R})$. It remains to show that if the sum f in (3.4) lies in $\mathbf{D}_n$, then each $b_k \mathbf{J}_k$ is in $\mathbf{R}$. We use induction on the degree n of f. Choose an integer m so that $m > \operatorname{ord}_P H_n$ and also such that $\pi^m f \in \mathbf{R}_{\mathbf{P}}[x]$. Now $\operatorname{ord}_{\mathbf{P}} f \geq 0$, so $\operatorname{ord}_{\mathbf{P}} \pi^m f \geq m$ and hence by Corollary 2.3:

$$\operatorname{ord}_{\mathbf{P}} \pi^m b_n \geq m - \operatorname{ord}_{\mathbf{P}} H_n.$$

Thus $\operatorname{ord}_{\mathbf{P}} b_n H_n \geq 0$ for all $\mathbf{P}$, so $b_n H_n \in \mathbf{D}_n$. Hence $f - b_n H_n \in \mathbf{D}_{n-1}$ and so induction works, the case $n = 0$ being trivial. Now $\operatorname{ord}_{\mathbf{P}} b_k \geq -\psi_k(\mathbf{P})$ for all $\mathbf{P}$, as $b_k H_k \subseteq \mathbf{D}_k$, hence $b_k \mathbf{J}_k \subseteq \mathbf{R}$.

We now show that $\mathbf{I}_n = \mathbf{J}_n$. By (1.4), $\mathbf{I}_n$ contains $n!$, and the sequence $\mathbf{I}_n$ is a descending chain of ideals of $\mathbf{R}$. We now apply (3.4): $\delta \in \mathbf{I}_n$ iff

$\delta \mathbf{D}_n \subseteq R[x]$, that is to say, whenever $b_k \mathbf{J}_k \in \mathbf{R}$ for all $k \leq n$, then $b_k \delta \in \mathbf{R}$ for all $k \leq n$. In other words, if $b_k \in \mathbf{J}_k^{-1}$ for $k \leq n$, then $b_k \delta \in \mathbf{R}$ for $k \leq n$. This is equivalent to δ lying in J_n. Finally, since $\mathbf{I}_n$ divides $n!$, there is an ideal $\mathbf{A}_n$ of $\mathbf{R}$ such that $\mathbf{A}_n \mathbf{I}_n = n!\mathbf{R}$.

With Lemmas 2.1, 2.2 and assertion (3.4), this concludes the proof of Theorem 1, except for expressing H_n as $(x - \beta_0) \cdots (x - \beta_{n-1})$. The existence of β is derived from that of the H_n of (3.2). We start with $H_0 = 1$, $H_1(x) = x$, so $\beta_0 = 0$. Inductively, if we have already modified H_k for $k \leq n$, so $H_n = (x - \beta_0) \cdots (x - \beta_{n-1})$, divide H_{n+1} by H_n, say

$$H_{n+1}(x) = (x - \beta) H_n(x) + \gamma$$

where β and γ lie in $\mathbf{R}$. Since $\gamma = H_{n+1}(\beta) \in I_{n+1}$, we can replace H_{n+1} by $H_n(x)(x - \beta)$, as claimed.

We saw in Lemma 2.2 a simple description of the corresponding local sequence $\beta(\mathbf{P})$, when $e < p$. The $\beta(\mathbf{P})$ for any exceptional $\mathbf{P}$ are dealt with below, and then $\beta_0, \ldots, \beta_n$ can be constructed by

$$\beta_t \equiv \beta_t(\mathbf{P}) \mod \mathbf{P}^{\psi_n(\mathbf{P})}$$

for each $\mathbf{P}$ of norm $N \leq n$.

4. The exceptional primes. We continue with the same notation.

THEOREM 2. *Let $\beta_n \in \mathbf{R}$ for all $n \geq 0$. Define*

$$g_n = \#\{ i | 0 \leq i < n, \beta_i = \beta_n \}. \tag{4.1}$$

Let $f_0(x) = 1, f_n(x) = (x - \beta_{n-1}) f_{n-1}(x)$ for $n \geq 1$. If for a prime ideal $\mathbf{P}$ of $\mathbf{R}$ there is a sequence β_n such that

$$\operatorname{ord}_{\mathbf{P}} f_n(x) = \operatorname{ord}_{\mathbf{P}} f_n^{(g_n)}(\beta_n) \tag{4.2}$$

for all n, then for all a_t in $\mathbf{K}$

$$\operatorname{ord}_{\mathbf{P}} \sum_{i=0}^{n} a_i f_i(x) = \operatorname{Min}\{ \operatorname{ord}_{\mathbf{P}} a_i f_i(x) | i = 0, 1, \ldots, n \} \tag{4.3}$$

and

$$\operatorname{ord}_{\mathbf{P}} f_n(x) = \psi_n(\mathbf{P}). \tag{4.4}$$

Proof. By (2.7) we can prove (4.3) by showing that

$$\operatorname{ord}_{\mathbf{P}}(a_0 f_0 + \cdots + a_n f_n) \leq \operatorname{Min} \operatorname{ord}_{\mathbf{P}} a_i f_i.$$

We do this by showing for each r, $0 \leq r \leq n$, that if

$$\operatorname{ord}_{\mathbf{P}}(a_r f_r + \cdots + a_n f_n) \geq a$$

then $\operatorname{ord}_{\mathbf{P}} a_i f_i \geq a$ for $i = r,\ldots,n$. This is trivial for $r = n$, so the proof will proceed by *downward* induction on r. Suppose it is proved down to $r > 0$, and assume that $\operatorname{ord}_{\mathbf{P}}(a_{r-1}f_{r-1} + \cdots + a_n f_n) \geq a$. Since $x - \beta_{r-1}$ divides f_{r-1} to multiplicity g_{r-1} but divides all higher f_k to a greater multiplicity, it follows that

$$\operatorname{ord}_{\mathbf{P}} a_{r-1} f_{r-1}^{(g_{r-1})}(\beta_{r-1}) \geq a.$$

Hence $\operatorname{ord}_{\mathbf{P}} a_{r-1}f_{r-1} \geq a$, by hypothesis (4.2), so we can subtract this term and deduce that $\operatorname{ord}_{\mathbf{P}}(a_r f_r + \cdots + a_n f_n) \geq a$, to which induction applies. To prove (4.4) we must show that if f is of degree n in $\mathbf{R}[x]$, not all of its coefficients in $\mathbf{P}$, then $\operatorname{ord}_{\mathbf{P}} f \leq \operatorname{ord}_{\mathbf{P}} f_n$. We can write f as $f = a_0 f_0 + \cdots + a_n f_n$, where all a_i lie in $\mathbf{R}$ but at least one is outside $\mathbf{P}$, say a_{i_0}:

$$\operatorname{ord}_{\mathbf{P}} f = \operatorname{Min} \operatorname{ord}_{\mathbf{P}} a_i f_i \leq \operatorname{ord}_{\mathbf{P}} a_{i_0} f_{i_0} = \operatorname{ord}_{\mathbf{P}} f_{i_0} \leq \operatorname{ord}_{\mathbf{P}} f_n.$$

LEMMA 4.1. *Let e, p be integers such that $e \geq p > 1$. Define*

$$\lambda_0 = 0, \lambda_k = \left[e \sum_{r=1}^{k} p^{-r} \right] \quad \text{for } k \geq 1. \tag{4.5}$$

Then there is a positive integer s such that

$$\lambda_0 < \lambda_1 < \cdots < \lambda_s = \lambda_{s+1} = \cdots = \max\{ m | m < e/(p-1) \}. \tag{4.6}$$

Proof. There is a positive integer k such that $p^k \leq e < p^{k+1}$: hence $1 \leq e/p^j$ for $j \leq k$, so $\lambda_0 < \lambda_1 < \cdots < \lambda_k$. Since all $\lambda_j < e/(p-1)$, it is enough to show that λ_{k+1} is the largest integer below $e/(p-1)$. We need only show that there is no integer in the range

$$e(p^{-1} + \cdots + p^{-k-1}) < m < e/(p-1),$$

which is equivalent to $e(p^{k+1} - 1) < mp^{k+1}(p-1) < ep^{k+1}$. Now $p^{k+1} > e$, so $e(p^{k+1} - 1) > (e-1)p^{k+1}$, and hence m would have to satisfy $(e-1)p^{k+1} < mp^{k+1}(p-1) < ep^{k+1}$. This would require that $e - 1 < m(p-1) < e$, impossible for integers m, e, p.

We shall use the notation $\langle x \rangle$ for $\max\{ m | m < x \}$: of course

$$\langle x \rangle = -[-x] - 1. \tag{4.7}$$

LEMMA 4.2. *Let p be a prime, e an integer, $e \geq p$, λ an integer. Define λ_k as in* (4.5), *so s is the least integer with*

$$\lambda_s = \langle e/(p-1) \rangle. \tag{4.8}$$

Then $\min\{ \lambda k - e \operatorname{ord}_p k! | 0 \leq k \leq m \}$ *occurs at* $k = [m/p^t]p^t$ *if* $\lambda_{t-1} < \lambda \leq \lambda_t$ *for some t on* $[2, s]$, *or if* $0 \leq \lambda \leq \lambda_1$ *for* $t = 1$. *The minimum occurs at* $k = 0$ *if* $\lambda > \lambda_s$.

Proof. We show first that if $\lambda \le \lambda_t$ and k is restricted to multiples of p^t, then the minimum occurs for largest possible k:

$$\begin{aligned}\lambda(b+1)p^t - e\,\mathrm{ord}_p((b+1)p^t)! - \lambda bp^t + e\,\mathrm{ord}_p(bp^t)! \\ = \lambda p^t - e\,\mathrm{ord}_p\{(bp^t+1)(bp^t+2)\cdots(bp^t+p^t)\} \\ \le \lambda p^t - e\,\mathrm{ord}_p p^t! \le \lambda_t p^t - e(1+p+\cdots+p^{t-1}) \le 0.\end{aligned}$$

It remains to show that, for appropriate λ, the values of $\lambda k - e\,\mathrm{ord}_p k!$ on the range $bp^t < k < (b+1)p^t$ are no less than the value at $k = bp^t$. Set $k = bp^t + j$, where $0 < j < p^t$:

$$\begin{aligned}&\lambda(bp^t+j) - e\,\mathrm{ord}_p(bp^t+j)! - \lambda bp^t + e\,\mathrm{ord}_p(bp^t)! \\ &\quad = \lambda j - e\,\mathrm{ord}_p\{(bp^t+1)\cdots(bp^t+j)\} = \lambda j - e\,\mathrm{ord}_p j! \\ &\quad \ge \begin{cases}\lambda j \ge 0 & \text{if } t = 1 \text{ and } \lambda \ge 0, \\ \lambda j - e(j/p + \cdots + j/p^{t-1}) > 0 & \text{if } \lambda \text{ integral and } \lambda > \lambda_{t-1}.\end{cases}\end{aligned}$$

Finally, if λ is integral and $\lambda > \lambda_s$, then $\lambda \ge e/(p-1)$:

$$\lambda k - e\,\mathrm{ord}_p k! \ge \frac{ek}{p-1} - e\sum_1^\infty \frac{k}{p^j} = 0$$

and this is the value at $k = 0$.

COROLLARY. *Let ξ and α be distinct elements of* $\mathbf{R}$, *and let* $\lambda = \mathrm{ord}_{\mathbf{P}}(\xi - \alpha)$. *Then*

$$\min\left\{ \mathrm{ord}_{\mathbf{P}}((x-\alpha)^m)^{(j)}_{x=\xi} \middle| 0 \le j \le m \right\}$$

is achieved at $j = 0$ if p^t divides m and $\lambda \le \lambda_t$ for some $t \le s$. But if $\lambda > \lambda_s$, or if $\lambda > \lambda_t$ and $m < p^{t+1}$ for some $t < s$, then the minimum is realized at $j = m$.

Proof. We are to minimize $e\,\mathrm{ord}_p m! + \lambda(m-j) - e\,\mathrm{ord}_p(m-j)!$ over j, $0 \le j \le m$, so Lemma 4.2 applies with $k = m - j$.

We come now to the construction of β_m and the proof that it satisfies condition (4.2) of Theorem 2. As before, let π denote an element of $\mathbf{P}$ outside $\mathbf{P}^2$, and let $\alpha_0, \ldots, \alpha_{N-1}$ be a complete set of representatives in $\mathbf{R}$ for $\mathbf{R}/\mathbf{P}$. Polya [2] constructed a complete set of residues mod $\mathbf{P}^k$ for each k, as follows. For each $n \ge 0$ expand N-adically:

$$n = a_0 + a_1 N + a_2 N^2 + \cdots + a_r N^r, \qquad 0 \le a_i < N, \text{ all } i \tag{4.9}$$

and then use these "digits" to define α_n for all $n \geq 0$ by

$$\alpha_n = \alpha_{a_0} + \pi\alpha_{a_1} + \cdots + \pi^r\alpha_{a_r}. \tag{4.10}$$

It is easy to show that $\alpha_m \equiv \alpha_n \bmod \mathbf{P}^j$ iff $m \equiv n \bmod N^j$, hence $\{\alpha_i | i = 0,\ldots,N^k - 1\}$ is a complete set of residues mod $\mathbf{P}^k$. Taking the liberty of using $\operatorname{ord}_N m$ to denote the highest exponent to which N divides m, we can write and shall frequently use:

$$\operatorname{ord}_{\mathbf{P}}(\alpha_m - \alpha_n) = \operatorname{ord}_N(m - n). \tag{4.11}$$

To define β_n for fixed $\mathbf{P}$, we need to expand n in "decimal" notation relative to the sequence

$$N,\quad pN^{1+\lambda_0},\quad pN^{1+\lambda_1},\quad p^2N^{1+\lambda_1},\quad p^2N^{1+\lambda_2},\ldots,p^sN^{1+\lambda_{s-1}},\quad p^sN^{1+\lambda_s}$$

where p, N are as in (1.2), e is the ramification index of (1.3), and $\lambda_0,\ldots,\lambda_s$ are as defined in Lemma 4.1. The expansion is the usual one relative to a sequence of positive integers where each divides the next. Because of the alternating pattern of ratios of consecutive terms, we call the "digits" $a_0, b_0,\ldots,a_s, b_s$:

$$n = a_0 + b_0N + \sum_{i=1}^{s}\left(a_ip^iN^{1+\lambda_{i-1}} + b_ip^iN^{1+\lambda_i}\right) \tag{4.12}$$

$$0 \leq a_0 < N, \quad \text{and} \quad 0 \leq a_i < N^{\lambda_i - \lambda_{i-1}}, \qquad 1 \leq i \leq s \tag{4.13}$$

$$0 \leq b_i < p, \quad \text{for } i < s, \qquad \text{and} \qquad b_s = \left[n/\left(p^sN^{1+\lambda_s}\right)\right]. \tag{4.14}$$

These digits will be called $a_i(n)$ and $b_i(n)$: they are uniquely determined by n and P. We use boldface $\mathbf{a}(n)$, $\mathbf{b}(n)$ for the corresponding vectors. Our concern is the exceptional primes, but we observe that if $e < p$ then $n = a_0 + b_0N$. Note that a_0 runs over $[0, N)$, $a_0 + b_0N$ over $[0, pN)$, and so on, until finally

$$a_0 + b_0N + \cdots + b_{s-1}p^{s-1}N^{1+\lambda_{s-1}} + a_sp^sN^{1+\lambda_{s-1}}$$

runs over the range $\left[0, p^sN^{1+\lambda_s}\right)$. Now use $\mathbf{a}(n)$ to define

$$n^* = a_0 + a_1N + a_2N^{1+\lambda_1} + \cdots + a_sN^{1+\lambda_{s-1}}. \tag{4.15}$$

Note that (4.15) is the expansion of n^* relative to the sequence

$$N, N^{1+\lambda_1},\ldots,N^{1+\lambda_{s-1}}$$

so conversely each n^* on $\left[0, N^{1+\lambda_s}\right)$ determines a unique $\mathbf{a}(n)$ that satisfies (4.15). We now define (for each $\mathbf{P}$):

$$\beta_n = \alpha_{n^*} \tag{4.16}$$

where $\boldsymbol{\alpha}$ is the sequence defined in (4.10). If $m \equiv n \bmod p^s N^{1+\lambda_s}$ then m and n have the same digits except for b_s, so $m^* = n^*$, thus $\beta_m = \beta_n$. Hence $\boldsymbol{\beta}$ has period $p^s N^{1+\lambda_s}$.

LEMMA 4.3. *Let S denote the set of integers $[0, N^{1+\lambda_s})$. With the notation of* (4.12), *define for each positive integer n:*

$$U_s^* = \{ m | m \in S, a_s(m) > a_s(n) \},$$

$$L_s^* = \{ m | m \in S, a_s(m) < a_s(n) \},$$

$$U_t^* = \{ m | m \in S, a_i(m) = a_i(n), t < i \le s, a_t(m) > a_t(n) \},$$

$$L_t^* = \{ m | m \in S, a_i(m) = a_i(n), t < i \le s, a_t(m) < a_t(n) \},$$

for $0 \le t < s$, and $E^* = \{ m | m \in S, \mathbf{a}(m) = \mathbf{a}(n) \}$. Together, these sets partition S, though some U or L may be empty. Let U_k, L_k, E denote the corresponding sets in which the condition "$m \in S$" is replaced by "$0 \le m < n$". Together, these sets partition $[0, n)$, though some U, L or E may be empty. Under the mapping $m \to m^*$, defined in (4.12), (4.15): *if U_k^* is not empty then each element is the image of exactly $b_k(n)p^k + \cdots + b_s(n)p^s$ elements of U_k; if L_k^* is not empty then each of its elements is the image of exactly $p^k + b_k(n)p^k + \cdots + b_s(n)p^s$ elements of L_k; and each element of E^* is the image of exactly $b_0(n) + b_1(n)p + \cdots + b_s(n)p^s$ elements of E.*

Proof. Each m in S determines a unique $\mathbf{a}(m)$ as in (4.15). Suppose $m \in U_s^*$: $a_s(m) > a_s(n)$: then $h^* = m$ iff $0 \le h < n$ and $\mathbf{a}(h) = \mathbf{a}(m)$, and $h < n$ iff $b_s(h) < b_s(n)$, so there are exactly $b_s p^s$ choices for $\mathbf{b}(h)$ and so for h. For L_s, where $a_s(m) < a_s(n)$, $m < n$ iff $b_s(m) \le b_s(n)$, so the number of choices is $(1 + b_s(n))p^s$. Consider the h in U_t with $h^* = m$: there are $b_s(n)p^s$ choices with $b_s(h) < b_s(n)$ and the other b on $[0, p)$; $b_{s-1}p^{s-1}$ choices with $b_s(h) = b_s(n)$ and $b_{s-1}(h) < b_{s-1}(n)$; and so on, down to $b_t(n)p^t$ choices with $b_j(h) = b_j(n)$ for $t < j \le s$ and $b_t(h) < b_t(n)$. There is a similar calculation for L_t: the extra p^t comes from the cases where $b_j(h) = b_j(n)$, $t \le j \le s$. The calculations for E are similar to those for U_0. Note that we have found the formula for g_n of (4.1), the number of times α_{n^*} occurs in $\boldsymbol{\beta}$ before β_n:

$$g_n = b_0(n) + b_1(n)p + \cdots + b_s(n)p^s. \tag{4.17}$$

Hence in f_n the factor $x - \alpha_{n^*}$ occurs to exponent g_n, whereas the exponent to which $x - \alpha_{m^*}$ occurs is $b_t(n)p^t + \cdots + b_s(n)p^s$ for $m^* \in U_t^*$, is $p^t + b_t(n)p^t + \cdots + b_s(n)p^s$ for $m^* \in L_t^*$, for $0 \le t \le s$. We shall regroup these factors by their exponents. All have $b_s p^s$ in the exponent, so the first group is all m^*, all of S. All except U_s^* and L_s^*

include $b_{s-1}(n)p^{s-1}$ in their exponent, so this group is all m^* with $a_s(m) = a_s(n)$. Similarly, there is a term $b_t(n)p^t$ in the exponent just for those m^* with $a_t(m) = a_t(n)$ for $t < i \leq s$. Finally, there is the extra term p^t in the exponent just for the m^* in L_t^*. Hence

$$(4.18)\quad f_n(x) = \prod_{i=0}^{s} \prod_{m^* \in A_t} (x - \alpha_{m^*})^{b_t(n)p^t} \cdot \prod_{j=0}^{s} \prod_{m^* \in B_j} (x - \alpha_{m^*})^{p^j}$$

where

$$(4.19)\quad \begin{cases} A_s = \{ m^* | 0 \leq m^* < N^{1+\lambda_s} \}, \\ B_s = \{ m^* | m^* \in A_s, a_s(m) < a_s(n) \} \\ A_t = \{ m^* | m^* \in A_s, a_i(m) = a_i(n) \text{ for } t < i \leq s \} \\ B_t = \{ m^* | m^* \in A_t, a_t(m) < a_t(n) \}. \end{cases}$$

We count these sets:

$$(4.20)\quad \begin{cases} \#(A_t) = N^{1+\lambda_t}, & 0 \leq t \leq s, \\ \#(B_t) = a_t(n)N^{1+\lambda_{t-1}}, & 0 < t \leq s, \\ \#(B_0) = a_0(n). \end{cases}$$

As a check on our counting we note that the degree of the right side of (4.18) is $\sum p^j \#(B_j) + \sum b_t(n)p^i \#(A_i) = n$.

LEMMA 4.4. *For all* t, $0 \leq t \leq s$:

$$(4.21)\quad \operatorname{ord}_{\mathbf{P}} \prod_{m^* \in A_t} (x - \alpha_{m^*})^{b_t(n)p^t}$$

$$= e \operatorname{ord}_p(b_t p^t)! + b_t p^t \left(\sum_{j=1}^{\lambda_t} s N^j - \lambda_t \right) \quad (= 0 \text{ at } t = 0).$$

Moreover, this minimum ordinal is realized, for any k^* *in* A_t, *by differentiating away the* $x - \alpha_{k^*}$ *factors and then setting* $x = \alpha_{k^*}$.

Proof. If $b_t(n) = 0$, (4.21) holds trivially, so we may assume that $0 < b_t(n)$, and we also note that $b_t(n) < p$ if $t < s$. Consider the derivatives of the product in (4.21), and their ordinals at $x = \xi$, where $\xi \in R$. There is a unique k^* in A_s, such that

$$\xi \equiv \alpha_{k^*} \mod \mathbf{P}^{1+\lambda_s}.$$

Thus $\operatorname{ord}_{\mathbf{P}}(\xi - \alpha_{k^*}) \geq 1 + \lambda_s$, and for $m^* \neq k^*$:

$$(4.22)\quad \operatorname{ord}_{\mathbf{P}}(\xi - \alpha_{m^*}) = \operatorname{ord}_{\mathbf{P}}(\alpha_{k^*} - \alpha_{m^*}) = \operatorname{ord}_N(k^* - m^*).$$

By the Corollary to Lemma 4.2, with $\lambda = \operatorname{ord}_{\mathbf{P}}(\xi - \alpha_{m^*})$, if $m^* \in A_t$:

$$\operatorname*{Min}_j \operatorname{ord}_{\mathbf{P}}\left\{\left((x-\alpha_{m^*})^{b_t(n)p^t}\right)^{(j)}\right\}_{x=\xi} = \begin{cases} b_t(n)p^t\lambda & \text{if } \lambda \le \lambda_t \\ e\operatorname{ord}_p\left(b_t(n)p^t\right)! & \text{if } \lambda > \lambda_t \end{cases}$$

the minimum being reached at $j = 0$, $b_t p^t$ respectively. If $m^* \in A_t$: $\lambda > \lambda_t$ iff

$$m^* = k_t^* = a_0(k) + \sum_{i=1}^{t} a_i(k)N^{1+\lambda_{i-1}} + \sum_{i=t+1}^{s} a_i(n)N^{1+\lambda_{i-1}}.$$

At $t = s$ this is clear: A_s is a complete set of residues $\bmod \mathbf{P}^{1+\lambda_s}$, so $\operatorname{ord}_{\mathbf{P}}(\xi - \alpha_{m^*}) > \lambda_s$ iff $m^* = k^*$. For $t < s$: $m^* \in A_t$ iff $a_i(m) = a_i(n)$, $t < i \le s$, and so $\operatorname{ord}_N(k^* - m^*) > \lambda_t$ iff $a_i(m) = a_i(n)$ for $0 \le i \le t$. Note that $k_t^* = k^*$ whenever $k^* \in A_t$. By (2.6) we can now infer that the left side of (4.21) is no less than

$$e\operatorname{ord}_p\left(b_t(n)p^t\right)! + b_t(n)p^t \sum_{m^* \in A_t,\, m^* \ne k_t^*} \operatorname{ord}_N\left(k_t^* - m^*\right)$$

which is also the value obtained when we differentiate away the factors $(x - \alpha_{k_t^*})$, set $x = \alpha_{k_t^*}$ and apply $\operatorname{ord}_{\mathbf{P}}$. Here we have used the fact that $k^* \equiv k_t^* \bmod N^{1+\lambda_t}$, so that the terms with $\lambda \le \lambda_t$ have $\lambda = \operatorname{ord}_N(k^* - m^*) = \operatorname{ord}_N(k_t^* - m^*)$. We show the sum is the same for all k:

$$\sum_{m^* \in A_t,\, m^* \ne k_t^*} \operatorname{ord}_N\left(k_t^* - m^*\right) = \sum_{j=1}^{\lambda_t} N^j - \lambda_t. \tag{4.22}$$

This will then complete the proof of Lemma 4.4. As in deriving the classical formula for $\operatorname{ord}_p n!$, we note that an m^* contributes 1 for each j such that $m^* \equiv k_t^* \bmod N^j$. Since these ordinals are at most λ_t, it remains only to show that for $1 \le j \le \lambda_t$:

$$\#\left\{\, m^* \middle| m^* \in A_t,\, m^* \ne k_t^*,\, m^* \equiv k_t^* \bmod N^j \right\} = N^{1+\lambda_t - j} - 1.$$

Since k_t^* and m^* have the same digits beyond the tth, $k_t^* - m^*$ equals

$$\left(a_0(k) + \sum_{i=1}^{t} a_i(k)N^{1+\lambda_{i-1}}\right) - \left(a_0(m) + \sum_{i=1}^{t} a_i(m)N^{1+\lambda_{i-1}}\right).$$

The part of m^* here runs precisely over the range $[0, N^{1+\lambda_t})$, giving exactly $N^{1+\lambda_t - j}$ copies of $[0, N^j) \bmod N^j$ as required.

LEMMA 4.5. *For $t = 0, 1, \ldots, s$, if $a_t(n) \ne 0$, then B_t is non-empty, and*

$$\operatorname{ord}_{\mathbf{P}} \prod_{m^* \in B_t} (x - \alpha_{m^*})^{p^t} = p^t \sum_{j=1}^{\lambda_t} \left[a_t(n)N^{1+\lambda_{t-1}-j}\right] \tag{4.23}$$

$$(= 0 \text{ at } t = 0).$$

This minimum ordinal can be realized by setting $x = \alpha_{n^*}$.

Proof. As in Lemma 4.4, we consider ordinals of derivatives of the product in (4.23), evaluated at $x = \xi \equiv \alpha_{k^*} \bmod P^{1+\lambda_s}$. Set $\lambda = \operatorname{ord}_p(\xi - \alpha_{m^*})$: by Lemma 4.2, if m^* lies in B_t, then

$$\operatorname*{Min}_j \operatorname{ord}_{\mathbf{P}}\left\{\left((x-\alpha_{m^*})^{p^t}\right)^{(j)}\right\} = \begin{cases} p^t\lambda & \text{if } \lambda \le \lambda_t \\ e \operatorname{ord}_p(p^t!) & \text{if } \lambda > \lambda_t. \end{cases}$$

Now $m^* \in B_t$ iff

$$m^* = a_0(m) + \sum_{i=1}^{t} a_i(m) N^{1+\lambda_{i-1}} + \sum_{i=t+1}^{s} a_i(n) N^{1+\lambda_{i-1}}$$

where $0 \le a_0(m) < N$, $0 \le a_i(m) < N^{\lambda_i - \lambda_{i-1}}$, for $0 < i < t$, and $0 \le a_t(m) < a_t(n)$. As before, $\lambda > \lambda_t$ iff $a_t(m) = a_t(k)$ for $0 \le i \le t$, and now this can happen if and only if $a_t(k) < a_t(n)$. We consider the two possibilities in turn.

(a) If $a_t(k) \ge a_t(n)$: this includes the case when $k^* = n^*$.

We must show that $p^t \Sigma_{m^* \in B_t} \operatorname{ord}_N(k^* - m^*)$ has minimum value equal to the right side of (4.23), achieved at $k^* = n^*$. As before, since $\lambda \le \lambda_t$, we can truncate both k^* and m^* by going only up to the tth digit. The truncated m^* goes precisely over the range $\left[0, a_t(n) N^{1+\lambda_{t-1}}\right)$, and so

$$\#\left\{ m^* | m^* \in B_t, m^* \equiv k^* \bmod N^j \right\} = a_t(n) N^{1+\lambda_{t-1}-j},$$

when j is in the range $[1, 1 + \lambda_{t-1}]$. But on the range $1 + \lambda_{t-1} < j \le \lambda_t$ we can only conclude that this set has at least $[a_t(n)/N^{j-\lambda_{t-1}-1}]$ elements. However, when $k^* = n^*$: $m^* \in B_t$, $m^* \equiv n^* \bmod N^j$ (where $1 + \lambda_{t-1} < j \le \lambda_t$) iff $a_t(m) \equiv a_t(n) \bmod N^{j-1-\lambda_{t-1}}$ and $0 \le a_t(m) < a_t(n)$ and $a_i(m) = a_i(n)$ for $i \ne t$. The number of such $a_t(m)$ is $[a_t(n)/N^{j-1-\lambda_{t-1}}]$, so the minimum ordinal is the right side of (4.23), achieved when $k^* = n^*$.

(b) *If* $a_t(k) < a_t(n)$. As in Lemma 4.4, $\lambda > \lambda_t$ iff $m^* = k_t^*$, and so in this case the ordinals of the derivatives of the product in (4.23), evaluated at $x = \xi \equiv \alpha_{k^*} \bmod P^{1+\lambda_s}$, are at least

$$e \operatorname{ord}_p(p^t!) + p^t \sum_{m^* \in B_t,\, m^* \ne k_t^*} \operatorname{ord}_N(k_t^* - m^*).$$

This sum was just evaluated in the case when there was no exceptional term. The lower estimate on the number of solutions of the appropriate congruence is unchanged, but the exceptional term was counted once for

each congruence: hence a term $-\lambda_t$ is needed now. This time we can only assert that the derivarives have ordinal no less than

$$e\,\mathrm{ord}_p(p^t!) + p^t\left\{a_t(n)\sum_{j=0}^{\lambda_{t-1}} N^j + \sum_{i=1}^{\lambda_t-\lambda_{t-1}-1}\left[a_t(n)/N^i\right] - \lambda_t\right\}.$$

We complete the proof of (4.23) by noting that

$$e\,\mathrm{ord}_p(p^t!) \geq p^t\lambda_t:$$

$$p^t\lambda_t = p^t\left[\sum_{i=1}^{t} ep^{-i}\right] \leq ep^t\sum_{i=1}^{t} p^{-i} = e\,\mathrm{ord}_p(p^t!).$$

THEOREM 3. *Let R be the ring of integers of an algebraic number field K. Let $\mathbf{P}$ be a prime ideal of R, with associated N, p and $e = e_{\mathbf{P}}$, as in* (1.2) *and* (1.3), *such that $e \geq p$. Define s, λ_i, $a_i(n)$ and $b_i(n)$, $0 \leq i \leq s$, as in Lemma* 4.2 *and* (4.12). *Define β_n and $f_n(x)$ as in* (4.15), (4.16) *and Theorem* 2. *Let $\psi_n(P)$ be defined as in section* 3, *let g_n be as in* (4.1). *Then*

$$\mathrm{ord}_{\mathbf{P}} f_n(x) = \mathrm{ord}_{\mathbf{P}} f_n^{(g_n)}(\beta_n) = \psi_n(\mathbf{P}) \tag{4.24}$$

$$\psi_n(\mathbf{P}) = e\,\mathrm{ord}_p(g_n!) + \sum_{t=0}^{s} p^t\left\{b_t(n)\left(\sum_{j=1}^{\lambda_t} N^j - \lambda_t\right) + \sum_{j=\lambda_{t-1}+1-\lambda_t}^{\lambda_{t-1}}\left[a_t(n)N^j\right]\right\}. \tag{4.25}$$

Proof. Denote by $\chi_n(P)$ the right side of (4.25). Then by (2.6), (4.18), Lemma 4.4 and Lemma 4.5

$$\mathrm{ord}_P f_n(x) \geq \chi_n(P) + e\sum_{t=0}^{s} \mathrm{ord}_p\left(b_t(n)p^t\right)! - e\,\mathrm{ord}_p\, g_n!. \tag{4.26}$$

Now g_n is the exponent to which $x - \alpha_{n^*}$ occurs as a factor of f_n, so the evaluation of $\mathrm{ord}_{\mathbf{P}} f_n^{(g_n)}(\beta_n)$ proceeds as in Lemmas 4.4 and 4.5. The factors $x - \alpha_{n^*}$ are differentiated away and contribute $e\,\mathrm{ord}_p\, g_n!$. By Lemma 4.4, the factors from A_t with $m^* \neq n^*$ contribute

$$b_t(n)\left(N + \cdots + N^{\lambda_t} - \lambda_t\right)$$

when we set $x = \alpha_{n^*}$ and take $\mathrm{ord}_{\mathbf{P}}$. The factors from B_t do not require differentiation, as now $k^* = n^*$, so Lemma 4.5 completes the proof that

$$\mathrm{ord}_{\mathbf{P}} f_n^{(g_n)}(\beta_n) = \chi_n(P). \tag{4.27}$$

We shall complete the proof of Theorem 3 by showing that the right sides of (4.26) and (4.27) are equal.

LEMMA 4.6. *Let b_i be integers such that $0 \le b_i < p$ for $0 \le i < s$, $0 \le b_s$, where p is a prime. Then*

$$\operatorname{ord}_p\left(\sum_{i=0}^{s} b_i p^i\right)! = \sum_{i=0}^{s} \operatorname{ord}_p\left(b_i p^i\right)!. \tag{4.28}$$

Proof. Since $\operatorname{ord}_p n! = \sum_{r=1}^{\infty}[n/p^r]$, it suffices to prove that

$$\left[\left(\sum_{i=0}^{s} b_i p^i\right)/p^r\right] = \sum_{i=0}^{s}\left[b_i p^i/p^r\right]. \tag{4.29}$$

We derive this inductively from the fact that if $0 \le b_i < p$ for $0 \le i < t$, and if b_i is integral, for $0 \le i \le t$, then

$$\left[\left(\sum_{i=0}^{t} b_i p^i\right)/p^r\right] = \left[\left(\sum_{i=0}^{t-1} b_i p^i\right)/p^r\right] + \left[b_t p^t/p^r\right]. \tag{4.30}$$

This is clear if $r \le t$, as then $b_t p^t/p^r$ is an integer. In case $r > t$, we use the rule $[x/n] = [[x]/n]$ and the inequality

$$0 \le \sum_{i=0}^{t-1} b_i p^i \le (p-1)\sum_{i=0}^{t-1} p^i = p^t - 1$$

as follows:

$$\left[\left(\sum_{i=0}^{t-1} b_i p^i\right)/p^r\right] + \left[b_t p^t/p^r\right] = 0 + \left[b_t p^t/p^r\right] = \left[b_t/p^{r-t}\right]$$

$$= \left[\left[\left(\sum_{i=0}^{t} b_i p^i\right)/p^t\right]/p^{r-t}\right] = \left[\left(\sum_{i=0}^{t} b_i p^i\right)/p^r\right].$$

This completes the proof of Lemma 4.6 and Theorem 3. We now have an algorithm for calculating the exponent $\psi_n(P)$ in the denominator ideal I_n of Theorem 1: if $pN > n$ then $\psi_n(P) = 0$, and for the finite number of primes with $pN \le n$, equation (1.7) or (4.25) applies.

REFERENCES

[1] A. Ostrowski, *uber ganzwertige Polynome in algebraischen Zahlkorpern*, J. reine angew. Math., **149** (1919), 117–124.

[2] G. Polya, *Uber ganzwertige Polynome in algebraischen Zahlkorpern*, J. reine angew. Math., **149** (1919), 97–116.

[3] E. G. Straus, *On the polynomials whose derivatives have integral values at the integers*, Proc. Amer. Math. Soc., **2** (1951), 24–27.

Received May 31, 1984.

UNIVERSITY OF HAWAII
HONOLULU, HI 96822