Pacific Journal of Mathematics

DIRICHLET'S THEOREM FOR THE RING OF POLYNOMIALS OVER GF(2)

Douglas Austin Hensley

Vol. 123, No. 1 March 1986

PACIFIC JOURNAL OF MATHEMATICS
Vol. 123, No. 1, 1986

DIRICHLET'S THEOREM FOR THE RING OF POLYNOMIALS OVER GF(2)

DOUGLAS HENSLEY

Let G denote the ring $\mathrm{GF}(2)[x]$ of polynomials $g(x)$ over the field of integers mod 2. Let

$$I(k) = \#\{p \in G\colon \deg p = k \text{ and } p \text{ is irreducible in } G\}.$$

It is well known that $I(k) = (1/k)\sum_{d|k}\mu(d)2^{k/d}$. Here we prove an analog to Dirichlet's Theorem on primes in arithmetic progressions. For any $m \in G$ the p counted in $I(k)$ are uniformly distributed among the congruence classes (b) mod m for which $(b, m) = 1$. The result is especially sharp when m is square-free.

1. Introduction and notation. As in the abstract, $G = \mathrm{GF}(2)[x]$. We will suppress the variable and write, for instance, 1011 in place of $x^3 + x + 1$. We denote the set of irreducible $p \in G$ by I. The only part of this work which does not seem to generalize easily to other $\mathrm{GF}(q)[x]$, q a prime, is the special role of square-free moduli. Defining $\phi\colon G \to Z$ in the natural way ($\phi(m) = \#\{a\colon \deg a = \deg m \text{ and } (a, m) = 1\}$), we have that

(1.1) $\phi(m)$ is odd if and only if m is square-free.

Consequently, none of the "Dirichlet characters" on G/mG can have as their range $\{-1, 0, 1\}$. The absence of this kind of Dirichlet character permits sharper bounds. For fixed $m \in G$, $b \in G$ with $(b, g) = 1$, let $I_b(n)$ denote the number of irreducible $p \in G$ of degree n such that $p \equiv b \bmod m$.

THEOREM. *There exist positive effectively computable constants C_1 and C_2 such that for all integers M, $N \geq 1$, for all square-free polynomials $m \in G$ of degree M, and for all congruence classes (b) mod m relatively prime to m,*

$$\left| I_b(N) - \frac{2^N}{N\phi(m)} \right| \leq \frac{C_1 M 2^N}{N} \exp\left(-C_2 N M^{-9} (\log M)^{-3}\right).$$

That is,

$$I_b(N) = \frac{2^N}{N\phi(m)}\left(1 + O\left(M\phi(m)e^{-C_2NM^{-9}(\log M)^{-3}}\right)\right)$$

uniformly in N, M, m *and* b.

The result, of course does not constitute any improvement on the trivial bounds $0 \le I_b(N) \le I(N)$ unless N is larger, roughly, than M^9. It differs from results of Uchiyama and Carlitz [**1, 3, 4**] in its generality and uniformity with respect to the modulus, treating the ring G as fixed. Basically they kept G variable and constrained m.

When m is not square-free, characters of the second kind intrude, and we must settle for $2^{-M}M^{-2}$ in place of $M^{-9}(\log M)^{-3}$ in Theorem 1.

2. Preliminaries. For much of its length our proof follows the path of the classic proof of Dirichlet's theorem. There are analogs to Dirichlet characters, to L-functions, and product expansions valid in a half-plane. The difference is that in this case the L-functions are essentially polynomial functions on **C**. This simplifies the analysis. We can dispense with contour integrations, and just compare coefficients in two expansions of

$$\sum_{\chi \bmod m} \frac{1}{\chi(b)} \frac{L'(s,\chi)}{L(s,\chi)},$$

as series in $t = 2^{-s}$. The reader who wants to see just what is *different* can skip this section.

Let $Na = 2^{\deg a}$, for $a \in G$. Let

(2.1) $$\phi(m) = \#\{a\colon \deg a = \deg m \text{ and } (a,m) = 1\}.$$

Note that for $p \in G$ irreducible, $\phi(p) = Np - 1$ and is odd. Finally, the usual proof that

(2.2) $$\phi(m) = (Nm)\prod_{p|m}\left(1 - \frac{1}{Np}\right)$$

is valid in this setting too, so $\phi(m)$ is multiplicative. Thus $\phi(m)$ is odd if and only if m is square-free.

A *character* mod m is a function $\chi\colon G \to \mathbf{C}$ such that

(2.3)
$$\begin{array}{lll} \text{(i)} & \chi(a)\chi(b) = \chi(ab) & \text{for } a, b \in G. \\ \text{(ii)} & \chi(a) = \chi(b) & \text{if } a \equiv b \bmod m \\ \text{(iii)} & \chi(a) = 0 & \text{for } (a,m) \ne 1. \end{array}$$

As with characters in the integers, $\chi(1) = 1$, and if $(a, m) = 1$ then $\chi(a)$ is a $\phi(m)$th root of 1. For every m except 1, 10, 11 and 110, there is a character other than the trivial character χ_0, where

$$\chi_0(a) = 1 \quad \text{for } (a, m) = 1, \qquad \chi_0(a) = 0 \quad \text{otherwise.}$$

Further, with the same exceptions,

$$\sum_{a \bmod m} \chi(a) = 0 \quad \text{for all } \chi \neq \chi_0 \tag{2.4}$$

$$\sum_{\chi \bmod m} \chi(a) = 0 \quad \text{for all } a \not\equiv 1 \bmod m. \tag{2.5}$$

(All irreducibles except the factors of m are $\equiv 1 \bmod m$ when $m = 1, 10, 11$ or 110, since only 1 mod m is relatively prime to m in these cases. From now on, we assume m is not 1, 10, 11 or 110.)

$$\sum_{\chi \bmod m} \chi(1) = \phi(m) \tag{2.6}$$

and

$$\sum_{a \bmod m} \chi_0(a) = \phi(m). \tag{2.7}$$

Proof. The classical proofs go over word for word. See e.g. Landau [**2**].

We now define a power series $f_\chi(t)$ corresponding to each χ mod m. With the substitution $t = 2^{-s}$ we get the analog of a Dirichlet L-series.

DEFINITION.

$$f_\chi(t) = \sum_{a \in G} \chi(a) t^{\deg a} = \sum_{j=0}^{\infty} \left\{ \sum_{\deg a = j} \chi(a) \right\} t^j, \tag{2.8}$$

and

$$L(s, \chi) = \sum_{\substack{a \in G \\ a \neq 0}} \chi(a)(Na)^{-s}.$$

Let $C_j(\chi) = \sum_{\deg a = j} \chi(a)$. Then by (2.4), for $\chi = \chi_0$, $C_j(\chi) = 0$ for $j \geq \deg m$.

Thus for $\chi \neq \chi_0$, and with $M = \deg m$,

$$f_\chi(t) = \sum_{j=0}^{m-1} C_j(\chi) t^j \tag{2.9}$$

and is a polynomial over the complex numbers of degree $\leq M - 1$. We note here that

$$f_\chi(0) = 1, \quad f_\chi(1) = 0, \quad \text{and} \quad |C_j| \leq 2^j. \tag{2.10}$$

If we forget temporarily that $f_\chi(t)$ is a polynomial, it is natural to ask for a product expansion. Formally,

$$f_\chi(t) = \prod_{p\in I}\left(1 - \frac{\chi(p)}{(Np)^s}\right)^{-1} = \prod_{p\in I}(1 - \chi(p)t^{\deg p})^{-1}, \tag{2.11}$$

and the product converges absolutely for $|t| < \frac{1}{2}$ (Re(s) > 1). The function corresponding to the Riemann zeta function here is

$$Z(t) := \sum_{a\neq 0} t^{\deg a} = \frac{1}{1-2t}, \tag{2.12}$$

and this has the product expansion

$$Z(t) = \prod_{k=1}^{\infty}(1 - t^k)^{-I(k)}. \tag{2.13}$$

Finally, for $\chi = \chi_0 \bmod m$,

$$f_{\chi_0}(t) = Z(t)\prod_{p|m}(1 - t^{\deg p}). \tag{2.14}$$

The well known identity

$$I(k) = \frac{1}{k}\sum_{d|k}\mu(d)2^{k/d} \tag{2.15}$$

now follows from a (*much*) simplified reprise of the proof of the prime number theorem. We have $Z'(t)/Z(t) = 2/(1-2t)$ on one hand, while from (2.13) it is $\sum_{k=1}^{\infty} kI(k)t^{k-1}/(1-t^k)$. Expanding both sides as series about $t = 0$ and equating coefficients gives

$$2^k = \sum_{d|k} dI(d), \tag{2.16}$$

which is equivalent to (2.15).

The same ideas feature in the proof of Theorem 1: differentiate $\log f_\chi(t)$, use the product formula on one side, expand things as series in t and equate coefficients.

3. Partial fractions. For $\chi = \chi_0 \bmod m$,

$$f_{\chi_0}(t) = \frac{1}{1-2t}\prod_{p|m}(1 - t^{\deg p}) \tag{3.1}$$

for $t \neq 1/2$. With the notations $I_m(k) = \#\{p \in I\colon p|m \text{ and } \deg p = k\}$, $e(r) = e^{2\pi i r}$, we have

$$\frac{f'_{\chi_0}(t)}{f_{\chi_0}(t)} = \frac{2}{1-2t}\sum_{k=1}^{M}\frac{1}{k}I_m(k)\sum_{j=0}^{k-1}\frac{1}{t - e(j/k)} \tag{3.2}$$

which has simple poles at $t = 1/2$ and at various roots of unity. In all, there are $1 + \sum_{k=1}^{M} kI_m(k)$ poles of $(f'_{\chi_0}/f_{\chi_0})(t)$, and for m square-free, this is just $M + 1$. Now for any polynomial $f(t)$ over $\mathbf{C}$ with zeros $w_1, w_2, \ldots, w_j$ to multiplicity $N_1, N_2, \ldots, N_j$,

$$\frac{f'(t)}{f(t)} = \sum_{i=1}^{j} \frac{N_i}{t - w_i}. \tag{3.3}$$

Thus for any character $\chi \neq \chi_0 \bmod m$,

$$\frac{f'_\chi(t)}{f_\chi(t)} = \sum_{w \in \Omega_\chi} \frac{N(w)}{t - w},$$

where Ω_χ is the set of zeros of $f_\chi(t)$ and $N(w)$ the corresponding multiplicity, for $w \in \Omega_\chi$. By (2.11), $f_\chi(t) \neq 0$ for $|t| < 1/2$, that is, $|w| \geq 1/2$ if $w \in \Omega_\chi$. We now fix $b \bmod m$, $(b, m) = 1$, and consider

$$\sum_{\chi \bmod m} \frac{1}{\chi(b)} \frac{f'_\chi(t)}{f_\chi(t)}. \tag{3.4}$$

On one hand, this is equal to

$$\sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \frac{1}{\chi(b)} \sum_{w \in W_\chi} \frac{N(w)}{t - w} + \frac{2}{1 - 2t} - \sum_{k=1}^{M} \frac{1}{k} I_m(k) \sum_{j=0}^{k-1} \frac{1}{t - e(j/k)}. \tag{3.5}$$

We anticipate that for small t, the series expansion of this about zero converges, and that the dominant contribution to the coefficient of t^n for large n comes from $2/(1 - 2t)$.

On the other hand, (3.4) equals

$$\begin{aligned} &\sum_{\chi \bmod m} \frac{1}{\chi(b)} \sum_{p \in I} \frac{\chi(p)(\deg p) t^{\deg p - 1}}{1 - \chi(p) t^{\deg p}} \\ &= \sum_{k=1}^{\infty} k \sum_{j=0}^{\infty} \sum_{p \in I} \sum_{\chi \bmod m} \frac{1}{\chi(b)} (\chi(p))^{j+1} t^{(j+1)k-1} \\ &= \sum_{n=1}^{\infty} n t^{n-1} \sum_{d|n} \frac{1}{d} \sum_{\substack{p \in I \\ \deg p = n/d}} \sum_{\chi \bmod m} \frac{1}{\chi(b)} (\chi(p))^d. \end{aligned} \tag{3.6}$$

Thus the coefficient of t^{n-1} in the expansion of (3.6) about $t = 0$ is

$$n \sum_{d|n} \frac{1}{d} \sum_{\substack{p \in I \\ \deg p = n/d}} \sum_{\chi \bmod m} \frac{1}{\chi(b)} \chi(p)^d. \tag{3.7}$$

In (3.7), the part due to $d = 1$ is predominant, as we shall see. This part simplifies by (2.5) and (2.6) to

$$n\phi(m) \sum_{\substack{p \in I \\ \deg p = n}} 1 = n\phi(m) I_b(n).$$

The other terms may be estimated rather crudely. For any d,

$$\left| \sum_{\chi \bmod m} \frac{1}{\chi(b)} \chi(p)^d \right| \leq \varphi(m),$$

and $I(d) \leq 2^d/d$. Thus in (3.7) the part of the sum due to a particular d has absolute value $\leq (n/d)2^d\phi(m)$.

This gives

$$(3.8) \qquad \sum_{\chi \bmod m} \frac{1}{\chi(b)} \frac{f_\chi'(t)}{f_\chi(t)} = \sum_{n=1}^{\infty} n\phi(m)\left\{ I_b(n) + O\left(\frac{1}{n} 2^{n/2}\right)\right\} t^{n-1}.$$

The implicit constant is independent of b, m, and n.

In (3.5) the expansion of $2/(1 - 2t)$ is simple, and the coefficients of t^n arising from $1/(t - e(j/k))$ are quite small by comparison. We just need a bound on $|w|$ for $w \in \Omega_\chi$, $\chi \neq \chi_0$. Here the distinction between characters of the *second kind* (real valued and taking -1 as well as $+1$) and *third kind* (not real) is important.

If χ is a character of the second kind then following Landau's treatment in [**2**] one sees that $f_\chi(1/2) \neq 0$. But then

$$f_\chi(1/2) = \sum_{j=0}^{M-1} c_j(1/2)^j$$

and $c_j = \sum_{\deg a = j} \chi(a)$ is an integer here, so $|f_\chi(1/2)| \geq 2^{-M}$. More sophisticated approaches led to no better an estimate. The estimate for $I_b(n)$ when m is not square-free is done the same way as that for when m is square-free, except at this point. Since the main interest attaches to the uniformly good estimates to be had for square-free m, we shall not go into this any more.

Assume now that m is square-free. Then there are no real characters other than χ_0.

4. The zeros of $f_\chi(t)$ for characters of the third kind. By the familiar device based on the inequality $3 + 4\cos\theta + \cos 2\theta \geq 0$ and the product expansion (2.11), we have

$$(4.1) \qquad \left| f_{\chi_0}^3(t) f_\chi^4(t) f_{\chi^2}(t) \right| \geq 1 \quad \text{for } |t| < 1/2.$$

Since χ takes on non-real values, $\chi^2 \neq \chi_0$, so $|f_{\chi^2}(t)| \leq M$ for $|t| \leq 1/2$. The factor involving χ_0 is easily estimated:

$$|f_{\chi_0}(t)| \leq \left|\frac{1}{1-2t}\right| \prod_{p|m}\left(1+\frac{1}{Np}\right), \quad \text{for } |t| < \frac{1}{2}.$$

It is well known that for integer $n \to \infty$, $\phi(n) \gg n/\log\log n$; the worst case is when n is the product of the first k primes for some k.

Similarly here we have for $\deg m = M$, $M \to \infty$ that

$$(4.2) \qquad \phi(m) \gg 2^M/\log M, \quad \text{uniformly in } m.$$

Since

$$\prod_{p|m}\left(1+\frac{1}{Np}\right) < \prod_{p|m}\left(1-\frac{1}{Np}\right)^{-1} = \frac{2^M}{\phi(m)},$$

$$\prod_{p|m}\left(1+\frac{1}{Np}\right) \ll \log M,$$

and so

$$(4.3) \qquad |f_{\chi_0}(t)| \ll \left|\frac{\log M}{1-2t}\right|, \qquad |t| < \frac{1}{2}.$$

Now from (4.1),

$$(4.4) \qquad |f_\chi(t)| \gg M^{-1/4}(\log M)^{-3/4}|t-1/2|^{3/4} \quad \text{in } |t| < 1/2.$$

To estimate $f'_\chi(t)/f_\chi(t)$ we also need an upper bound for $f'_\chi(t) = \sum_{j=1}^{m-1} jC_j t^{j-1}$, in $|t| < 1/2$.

Each $|C_j| \leq 2^j$, so $|C_j t^{j-1}| \leq 2$. Thus

$$(4.5) \qquad |f'_\chi(t)| \leq M^2 \quad \text{for } |t| \leq 1/2.$$

Since no polynomial can have a zero of fractional order, for fixed χ, $|f_\chi(t)| \gg 1$ in $|t| < 1/2$. But for variable M, we need a lemma.

LEMMA. *Uniformly in $M \geq 1$, in m with* deg $m = M$, *in* χ mod m *of the third kind, and in* $|t| \leq 1/2$,

$$|f_\chi(t)| \gg M^{-7}(\log M)^{-3}.$$

Proof. By (4.4), there exists $C > 0$ such that

$$|f_\chi(t)| \geq CM^{-1/4}(\log M)^{-3/4}|t-1/2|^{3/4}.$$

Let t_0, $0 < t_0 < 1/2$, be the unique solution of

$$M^2 = \tfrac{3}{4}CM^{-1/4}(\log M)^{-3/4}\left|t-\tfrac{1}{2}\right|^{-1/4}: \quad t_0 = \tfrac{1}{2} - \left(\tfrac{3}{4}\right)^4 C^4 M^{-9}(\log M)^{-3}.$$

Then

$$|f_\chi(1/2)| \geq |f_\chi(t_0)| - M^2(1/2 - t_0)$$

from (4.5), and this is $\geq (\frac{3}{4})^3 \frac{1}{4} C^4 M^{-7} (\log M)^{-3}$ from (4.4). Now for $|\frac{1}{2} - t| < \frac{1}{10}|\frac{1}{2} - t_0|$,

$$|f_\chi(t)| \geq |f_\chi(t_0)| - \tfrac{1}{10} M^2 |\tfrac{1}{2} - t_0| \geq (\tfrac{3}{4})^3 (\tfrac{1}{4} - \tfrac{1}{10}) C^4 M^{-7} (\log M)^{-3}.$$

For $|t - \frac{1}{2}| \geq \frac{1}{10}|t_0 - \frac{1}{2}|$, though,

$$\begin{aligned} |f_\chi(t)| &\geq C M^{-1/4} (\log M)^{-3/4} |t - \tfrac{1}{2}|^{3/4} \qquad \text{by (4.4)}, \\ &\geq (\tfrac{3}{4})^3 (\tfrac{1}{10})^{3/4} C^4 M^{-7} (\log M)^{-3}. \end{aligned}$$

Thus uniformly in M, m, $\chi \bmod m$ of the third kind, and for t, $|t| < 1/2$,

$$|f_\chi(t)| \geq C_1 M^{-7} (\log M)^{-3}. \tag{4.6}$$

The lemma follows by the continuity of the $f_\chi(t)$.

Now

$$f_\chi(t)^{(n)} = \sum_{j=n}^{M-1} C_j \frac{n!}{j!} t^{j-n},$$

so $|f_\chi(t)^{(n)}| \leq (2M)^{n+1}$ in $|t| \leq 1/2$. Thus for $|v| \leq M^{-9}$ and $|T| = 1/2$ we have

$$f_\chi(T + v) = f_\chi(T) + O\left(\sum_{j=1}^{M-1} \frac{1}{j!} |v|^j (2M)^{j+1} \right) \tag{4.7}$$

(with the implicit constant $= 1$)

$$= f_\chi(T) + O(M^2 |v|).$$

Thus uniformly in M, m, and χ,

$$f_\chi(t) \neq 0 \quad \text{in } |t| \leq 1/2 + C_2\left(M^{-9} (\log M)^{-3}\right) \tag{4.8}$$

for some $C_2 > 0$.

5. Conclusions. We now expand (3.5) as a series in t, and estimate the coefficient of t^{n-1}.

From χ_0, we get

$$\sum_{n=1}^{\infty} 2^n t^{n-1} + \sum_{k=1}^{M} \frac{1}{k} I_m(k) \sum_{j=0}^{k-1} \sum_{n=1}^{\infty} t^{n-1} e\left(\frac{(n-1)j}{k} \right), \tag{5.1}$$

so the coefficient of t^{n-1} is

$$2^n + \sum_{k=1}^{M} \frac{1}{k} I_m(k) \sum_{j=0}^{k-1} e\left(\frac{(n-1)j}{k}\right). \tag{5.2}$$

Now $|\sum_{j=0}^{k-1} e((n-1)j/k)| \le k$, so the second term of (5.2) is $O(\sum_{k=1}^{M} I_m(k))$. Now trivially this latter is $O(M)$. (A little thought shows it to be $O(M/\log M)$ but we have larger errors elsewhere.) Thus in (3.5) the coefficient of t^{n-1} due to χ_0 is

$$2^n + O(M). \tag{5.3}$$

The expansion of the rest of (3.5) works out to $\sum_{n=1}^{\infty} r_n t^{n-1}$, where

$$\begin{aligned} r_n &= \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \frac{1}{\chi(b)} \sum_{w \in \Omega_\chi} \frac{-N(w)}{w} \left(\frac{1}{w}\right)^{n-1} \\ &= -\sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \frac{N(w)}{\chi(b)} w^{-n}. \end{aligned} \tag{5.4}$$

Now $|w| \ge 1/2 + C_2 M^{-9} (\log M)^{-3}$. Thus

$$|r_n| \le M\phi(m) 2^n \exp\left(-C_3 n M^{-9} (\log M)^{-3}\right). \tag{5.5}$$

Now from (5.5), (5.3), and (3.8) we have

$$\begin{aligned} &n\phi(m)\left(I_b(n) + O\left(\tfrac{1}{n}2^{n/2}\right)\right) \\ &\quad = 2^n + O(M) + O\left(M\phi(m) 2^n \exp\left(-C_3 n M^{-9} (\log M)^{-3}\right)\right). \end{aligned} \tag{5.6}$$

The theorem follows upon renumbering the constants.

References

[1] L. Carlitz, *A theorem of Dickson on irreducible polynomials*, Proc. Am. Math. Soc., **3** (1952), 693–700.

[2] E. Landau, *Elementary Number Theory*, Chelsea, NY, 1966.

[3] Saburô Uchiyama, *Sur les polynomes irréductibles dans un corps fini I*, Proc. Japan Acad., **30** (1954), 523–527.

[4] ______, II, Proc. Japan Acad., **31** (1955), 267–269.

Received December 28, 1984.

TEXAS A & M UNIVERSITY
COLLEGE STATION, TX 77843-3368

Pacific Journal of Mathematics

Vol. 123, No. 1 March, 1986