NOTE ON A CONJECTURE OF ANDRÉ WEIL

L. CARLITZ

1. In discussing the number of solutions of equations in finite fields [2, p. 507], Weil was led to the following conjecture. Let V be a variety of dimension n without singular points defined over $GF(q)$, $q=p^n$; let N_m be the number of *rational* points on V over the extended field $GF(q^m)$. Then

$$\sum_{m=1}^{\infty} N_m u^{m-1} = \frac{d}{du} \log Z(u), \tag{1.1}$$

where $Z(u)$ is a rational function of u which satisfies a functional equation of the type

$$Z\left(\frac{1}{q^n u}\right) = \pm q^{nh/2} u^h Z(u). \tag{1.2}$$

Moreover

$$Z(u) = \frac{P_1(u)P_3(u)\cdots P_{2n-1}(u)}{P_0(u)P_2(u)\cdots P_{2n}(u)}, \tag{1.3}$$

where $P_0(u)=1-u$, $P_{2n}(u)=1-q^n u$, and

$$P_h(u) = \prod_{i=1}^{B} (1 - \alpha_{h_i} u) \qquad (|\alpha_{h_i}| = q^{h/2},\ 1 \leqq h \leqq 2n-1).$$

(Weil also makes some additional remarks that we shall not discuss.)

The purpose of this note is to examine this conjecture in several cases in which explicit formulas are available for N_m, so that $Z(u)$ can be computed. In some of the cases considered V may have singular points; as might be expected the conjectured formulas may require modification in such cases.

2. Let $p>2$. A well known instance in which an explicit formula is available is

$$Q(x_1, \cdots, x_s) = \alpha, \tag{2.1}$$

where $Q(x)$ denotes the quadratic form of discriminant δ:

$$Q(x) = \sum_{1}^{s} \alpha_{ij} x_i x_j, \qquad \delta = |\alpha_{ij}| \neq 0.$$

Received by the editors April 16, 1952.

The total number of solutions of (2.1) with $s=2t$ is

$$(2.2)\qquad \begin{cases} q^{2t-1} - \zeta q^{t-1} & (\alpha \neq 0), \\ q^{2t-1} + \zeta q^{t-1}(q-1) & (\alpha = 0), \end{cases}$$

where $\zeta = +1$ or -1 according as $(-1)^t\delta$ is a square or a nonsquare in $GF(q)$; for $s=2t+1$ the number of solutions is

$$(2.3)\qquad q^{2t} + \omega q^t,$$

where $\omega = +1, -1$, or 0 according as $(-1)^t\alpha\delta$ is a square, a nonsquare, or zero in the field.

Let $\alpha=0$. Then the number of *rational points* on (2.1) is given by

$$(2.4)\qquad N_m = \begin{cases} \dfrac{q^{2mt}-1}{q^m-1} & (s = 2t+1), \\ \dfrac{q^{m(2t-1)}-1}{q^m-1} + \zeta^m q^{m(t-1)} & (s = 2t). \end{cases}$$

A simple computation yields

$$\sum_{m=1}^{\infty} N_m u^{m-1} = \begin{cases} \displaystyle\sum_{r=0}^{2t-1} \frac{q^r}{1-q^r u} & (s = 2t+1), \\ \displaystyle\sum_{r=0}^{2t-2} \frac{q^r}{1-q^r u} + \frac{\zeta q^{t-1}}{1-\zeta q^{t-1}u} & (s = 2t). \end{cases}$$

Then using the notation of (1.1) we get

$$(2.5)\qquad Z(u) = \begin{cases} \displaystyle\prod_{r=0}^{2t-1} (1-q^r u)^{-1} & (s = 2t+1), \\ (1-\zeta q^{t-1})^{-1} \displaystyle\prod_{r=0}^{2t-2} (1-q^r u)^{-1} & (s = 2t). \end{cases}$$

In particular we note that (1.2) holds and that $k=2t$ for $s=2t+1$, $k=2t-2$ for $s=2t$.

A word may be added about the case $\alpha \neq 0$. Let $N_m(\alpha)$ represent the number of solutions over $GF(q^m)$ and let N_m^* represent the number of rational points on $Q(x_1, \cdots, x_s) = \alpha x_{s+1}^2$; also let $Z(u, \alpha)$ and $Z^*(u)$ denote the corresponding Z-functions. Clearly $N_m(\alpha) = N_m^* - N_m$ and it follows that

$$(2.6)\qquad Z(u, \alpha) = \frac{Z^*(u)}{Z(u)} \qquad (\alpha \neq 0).$$

Alternatively it follows directly from (2.2) and (2.3) that

$$Z(u,\alpha)=\begin{cases}(1-\zeta q^{t-1}u)(1-q^{2t-1}u)^{-1} & (s=2t),\\ (1-\omega q^{t}u)^{-1}(1-q^{2t}u)^{-1} & (s=2t+1);\end{cases} \tag{2.7}$$

it is easily verified that (2.6) and (2.7) are in agreement.

3. Let e, f be fixed integers $\geqq 1$ and suppose $(e, f)=1$. It is not difficult to show that the total number of solutions of

$$\alpha_1 x_1^e y_1^f + \cdots + \alpha_s x_s^e y_s^f = 0 \tag{3.1}$$

is $q^{2s-1}+(q-1)q^{s-1}$, and therefore the number of rational points over $GF(q^m)$ is given by

$$N_m = \frac{q^{m(2s-1)}-1}{q^m-1} + q^{m(s-1)}. \tag{3.2}$$

Comparison of (3.2) with the second of (2.2) indicates that Weil's conjecture holds for (3.1). We remark that for $ef>1$, the variety defined by (3.1) contains singular points.

If we waive the condition $(e, f)=1$ then the number of solutions, when obtainable, is not quite so simple. For example we can determine the number of solutions of

$$\alpha_1 x_1^2 y_1^2 + \cdots + \alpha_s x_s^2 y_s^2 = 0, \tag{3.3}$$

but the corresponding function $Z(u)$ is rather complicated.

For the equation

$$\alpha_1 x_1^e y_1^f z_1^g + \cdots + \alpha_s x_s^e y_s^f z_s^g = 0, \tag{3.4}$$

where $(e, f, g)=1$, we have

$$N_m = \frac{q^{m(3s-1)}-1}{q^m-1} + (2q^m-1)^s q^{m(s-1)}.$$

A simple calculation now yields

$$Z(u) = \prod_{r=0}^{s} (1-q^{r+s-1}u)^{-(-1)^{s-r}C_{s,r}2^r} \prod_{r=0}^{3s-2} (1-q^r u)^{-1}. \tag{3.5}$$

It can be verified that (3.5) implies

$$Z\left(\frac{1}{q^{3s-2}u}\right) = (-1)^{s-1}q^{9s(s-1)/2}u^{3s-1}\prod_{r=0}^{s} (1-q^{r+s-1}u)^{-(-1)^r C_{s,r}2^{s-r}} \cdot \prod_{r=0}^{3s-2} (1-q^r u)^{-1},$$

so that (1.2) is not quite satisfied.

4. Returning to (2.1) the weighted sum

$$\sum_{Q(x)=\gamma} e(2\lambda_1 x_1 + \cdots + 2\lambda_s x_s), \tag{4.1}$$

where

$$e(\lambda) = e^{2\pi i t(\lambda)/p}, \qquad t(\lambda) = \lambda + \lambda^p + \cdots + \lambda^{p^{m-1}},$$

is of interest. In particular for $\gamma = 0$, (4.1) can be evaluated explicitly and indeed reduces to (2.2) and (2.3), where now

$$\alpha = Q'(\lambda_1, \cdots, \lambda_s)$$

and Q' denotes the quadratic form inverse to Q. Thus (2.4) and (2.5) may be thought of as applying in this case also. For $\gamma \neq 0$ the situation is somewhat more complicated.

5. A problem that includes (2.1) is that of the number of solutions of

$$Q(U_1, \cdots, U_s) = A \tag{5.1}$$

in polynomials $U_i \in GF[q, x]$, deg $U_i < r$. Clearly this problem is equivalent to the determination of the number of solutions of a certain system of equations of the form (2.1). We shall consider only the case $A = 0$, $s = 2t$. Then Cohen [1, p. 556] has found that the number of solutions of (5.1) is

$$\zeta^r q^{rt} + (q^t - \zeta) q^{(t-1)(2r-1)} \sum_{i=0}^{r-1} \zeta^i q^{-i(t-2)},$$

where ζ has the same meaning as in (2.2). Thus the corresponding value of N_m is

$$\zeta^{mr} q^{m(rt-1)} + \sum_{i=0}^{2r(t-1)} q^{mi(t-1)} + \sum_{i=1}^{r-1} \zeta^{mi} q^{m(2rt-2r-1)-mi(t-2)}(q^m + 1),$$

and therefore

$$\begin{aligned} Z(u) = &\prod_{i=1}^{r} (1 - \zeta^i q^{2rt-2r-1-i(t-2)} u)^{-1} \\ &\cdot \prod_{i=1}^{r-1} (1 - \zeta^i q^{2rt-2r-i(t-2)} u)^{-1} \prod_{i=0}^{2r(t-1)} (1 - q^i u)^{-1}. \end{aligned} \tag{5.2}$$

It is easily verified that each product in the right member of (5.2) satisfies an equation of the form (1.2).

References

1. Eckford Cohen, *Sums of an even number of squares in GF[p^n, x]. II*, Duke Math. J. vol. 14 (1947) pp. 543–557.

2. André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 497–508.

DUKE UNIVERSITY

CONGRUENCES CONNECTED WITH THREE-LINE LATIN RECTANGLES

L. CARLITZ

1. Introduction. In a recent paper [1], J. Riordan set up the recurrences

$$K_n = n^2K_{n-1} + (n)_2K_{n-2} + 2(n)_3K_{n-3} + k_n, \tag{1.1}$$

where $(n)_r = n(n-1)\cdots(n-r+1)$, and

$$k_n + nk_{n-1} = -(n-1)2^n; \tag{1.2}$$

here $K_n = K(3, n)$, the number of reduced three-line latin rectangles. He also proved the congruences

$$k_{n+p} \equiv 2k_n, \qquad K_{n+p} \equiv 2K_n \pmod{p}, \tag{1.3}$$

where p is a prime >2.

In the present note we shall extend (1.3). We show first that for arbitrary m,

$$k_{n+m} \equiv 2^m k_n, \qquad K_{n+m} \equiv 2^m K_n \pmod{m}. \tag{1.4}$$

More generally if we define

$$\Delta f(n) = f(n+m) - 2^m f(n), \qquad \Delta^s f(n) = \Delta\Delta^{s-1}f(n) \tag{1.5}$$

for fixed $m \geqq 1$, then

$$\Delta^r k_n \equiv 0 \equiv \Delta^r K_n \pmod{m^r} \tag{1.6}$$

for all $r \geqq 1$.

2. Proof of (1.4). In (1.2) replace n by $n+m$ so that

Presented to the Society, June 21, 1952; received by the editors April 16, 1952.