Proc. Indian Acad. Sci. (Math. Sci.) Vol. 115, No. 1, February 2005, pp. 1–14.

Zeta function of the projective curve $aY^{2l} = bX^{2l} + cZ^{2l}$ over a class of finite fields, for odd primes l

N ANURADHA

Institute of Mathematical Sciences, C.I.T. Campus, Taramani, Chennai 600 113, India
E-mail: anuradha@imsc.res.in

MS received 18 June 2003

Abstract. Let p and l be rational primes such that l is odd and the order of p modulo l is even. For such primes p and l, and for $e = l, 2l$, we consider the non-singular projective curves $aY^e = bX^e + cZ^e$ $(abc \neq 0)$ defined over finite fields $\mathbf{F}_q$ such that $q = p^\alpha \equiv 1 (\bmod\ e)$. We see that the Fermat curves correspond precisely to those curves among each class (for $e = l, 2l$), that are maximal or minimal over $\mathbf{F}_q$. We observe that each Fermat prime gives rise to explicit maximal and minimal curves over finite fields of characteristic 2. For $e = 2l$, we explicitly determine the ζ-function(s) for this class of curves, over $\mathbf{F}_q$, as rational functions in the variable t, for distinct cases of a, b, and c, in $\mathbf{F}_q^*$. The ζ-function in each case is seen to satisfy the Weil conjectures (now theorems) for this concrete class of curves.

For $e = l, 2l$, we determine the class numbers for the function fields associated to each class of curves over $\mathbf{F}_q$. As a consequence, when the field of definition of the curve(s) is fixed, this provides concrete information on the growth of class numbers for constant field extensions of the function field(s) of the curve(s).

Keywords. Finite fields; curves; maximal curves; zeta functions; function fields.

1. Introduction

Let p and l be rational primes such that l is odd and the order of p modulo l, written as ord $p(\bmod l)$, is even. Let $f = \text{ord } p(\bmod l)$; this is defined to be the least positive integer such that $p^f \equiv 1(\bmod l)$. For such primes p and l, we consider finite fields $\mathbf{F}_q$ such that $q = p^\alpha \equiv 1(\bmod e)$, for $e = l, 2l$; thus $\alpha = fs$ for some integer $s \geq 1$. If $e = 2l$, clearly p is odd.

In ([1], Theorems 6, 7), we had considered the non-singular projective curves $aY^e = bX^e + cZ^e$ $(abc \neq 0$, and $e = l, 2l)$ defined over such finite fields $\mathbf{F}_q$, and had explicitly obtained the number of $\mathbf{F}_{q^n}$-rational points on these curves for each integer $n \geq 1$. This was done by applying explicit results obtained in [1] for the cyclotomic numbers of order e over $\mathbf{F}_q$.

Further, for the case $e = l$, we had obtained in ([1], Theorem 8) the explicit ζ-function(s) for this class of curves defined over $\mathbf{F}_q$. In this paper, we consider the case $e = 2l$ and apply the results of ([1], Theorem 7) to obtain the explicit ζ-function(s), in Theorem 1 (§3), for the class of non-singular projective curves $aY^{2l} = bX^{2l} + cZ^{2l}$ $(abc \neq 0)$ defined over $\mathbf{F}_q$, as rational function(s) in the variable t. We do this for all distinct cases of a, b, and c, in $\mathbf{F}_q^*$. There are seven distinct cases, and the ζ-function in each case is seen to satisfy the Weil conjectures (proven in generality) for this concrete class of curves.

In §2, we define maximal and minimal curves over finite fields, and we interpret the results obtained in ([1], Theorems 6, 7), in this context, to link these results with facts previously known in the literature. In addition, we make some simple but pertinent observations pertaining to these results.

In §3, as a consequence to the explicit ζ-functions obtained in Theorem 1 and ([1], Theorem 8), for the projective curves $aY^e = bX^e + cZ^e$ $(e = l, 2l)$ defined over $\mathbf{F}_q$, we obtain the class numbers of the associated function fields in Theorems 2 and 3, for all distinct cases of $a, b, c \in \mathbf{F}_q^*$. Further, for $e = l, 2l$, if we fix the field of definition $\mathbf{F}_q$, and consider the curve(s) over all finite extensions of $\mathbf{F}_q$, these results provide concrete information on the growth of class numbers for constant field extensions of the function field of the curve(s) over $\mathbf{F}_q$.

For easy reference, we restate ([1], Theorems 6, 7) as Lemmas 1 and 2 below:

Lemma 1 ([1], Theorem 6). *Let p be any prime such that $f = \text{ord}\ p (\text{mod}\ l)$ is even. Let $q = p^\alpha \equiv 1 (\text{mod}\ l)$, and $\alpha = fs$ for some integer $s \geq 1$. Consider the projective curve $aY^l = bX^l + cZ^l$ $(abc \neq 0)$ defined over the finite field $\mathbf{F}_q$. Fix any generator γ of $\mathbf{F}_q^*$ and let $\text{ind}_\gamma (b/c) \equiv i (\text{mod}\ l)$ and $\text{ind}_\gamma (a/c) \equiv j (\text{mod}\ l)$. Then for each $n \geq 1$, the number $a_l(n)$ of $\mathbf{F}_{q^n}$-rational points on this curve is given as below*:

$$a_l(n) = q^n + 1 - (l-1)(l-2)(-1)^{ns} q^{n/2}, \quad if\ \ in, jn \equiv 0 (\text{mod}\ l),$$

$$a_l(n) = q^n + 1 - 2(-1)^{ns} q^{n/2}, \quad if\ \ in, jn, in - jn \not\equiv 0 (\text{mod}\ l),$$

$$a_l(n) = q^n + 1 + (l-2)(-1)^{ns} q^{n/2}, \quad in\ all\ other\ cases\ of\ in,\ jn (\text{mod}\ l).$$

Lemma 2 ([1], Theorem 7). *Let p be an odd prime such that $f = \text{ord}\ p (\text{mod}\ l)$ is even. Let $q = p^\alpha \equiv 1 (\text{mod}\ 2l)$, and $\alpha = fs$ for some integer $s \geq 1$. Consider the projective curve $aY^{2l} = bX^{2l} + cZ^{2l}$ $(abc \neq 0)$ defined over the finite field $\mathbf{F}_q$. Fix any generator γ of $\mathbf{F}_q^*$ and let $\text{ind}_\gamma (b/c) \equiv i (\text{mod}\ 2l)$ and $\text{ind}_\gamma (a/c) \equiv j (\text{mod}\ 2l)$. Then for each $n \geq 1$, the number $a_{2l}(n)$ of $\mathbf{F}_{q^n}$-rational points on this curve is given as below*:

$$a_{2l}(n) = q^n + 1 - (2l-1)(2l-2)(-1)^{ns} q^{n/2}, \quad if\ \ in, jn \equiv 0 (\text{mod}\ 2l),$$

$$a_{2l}(n) = q^n + 1 - 2(-1)^{ns} q^{n/2}, \quad if\ \ in, jn, in - jn \not\equiv 0 (\text{mod}\ 2l),$$

$$a_{2l}(n) = q^n + 1 + 2(l-1)(-1)^{ns} q^{n/2}, \quad in\ all\ other\ cases\ of\ in,\ jn (\text{mod}\ 2l).$$

2. Maximal curves defined over finite fields

Denote by $C/\mathbf{F}_q$ a non-singular projective algebraic curve C defined over a finite field $\mathbf{F}_q$. Denote by $a(n, C)$ the number of $\mathbf{F}_{q^n}$-rational points on C, for each integer $n \geq 1$. Let $g \geq 0$ be the genus of C. The Weil conjectures for the curve C state that the ζ-function of C over $\mathbf{F}_q$, which is defined as

$$Z(t, C) = Z(t, C/\mathbf{F}_q) = \exp\left(\sum_{n=1}^{\infty} \frac{a(n, C) t^n}{n}\right),$$

satisfies the following properties:

1. $Z(t, C)$ is a rational function in the variable t of the form $P(t)/(1-t)(1-qt)$, where $P(t)$ is a polynomial in t of degree $2g$, having integer coefficients, leading term q^g, and constant term 1.
2. $Z(t, C)$ satisfies a functional equation given by

$$q^{g-1}t^{2g-2}Z(1/qt, C) = Z(t, C).$$

   Equivalently, if we express $P(t) = \prod_{k=1}^{2g}(1-\alpha_k t)$, we may pair the α_k's in such a way that $\alpha_k\alpha_{g+k} = q$ for $1 \leq k \leq g$.
3. The reciprocal roots α_k of $P(t)$ satisfy the property that $|\alpha_k| = q^{1/2}$ for $1 \leq k \leq 2g$. This is known as the Riemann hypothesis for $C/\mathbf{F}_q$.

These conjectures were first stated (in full generality) by André Weil [15] in 1949, for non-singular projective varieties of dimension ≥ 1 defined over finite fields. Curves are varieties of dimension 1. These conjectures have been proven in complete generality (see, for example, [2]). For a proof of these conjectures for curves, see [10].

The first general proof of these conjectures for *curves* was given by Weil [14]. He showed that for such a curve $C/\mathbf{F}_q$,

$$a(n, C) = q^n + 1 - \sum_{k=1}^{2g} \alpha_k^n, \quad \text{for each } n \geq 1.$$

As a consequence of the Riemann hypothesis for $C/\mathbf{F}_q$, he obtained the following bounds on $a(n, C)$, given by

$$|a(n, C) - (q^n + 1)| \leq 2gq^{n/2}, \quad \text{for each } n \geq 1.$$

These bounds, and a proof of the Riemann hypothesis, were earlier obtained by Hasse in 1936 for curves of genus $g = 1$ (or elliptic curves), and have come to be known as the Hasse–Weil bounds for the curve C, sometimes simply referred to as the Weil bounds for C.

There has been considerable interest and search in the literature for curves $C/\mathbf{F}_q$ for which the upper Weil bounds are attained for the number of $\mathbf{F}_q$-rational points on C. Such curves are called maximal, and the associated function fields are called maximal function fields. Maximal curves are of theoretical interest; they provide examples of curves with large automorphism groups, and have interesting arithmetic and geometric properties (cf. [3, 8, 9, 11, 12]). Such curves, and curves $C/\mathbf{F}_q$ with large number of $\mathbf{F}_q$-rational points, find important applications in coding theory, since the construction by Goppa of codes with good parameters from such curves (cf. [4, 5]).

In keeping with the terminology for maximal curves, one may define minimal curves to be curves $C/\mathbf{F}_q$ for which the lower Weil bounds are attained for the number of $\mathbf{F}_q$-rational points on C (i.e, $a(1, C) = q + 1 - 2gq^{1/2}$). It is clear from the expression for the Weil bounds that curves $C/\mathbf{F}_q$ are maximal or minimal only when q is a square (even power of p), or the genus $g = 0$.

As a special case of the curves treated in Lemmas 1 and 2, consider the Fermat curves $Y^e = X^e + Z^e$ (for $e = l, 2l$) defined over finite fields $\mathbf{F}_q$, $q = p^\alpha \equiv 1 (\text{mod } e)$, when $f = \text{ord } p (\text{mod } l)$ is even. If we fix $q = p^f$, it is clear from Lemmas 1 and 2 that these curves are maximal over finite odd degree extensions of $\mathbf{F}_q$, and are minimal over finite

even degree extensions of $\mathbf{F}_q$. It would thus appear that there is a close inter-relationship between maximal and minimal curves defined over finite fields.

Further, keeping $q = p^f$, if we write $q - 1 = et$, for $e = l, 2l$, and $t \geq 1$, then since $f = \text{ord } p(\text{mod } l)$, it follows that $q^{1/2} + 1 = et'$ for some $t' \geq 1, t'|t$. For $t' = 1$, the corresponding Fermat curves are then defined by

$$Y^{q^{1/2}+1} = X^{q^{1/2}+1} + Z^{q^{1/2}+1}$$

over the finite field $\mathbf{F}_q$. These are just the Hermitian curves which have been studied in the literature and known to be maximal over $\mathbf{F}_q$. The corresponding function fields are called Hermitian function fields. Hermitian curves have been characterized as the (essentially) unique maximal curves over $\mathbf{F}_q$ with genus $g = q^{1/2}(q^{1/2} - 1)/2$. This is the maximum possible genus for a maximal curve defined over $\mathbf{F}_q$ (cf. [6, 11]). For $t' > 1$, we have $e|q^{1/2} + 1$, and the corresponding Fermat curves are again known to be maximal over $\mathbf{F}_q$; these are not Hermitian, but the function fields associated to these curves occur as subfields of the Hermitian function field (cf. ([13], pp. 196–203)).

The case when l is a Fermat prime is interesting; if $l = 2^{2^n} + 1$, the corresponding Fermat curve $Y^l = X^l + Z^l$ is a Hermitian curve over the finite field $\mathbf{F}_q$, $q = 2^{2^{n+1}}$, of characteristic 2, with genus $g = 2^{2^n-1}(2^{2^n} - 1)$. Further, as observed above, these curves are maximal (resp. minimal) over finite odd degree (resp. even degree) extensions of $\mathbf{F}_q$. Thus each Fermat prime gives rise to explicit maximal and minimal curves over finite fields of characteristic 2. The converse, however, is not true. For example, take $n = 5$; then $r = 2^{2^5} + 1$ is *not* a prime, but the corresponding Fermat curve $Y^r = X^r + Z^r$ is maximal (or minimal) over finite extensions of the field $\mathbf{F}_q$, $q = 2^{2^6}$.

From the explicit results in Lemmas 1 and 2, it is also clear that the only class of coefficients a, b, c in $\mathbf{F}_q^*$ for which the curves $aY^e = bX^e + cZ^e$ are maximal (or minimal) over $\mathbf{F}_q$ are those that correspond to the Fermat curves $Y^e = X^e + Z^e$ (for $e = l, 2l$) (i.e., the coefficients reduce to the case $a = b = c = 1$). The cases for a, b, c which do not correspond to the Fermat curves are *never* maximal or minimal. (Note that in Lemma 1, for $l = 3$, we have $f = \text{ord } p(\text{mod } 3) = 2$, and $q = p^{2s}$. For s odd, each element of $\mathbf{F}_{p^s}^*$ is a cube, and hence, all cases when $a, b, c \in \mathbf{F}_{p^s}^*$ correspond to the Fermat curve $Y^3 = X^3 + Z^3$, and this curve is maximal over $\mathbf{F}_q$.)

3. Zeta function(s) of the projective curve $aY^{2l} = bX^{2l} + cZ^{2l}$ over $\mathbf{F}_q$

Theorem 1. *Let p and l be odd rational primes such that $f = \text{ord } p(\text{mod } l)$ is even. Consider the projective curve $C: aY^{2l} = bX^{2l} + cZ^{2l}$ $(abc \neq 0)$ defined over the finite field $\mathbf{F}_q$, where $q = p^\alpha \equiv 1(\text{mod } 2l)$, and $\alpha = fs$ for $s \geq 1$. Fix a generator γ of $\mathbf{F}_q^*$ and let $\text{ind}_\gamma(b/c) \equiv i(\text{mod } 2l)$ and $\text{ind}_\gamma(a/c) \equiv j(\text{mod } 2l)$. Let $\theta = (-1)^s q^{1/2}$ and let ζ be any primitive (complex) l-th root of unity. Then the ζ-function $Z(t, C)$ of the curve $C/\mathbf{F}_q$ is a rational function in the variable t, of the form $P(t)/(1 - t)(1 - qt)$, and the polynomial $P(t)$ is given explicitly for distinct cases of $i, j(\text{mod } 2l)$ as below*:

1. *For $i \equiv j \equiv 0(\text{mod } 2l)$,*

$$P(t) = (1 - \theta t)^{(2l-1)(2l-2)}.$$

2. *For* $i, j \equiv 0 (\mathrm{mod}\ 2)$, $i, j, i - j \not\equiv 0 (\mathrm{mod}\ 2l)$,

$$P(t) = (1 - \theta t)^{4l-4} \prod_{r=1}^{l-1} (1 - \zeta^r \theta t)^{4l-6}.$$

3. *For* $i, j \equiv 0 (\mathrm{mod}\ 2)$ *and* (i) $i \equiv 0$, $j \not\equiv 0 (\mathrm{mod}\ 2l)$, (ii) $i \not\equiv 0$, $j \equiv 0 (\mathrm{mod}\ 2l)$, (iii) $i, j \not\equiv 0$, $i \equiv j (\mathrm{mod}\ 2l)$,

$$P(t) = (1 - \theta t)^{2l-2} \prod_{r=1}^{l-1} (1 - \zeta^r \theta t)^{4l-4}.$$

4. *For* (i) $i \equiv 0$, $j \equiv l (\mathrm{mod}\ 2l)$, (ii) $i \equiv l$, $j \equiv 0 (\mathrm{mod}\ 2l)$, *and* (iii) $i \equiv j \equiv l (\mathrm{mod}\ 2l)$,

$$P(t) = (1 - \theta t)^{2(l-1)^2} (1 + \theta t)^{2l(l-1)}.$$

5. *For* (i) $j \not\equiv 0 (\mathrm{mod}\ 2)$, $i \equiv 0$, $j \not\equiv l (\mathrm{mod}\ 2l)$, (ii) $i \not\equiv 0 (\mathrm{mod}\ 2)$, $i \not\equiv l$, $j \equiv 0 (\mathrm{mod}\ 2l)$, *and* (iii) $i \not\equiv 0 (\mathrm{mod}\ 2)$, $i \equiv j$, $i \not\equiv l (\mathrm{mod}\ 2l)$,

$$P(t) = (1 + \theta t)^{2l-2} \prod_{r=1}^{l-1} ((1 - \zeta^r \theta t)(1 + \zeta^r \theta t))^{2l-2}$$

$$= \prod_{r=1}^{2l-1} (1 - \xi^r \theta t)^{2l-2},$$

where ξ *is a primitive complex* $2l$*-th root of unity.*

6. *For* $i, j, i - j \not\equiv 0, l (\mathrm{mod}\ 2l)$ *and* (i) $i \not\equiv j (\mathrm{mod}\ 2)$, (ii) $i, j \not\equiv 0 (\mathrm{mod}\ 2)$,

$$P(t) = ((1 - \theta t)(1 + \theta t))^{2l-2} \prod_{r=1}^{l-1} ((1 - \zeta^r \theta t)^{2l-4} (1 + \zeta^r \theta t)^{2l-2}).$$

7. *For* (i) $i \equiv l$, $j \not\equiv 0, l (\mathrm{mod}\ 2l)$, (ii) $i \not\equiv 0, l$, $j \equiv l (\mathrm{mod}\ 2l)$, *and* (iii) $i, j \not\equiv 0, l$, $i - j \equiv l (\mathrm{mod}\ 2l)$,

$$P(t) = ((1 - \theta t)(1 + \theta t))^{l-1} \prod_{r=1}^{l-1} ((1 - \zeta^r \theta t)^{2l-3} (1 + \zeta^r \theta t)^{2l-1}).$$

Proof. The number $a_{2l}(n)$ of $\mathbf{F}_{q^n}$-rational points on the curve C, for each $n \geq 1$, has been determined explicitly in ([1], Theorem 7) (cf. Lemma 2 above). Taking into account the distinct cases that arise when $l | n$, $l \not| n$, $2 | n$, and $2 \not| n$, and substituting the corresponding values for $a_{2l}(n)$ in the definition of $Z(t, C)$, we obtain the ζ-function of the curve $C/\mathbf{F}_q$, for distinct cases of $i, j (\mathrm{mod}\ 2l)$, as below:

1. For $i \equiv j \equiv 0 (\mathrm{mod}\ 2l)$,

$$\log Z(t, C) = \sum_{n=1}^{\infty} \frac{(q^n + 1 - (2l-1)(2l-2)(-1)^{ns} q^{n/2}) t^n}{n}$$

$$= \log \frac{1}{1 - qt} + \log \frac{1}{1 - t} - (2l-1)(2l-2)$$

$$\times \log \frac{1}{1 - (-1)^s q^{1/2} t}.$$

Hence

$$Z(t, C) = \frac{(1 - (-1)^s q^{1/2} t)^{(2l-1)(2l-2)}}{(1-t)(1-qt)}.$$

2. For $i, j \equiv 0 (\mathrm{mod}\ 2)$, $i, j, i - j \not\equiv 0 (\mathrm{mod}\ 2l)$,

$$\begin{aligned}
\log Z(t, C) &= \sum_{l|n} \frac{a_{2l}(n) t^n}{n} + \sum_{l \not| n} \frac{a_{2l}(n) t^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{(q^{ln} + 1 - (2l-1)(2l-2)(-1)^{lns} q^{ln/2}) t^{ln}}{ln} \\
&\quad + \sum_{n=1}^{\infty} \frac{(q^n + 1 - 2(-1)^{ns} q^{n/2}) t^n}{n} \\
&\quad - \sum_{n=1}^{\infty} \frac{(q^{ln} + 1 - 2(-1)^{lns} q^{ln/2}) t^{ln}}{ln} \\
&= \sum_{n=1}^{\infty} \frac{(q^n + 1 - 2(-1)^{ns} q^{n/2}) t^n}{n} \\
&\quad - (4l-6) \sum_{n=1}^{\infty} \frac{(-1)^{lns} q^{ln/2} t^{ln}}{n} \\
&= \log \frac{1}{1-qt} + \log \frac{1}{1-t} - 2 \log \frac{1}{1 - (-1)^s q^{1/2} t} \\
&\quad - (4l-6) \log \frac{1}{1 - (-1)^{ls} q^{l/2} t^l}.
\end{aligned}$$

Hence

$$\begin{aligned}
Z(t, C) &= \frac{(1 - (-1)^s q^{1/2} t)^2 (1 - (-1)^{ls} q^{l/2} t^l)^{4l-6}}{(1-t)(1-qt)} \\
&= \frac{(1 - \theta t)^{4l-4} \prod_{r=1}^{l-1} (1 - \zeta^r \theta t)^{4l-6}}{(1-t)(1-qt)}.
\end{aligned}$$

3. For $i, j \equiv 0 (\mathrm{mod}\ 2)$ and (i) $i \equiv 0,\ j \not\equiv 0 (\mathrm{mod}\ 2l)$, (ii) $i \not\equiv 0,\ j \equiv 0 (\mathrm{mod}\ 2l)$, (iii) $i, j \not\equiv 0,\ i \equiv j (\mathrm{mod}\ 2l)$,

$$\begin{aligned}
\log Z(t, C) &= \sum_{l|n} \frac{a_{2l}(n) t^n}{n} + \sum_{l \not| n} \frac{a_{2l}(n) t^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{(q^{ln} + 1 - (2l-1)(2l-2)(-1)^{lns} q^{ln/2}) t^{ln}}{ln} \\
&\quad + \sum_{n=1}^{\infty} \frac{(q^n + 1 + 2(l-1)(-1)^{ns} q^{n/2}) t^n}{n}
\end{aligned}$$

$$
\begin{aligned}
&- \sum_{n=1}^{\infty} \frac{(q^{ln} + 1 + 2(l-1)(-1)^{lns} q^{ln/2}) t^{ln}}{ln} \\
&= \sum_{n=1}^{\infty} \frac{(q^n + 1 + 2(l-1)(-1)^{ns} q^{n/2}) t^n}{n} \\
&\quad - (4l-4) \sum_{n=1}^{\infty} \frac{(-1)^{lns} q^{ln/2} t^{ln}}{n} \\
&= \log \frac{1}{1-qt} + \log \frac{1}{1-t} + 2(l-1) \log \frac{1}{1-(-1)^s q^{1/2} t} \\
&\quad - (4l-4) \log \frac{1}{1-(-1)^{ls} q^{l/2} t^l}.
\end{aligned}
$$

It follows that

$$
\begin{aligned}
Z(t, C) &= \frac{(1-(-1)^{ls} q^{l/2} t^l)^{4l-4}}{(1-t)(1-qt)(1-(-1)^s q^{1/2} t)^{2l-2}} \\
&= \frac{(1-\theta t)^{2l-2} \prod_{r=1}^{l-1} (1-\zeta^r \theta t)^{4l-4}}{(1-t)(1-qt)}.
\end{aligned}
$$

4. For (i) $i \equiv 0,\ j \equiv l \pmod{2l}$, (ii) $i \equiv l,\ j \equiv 0 \pmod{2l}$, and (iii) $i \equiv j \equiv l \pmod{2l}$,

$$
\begin{aligned}
\log Z(t, C) &= \sum_{2|n} \frac{a_{2l}(n) t^n}{n} + \sum_{2 \nmid n} \frac{a_{2l}(n) t^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{(q^{2n} + 1 - (2l-1)(2l-2)(-1)^{2ns} q^{2n/2}) t^{2n}}{2n} \\
&\quad + \sum_{n=1}^{\infty} \frac{(q^n + 1 + 2(l-1)(-1)^{ns} q^{n/2}) t^n}{n} \\
&\quad - \sum_{n=1}^{\infty} \frac{(q^{2n} + 1 + 2(l-1)(-1)^{2ns} q^{2n/2}) t^{2n}}{2n} \\
&= \sum_{n=1}^{\infty} \frac{(q^n + 1 + 2(l-1)(-1)^{ns} q^{n/2}) t^n}{n} \\
&\quad - 2l(l-1) \sum_{n=1}^{\infty} \frac{(-1)^{2ns} q^{2n/2} t^{2n}}{n} \\
&= \log \frac{1}{1-qt} + \log \frac{1}{1-t} + 2(l-1) \log \frac{1}{1-(-1)^s q^{1/2} t} \\
&\quad - 2l(l-1) \log \frac{1}{1-(-1)^{2s} q t^2}.
\end{aligned}
$$

It follows that

$$Z(t, C) = \frac{(1-(-1)^{2s}qt^2)^{2l(l-1)}}{(1-t)(1-qt)(1-(-1)^s q^{1/2}t)^{2(l-1)}}$$
$$= \frac{(1-\theta t)^{2(l-1)^2}(1+\theta t)^{2l(l-1)}}{(1-t)(1-qt)}.$$

5. For (i) $j \not\equiv 0 (\mathrm{mod}\ 2)$, $i \equiv 0$, $j \not\equiv l (\mathrm{mod}\ 2l)$, (ii) $i \not\equiv 0 (\mathrm{mod}\ 2)$, $i \not\equiv l$, $j \equiv 0 (\mathrm{mod}\ 2l)$, and (iii) $i \not\equiv 0 (\mathrm{mod}\ 2)$, $i \equiv j$, $i \not\equiv l (\mathrm{mod}\ 2l)$,

$$\log Z(t, C) = \sum_{2l|n} \frac{a_{2l}(n)t^n}{n} + \sum_{2l \not| n} \frac{a_{2l}(n)t^n}{n}$$
$$= \sum_{n=1}^{\infty} \frac{(q^{2ln} + 1 - (2l-1)(2l-2)(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}$$
$$+ \sum_{n=1}^{\infty} \frac{(q^n + 1 + 2(l-1)(-1)^{ns}q^{n/2})t^n}{n}$$
$$- \sum_{n=1}^{\infty} \frac{(q^{2ln} + 1 + 2(l-1)(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}$$
$$= \sum_{n=1}^{\infty} \frac{(q^n + 1 + 2(l-1)(-1)^{ns}q^{n/2})t^n}{n}$$
$$- 2(l-1) \sum_{n=1}^{\infty} \frac{(-1)^{2lns}q^{2ln/2}t^{2ln}}{n}$$
$$= \log \frac{1}{1-qt} + \log \frac{1}{1-t} + 2(l-1) \log \frac{1}{1-(-1)^s q^{1/2}t}$$
$$- 2(l-1) \log \frac{1}{1-(-1)^{2ls}q^l t^{2l}}.$$

This implies that

$$Z(t, C) = \frac{(1-(-1)^{2ls}q^l t^{2l})^{2l-2}}{(1-t)(1-qt)(1-(-1)^s q^{1/2}t)^{2l-2}}$$
$$= \frac{(1+\theta^l t^l)^{2l-2} \prod_{r=1}^{l-1}(1-\zeta^r \theta t)^{2l-2}}{(1-t)(1-qt)}.$$

6. For $i, j, i-j \not\equiv 0, l (\mathrm{mod}\ 2l)$ and (i) $i \not\equiv j (\mathrm{mod}\ 2)$, (ii) $i, j \not\equiv 0 (\mathrm{mod}\ 2)$,

$$\log Z(t, C) = \sum_{2l|n} \frac{a_{2l}(n)t^n}{n} + \sum_{2 \not| n,\ l|n} \frac{a_{2l}(n)t^n}{n} + \sum_{l \not| n} \frac{a_{2l}(n)t^n}{n}$$
$$= \sum_{n=1}^{\infty} \frac{(q^{2ln} + 1 - (2l-1)(2l-2)(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}$$

$$
\begin{aligned}
&+\sum_{n=1}^{\infty}\frac{(q^{ln}+1+2(l-1)(-1)^{lns}q^{ln/2})t^{ln}}{ln}\\
&-\sum_{n=1}^{\infty}\frac{(q^{2ln}+1+2(l-1)(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}\\
&+\sum_{n=1}^{\infty}\frac{(q^{n}+1-2(-1)^{ns}q^{n/2})t^{n}}{n}\\
&-\sum_{n=1}^{\infty}\frac{(q^{ln}+1-2(-1)^{lns}q^{ln/2})t^{ln}}{ln}\\
=&\sum_{n=1}^{\infty}\frac{(q^{n}+1-2(-1)^{ns}q^{n/2})t^{n}}{n}\\
&-(2l-2)\sum_{n=1}^{\infty}\frac{(-1)^{2lns}q^{2ln/2}t^{2ln}}{n}+2\sum_{n=1}^{\infty}\frac{(-1)^{lns}q^{ln/2}t^{ln}}{n}\\
=&\log\frac{1}{1-qt}+\log\frac{1}{1-t}-2\log\frac{1}{1-(-1)^{s}q^{1/2}t}\\
&-(2l-2)\log\frac{1}{1-(-1)^{2ls}q^{l}t^{2l}}+2\log\frac{1}{1-(-1)^{ls}q^{l/2}t^{l}}.
\end{aligned}
$$

Thus we obtain

$$
\begin{aligned}
Z(t,C)&=\frac{(1-(-1)^{s}q^{1/2}t)^{2}(1-(-1)^{2ls}q^{l}t^{2l})^{2l-2}}{(1-t)(1-qt)(1-(-1)^{ls}q^{l/2}t^{l})^{2}}\\
&=\frac{(1-\theta t)^{2}(1-\theta^{l}t^{l})^{2l-4}(1+\theta^{l}t^{l})^{2l-2}}{(1-t)(1-qt)}.
\end{aligned}
$$

7. For (i) $i\equiv l,\ j\not\equiv 0,l(\mathrm{mod}\ 2l)$, (ii) $i\not\equiv 0,l,\ j\equiv l(\mathrm{mod}\ 2l)$, and (iii) $i,j\not\equiv 0,l,\ i-j\equiv l(\mathrm{mod}\ 2l)$,

$$
\begin{aligned}
\log Z(t,C)=&\sum_{2l|n}\frac{a_{2l}(n)t^{n}}{n}+\sum_{2\not|n,\ l|n}\frac{a_{2l}(n)t^{n}}{n}\\
&+\sum_{2|n,\ l\not|n}\frac{a_{2l}(n)t^{n}}{n}+\sum_{2\not|n,\ l\not|n}\frac{a_{2l}(n)t^{n}}{n}\\
=&\sum_{n=1}^{\infty}\frac{(q^{2ln}+1-(2l-1)(2l-2)(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}\\
&+\sum_{n=1}^{\infty}\frac{(q^{ln}+1+2(l-1)(-1)^{lns}q^{ln/2})t^{ln}}{ln}\\
&-\sum_{n=1}^{\infty}\frac{(q^{2ln}+1+2(l-1)(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}
\end{aligned}
$$

$$
\begin{aligned}
&+\sum_{n=1}^{\infty}\frac{(q^{2n}+1+2(l-1)(-1)^{2ns}q^{2n/2})t^{2n}}{2n}\\
&-\sum_{n=1}^{\infty}\frac{(q^{2ln}+1+2(l-1)(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}\\
&+\sum_{n=1}^{\infty}\frac{(q^{n}+1-2(-1)^{ns}q^{n/2})t^{n}}{n}\\
&-\sum_{n=1}^{\infty}\frac{(q^{2n}+1-2(-1)^{2ns}q^{2n/2})t^{2n}}{2n}\\
&-\sum_{n=1}^{\infty}\frac{(q^{ln}+1-2(-1)^{lns}q^{ln/2})t^{ln}}{ln}\\
&+\sum_{n=1}^{\infty}\frac{(q^{2ln}+1-2(-1)^{2lns}q^{2ln/2})t^{2ln}}{2ln}\\
=&\sum_{n=1}^{\infty}\frac{(q^{n}+1-2(-1)^{ns}q^{n/2})t^{n}}{n}+2\sum_{n=1}^{\infty}\frac{(-1)^{lns}q^{ln/2}t^{ln}}{n}\\
&-(2l-1)\sum_{n=1}^{\infty}\frac{(-1)^{2lns}q^{2ln/2}t^{2ln}}{n}+l\sum_{n=1}^{\infty}\frac{(-1)^{2ns}q^{2n/2}t^{2n}}{n}\\
=&\log\frac{1}{1-qt}+\log\frac{1}{1-t}-2\log\frac{1}{1-(-1)^{s}q^{1/2}t}\\
&+2\log\frac{1}{1-(-1)^{ls}q^{l/2}t^{l}}-(2l-1)\log\frac{1}{1-(-1)^{2ls}q^{l}t^{2l}}\\
&+l\log\frac{1}{1-(-1)^{2s}qt^{2}}.
\end{aligned}
$$

Hence we obtain

$$
\begin{aligned}
Z(t,C)&=\frac{(1-(-1)^{s}q^{1/2}t)^{2}(1-(-1)^{2ls}q^{l}t^{2l})^{2l-1}}{(1-t)(1-qt)(1-(-1)^{ls}q^{l/2}t^{l})^{2}(1-(-1)^{2s}qt^{2})^{l}}\\
&=\frac{(1-\theta^{l}t^{l})^{2l-3}(1+\theta^{l}t^{l})^{2l-1}}{(1-t)(1-qt)(1-\theta t)^{l-2}(1+\theta t)^{l}}\\
&=\frac{((1-\theta t)(1+\theta t))^{l-1}\prod_{r=1}^{l-1}((1-\zeta^{r}\theta t)^{2l-3}(1+\zeta^{r}\theta t)^{2l-1})}{(1-t)(1-qt)}.
\end{aligned}
$$

Hence the theorem. □

The curve C in Theorem 1 is non-singular of degree $2l$; hence it has genus $g=(2l-1)(2l-2)/2$. From the expressions for $P(t)$ in Theorem 1, it is clear that in each case for $i, j \pmod{2l}$,

- $P(t)$ is a polynomial of degree $2g = (2l-1)(2l-2)$ of the form $P(t) = \prod_{k=1}^{2g}(1-\alpha_k t)$, and the α_k's are algebraic integers equal to $\pm q^{1/2}\zeta^r$, $0 \le r \le l-1$. Thus $|\alpha_k| = q^{1/2}$ for $1 \le k \le 2g$.
- We may pair the α_k's in such a way that $\alpha_k \alpha_{g+k} = q$ for $1 \le k \le g$. The polynomial $P(t)$ has integer coefficients (as $q^{1/2}$ is an integer), constant term 1, and leading term q^g (since $\prod_{k=1}^{2g} \alpha_k = q^g$ by the above pairing).

This corroborates the Weil conjectures for the concrete class of curves $C/\mathbf{F}_q$ considered in Theorem 1.

Given a non-singular projective curve X defined over a finite field k, it is well-known that the class number h of the function field of X/k satisfies the relation $h = P(1)$, where $P(t)$ is the polynomial that appears in the numerator of the ζ-function of the curve X/k.

For the curve $C/\mathbf{F}_q$ considered in Theorem 1, and the ζ-function(s) obtained therein, we may thus substitute $t = 1$ in the expressions for the polynomials $P(t)$, to obtain the class number(s) of the associated function field(s) in Theorem 2 below.

Theorem 2. *Consider the projective curve* $C\colon aY^{2l} = bX^{2l} + cZ^{2l}$ $(abc \neq 0)$ *defined over the finite field* $\mathbf{F}_q$, *with notations as in Theorem* 1. *Set* $q_0 = p^f$ *and* $u = \sqrt{q_0}$. *Thus* u *is an integer,* $q = q_0^s$, *and* $\sqrt{q} = u^s$. *For each* $s \ge 1$, *let* K_s *denote the function field of the curve* $C/\mathbf{F}_q$, $q = p^{fs}$, *and let* h_s *denote its class number. Let* $h_s = h_1$ *for* s *odd, and* $h_s = h_2$ *for* s *even. Substituting* $h_s = P(1)$, *we obtain the class numbers* h_1 *and* h_2, *for the seven distinct cases in Theorem* 1, *as below*:

1. *For* $i \equiv j \equiv 0 (\mathrm{mod}\ 2l)$,

$$h_1 = (u^s+1)^{(2l-1)(2l-2)}, \quad h_2 = (u^s-1)^{(2l-1)(2l-2)}.$$

2. *For* $i, j \equiv 0 (\mathrm{mod}\ 2)$, $i, j, i-j \not\equiv 0 (\mathrm{mod}\ 2l)$,

$$h_1 = (u^s+1)^2(u^{ls}+1)^{4l-6}, \quad h_2 = (u^s-1)^2(u^{ls}-1)^{4l-6}.$$

3. *For* $i, j \equiv 0 (\mathrm{mod}\ 2)$ *and* (i) $i \equiv 0$, $j \not\equiv 0 (\mathrm{mod}\ 2l)$, (ii) $i \not\equiv 0$, $j \equiv 0 (\mathrm{mod}\ 2l)$, (iii) $i, j \not\equiv 0$, $i \equiv j (\mathrm{mod}\ 2l)$,

$$h_1 = (u^{ls}+1)^{4l-4}/(u^s+1)^{2l-2}, \quad h_2 = (u^{ls}-1)^{4l-4}/(u^s-1)^{2l-2}.$$

4. *For* (i) $i \equiv 0$, $j \equiv l (\mathrm{mod}\ 2l)$, (ii) $i \equiv l$, $j \equiv 0 (\mathrm{mod}\ 2l)$, *and* (iii) $i \equiv j \equiv l (\mathrm{mod}\ 2l)$,

$$h_1 = (u^s+1)^{2(l-1)^2}(u^s-1)^{2l(l-1)}, \quad h_2 = (u^s-1)^{2(l-1)^2}(u^s+1)^{2l(l-1)}.$$

5. *For* (i) $j \not\equiv 0 (\mathrm{mod}\ 2)$, $i \equiv 0$, $j \not\equiv l (\mathrm{mod}\ 2l)$, (ii) $i \not\equiv 0 (\mathrm{mod}\ 2)$, $i \not\equiv l$, $j \equiv 0 (\mathrm{mod}\ 2l)$, *and* (iii) $i \not\equiv 0 (\mathrm{mod}\ 2)$, $i \equiv j$, $i \not\equiv l (\mathrm{mod}\ 2l)$,

$$h_1 = ((u^{2ls}-1)/(u^s+1))^{2l-2}, \quad h_2 = ((u^{2ls}-1)/(u^s-1))^{2l-2}.$$

6. *For* $i, j, i-j \not\equiv 0, l (\mathrm{mod}\ 2l)$ *and* (i) $i \not\equiv j (\mathrm{mod}\ 2)$, (ii) $i, j \not\equiv 0 (\mathrm{mod}\ 2)$,

$$h_1 = (u^s+1)^2(u^{ls}+1)^{2l-4}(u^{ls}-1)^{2l-2},$$

$$h_2 = (u^s-1)^2(u^{ls}-1)^{2l-4}(u^{ls}+1)^{2l-2}.$$

7. *For* (i) $i \equiv l,\ j \not\equiv 0, l \pmod{2l}$, (ii) $i \not\equiv 0, l,\ j \equiv l \pmod{2l}$, *and* (iii) $i, j \not\equiv 0, l,\ i - j \equiv l \pmod{2l}$,

$$h_1 = (u^{ls}+1)^{2l-3}(u^{ls}-1)^{2l-1}/(u^s+1)^{l-2}(u^s-1)^l,$$
$$h_2 = (u^{ls}-1)^{2l-3}(u^{ls}+1)^{2l-1}/(u^s-1)^{l-2}(u^s+1)^l.$$

For the class of curves $C/\mathbf{F}_q$ considered in Lemma 1, the explicit form of the polynomials $P(t)$ in the ζ-function(s) for $C/\mathbf{F}_q$ were obtained in ([1], Theorem 8). Substituting $t = 1$ in these expressions for $P(t)$, we obtain the class number(s) of the associated function field(s) in Theorem 3 below.

Theorem 3. *Consider the projective curve* $C: aY^l = bX^l + cZ^l$ $(abc \neq 0)$ *defined over the finite field* $\mathbf{F}_q$, *with notations as in Lemma* 1. *Let* $q_0 = p^f$ *and* $u = \sqrt{q_0}$. *Thus* u *is an integer,* $q = q_0^s$, *and* $\sqrt{q} = u^s$. *Let* $\theta = (-1)^s q^{1/2}$ *and let* ζ *be a primitive* (*complex*) l*-th root of unity. For each* $s \geq 1$, *let* K_s *denote the function field of the curve* $C/\mathbf{F}_q$, $q = p^{fs}$, *and let* h_s *denote its class number. Let* $h_s = h_1$ *for* s *odd, and* $h_s = h_2$ *for* s *even. Substituting* $h_s = P(1)$ *in the expressions for the polynomial* $P(t)$ *in the* ζ*-function*(*s*) *of the curve* $C/\mathbf{F}_q$ (*cf.* ([1], *Theorem* 8), *reproduced below*), *we obtain the class numbers* h_1 *and* h_2, *for the distinct cases in Lemma* 1, *as below*:

1. *For* $i, j \equiv 0 \pmod{l}$,

$$P(t) = (1-\theta t)^{(l-1)(l-2)},$$
$$h_1 = (u^s+1)^{(l-1)(l-2)}, \quad h_2 = (u^s-1)^{(l-1)(l-2)}.$$

2. *For* (i) $i \equiv 0 \pmod{l}$, $j \not\equiv 0 \pmod{l}$, (ii) $i \not\equiv 0 \pmod{l}$, $j \equiv 0 \pmod{l}$, *and* (iii) $i, j \not\equiv 0 \pmod{l}$, $i \equiv j \pmod{l}$,

$$P(t) = \prod_{r=1}^{l-1}(1-\zeta^r\theta t)^{l-2},$$
$$h_1 = ((u^{ls}+1)/(u^s+1))^{l-2}, \quad h_2 = ((u^{ls}-1)/(u^s-1))^{l-2}.$$

3. *For* $i, j, i - j \not\equiv 0 \pmod{l}$,

$$P(t) = (1-\theta t)^{l-1}\prod_{r=1}^{l-1}(1-\zeta^r\theta t)^{l-3},$$
$$h_1 = (u^s+1)^2(u^{ls}+1)^{l-3}, \quad h_2 = (u^s-1)^2(u^{ls}-1)^{l-3}.$$

Consider now the projective curves $C/\mathbf{F}_q$ in Theorems 2 and 3 as defined over some fixed base field $\mathbf{F}_q$, $q = p^{fs_0}$, with associated function field K_{s_0}. Then for each $s \geq 1$, the function fields K_{ss_0} of the curves $C/\mathbf{F}_{q^s}$, are isomorphic to the constant field extensions $K_{s_0} \cdot \mathbf{F}_{q^s}$ of the function field K_{s_0}. In this case, the results in Theorems 2 and 3 provide concrete information on the growth of class numbers h_{ss_0} $(s \geq 1)$ for the constant field extensions $K_{s_0} \cdot \mathbf{F}_{q^s}/K_{s_0}$, for each class of curves. Note that in this consideration, two cases arise: (i) for s_0 odd, the results for both h_1 and h_2 come into picture, while (ii) for s_0 even, only the results for h_2 are required.

Concluding Remarks.

1. In Theorem 1, for each distinct case, the roots of the polynomial $P(t)$, all of which lie on the circle $|z| = q^{-1/2}$ in the complex plane, are *not* uniformly distributed on this circle. In each case, the roots are of the form $\beta = \xi q^{-1/2}$, where ξ is a complex $2l$-th root of unity. This is similarly the case for the class of curves $aY^l = bX^l + cZ^l$ considered in ([1], Theorem 8).
2. For each distinct case in Theorems 2 and 3, the class number is a polynomial in $\sqrt{q}$, of degree $2g$, with integral coefficients and constant term 1, where g is the genus of the curve $C/\mathbf{F}_q$. (The genus of the curve $C/\mathbf{F}_q$ in Theorem 3 is $g = (l-1)(l-2)/2$.)
3. The polynomial $P(t)$ in the ζ-function of a maximal curve $C/\mathbf{F}_q$ is of the form

$$P(t) = (1 + q^{1/2}t)^{2g},$$

and that of a minimal curve $C/\mathbf{F}_q$ is of the form

$$P(t) = (1 - q^{1/2}t)^{2g}.$$

These expressions follow easily from the Weil conjectures applied to the expression for $a(1, C)$ in §2. Conversely, given a non-singular projective curve $C/\mathbf{F}_q$, such that the polynomial $P(t)$ in its ζ-function has the above form(s), one sees that the curve C is maximal (resp. minimal) over $\mathbf{F}_q$.

From the explicit expressions for the polynomial $P(t)$ in the ζ-function(s) of the projective curve $aY^e = bX^e + cZ^e$ defined over $\mathbf{F}_q$ (cf. [1], Theorem 8) (for $e = l$) and Theorem 1 (for $e = 2l$)), it is clear that these curves are maximal (or minimal) over $\mathbf{F}_q$ precisely when the coefficients a, b, c reduce to the case $a = b = c = 1$ corresponding to the Fermat curves.
4. In ([7], Proposition 2), the author has stated results (to appear) for the polynomials $P(t)$ in the ζ-functions of the projective curves $aY^e = bX^e + cZ^e$ ($abc \neq 0$) defined over finite fields $\mathbf{F}_q$, $q = p^\alpha \equiv 1 (\mathrm{mod}\ e)$, for integers $e \geq 3$ and primes p such that ord $p(\mathrm{mod}\ e)$ is even. These results generalize the results obtained for the polynomials $P(t)$ in ([1], Theorem 8) and Theorem 1 of this paper.

Acknowledgements

The author thanks CSIR, India for support received in the form of a research fellowship, when this paper was conceived.

References

[1] Anuradha N and Katre S A, Number of points on the projective curves $aY^l = bX^l + cZ^l$ and $aY^{2l} = bX^{2l} + cZ^{2l}$ defined over finite fields, l an odd prime, *J. Number Theory* **77** (1999) 288–313

[2] Freitag E and Kiehl R, Étale cohomology and the Weil conjectures, *Ergebnisse Math.* **3** Folge 13 (Springer-Verlag) (1987)

[3] Fuhrmann R, Garcia A and Torres F, On maximal curves, *J. Number Theory* **67** (1997) 29–51

[4] Goppa V D, Algebraic-geometric codes, *Math. USSR-Izv.* **21(1)** (1983) 75–91

[5] Goppa V D, Geometry and codes, Mathematics and its applications, Soviet Series (Dordrecht: Klüwer Academic Publishers) (1988) vol. 24
[6] Ihara Y, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. 1A Math.* **28** (1981) 721–724
[7] Katre S A, The cyclotomic problem, in: Current trends in number theory (eds) S D Adhikari *et al* (New Delhi: Hindustan Book Agency) (2002) pp. 59–72
[8] Kontogeorgis A I, The group of automorphisms of the function fields of the curve $x^n + y^m + 1 = 0$, *J. Number Theory* **72** (1998) 110–136
[9] Leopoldt H W, Über die Automorphismengruppe des Fermatkörpers, *J. Number Theory* **56** (1996) 256–282
[10] Moreno C, Algebraic curves over finite fields, Cambridge Tracts in Mathematics (Cambridge, MA: Cambridge Univ. Press) (1991) vol. 97
[11] Rück H G and Stichtenoth H, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457** (1994) 185–188
[12] Stichtenoth H, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, I, II, *Arch. Math.* **24** (1973) 527–544, 615–631
[13] Stichtenoth H, Algebraic function fields and codes, Universitext (Berlin: Springer-Verlag) (1993)
[14] Weil A, Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. Ind. (Paris: Hermann) (1948) No. 1041
[15] Weil A, Numbers of solutions of equations in finite fields, *Bull. Am. Math. Soc.* **55** (1949) 497–508