ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 8, Number 4, Fall 1978

POLYNOMIAL CHARACTERISTIC FUNCTIONS FOR $GF(p)$ AND IRREGULAR PRIMES

L. CARLITZ

1. Let $P(x)$ be a polynomial with coefficients in $F = GF(p)$, where p is an odd prime, that takes on only the values 0 and 1. It will be convenient to assume that $P(0) = 0$. Note that if $P(x)$ is a 0-1 polynomial then $P(cx)$ is also a 0-1 polynomial for all $c \in F$, $c \neq 0$. Let

$$U = \{u_1, u_2, \cdots, u_k\} \tag{1.1}$$

denote the subset of $F - \{0\}$ such that

$$P(u_i) = 1 \quad (i = 1, 2, \cdots, k). \tag{1.2}$$

By the Lagrange interpolation formula, the unique 0-1 polynomial of degree $< p$ and satisfying (1.2) is given by

$$P(x) = \sum_{i=1}^{k} \{1 - (x - u_i)^{p-1}\}. \tag{1.3}$$

Since

$$(x - y)^{p-1} = \sum_{j=0}^{p-1} x^j y^{p-j-1},$$

we have

$$(x - u_i)^{p-1} = \sum_{j=0}^{p-1} x^j u_i^{p-j-1} = \sum_{j=0}^{p-1} x^j u_i^{-j}. \tag{1.4}$$

Thus (1.3) becomes

$$P(x) = - \sum_{j=1}^{p-2} x^j \sum_{i=1}^{k} u_i^{-j} - kx^{p-1}. \tag{1.5}$$

An alternate representation for $P(x)$ is the following. Put

$$\phi(x) = \prod_{u \in U} (x - u), \ \psi(x) = \frac{x^{p-1} - 1}{\phi(x)}. \tag{1.6}$$

Since

Received by the editors on September 24, 1976.

$$\frac{\phi'(x)}{\phi(x)} = \sum_{u \in U} (x-u)^{-1},$$

it follows from (1.3) that

$$P(x) = -\sum_{u \in U} \frac{x^p - x}{x - u} = -\frac{\phi'(x)}{\phi(x)}(x^p - x).$$

Hence

$$P(x) = -x\phi'(x)\psi(x). \tag{1.7}$$

For example, if U consists of the non-zero squares of F then

$$\phi(x) = x^{(1/2)(p-1)} - 1,\ \psi(x) = x^{(1/2)(p-1)} + 1$$

and it follows that

$$\begin{aligned} P(x) &= -(1/2)(p-1)\, x^{(1/2)(p-1)}(x^{(1/2)(p-1)} + 1) \\ &= (1/2)(x^{p-1} + x^{(1/2)(p-1)}). \end{aligned}$$

This result is easily generalized. Let $p = rs + 1$ and let U denote the set of non-zero s-th powers of F. Then

$$\phi(x) = x^r - 1,\ \psi(x) = \frac{x^{p-1} - 1}{x^r - 1}$$

and we get

$$P(x) = -r(x^{rs} + x^{r(s-1)} + \cdots + x^r). \tag{1.9}$$

Returning to (1.5), we can rewrite it in the form

$$P(x) = a_1 x^{r_1} + a_2 x^{r_2} + \cdots + a_m x^{r_m} - kx^{p-1} \tag{1.10}$$

where $0 < r_1 < r_2 < \cdots < r_m < p - 1$ and none of the coefficients a_i vanishes. Thus the question arises of what exponent patterns $(r_1, r_2, \cdots, r_m)$ can occur. In (1.9) the exponents (including $p - 1$) form an arithmetic progression.

As another example in which $(r_1, r_2, \cdots, r_m)$ alone form an arithmetic progression we cite $U = 1, 2, 3$ with $p = 7$. It can be verified that in this case

$$P(x) = -3x^6 + x^5 - x^3 - 3x. \tag{1.11}$$

2. We shall now examine the more general case

$$U = \{1, 2, \cdots, (1/2)(p-1)\} \tag{2.1}$$

in some detail. By (1.5) we now have

$$P(x) = -\sum_{j=1}^{p-2} x^j \sum_{a=1}^{(1/2)(p-1)} a^{p-1-j} - (1/2)(p-1)x^{p-1}.$$

Since

$$\sum_{a=1}^{p-1} a^r = 0 \qquad (1 \leqq r < p-1),$$

it follows that

$$\sum_{a=1}^{(1/2)(p-1)} a^{2r} = 0 \qquad (1 \leqq r < p-1), \tag{2.2}$$

To evaluate the corresponding sum with an odd exponent, we make use of the formula [**2**, Ch. 2]

$$\sum_{a=1}^{(1/2)(p-1)} a^{2r+1} = \frac{B_{2r+2}(1/2(p+1)) - B_{2r+2}}{2r+2},$$

where $B_n(x)$ is the Bernoulli polynomial of degree n and B_n is the n-th Bernoulli number. For $2r + 2 \leqq p - 1$, it follows from the Staudt-Clausen theorem that

$$\begin{aligned} B_{2r+2}(1/2(p+1)) - B_{2r+2} &= \sum_{j=0}^{2r+1} \binom{2r+2}{j} B_j(1/2(p+1))^{2r-j+2} \\ &= \sum_{j=0}^{2r+1} \binom{2r+2}{j} B_j(1/2)^{2r-j+2} \\ &= B_{2r+2}(1/2) - B_{2r+2}. \end{aligned}$$

Since [**2**, p. 22] $B_n(1/2) = (2^{1-n} - 1)B_n$, it follows that

$$\sum_{a=1}^{(1/2)(p-1)} a^{2r+1} = \frac{2^{-2r-2}}{r+1}(1 - 2^{2r+2})B_{2r+2} \quad (2r+2 \leqq p-1). \tag{2.3}$$

Therefore by (2.2) and (2.3),

$$P(x) = -\sum_{r=1}^{(1/2)(p-1)} \frac{2^{-2r}}{r}(1 - 2^{2r})B_{2r}x^{p-2r} - (1/2)(p-1)x^{p-1}. \tag{2.4}$$

Recall that a prime p is *regular* [3, p. 82] if it divides none of the Bernoulli numbers $B_2, B_4, \cdots, B_{p-3}$. Moreover it is known that there are infinitely many irregular primes. Those less than 100 are $p = 37, 59, 67$.

If p is irregular, at least one of the coefficients on the right of (2.4) vanishes. If p is regular it is still possible that $2^{2r} \equiv 1 \pmod p$. Hence if we assume that p is regular and that 2 is a primitive root $(\mathrm{mod}\, p^2)$, it follows that none of the coefficients in (2.4) vanishes. If $p \equiv 3 \pmod 4$ and 2 belongs to the exponent $(p-1)/2$, it is still true that none of the coefficients in (2.4) vanishes. For example, for $p = 7$, (1.11) illustrates this situation.

More generally let the smallest *even* exponent to which 2 belongs $(\mathrm{mod}\, p)$ be $2t$ and put $p = 2st + 1$. Then, for p regular, the vanishing coefficients in (2.4) are those corresponding to the exponents $p - 2rs$ $(r = 1, 2, \cdots, t)$.

3. Results of an analogous nature also hold in the following situation. Let $p \equiv 1 \pmod 4$ and take

$$U = \{1, 2, \cdots, \tfrac{1}{4}(p-1), -1, -2, \cdots, -\tfrac{1}{4}(p-1)\}. \tag{3.1}$$

Then as above

$$\begin{aligned} P(x) &= -\sum_{j=1}^{p-2} x^j \sum_{a=1}^{(1/4)(p-1)} (a^{p-1-j} \\ &\quad + (-a)^{p-1-j}) - \tfrac{1}{2}(p-1)x^{p-1} \\ &= -2 \sum_{j=1}^{(1/2)(p-3)} x^{2j} \sum_{a=1}^{(1/4)(p-1)} a^{p-1-2j} - 1/2(p-1)x^{p-1}. \end{aligned}$$

Now, for $r \geqq 1$,

$$\begin{aligned} \sum_{a=1}^{1/4(p-1)} a^{2r} &= \frac{B_{2r+1}((p+3)/4) - B_{2r+1}(1)}{2r+1} \\ &= \frac{1}{2r+1} B_{2r+1}(1/4(p+3)) \\ &= \frac{1}{2r+1} B_{2r+1}(3/4). \end{aligned}$$

Since [2, p. 21 and p. 29]

$$B_{2r+1}(3/4) = -B_{2r+1}(1/4) = (2r+1)4^{-2r-1}E_{2r},$$

where E_{2r} is an Euler number, it follows that

$$P(x) = -2 \sum_{r=1}^{(1/2)(p-3)} 4^{-2r-1} E_{2r} x^{p-2r-1} \tag{3.2}$$
$$- (1/2)(p-1)x^{p-1}.$$

Corresponding to the definition of regular primes above we may define a prime p as regular with respect to the Euler numbers if none of the numbers $E_2, E_4, \cdots, E_{p-3}$ is divisible by p. It is proved in [1] that the number of primes irregular with respect to the Euler numbers is infinite.

Hence if p is regular with respect to the Euler numbers it follows that none of the coefficients in (3.2) vanishes. For example, 5 is regular in this sense (as well as the previous sense) and we have from (1.3)

$$P(x) = (1 - (x-1)^4) + (1 - (x+1)^4) = -2x^2 - 2x^4,$$

in agreement with (3.2).

References

1. L. Carlitz, *Note on irregular primes*, Proceedings of the American Mathematical Society, **5** (1954), 329–331.

2. N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Springer, Berlin, 1924.

3. H. S. Vandiver and G. E. Wahlin, *Algebraic Numbers* II, Bulletin of the National Research Council **62**, 1928.

Duke University, Durham, North Carolina 27706