A THEOREM OF DICKSON ON IRREDUCIBLE POLYNOMIALS

L. CARLITZ

1. **Introduction.** Let $p>2$, $n\geqq 1$. In 1911 Dickson [3] studied the distribution of irreducible cubics

$$Q(x) = x^3 - x^2 + ax + b^2 \qquad (a, b \in GF(p^n)).$$

Using elementary methods he determined the number of such irreducibles. (The results are reproduced in §5 below.)

In the present paper we consider the more general problem of irreducibles

$$Q(x) = x^m + c_1x^{m-1} + \cdots + c_m \qquad (c_i \in GF(p^n))$$

with preassigned c_1, c_m; for brevity we shall call c_1 and c_m the first and last coefficients, respectively, of $Q(x)$. We first derive an asymptotic formula for the number of such irreducibles, namely,

$$\frac{1}{m} p^{n(m-2)} + O(p^{nm/2}) \qquad (m \to \infty).$$

It is of interest to note that for the L-functions arising in this connection the Riemann hypothesis is very easily proved (compare [2]).

In the second place we consider irreducibles $Q(x)$ with assigned first coefficient and last coefficient equal to a square (or a nonsquare) of the field, thus directly generalizing Dickson's problem. We now obtain *exact* results (see (5.6) below). Finally we determine the number of irreducibles with assigned first coefficient.

2. For $a\in GF(p^n)$ we put

$$E(a) = e^{2\pi i t(a)/p}, \qquad t(a) = a + a^p + \cdots + a^{p^{n-1}}. \tag{2.1}$$

Then if $M=x^m+a_1x^{m-1}+ \cdots +a_m$ $(a_i\in GF(p^n))$, and b is an arbitrary number of $GF(p^n)$, we define

$$\lambda(M) = \lambda_b(M) = E(ba_1) \qquad (\deg M \geqq 1); \tag{2.2}$$

also $\lambda(1)=1$. There are thus p^n functions λ; in particular $\lambda_0(M)\equiv 1$. We note that

$$\sum_\lambda \lambda(M) = \begin{cases} p^n & (a_1 = 0), \\ 0 & (a_1 \neq 0), \end{cases} \tag{2.3}$$

Presented to the Society, April 26, 1952; received by the editors January 15, 1952.

where the sum in the left member is extended over all λ.

In the next place let γ be a primitive root of the field. Then if $a=\gamma^r$, we put

$$X(a) = e^{2\pi i r/(p^n-1)}, \qquad X(0) = 0.$$

If now c is an integer, $0 \leqq c < p^n - 1$, we define

$$\chi(M) = \chi_c(M) = X(a_m^c). \tag{2.4}$$

There are $p^n - 1$ functions χ; in particular, $\chi_0(M) \equiv 1$ for $x \nmid M$. We note that

$$\sum_{\chi} \chi(M) = \begin{cases} p^n - 1 & (a_m = 1), \\ 0 & (a_m \neq 1). \end{cases} \tag{2.5}$$

It is clear from the definitions that

$$\lambda(AB) = \lambda(A)\lambda(B), \qquad \chi(AB) = \chi(A)\chi(B) \tag{2.6}$$

and for $m \geqq 1$

$$\begin{aligned} \sum_{\deg M = m} \lambda(M) &= 0 & (\lambda \neq \lambda_0), \\ \sum_{\deg M = m} \chi(M) &= 0 & (\chi \neq \chi_0). \end{aligned} \tag{2.7}$$

3. We next define the function

$$L(s, \lambda, \chi) = \sum_{M} \lambda(M)\chi(M) \, | M |^{-s} \qquad (| M | = p^{n \deg M}), \tag{3.1}$$

the sum extending over all primary $M \in GF[p^n, x]$. If we put

$$\tau_m = \tau_m(\lambda, \chi) = \sum_{\deg M = m} \lambda(M)\chi(M), \tag{3.2}$$

it is clear that (3.1) implies

$$L(s, \lambda, \chi) = \sum_{m=0}^{\infty} \tau_m(\lambda, \chi) p^{-nms}. \tag{3.3}$$

Now in the first place

$$L(s, \lambda_0, \chi_0) = \sum_{x \nmid M} | M |^{-s} = (1 - p^{-ns})(1 - p^{n(1-s)})^{-1}. \tag{3.4}$$

Secondly for $\chi \neq \chi_0$, by the second of (2.7),

$$L(s, \lambda_0, \chi) = \sum_{M} \chi(M) \, | M |^{-s} = 1; \tag{3.5}$$

similarly for $\lambda \neq \lambda_0$ by the first of (2.7)

$$L(s, \lambda, \chi_0) = \sum_M \lambda(M) \mid M \mid^{-s} = 1 - p^{-ns}. \tag{3.6}$$

It remains to consider $L(s, \lambda, \chi)$, where $\lambda \neq \lambda_0$, $\chi \neq \chi_0$. We remark first that by (2.2) and (2.4)

$$\tau_1 = \tau_1(\lambda, \chi) = \sum_{a \in GF(p^n)} E(ba)X(a^c);$$

then we have the easily proved formula [2]

$$\mid \tau_1 \mid = p^{n/2} \qquad (\lambda \neq \lambda_0, \chi \neq \chi_0). \tag{3.7}$$

As for $n > 1$, it is evident from (3.2) that

$$\tau_m(\lambda, \chi) = p^{n(m-2)} \sum_{a_1, a_m} E(ba_1)X(a_m^c);$$

thus

$$\tau_m(\lambda, \chi) = 0 \qquad (\lambda \neq \lambda_0, \chi \neq \chi_0, m > 1). \tag{3.8}$$

Hence by (3.3) and (3.8), we have

$$L(s, \lambda, \chi) = 1 + \tau_1(\lambda, \chi)p^{-ns} \qquad (\lambda \neq \lambda_0, \chi \neq \chi_0). \tag{3.9}$$

4. Returning to (3.1) it is clear that

$$L(s, \lambda, \chi) = \prod_P (1 - \lambda(P)\chi(P) \mid P \mid^{-s})^{-1}, \tag{4.1}$$

the product extending over all (primary) irreducibles $P \in GF[p^n, x]$. Taking logarithms, we get

$$\log L(s, \lambda, \chi) = \sum_P \sum_{r=1}^{\infty} \frac{1}{r} \lambda(P^r)\chi(P^r) \mid P \mid^{-rs}. \tag{4.2}$$

Now let a, l be fixed numbers of $GF(p^n)$, $l \neq 0$. Then by (2.3) and (2.5), (4.2) implies

$$\sum_{\lambda, \chi} E(-ba)X(l^{-c}) \log L(s, \lambda, \chi) = p^n(p^n - 1) {\sum_{P,r}}' \frac{1}{r} \mid P \mid^{-rs}, \tag{4.3}$$

where in the right member of (4.3) the summation is restricted to P and r such that P^r has first coefficient a and last coefficient l. Let $\pi(t, r) = \pi(t, r; a, l)$ denote the number of such P of degree t/r.

As for the left member of (4.3), we have first from (3.4) the contribution

$$\log L(s, \lambda_0, \chi_0) = \sum_{r=1}^{\infty} \frac{1}{r} (p^{nr} - 1)p^{-nrs}.$$

In view of (3.5), $\log L(s, \lambda_0, \chi)=0$, but by (3.6)

$$\log L(s, \lambda, \chi_0) = -\sum_{r=1}^{\infty} \frac{1}{r} p^{-nrs}.$$

Also (3.9) yields

$$\log L(s, \lambda, \chi) = \sum_{r=1}^{\infty} \frac{(-1)^{r-1}}{r} \tau_1^r p^{-nrs}.$$

Thus in all we have for the left member of (4.3)

$$\sum_{r=1}^{\infty} \frac{1}{r} p^{-nrs} W_r,$$

where

$$W_r = p^{nr} - \sum_b E(-ba) + (-1)^{r-1} \sum_{\lambda\neq\lambda_0, \chi\neq\chi_0} E(-ba)X(l^{-c})\tau_1^r(\lambda, \chi).$$

Hence it is clear that

$$p^n(p^n - 1)\sum_{r|t} \frac{1}{r} \pi(t, r; a, l) = \frac{1}{t} W_t. \tag{4.4}$$

Now since on the one hand

$$\sum_{r|t, r>1} \frac{1}{r} \pi(t, r; a, l) = O(p^{nt/2}),$$

and on the other hand by (3.7)

$$\sum_{\lambda\neq\lambda_0, \chi\neq\chi_0} E(-ba)X(l^{-c})\tau_1^t(\lambda, \chi) = O(p^{nt/2})$$

it is evident that (4.4) implies

$$\pi(t, 1; a, l) = \frac{1}{t} p^{n(t-2)} + O(p^{nt/2}) \qquad (t \to \infty). \tag{4.5}$$

This proves:

Theorem 1. *The number of primary irreducibles of degree t with assigned first and last coefficients a, l, $l\neq 0$, satisfies* (4.5).

5. We now assume $p>2$ and consider the special case of irreducible polynomials with preassigned first coefficient and with last coefficient required to be a square (or a nonsquare) of the field. It is convenient to define a function $\psi(a)$, $a\in GF(p^n)$, $=0$, $+1$, -1 according as $a=0$,

square, nonsquare. Then corresponding to ψ will be a single function $\chi_1(M)$. The preceding discussion applies except that in place of the χ's we now use only χ_0, χ_1. We first replace (3.7) by an exact formula. It is clear that

$$\tau_1(\lambda, \chi_1) = \sum_a E(ba)\psi(a) = G(b), \tag{5.1}$$

where $G(b)$ denotes a Gauss sum [1, §3]. We recall the following formulas

$$G(b) = \psi(b)G(1), \qquad G^2(1) = \psi(-1)p^n; \tag{5.2}$$

since $G(b)=0$, the first of (5.2) is valid for all b.

In the next place it is clear that corresponding to the right member of (4.4), we get

$$\frac{1}{t}\left\{p^{nt} - \sum_b E(-ba) + (-1)^{t-1}\sum_{b\neq 0} E(-ba)\psi(l)G^t(b)\right\}. \tag{5.3}$$

We now use (5.2) and consider separately two cases.

(i) t even. In this case the second sum in (5.3) becomes

$$-p^{nt/2}\psi((-1)^{t/2}l)\sum_{b\neq 0} E(-ba); \tag{5.4}$$

the sum in (5.4) $=p^n-1$ or -1 according as $a=0$ or $\neq 0$.

(ii) t odd. In this case the sum in (5.3) yields

$$\begin{aligned}\psi(l)G^t(1)&\sum_b E(-ba)\psi(b)\\ &= \psi(a)G^t(1)G(-a) = \psi((-1)^{(t-1)/2}al)p^{n(t+1)/2},\end{aligned} \tag{5.5}$$

which holds for all a (including $a=0$).

Now for $r\mid t$, let $\pi(t, r; a, 1)$ denote the number of irreducibles P of degree t/r such that the first coefficient of P^r is a, while the last is a square; $\pi(t, r; a, -1)$ is the corresponding number with the last coefficient a nonsquare. Then as in §4, we get, making use of (5.3), (5.4), (5.5),

THEOREM 2.

$$\sum_{r\mid t} \frac{1}{r}\pi(t, r; a, \eta) = \frac{1}{2t}(p^{n(t-1)} - \epsilon + S), \tag{5.6}$$

where S is determined by

$$S = \begin{cases} -(\epsilon p^n - 1)p^{n(t/2-1)}\psi((-1)^{t/2}l) & (t\ \textit{even}),\\ p^{n(t-1)/2}\psi((-1)^{(t-1)/2}al) & (t\ \textit{odd}),\end{cases} \tag{5.7}$$

$\epsilon=1$ *for* $a=0$, $\epsilon=0$ *for* $a\neq 0$, *and* $\eta=\psi(l)$.

Suppose now t prime $\geqq 3$. Then for $t=p$

$$\pi(t, t; a, \eta) = \begin{cases} 0 & (a \neq 0), \\ (p^n - 1)/2 & (a = 0), \end{cases}$$

while for $t\neq p$

$$\pi(t, t; a, \eta) = \begin{cases} 1 & (\psi(tal) = 1), \\ 0 & (\text{otherwise}). \end{cases}$$

In conjunction with (5.7), this gives for $a=0$

$$\pi(t, 1; 0, \eta) = \begin{cases} \frac{1}{2t}(p^{n(t-1)} - 1) & (t \neq p), \\ \frac{1}{2p}(p^{n(t-1)} - p^n) & (t = p), \end{cases} \tag{5.8}$$

while for $a\neq 0$, we have

$$\pi(t, 1; a, \eta) = \begin{cases} \frac{1}{2t}(p^{n(t-1)} + S - 2) & (t \neq p,\ \psi(tal) = 1), \\ \frac{1}{2t}(p^{n(t-1)} + S) & (\text{otherwise}). \end{cases} \tag{5.9}$$

In Dickson's theorem, $t=3$, $a=1$, $\eta=+1$. Using the quadratic reciprocity theorem we can verify that (5.9) implies that the number of irreducible cubics satisfying these conditions is equal to

$$\begin{aligned} &(p^n - 1)(p^n + 2)/6 && (p^n \equiv 1 \pmod{12}), \\ &(p^n + 1)(p^n - 2)/6 && (p^n \equiv -1 \pmod{12}), \\ &p^n(p^n + 1)/6 && (p^n \equiv 5 \pmod{12}), \\ &p^n(p^n - 1)/6 && (p^n \equiv -5 \pmod{12}), \end{aligned}$$

while for $p=3$ we get

$$\begin{aligned} &p^n(p^n + 1)/6 && (n \text{ even}), \\ &p^n(p^n - 1)/6 && (n \text{ odd}). \end{aligned}$$

These results check with Dickson's, thus affording a partial check for the more general formulas derived above.

6. It may be worth while mentioning briefly the formula for the number of irreducibles of degree t with given first coefficient a. If

$p \nmid t$, then it is clear (by considering $P(x+b)$) that the number of irreducibles is independent of a and is therefore $f(t)/p^n$, where $f(t)=f(t, p^n)$ is the total number of (primary) irreducibles of degree t. For $p \mid t$, the transformation $c^t P(c^{-1}x)$ indicates that the number of irreducibles with first coefficient a is independent of a provided $a \neq 0$, but this gives no information for the case $a=0$. Accordingly we make use of the λ's defined above and set up

$$L(s, \lambda) = \sum_M \lambda(M) \mid M \mid^{-s} = \begin{cases} (1 - p^{n(1-s)})^{-1} & (\lambda = \lambda_0), \\ 1 & (\lambda \neq \lambda_0). \end{cases}$$

For $r \mid t$, let $\pi(t, r; a)$ denote the number of irreducibles P of degree t/r such that the first coefficient of P^r is a. Then exactly as in §§4, 5 we find that

$$\sum_{r \mid t} \frac{1}{r} \pi(r, t; a) = \frac{1}{t} p^{n(t-1)}. \tag{6.1}$$

If $t=p$, it is evident that $\pi(p, p; a)=0$ for $a \neq 0$, while $\pi(p, p; 0) = p^n$. Hence (6.1) implies

$$\pi(p, 1; a) = \begin{cases} p^{np-n-1} & (a \neq 0), \\ p^{np-n-1} - p^{n-1} & (a = 0). \end{cases} \tag{6.2}$$

We now determine $\pi(t, 1; a)$ for arbitrary t; we need only consider the case $p \mid t$. Now it is clear $\pi(t, r; a)=0$ for $p \mid r$, $a \neq 0$, while $\pi(t, r; 0) = f(t/r)$ for $p \mid r$. On the other hand for $p \nmid r$, we have $\pi(t, r; a) = \pi(t/r, 1; a/r)$ for all a. Now let $t=p^k m$, $p \nmid m$, and consider (6.1) with $a=1$. Then it is evident that we need only take such r for which $p \nmid r$; thus (6.1) becomes

$$\sum_{r \mid m} \frac{1}{r} \pi(t, r; 1) = \frac{1}{t} p^{n(t-1)},$$

which reduces to

$$\sum_{r \mid m} \frac{1}{r} \pi(t/r, 1; 1) = \frac{1}{t} p^{n(t-1)},$$

or what is the same thing

$$p^{n+k} \sum_{d \mid m} d\pi(p^k d, 1; 1) = p^{np^k m}. \tag{6.3}$$

Comparing (6.3) with the familiar equation

$$\sum_{d \mid m} df(d, p^n) = p^{nm},$$

which has the unique solution $f(d, p^n)$, it follows that

$$p^{n+k}\pi(p^k m, 1; 1) = f(m, p^{np^k}). \tag{6.4}$$

Since $(p^n-1)\pi(m, 1; 1)+\pi(m, 1; 0)=f(m)$, we have also

$$p^{n+k}\pi(p^k m, 1; 0) = p^{n+k}f(p^k m, p^n) - (p^n - 1)f(m, p^{np^k}). \tag{6.5}$$

It is easily verified that for $k=1$, $m=1$, (6.4) and (6.5) reduce to (6.2).

THEOREM 3. *The number of primary irreducible polynomials of degree $p^k m$ and assigned first coefficient is determined by* (6.4) *and* (6.5).

REFERENCES

1. L. Carlitz, *The singular series for sums of squares of polynomials*, Duke Math. J. vol. 14 (1947) pp. 1105–1120.

2. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. vol. 172 (1935) pp. 151–182.

3. L. E. Dickson, *An invariantive investigation of irreducible binary modular form*, Trans. Amer. Math. Soc. vol. 12 (1911) pp. 1–18.

DUKE UNIVERSITY