ACTA ARITHMETICA
132.4 (2008)

Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm

by

Marko Moisio (Vaasa)

1. Introduction. Let $\mathbb{F}_q$ be a finite field with $q = p^r$, and let $a, b \in \mathbb{F}_q$, $b \neq 0$. Fairly little is known about the number $P_m(a,b)$ of irreducible polynomials $p(x) = x^m - ax^{m-1} + \cdots + (-1)^m b$ in $\mathbb{F}_q[x]$. Carlitz [1] obtained the asymptotic formula

$$P_m(a,b) = \frac{q^m - 1}{mq(q-1)} + \mathcal{O}(q^{m/2}) \quad (m \to \infty),$$

and evaluated $\sum_b P_m(a,b)$ where b runs over $\mathbb{F}_q^*$, and over the set of squares (resp. non-squares) in $\mathbb{F}_q^*$. Later Yucas [20] calculated elementarily the numbers $\sum_a P_m(a,b)$ and $\sum_b P_m(a,b)$ where a, b run over $\mathbb{F}_q$.

By the bijection $p(x) \mapsto (-1)^m b^{-1} x^m p(1/x)$ we see that $P_m(a,b)$ equals the number of irreducible monic polynomials of degree m in the arithmetic progression

$$\{cx + d + f(x)x^2 : f(x) \in \mathbb{F}_q[x]\},$$

where $c = (-1)^{m+1} ab^{-1}$ and $d = (-1)^m b^{-1}$. Applying a general asymptotic bound on the number of primes on an arithmetic progression (see e.g. [16, p. 40]) we actually have the asymptotic bound

$$P_m(a,b) = \frac{q^{m-1}}{m(q-1)} + \mathcal{O}\left(\frac{q^{m/2}}{m}\right) \quad (m \to \infty).$$

Finally, Wan [18, Thm. 5.1] obtained the following effective bound:

$$\left| P_m(a,b) - \frac{q^{m-1}}{m(q-1)} \right| \leq \frac{3}{m} q^{m/2}. \tag{1.1}$$

For a more complete survey the reader is referred to [5].

The bounds above are obtained by using Dirichlet L-series over $\mathbb{F}_q[x]$ and the Riemann hypothesis for function fields over a finite field. In this paper

2000 *Mathematics Subject Classification*: 11T06, 11T23.

Key words and phrases: elliptic curve, exponential sum, finite field, irreducible polynomial, Kloosterman sum, Kronecker class number.

we express $P_m(a,b)$ in terms of the numbers $N_t(a,b)$ of elements $x \in \mathbb{F}_{q^t}$ (with $t \mid m$) satisfying $\mathrm{Trace}(x) = a$ and $\mathrm{Norm}(x) = b$ (Trace, Norm are from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$), which, in turn, are expressed in terms of exponential sums. This opens up a possibility to calculate $P_m(a,b)$ explicitly in certain special cases. Moreover, we shall obtain an improvement of the bound (1.1) if m is small compared to q, more precisely, if $m \le \frac{3}{2}(q-1)$. If $a = 0$ the bound is obtained elementarily, but if $a \neq 0$ this is done by linking the problem to the number of solutions of certain system of equations, and making use of the Katz bound [11]:

$$\left| N_m(a,b) - \frac{q^m - 1}{q(q-1)} \right| \le m q^{(m-2)/2}, \tag{1.2}$$

proved by using deep algebraic geometry.

The Katz bound with $m = 3$ plays a significant role in the proof by Huczynska and Cohen [10] of the existence of a primitive free (normal) cubic polynomial with $a\,(\neq 0)$ and b fixed, which completed a general existence theorem (see also [4, 6, 5]). We shall improve the Katz bound in this case. In fact, we get sharp lower and upper bounds for $N_3(a,b)$, and as a corollary for $P_3(a,b)$, by using only the Hasse–Weil bound for elliptic curves together with a simple divisibility argument.

Another special case where the Katz bound can be improved is the case $m = p^k$ for some k. In particular, if $p = 3$ (resp. $p = 2$) a result on the distribution of irreducible cubic (resp. quartic) polynomials in $\mathbb{F}_q[x]$ with trace and norm prescribed is obtained in terms of Kronecker class numbers by using the known value distribution of a Kloosterman sum over $\mathbb{F}_q$ [12, 13].

Next, necessary and sufficient conditions for a Kloosterman sum over $\mathbb{F}_{2^r}$ divisible by 3 is given. In the case of r odd this result follows also from [3, Thm. 3]. Finally, a new proof for the value distribution of a Kloosterman sum over the field $\mathbb{F}_{3^r}$ is given. The proof uses only elementary properties of elliptic curves together with a result by Deuring [8] which lies deeper: the knowledge of the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ having $q + 1 + t$ points with $\gcd(q,t) = 1$.

Acknowledgments. The author is indebted to the anonymous referee for helpful comments and suggestions which improved the clarity of the paper considerably.

2. Basic formulae.

The aim of this section is to establish a link between the numbers $N_m(a,b)$ and $P_m(a,b)$, and to give basic formulae for $N_m(a,b)$ and $P_m(a,b)$ in terms of exponential sums. The formulae will be studied more closely in later sections.

m, p, r	fixed positive integers, $m \geq 2$, p a prime
$\mathbb{F}_q$	the finite field with p^r elements
a, b	fixed elements in $\mathbb{F}_q$, $b \neq 0$
$P_m(a, b)$	the number of irreducible polynomials $x^m - ax^{m-1} + \cdots + (-1)^m b \in \mathbb{F}_q[x]$
t	a positive factor of m
d	equals $\gcd(q-1, m/t)$
γ_t	a primitive element of $\mathbb{F}_{q^t}$
g	the primitive element of $\mathbb{F}_q$ defined by $g = \mathrm{Norm}_t(\gamma_t)$
$\mathrm{tr}_t(x)$	the trace function from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$
$\mathrm{Norm}_t(x)$	the norm function from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$
$S_t(a, b)$	the set of the elements x in $\mathbb{F}_{q^t}^*$ with $\mathrm{tr}_m(x) = a$ and $\mathrm{Norm}_m(x) = b$
$N_t(a, b)$	the number of elements in $S_t(a, b)$
μ	the Möbius function
χ and e	the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^t}$
$\mathcal{X}(\mathbb{F}_q)$	the set of rational points on an algebraic curve $\mathcal{X}$ defined over $\mathbb{F}_q$

The following two lemmas relate the numbers $P_m(a, b)$ and $N_t(a, b)$:

Lemma 2.1.

$$P_m(a, b) = \frac{1}{m} \sum_{t \mid m} \mu(t) N_{m/t}(a, b).$$

Proof. Let

$$H_t(a, b) = |\{x \in \mathbb{F}_{q^t}^* : \mathrm{tr}_m(x) = a,\ \mathrm{Norm}_m(x) = b,\ \text{and } x \notin \mathbb{F}_{q^s} \text{ if } s < t\}|.$$

Obviously $N_m(a, b) = \sum_{t \mid m} H_t(a, b)$, and now by the Möbius inversion formula

$$H_m(a, b) = \sum_{t \mid m} \mu(t) N_{m/t}(a, b).$$

But $H_m(a, b) = mP_m(a, b)$, completing the proof. ■

Lemma 2.2. *Let $m = p_1^{e_1} \cdots p_k^{e_k}$ be the canonical prime number decomposition of m $(p_1 < p_2 < \cdots)$, and let $m' = p_1 \cdots p_k$. Then*

$$N_m(a, b) - M_1 m'/2 \leq mP_m(a, b) \leq N_m(a, b) + M_2(m' - 2)/2$$

with $M_1 = \max_h\{N_{m/h}(a, b)\}$, $M_2 = \max_s\{N_{m/s}(a, b)\}$ where h (resp. $s > 1$) runs over the factors of m' having an odd (resp. even) number of prime factors. If $k = 1$, set $M_2 = 0$.

Proof. Assume $k = 1$. Now $mP_m(a,b) = N_m(a,b) - N_{m/p_1}(a,b)$ by Lemma 2.1. Moreover, since $M_1 = N_{m/p_1}(a,b)$ and $M_2 = 0$, the conclusion follows in this case. Assume $k > 1$. By Lemma 2.1 we have

$$mP_m(a,b) = N_m(a,b) + \sum_s N_{m/s}(a,b) - \sum_h N_{m/h}(a,b).$$

Since $m' \geq 2^k$, we now get

$$\begin{aligned} mP_m(a,b) - N_m(a,b) &\geq -M_1 \sum_h 1 = -M_1 \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i+1} = -M_1 2^{k-1} \\ &\geq -M_1 m'/2. \end{aligned}$$

Moreover,

$$\begin{aligned} mP_m(a,b) - N_m(a,b) &\leq M_2 \sum_s 1 = M_2 \sum_{i=1}^{\lfloor k/2 \rfloor} \binom{k}{2i} = M_2(2^{k-1} - 1) \\ &\leq M_2(m'-2)/2, \end{aligned}$$

and the proof is complete. ■

Next we derive a formula for $N_t(a,b)$. First, we observe that if $a \neq 0$, then

$$x \in S_t(a,b) \ \Leftrightarrow\ p \nmid m/t \text{ and } \operatorname{tr}_t(x) = (t/m)a \text{ and } \operatorname{Norm}_t(x^{m/t}) = b, \tag{2.1}$$

and if $a = 0$, then

$$\begin{aligned} x \in S_t(a,b) \ \Leftrightarrow\ & p \mid m/t \text{ and } \operatorname{Norm}_t(x^{m/t}) = b, \\ & \text{or } p \nmid m/t,\ \operatorname{tr}_t(x) = 0,\ \text{and } \operatorname{Norm}_t(x^{m/t}) = b. \end{aligned} \tag{2.2}$$

Second, we see that

$$\begin{aligned} \operatorname{Norm}_t(x^{m/t}) = b \ &\Leftrightarrow\ (m/t)i \equiv \operatorname{ind}_g b \pmod{q-1} \\ &\Leftrightarrow\ d \mid \operatorname{ind}_g b \text{ and } i = i_0 + (q-1)j/d, \end{aligned} \tag{2.3}$$

where j runs over the set $\bigl\{0, \ldots, \frac{q^t-1}{(q-1)/d} - 1\bigr\}$, and i_0 is a solution of the congruence $mi/dt \equiv (\operatorname{ind}_g b)/d \pmod{(q-1)/d}$.

LEMMA 2.3. *Assume $p \nmid m/t$ and $d \mid \operatorname{ind}_g b$. Let i_0 be a solution of the congruence $mi/dt \equiv (\operatorname{ind}_g b)/d \pmod{(q-1)/d}$ and let $a_0 = ta/m$. Then*

$$N_t(a,b) = \frac{d}{q(q-1)}\,(q^t - 1 + \sigma_t(a,b)),$$

where

$$\sigma_t(a,b) = \sum_{c \in \mathbb{F}_q^*} \chi(-ca_0) \sum_{x \in \mathbb{F}_{q^t}^*} e(c\gamma_t^{i_0} x^{(q-1)/d}). \tag{2.4}$$

Proof. Let α be an element in $\mathbb{F}_{q^t}$ with $\mathrm{tr}_t(\alpha) = t/m$. Now, by (2.3) and by the orthogonality of characters we get

$$\begin{aligned} qN_t(a,b) &= \sum_{j=0}^{\frac{q^t-1}{(q-1)/d}-1} \sum_{c\in\mathbb{F}_q} \chi(c\,\mathrm{tr}_m(\gamma_t^{i_0+(q-1)j/d} - \alpha a)) \\ &= \sum_{c\in\mathbb{F}_q} \chi(-ca) \sum_{j=0}^{\frac{q^t-1}{(q-1)/d}-1} e\biggl(\frac{m}{t}\,c\gamma_t^{i_0}\gamma_t^{(q-1)j/d}\biggr) \\ &\overset{c\mapsto \frac{t}{m}c}{=} \frac{d}{q-1} \sum_{c\in\mathbb{F}_q} \chi(-ca_0) \sum_{x\in\mathbb{F}_{q^t}^*} e(c\gamma_t^{i_0}x^{(q-1)/d}) \\ &= \frac{d}{q-1}\,(q^t - 1 + \sigma_t(a,b)). \ \blacksquare \end{aligned}$$

3. Zero trace. In this section we assume that $a = 0$ and simplify formula (2.4) by using Gauss sums and some very elementary group theory. This will enable us to obtain an improvement of the Katz bound and the Wan bound in the case $a = 0$. We use the following notations:

H_n	the subgroup of order n of the multiplicative character group of $\mathbb{F}_q$
λ_0	the trivial character of H_n

For a multiplicative character ψ of $\mathbb{F}_{q^t}$ we define a Gauss sum

$$G(\psi) := \sum_{x\in\mathbb{F}_{q^t}^*} e(x)\psi(x).$$

LEMMA 3.1. *Let n be a factor of $q-1$ and let $\alpha \in \mathbb{F}_{q^t}^*$. Then*

$$\sum_{x\in\mathbb{F}_{q^t}^*} e(\alpha x^n) = \sum_{\lambda\in H_n} G(\overline{\lambda}\circ \mathrm{Norm}_t)\lambda(\mathrm{Norm}_t(\alpha)),$$

where $\overline{\lambda} = \lambda^{-1}$.

Proof. It is easy to see [14, p. 217] that

$$\sum_{x\in\mathbb{F}_{q^t}^*} e(\alpha x^n) = \sum_{\psi\in H_n'} G(\overline{\psi})\psi(\alpha),$$

where H_n' is the subgroup of order n of the multiplicative character group of $\mathbb{F}_{q^t}$. But the surjectivity of Norm_t implies that $H_n' = \{\lambda\circ\mathrm{Norm}_t : \lambda \in H_n\}$. ■

Assume $a = 0$, $p \nmid m/t$, and $d \,|\, \operatorname{ind}_g b$. Now, by Lemma 3.1 we get

$$\sigma_t(0,b) = \sum_{c \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^t}^*} e(c\gamma_t^{i_0} x^{(q-1)/d}) = \sum_{c \in \mathbb{F}_q^*} \sum_{\lambda \in H_{(q-1)/d}} G(\overline{\lambda} \circ \mathrm{Norm}_t)\lambda(c^t g^{i_0})$$
$$= \sum_{\lambda \in H_{(q-1)/d}} G(\overline{\lambda} \circ \mathrm{Norm}_t)\lambda(g^{i_0}) \sum_{c \in \mathbb{F}_q^*} \lambda(c^n),$$

where $n = \gcd(q-1, t)$. Since

$$\sum_{c \in \mathbb{F}_q^*} \lambda(c^n) = \sum_{c \in \mathbb{F}_q^*} \lambda^n(c) = \begin{cases} 0 & \text{if } \lambda^n \neq \lambda_0, \\ q-1 & \text{if } \lambda^n = \lambda_0, \text{ i.e. if } \lambda \in H_n \cap H_{(q-1)/d}, \end{cases}$$

we get

$$\sigma_t(0,b) = (q-1) \sum_{\lambda \in H_s} G(\overline{\lambda} \circ \mathrm{Norm}_t)\lambda(g^{i_0}) = (q-1) \sum_{x \in \mathbb{F}_{q^t}^*} e(\gamma_t^{i_0} x^s),$$

where $s = \gcd(n, (q-1)/d)$. Thus,

$$N_t(0,b) = \frac{d}{q}\biggl(\frac{q^t - 1}{q-1} + \sum_{x \in \mathbb{F}_{q^t}^*} e(\gamma_t^{i_0} x^s)\biggr),$$

implying the following

Theorem 3.2. *Assume $p \nmid m/t$ and $d \,|\, \operatorname{ind}_g b$. Then*

$$N_t(0,b) = d\biggl(\frac{q^{t-1} - 1}{q-1} + \frac{1}{q} \sum_{x \in \mathbb{F}_{q^t}} e(\gamma_t^{i_0} x^s)\biggr),$$

where $s = \gcd(t, (q-1)/d)$ and $d = \gcd(m/t, q-1)$.

Theorem 3.2 and the Weil bound (see e.g. [14, p. 223]) imply an improvement of the Katz bound (see (1.2)) in the case $a = 0$:

Corollary 3.3.

$$\left| N_m(0,b) - \frac{q^{m-1} - 1}{q-1} \right| \leq (s-1) q^{(m-2)/2},$$

where $s = \gcd(m, q-1)$.

We can now improve the Wan bound (see (1.1)) in the case $a = 0$ and $m \leq \frac{3}{2}(q-1)$:

Corollary 3.4.

$$\left| P_m(0,b) - \frac{q^{m-1} - 1}{m(q-1)} \right| \leq \frac{s-1}{m} q^{(m-2)/2} + \frac{q^{m/2} - 1}{q-1} < \frac{2}{q-1} q^{m/2},$$

where $s = \gcd(m, q-1)$.

Proof. Since $d \le m/t$, it follows from (2.2) and (2.3) that the numbers M_1 and M_2 in Lemma 2.2 satisfy

$$M_2 < M_1 \le p_1 \frac{q^{m/p_1} - 1}{q - 1} \le 2 \frac{q^{m/2} - 1}{q - 1},$$

and now, by Lemma 2.2 and Corollary 3.3, we get

$$\left| mP_m(0, b) - \frac{q^{m-1} - 1}{q - 1} \right| \le (s - 1)q^{(m-2)/2} + m \frac{q^{m/2} - 1}{q - 1}. \ \blacksquare$$

By Lemma 2.1, Theorem 3.2, (2.3), and (2.2) we get explicit expressions for $P_m(0, b)$ e.g. in the following special cases:

EXAMPLE 3.5. If $\gcd(p, m, q - 1) = 1$, then

$$P_m(0, b) = \frac{1}{m(q - 1)} \sum_{t \mid m} \mu\left(\frac{m}{t}\right)(q^{t-1} - 1).$$

EXAMPLE 3.6. If $m = p^k > 1$, then

$$mP_m(0, b) = \frac{q^{m-1} - 1}{q - 1} - \frac{q^{m/p} - 1}{q - 1}.$$

4. Non-zero trace. In this section we assume that $a \ne 0$. This case is much harder than the zero trace case, and we are not able to find such a simple expression for $N_t(a, b)$ as in case $a = 0$. The best we can do is to give $N_t(a, b)$ in terms of the number of solutions of a system of equations, and estimate that number by using the Katz bound. This method will lead us to an improvement of the Wan bound also in the case $a \ne 0$.

Let $n = (q - 1)/d$. By Lemma 3.1 and by substitution $c \mapsto -a_0^{-1}c$ we see that $\sigma_t(a, b)$ (see (2.4)) can be written in the form

$$\begin{aligned}\sigma_t(a, b) &= \sum_{c \in \mathbb{F}_q^*} \chi(c) \sum_{\lambda \in H_n} G(\overline{\lambda} \circ \mathrm{Norm})\lambda(c^t(-a_0)^{-t} g^{i_0}) \\ &= \sum_{\lambda \in H_n} G(\overline{\lambda} \circ \mathrm{Norm})\lambda(g^{i_0}(-a_0)^{-t}) \sum_{c \in \mathbb{F}_q^*} \chi(c)\lambda^t(c) \\ &= \sum_{\lambda \in H_n} G(\overline{\lambda} \circ \mathrm{Norm})G(\lambda^t)\lambda(g^{i_0}(-a_0)^{-t}).\end{aligned}$$

Let $c = g^{i_0} a_0^{-t}$ and use the Davenport–Hasse theorem [14, p. 197] to get

$$\begin{aligned}\sigma_t(a, b) &= (-1)^{t-1} \sum_{\lambda \in H_n} G(\overline{\lambda})^t G(\lambda^t)\lambda((-1)^t c) \\ &= (-1)^{t-1} \sum_{\lambda \in H_n} G(\lambda)^t G(\overline{\lambda}^t)\overline{\lambda}((-1)^t c).\end{aligned}$$

Now, by the definition of a Gauss sum we get

$$\sigma_t(a,b) = (-1)^{t-1} \sum_{x_1,\dots,x_t,u\in\mathbb{F}_q^*} \chi(x_1+\dots+x_t+u) \sum_{\lambda\in H_n} \lambda(x_1\cdots x_t(-u)^{-t}c^{-1}),$$

and consequently, by substituting $x_1 \mapsto -ux_1, \dots, x_t \mapsto -ux_t$, we obtain

$$(4.1)\quad \sigma_t(a,b) = (-1)^{t-1} \sum_{x_1,\dots,x_t,u\in\mathbb{F}_q^*} \chi(-u(x_1+\dots+x_t-1)) \times \sum_{\lambda\in H_n} \lambda(x_1\cdots x_t c^{-1}).$$

We can now prove the following

Theorem 4.1. *If $a \neq 0$, $p \nmid m/t$, and $d \mid \operatorname{ind}_g b$, then*

$$N_t(a,b) = \frac{d(q^t-1)}{q(q-1)} + (-1)^{t-1}\Bigl(\sum_{i=0}^{d-1} N(c_i) - \frac{d(q-1)^t}{q(q-1)}\Bigr),$$

where $N(c_i)$ is the number of solutions of

$$\begin{cases} x_1+\dots+x_t = 1,\\ x_1\cdots x_t = c_i,\end{cases}$$

in $\mathbb{F}_q^t$ with $c_i = g^{(q-1)i/d+i_0}a_0^{-t}$.

Proof. Let $n = (q-1)/d$ and $c = g^{i_0}a_0^{-t}$. The orthogonality of characters implies that

$$q(q-1)N(c_i) = \sum_{x_1,\dots,x_t\in\mathbb{F}_q^*} \sum_{u\in\mathbb{F}_q} \chi(u(x_1+\dots+x_t-1)) \sum_{\lambda\in H_{q-1}} \lambda(c_i^{-1}x_1\cdots x_t),$$

and consequently

$$q(q-1)\sum_{i=0}^{d-1} N(c_i) = \sum_{x_1,\dots,x_t\in\mathbb{F}_q^*} \sum_{u\in\mathbb{F}_q} \chi(u(x_1+\dots+x_t-1)) \times \sum_{\lambda\in H_{q-1}} \sum_{i=0}^{d-1} \lambda(c_i^{-1}x_1\cdots x_t).$$

Here

$$\sum_{i=0}^{d-1} \lambda(c_i^{-1}x_1\cdots x_t) = \lambda(c^{-1}x_1\cdots x_t)\sum_{i=0}^{d-1}\lambda(g^{-ni}) = \begin{cases} \lambda(c^{-1}x_1\cdots x_t)d & \text{if } \lambda\in H_n,\\ 0 & \text{otherwise,}\end{cases}$$

and now, by (4.1), we get

$$\begin{aligned}q(q-1)\sum_{i=0}^{d-1}N(c_i) &= d\sum_{x_1,\dots,x_t\in\mathbb{F}_q^*}\sum_{u\in\mathbb{F}_q}\chi(u(x_1+\dots+x_t-1))\\ &\qquad\times\sum_{\lambda\in H_n}\lambda(c^{-1}x_1\cdots x_t)\\ &= d(-1)^{t-1}\sigma_t(a,b)+d\sum_{x_1,\dots,x_t\in\mathbb{F}_q^*}\sum_{\lambda\in H_n}\lambda(c^{-1}x_1\cdots x_t).\end{aligned}$$

Here

$$\sum_{x_1,\dots,x_t\in\mathbb{F}_q^*}\sum_{\lambda\in H_n}\lambda(c^{-1}x_1\cdots x_t)=\sum_{\lambda\in H_n}\Big(\sum_{x\in\mathbb{F}_q^*}\lambda(c^{-1}x)\Big)^t=(q-1)^t$$

and it follows that

$$\sigma_t(a,b)=(-1)^{t-1}\bigg(\frac{q(q-1)}{d}\sum_{i=0}^{d-1}N(c_i)-(q-1)^t\bigg).$$

Lemma 2.3 now completes the proof. ∎

Lemma 4.2. *Let n be a positive integer and let $c\in\mathbb{F}_q^*$. The number $N(c)$ of solutions $(x_1,\dots,x_n)$ in $\mathbb{F}_q^n$ of*

$$\begin{cases}x_1+\dots+x_n=1,\\ x_1\cdots x_n=c,\end{cases}$$

satisfies

$$\left|N(c)-\frac{(q-1)^n}{q(q-1)}\right|\le nq^{(n-2)/2}.$$

Proof. Choose $m=t=n$, and $a=1$, $b=c$. Now $d=\gcd(m/t,q-1)=1$ and we choose $i_0=\operatorname{ind}_g b$ (see (2.3)). Now $c=g^{i_0}/a^t$, and by Theorem 4.1 we get

$$N_n(a,b)=\frac{q^n-1}{q(q-1)}+N(c)-\frac{(q-1)^n}{q(q-1)}$$

or, equivalently,

$$N(c)-\frac{(q-1)^n}{q(q-1)}=N_n(a,b)-\frac{q^n-1}{q(q-1)}.$$

The Katz bound (1.2) now completes the proof. ∎

We are now able to improve the Wan bound (1.1) in the case $a\ne0$ and $m\le\frac32(q-1)$:

Corollary 4.3. *Let $a,b\in\mathbb{F}_q^*$. Then*

$$\left|P_m(a,b)-\frac{q^m-1}{mq(q-1)}\right|\le q^{(m-2)/2}+\frac{q^{m/2}-1}{q(q-1)}+\frac{m}{2}\,q^{(m-4)/4}<\frac{2}{q-1}\,q^{m/2}.$$

Proof. If $p \mid m/t$ or $d \nmid \operatorname{ind}_g b$, then $N_t(a,b) = 0$ by (2.1) and (2.3). Assume $p \nmid m/t$ and $d \mid \operatorname{ind}_g b$. If t is even Theorem 4.1 implies

$$N_t(a,b) \le \frac{d(q^t-1)}{q(q-1)} - dN(c) + \frac{d(q-1)^t}{q(q-1)}$$

for some $c \in \mathbb{F}_q^*$. Now, by Lemma 4.2,

$$\begin{aligned} N_t(a,b) &\le \frac{d(q^t-1)}{q(q-1)} - d\biggl(\frac{(q-1)^t}{q(q-1)} - tq^{(t-2)/2}\biggr) + \frac{d(q-1)^t}{q(q-1)} \\ &= \frac{d(q^t-1)}{q(q-1)} + dtq^{(t-2)/2}. \end{aligned}$$

Since $d \le m/t$, we get

$$N_t(a,b) \le \frac{m(q^t-1)}{tq(q-1)} + mq^{(t-2)/2}. \tag{4.2}$$

If t is odd, then

$$N_t(a,b) \le \frac{d(q^t-1)}{q(q-1)} + dN(c) - \frac{d(q-1)^t}{q(q-1)}$$

for some $c \in \mathbb{F}_q^*$, and

$$\begin{aligned} N_t(a,b) &\le \frac{d(q^t-1)}{q(q-1)} + d\biggl(\frac{(q-1)^t}{q(q-1)} + tq^{(t-2)/2}\biggr) - \frac{d(q-1)^t}{q(q-1)} \\ &= \frac{d(q^t-1)}{q(q-1)} + dtq^{(t-2)/2}. \end{aligned}$$

Hence, the bound (4.2) holds in this case too.

Now, by (4.2), the numbers M_1 and M_2 in Lemma 2.2 clearly satisfy

$$M_2 < M_1 \le 2\,\frac{q^{m/2}-1}{q(q-1)} + mq^{(m-4)/4},$$

and consequently, by Lemma 2.2 and by the Katz bound (1.2), we get

$$\left| mP_m(a,b) - \frac{q^m-1}{q(q-1)} \right| < mq^{(m-2)/2} + m\,\frac{q^{m/2}-1}{q(q-1)} + \frac{m^2}{2}\,q^{(m-4)/4}.$$

Hence,

$$\begin{aligned} \left| P_m(a,b) - \frac{q^m-1}{mq(q-1)} \right| &\le q^{(m-2)/2} + \frac{q^{m/2}-1}{q(q-1)} + \frac{m}{2}\,q^{(m-4)/4} \\ &< \frac{1}{q}\biggl(1 + \frac{1}{q-1} + \frac{m}{2}\,q^{-mq/4}\biggr)q^{m/2} \\ &= \biggl(\frac{1}{q-1} + \frac{m}{2}\,q^{-(m+4)/4}\biggr)q^{m/2}. \end{aligned}$$

Obviously $(m/2)q^{-(m+4)/4} < 1/(q-1)$, and so the proof is complete. ■

5. Cubics and cubic extensions. In this section we assume that $m = 3$. Now the system of equations defined in the previous section is of degree 3, and therefore we can give $N_3(a,b)$, and also $P_3(a,b)$, in terms of the number of rational points on a cubic curve defined over $\mathbb{F}_q$. Some elementary manipulations of cubic curves together with the Hasse–Weil bound for elliptic curves, and the link between $P_3(a,b)$ and $N_3(a,b)$, will then lead to a sharp bound for $N_3(a,b)$, which is also an improvement of the Katz bound in the case $m = 3$. The following result is a key for such an improvement:

THEOREM 5.1. *Let $c = ba^{-3}$, and let $\mathcal{X}$ be the projective curve over $\mathbb{F}_q$ defined by*

$$\mathcal{X}:\ y^2 + cy + xy = x^3.$$

Then $N_3(a,b) = |\mathcal{X}(\mathbb{F}_q)|$ and

$$P_3(a,b) = \tfrac{1}{3}(|\mathcal{X}(\mathbb{F}_q)| - \epsilon),$$

where

$$\epsilon = \begin{cases} 1 & \textit{if } p \neq 3 \textit{ and } c = 1/27, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Let $m = 3$ and apply Theorem 4.1 with $t = 3$ to get

$$N_3(a,b) = \frac{q^3-1}{q(q-1)} + N(c_0) - \frac{(q-1)^3}{q(q-1)} = N(c_0) + 3, \tag{5.1}$$

where $N(c_0)$ is the number of solutions (x,y,z) in $\mathbb{F}_q^3$ of

$$\begin{cases} x + y + z = 1, \\ xyz = c_0, \end{cases}$$

with $c_0 = g^{i_0}/a^3 = b/a^3$, or equivalently, $N(c_0)$ is the number of solutions of

$$x^2y + xy^2 - xy = -c_0, \tag{5.2}$$

in $\mathbb{F}_q^3$.

Equation (5.2) defines an affine component of the projective curve defined by

$$\mathcal{X}':\ y^2 + y - xy = -c_0x^3,$$

and that affine component has exactly three points at infinity. Hence

$$N_3(a,b) = |\mathcal{X}'(\mathbb{F}_q)|$$

by (5.1). By multiplying both sides of the equation of $\mathcal{X}'$ by c_0^2 and then substituting $x \mapsto -c_0^{-1}x$ and $y \mapsto c_0^{-1}y$ we see that $\mathcal{X}'$ is isomorphic over $\mathbb{F}_q$ to $\mathcal{X}$.

It follows from Lemma 2.1 that $3P_3(a,b) = N_3(a,b) - N_1(a,b)$, and by (2.1), $x \in S_1(a,b)$ if and only if $p \neq 3$ and $b = (a/3)^3$. This completes the proof. ∎

Corollary 5.2. *Assume $p \neq 3$, and let $b = (a/3)^3$. Then*

$$P_3(a,b) = \tfrac{1}{3}(q \pm 1),$$

where the sign is plus if $p \equiv 2 \pmod 3$ and $2 \nmid r$, and otherwise the sign is minus.

Proof. If $p = 2$ then the equation of $\mathcal{X}$ is $y^2+(x+1)y = x^3$. This equation has only three solutions with $x = 0, 1$. By substituting $y \mapsto (x+1)y$, we can write the equation in the form $y^2+y = x^3/(x+1)^2$, and then by substituting $x \mapsto x+1$ we get the equation

$$y^2 + y = x + 1 + x^{-1} + x^{-2}. \tag{5.3}$$

Since the absolute trace of $x^{-1}+x^{-2}$ equals zero we have $\chi(x^{-1}+x^{-2}) = 1$, and therefore equation (5.3) has exactly

$$\sum_{x\in\mathbb{F}_q^*\setminus\{1\}} (1+\chi(x+1)) = q-2+\chi(1)\Big(\sum_{x\in\mathbb{F}_q^*} \chi(x) - \chi(1)\Big) = q-3-\chi(1)$$

solutions in $\mathbb{F}_q^2$ with $x \neq 0, 1$. Hence, in the case $p = 2$, $|\mathcal{X}(\mathbb{F}_q)| = q-3-\chi(1)+3+1$ and $P_3(a,b) = (q-\chi(1))/3$.

Assume $p \neq 2$ and write the equation $y^2 + cy + xy = x^3$ in the form $\big(y + \frac{1}{2}(c+x)\big)^2 = x^3 + \frac{1}{4}(c+x)^2$. Substitute $y \mapsto y - \frac{1}{2}(c+x)$ to get

$$y^2 = x^3 + \tfrac{1}{4}x^2 + \tfrac{1}{2}cx + c^2/4 = (x+1/9)^2(x+1/36).$$

Finally, by substituting $x \mapsto x - 1/9$, we see that $\mathcal{X}$ is isomorphic over $\mathbb{F}_q$ to

$$C: \; y^2 = x^2(x-1/12).$$

Let F be the set of finite points of C and let F' be the set of finite points of the curve C' defined over $\mathbb{F}_q$ by

$$C': \; z^2 = u - 1/12.$$

We note that the map $(x,y) \mapsto (u = x, z = y/x)$ from $F \setminus \{(0,0)\}$ to F' is injective, and it follows that $|F| = |F'| \pm 1$ depending on whether the equation $z^2 = -1/12$ has, or has not, a solution in $\mathbb{F}_q$. Hence, $|C(\mathbb{F}_q)| = |C'(\mathbb{F}_q)| \pm 1 = q+1\pm 1$, and now, by Theorem 5.1, we get $P_3(a,b) = \frac{1}{3}(q+1\pm 1-1)$. ∎

We can now improve the Katz bound in the case $m = 3$:

Theorem 5.3. *Let $a, b \in \mathbb{F}_q$, $b \neq 0$. Then*

$$3\left\lceil \frac{q+1-2\sqrt{q}}{3} \right\rceil \leq N_3(a,b) \leq 3\left\lfloor \frac{q+1+2\sqrt{q}}{3} \right\rfloor.$$

Proof. By Lemma 2.1 we have

$$3P_3(a,b) = N_3(a,b) - N_1(a,b).$$

Assume first that $a = 0$. If $p = 3$ then $N_1(a,b) = 1$ by (2.2), and $3P_3(a,b) = q+1-1$ by Example 3.6. Hence, $N_3(a,b) = q+1$, and the conclusion follows in the case $a = 0$ and $p = 3$.

If $p \neq 3$ then $N_1(a,b) = 0$ by (2.2), and Corollary 3.3 now implies

$$q + 1 - 2\sqrt{q} \leq 3P_3(a,b) \leq q + 1 + 2\sqrt{q}, \tag{5.4}$$

and therefore

$$\left\lceil \frac{q+1-2\sqrt{q}}{3} \right\rceil \leq P_3(a,b) \leq \left\lfloor \frac{q+1+2\sqrt{q}}{3} \right\rfloor.$$

Since $3P(a,b) = N_3(a,b)$, the proof is complete in case $a = 0$ and $p \neq 3$.

Assume next that $a \neq 0$. It is easy to see that if $\mathcal{X} : y^2 + cy + xy = x^3$ is singular then $p \neq 3$ and $c = 1/27$. Hence, if $\mathcal{X}$ is singular then $q \pm 1 = 3P_3(a,b) = N_3(a,b) - 1$ by Corollary 5.2 and Theorem 5.1, and therefore $N_3(a,b) = q \pm 1 + 1$, proving the assertion if $\mathcal{X}$ is singular.

Assume that $\mathcal{X}$ is non-singular. Now, by the proof of Corollary 5.2, we see that $p = 3$ or $c \neq 1/27$, and therefore $3P_3(a,b) = |\mathcal{X}(\mathbb{F}_q)| = N_3(a,b)$ by Theorem 5.1. Now, since $\mathcal{X}$ is elliptic, the Hasse–Weil bound (see e.g. [19, p. 91]) implies that the bounds in (5.4) hold in this case too, and the proof is complete. ∎

Remark 5.4. The bounds in Theorem 5.3 are sharp. Take $q = 5$, for example. If $a = b = 1$, we have $N_3(a,b) = |\mathcal{X}(\mathbb{F}_q)| = 9 = 3\lfloor(5+1+2\sqrt{5})/3\rfloor$. If $a = 1$, $b = 2$, we have $N_3(a,b) = |\mathcal{X}(\mathbb{F}_q)| = 3 = 3\lceil(5+1-2\sqrt{5})/3\rceil$. These calculations can be verified e.g. by MAGMA.

6. Degree a power of the characteristic. An improvement of the Katz bound can also be obtained in the special case $m = p^k\,(> 2)$, as we shall see in this section. The key point is that in this case the number of solutions of our system of equations, and therefore $N_m(a,b)$ and $P_m(a,b)$, can be given in terms of hyper-Kloosterman sums over $\mathbb{F}_q$ which can be estimated by the Deligne bound obtained in [7] (see also [14, p. 254]).

In the special cases $(p,m) = (3,3), (2,4)$ we can go even further since then we can use the known value distributions of Kloosterman sums to get fairly precise information on the distribution of the irreducible cubic and quartic polynomials over the fields $\mathbb{F}_{3^r}$ and $\mathbb{F}_{2^r}$, respectively. These cases are considered in Subsections 6.1 and 6.2.

For a positive integer n and c in $\mathbb{F}_q^*$ let $k_n(c)$ be an *n-dimensional Kloosterman sum* (or a *hyper-Kloosterman sum*)

$$k_n(c) = \sum_{x_1,\ldots,x_n \in \mathbb{F}_q^*} \chi\left(x_1 + \cdots + x_n + \frac{c}{x_1 \cdots x_n}\right).$$

THEOREM 6.1. *Assume $m = p^k > 2$, and let $a, b \in \mathbb{F}_q^*$. Then*

$$N_m(a,b) = \frac{q^{m-1}-1}{q-1} + (-1)^{m-1} k_{m-2}(c),$$

where $c = b/a^m$. Moreover,

$$\left| N_m(a,b) - \frac{q^{m-1}-1}{q-1} \right| \leq (m-1) q^{(m-2)/2}.$$

Proof. Apply Theorem 4.1 with $m = t$ to get

$$N_m(a,b) = \frac{q^m - 1}{q(q-1)} + (-1)^{m-1}\left(N(c) - \frac{(q-1)^m}{q(q-1)} \right), \tag{6.1}$$

where $N(c)$ is the number of solutions of

$$\begin{cases} x_1 + \cdots + x_m = 1, \\ x_1 \cdots x_m = c. \end{cases}$$

Obviously $N(c)$ is equal to the number of solutions of

$$x_1 + \cdots + x_{m-1} + \frac{c}{x_1 \cdots x_{m-1}} - 1 = 0,$$

and therefore, by the orthogonality of characters, we get

$$\begin{aligned} qN(c) &= \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q^*} \sum_{u \in \mathbb{F}_q} \chi\left(u\left(x_1 + \cdots + x_{m-1} + \frac{c}{x_1 \cdots x_{m-1}} - 1 \right) \right) \\ &= \sum_{u \in \mathbb{F}_q^*} \chi(-u) \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q^*} \chi\left(ux_1 + \cdots + ux_{m-1} + \frac{uc}{x_1 \cdots x_{m-1}} \right) \\ &\quad + (q-1)^{m-1}. \end{aligned}$$

Now, by substitutions $x_1 \mapsto x_1/u, \ldots, x_{m-1} \mapsto x_{m-1}/u$, and by noting that $x \mapsto x^m$ is a permutation of $\mathbb{F}_q$, we get

$$\begin{aligned} &qN(c) - (q-1)^{m-1} \\ &= \sum_{u \in \mathbb{F}_q^*} \chi(-u) \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q^*} \chi\left(x_1 + \cdots + x_{m-1} + \frac{u^m c}{x_1 \cdots x_{m-1}} \right) \\ &= \sum_{u \in \mathbb{F}_q^*} \chi(-u) \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q^*} \chi\left(x_1^m + \cdots + x_{m-1}^m + \frac{u^m c}{x_1^m \cdots x_{m-1}^m} \right) \\ &= \sum_{u \in \mathbb{F}_q^*} \chi(-u) \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q^*} \chi\left(\left(x_1 + \cdots + x_{m-1} + \frac{uc^{1/m}}{x_1 \cdots x_{m-1}} \right)^m \right) \\ &= \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q^*} \chi(x_1 + \cdots + x_{m-1}) \sum_{u \in \mathbb{F}_q^*} \chi\left(u\left(\frac{c^{1/m}}{x_1 \cdots x_{m-1}} - 1 \right) \right). \end{aligned}$$

The inner sum equals $q-1$ or -1 according as $x_1\cdots x_{m-1}$ is equal to $c^{1/m}$ or not. Hence,

$$\begin{aligned} qN(c)-(q-1)^{m-1} &= qk_{m-2}(c^{1/m}) - \sum_{x_1,\ldots,x_{m-1}\in\mathbb{F}_q^*} \chi(x_1+\cdots+x_{m-1}) \\ &= qk_{m-2}(c^{1/m}) - (-1)^{m-1}, \end{aligned}$$

and consequently

$$N(c) = k_{m-2}(c) + \frac{1}{q}\left((q-1)^{m-1} - (-1)^{m-1}\right),$$

since $k_{m-2}(c^{1/m}) = k_{m-2}(c)$. It now follows from (6.1) that

$$N_m(a,b) = \frac{q^{m-1}-1}{q-1} + (-1)^{m-1}k_{m-2}(c),$$

and the Deligne bound concludes the proof. ∎

By Theorem 6.1, equation (2.1), and Lemma 2.1 we get an expression for $P_m(a,b)$ in terms of a hyper-Kloosterman sum:

Corollary 6.2. *If $m = p^k > 2$ and $ab \neq 0$, then*

$$mP_m(a,b) = \frac{q^{m-1}-1}{q-1} + (-1)^{m-1}k_{m-2}(b/a^m).$$

6.1. *Irreducible cubics over $\mathbb{F}_{3^r}$.* Next we consider the number of irreducible cubics $P_3(a,b)$ when $q = 3^r$. The main result of this section is the following:

Corollary 6.3. *Let $q = 3^r$ and let $a,b \in \mathbb{F}_q$ with $ab \neq 0$. Then $P_3(a,b) = (q+1+t)/3$ where t is an integer satisfying the following two conditions*:

(i) $t \equiv -1 \pmod 3$,
(ii) $|t| < 2\sqrt{q}$.

Conversely, for a given integer t satisfying conditions (i) *and* (ii) *there are exactly $(q-1)H(t^2-4q)$ pairs $(a,b) \in \mathbb{F}_q^2$ with $ab \neq 0$ and $P_3(a,b) = (q+1+t)/3$. Here $H(d)$ is the Kronecker class number of d.*

Proof. For a given $c \in \mathbb{F}_q^*$ there are exactly $q-1$ pairs $(a,b) \in \mathbb{F}_q^2$ such that $c = b/a^3$. Corollary 6.2 and Theorem 6.4 below complete the proof. ∎

Theorem 6.4 ([12]). *Let $q = 3^r$. The range S of $k_1(c)$, as c runs over $\mathbb{F}_q^*$, is given by*

$$S = \{t \in \mathbb{Z} : |t| < 2\sqrt{q} \text{ and } t \equiv -1 \pmod 3\}.$$

Moreover, each value $t \in S$ is attained exactly $H(t^2-4q)$ times.

Example 6.5. Let $q = 3$. If t is an integer satisfying conditions (i) and (ii) then $t = -1$ or $t = 2$. There should be exactly $(3-1)H(1-12) = 2$ pairs (a, b) with $ab \neq 0$ and $P_3(a, b) = 1$, and exactly $(3-1)H(4-12) = 2$ pairs (a, b) with $ab \neq 0$ and $P_3(a, b) = 2$.

Indeed, the two pairs (a, b) for which there is exactly one irreducible polynomial $x^3 + ax^2 + cx + b \in \mathbb{F}_3[x]$ are $(a, b) = (1, 1), (2, 2)$, and the corresponding irreducible cubics are

$$x^3 + x^2 + 2x + 1, \qquad x^3 + 2x^2 + 2x + 2.$$

The two pairs (a, b) for which there are exactly two irreducible cubics are $(a, b) = (1, 2), (2, 1)$ and the corresponding irreducible cubics are

$$x^3 + x^2 + 2, \qquad x^3 + x^2 + x + 2, \qquad x^3 + 2x^2 + 1, \qquad x^3 + 2x^2 + x + 1.$$

Finally, for a pair $(0, b)$ there should be, by Example 3.6, exactly one irreducible cubic. Indeed, the corresponding polynomials are

$$x^3 + 2x + 1, \qquad x^3 + 2x + 2.$$

Thus we have counted all the eight irreducible cubics in $\mathbb{F}_3[x]$.

6.2. *Irreducible quartics over* $\mathbb{F}_{2^r}$. We conclude Section 6 by considering the number of irreducible quartics $P_4(a, b)$ when $q = 2^r$. We need the following result by Carlitz which links one- and two-dimensional Kloosterman sums:

Theorem 6.6 ([2]). *Let $c \in \mathbb{F}_q^*$. Then*

$$k_2(c) = k_1(c)^2 - q.$$

Now we are able to prove the main result of this section:

Corollary 6.7. *Let $q = 2^r$ $(r > 1)$ and let $a, b \in \mathbb{F}_q$ with $ab \neq 0$. Then $P_4(a, b) = (q^2 + 2q + 1 - t^2)/4$, where t is an integer satisfying the following two conditions*:

(i) $t \equiv 1 \pmod 2$,
(ii) $1 \le t < 2\sqrt{q}$.

Conversely, for a given integer t satisfying conditions (i) *and* (ii) *there are exactly $(q-1)H(t^2 - 4q)$ pairs $(a, b) \in \mathbb{F}_q^2$ with $ab \neq 0$ and $P_4(a, b) = (q^2 + 2q + 1 - t^2)/4$.*

Proof. Let $c = b/a^4$. By Corollary 6.2, $4P_4(a, b) = q^2 + q + 1 - k_2(c)$, and now, by Theorem 6.6, we get

$$4P_4(a, b) = q^2 + 2q + 1 - k_1(c)^2.$$

Theorem 6.8 below completes the proof. ∎

THEOREM 6.8 ([13]). *Let $q = 2^r$. The range S of $k_1(c)$, as c runs over $\mathbb{F}_q^*$, is given by*

$$S = \{t \in \mathbb{Z} : |t| < 2\sqrt{q} \textit{ and } t \equiv -1 \pmod 4\}.$$

Moreover, each value $t \in S$ is attained exactly $H(t^2 - 4q)$ times.

EXAMPLE 6.9. Let $q = 4$. Now $t = 1$ and $t = 3$ are the only integers satisfying (i) and (ii). There should be exactly $(4-1)H(1-16) = 6$ pairs (a, b) with $ab \neq 0$ and $P_4(a, b) = (16 + 8 + 1 - 1)/4 = 6$, and exactly $(4-1)H(9-16) = 3$ pairs (a, b) with $ab \neq 0$ and $P_4(a, b) = (16+8+1-9)/4 = 4$.

Indeed, if $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$, then the six pairs (a, b) for which there are exactly six irreducible polynomials $x^4 + ax^3 + \cdots + b \in \mathbb{F}_4[x]$ are

$$(a, b) = (1, \alpha), (1, \beta), (\alpha, 1), (\alpha, \beta), (\beta, 1), (\beta, \alpha),$$

and the three pairs (a, b) for which there are exactly four irreducible quartics are

$$(a, b) = (1, 1), (\alpha, \alpha), (\beta, \beta).$$

Finally, for a pair $(0, b)$ there should be, by Example 3.6, exactly $(q^2 + q + 1 - (q + 1))/4 = 4$ irreducible quartics. This is indeed the case, and so we counted all the $6 \cdot 6 + 3 \cdot 4 + 4 \cdot 3 = 60$ irreducible quartics in $\mathbb{F}_4[x]$.

7. Divisibility modulo three of Kloosterman sums, $q = 2^r$. Let $q = 2^r$. We consider the divisibility modulo three of Kloosterman sums $k(c) := k_1(c)$. We use the following notations:

$\mathrm{Tr}^q_{2^s}$	the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_{2^s}$
A	the set of elements $a \in \mathbb{F}_q$ with $\mathrm{Tr}^q_2(a) = 0$
$T_3(b)$	the number of irreducibles $x^3 + ax^2 + cx + b \in \mathbb{F}_q[x]$ with b fixed and a running over the set A

We need the following

THEOREM 7.1 ([15]). *Let $\alpha \in \mathbb{F}_{q^m}^*$. Then*

$$\sum_{x \in \mathbb{F}_{q^m}^*} e(\alpha x^{q-1}) = (-1)^{m-1}(q-1)k_{m-1}(\mathrm{Norm}_m(\alpha)).$$

LEMMA 7.2. *Let $b \in \mathbb{F}_q^*$. Then*

$$T_3(b) = \tfrac{1}{3}\big(\tfrac{1}{2}(q^2 + 1 + k(b)^2) - N(b)\big),$$

where $N(b)$ is the number of solutions of $x^3 = b$ in A.

Proof. By Lemma 2.1,

$$3T_3(b) = \sum_{a \in A} N_3(a, b) - \sum_{a \in A} N_1(a, b). \tag{7.1}$$

By (2.1) the latter sum is equal to $N(b)$. Consider next the first sum. Apply Lemma 2.3 with $t = m = 3$ to get

$$\sum_{a\in A} N_3(a,b) = \frac{q^3-1}{2(q-1)} + \frac{1}{q(q-1)} \sum_{a\in A} \sigma_3(a,b),$$

where

$$\begin{aligned}\sum_{a\in A} \sigma_3(a,b) &= \sum_{c\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^3}^*} e(c\gamma_3^{i_0} x^{q-1}) \sum_{a\in A} \chi(ca)\\ &= \frac{1}{2} \sum_{c\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^3}^*} e(c\gamma_3^{i_0} x^{q-1}) \sum_{a\in\mathbb{F}_q} \chi(c(a+a^2)).\end{aligned}$$

Since $\chi(ca) = \chi(c^2a^2)$ the orthogonality of characters implies

$$\begin{aligned}\sum_{a\in A} \sigma_3(a,b) &= \frac{1}{2} \sum_{c\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^3}^*} e(c\gamma_3^{i_0} x^{q-1}) \sum_{a\in\mathbb{F}_q} \chi((c+c^2)a^2)\\ &= \frac{q}{2} \sum_{x\in\mathbb{F}_{q^3}^*} e(\gamma_3^{i_0} x^{q-1}).\end{aligned}$$

By Theorems 7.1 and 6.6 we get

$$\sum_{a\in A} \sigma_3(a,b) = \tfrac{1}{2} q(q-1)k_2(b) = \tfrac{1}{2} q(q-1)(k_1(b)^2 - q)$$

(note that $\mathrm{Norm}_3(\gamma_3^{i_0}) = g^{i_0} = b$), and therefore

$$\sum_{a\in A} N_3(a,b) = \tfrac{1}{2}(q^2 + q + 1 + k_1(b)^2 - q).$$

Equation (7.1) now completes the proof. ■

Theorem 7.3. *Let $q = 2^r$, and let $b \in \mathbb{F}_q^*$. Then 3 divides $k(b)$ if and only if one of the following condition holds*:

(1) *r is odd and* $\mathrm{Tr}_2^q(\sqrt[3]{b}) = 0$,

(2) *r is even, $b = a^3$ for some $a \in \mathbb{F}_q$, and* $\mathrm{Tr}_4^q(a) \neq 0$.

Proof. We have, by Lemma 7.2,

$$\tfrac{1}{2}(q^2 + 1 + k(b)^2) - N(b) \equiv 0 \pmod 3,$$

or equivalently,

$$k(b)^2 \equiv -N(b) - 2 \pmod 3.$$

Hence, $3 \mid k(b)$ if and only if $N(b) \equiv 1 \pmod 3$ if and only if $N(b) = 1$. If r is odd, then $x^3 = b$ has the unique solution $x = \sqrt[3]{b}$ in $\mathbb{F}_q$ and therefore $N(b) = 1$ if and only if $\mathrm{Tr}_2^q(\sqrt[3]{b}) = 0$.

Assume r is even and let ζ ($\in \mathbb{F}_4$) be a primitive third root of unity. Now $N(b) = 1$ if and only if $b = a^3$ and $\mathrm{Tr}_2^q(a\zeta^i) = 0$, for some $a \in \mathbb{F}_q$ and for unique $i \in \{0,1,2\}$. It follows by the transitivity of Tr_2^q that the latter condition is equivalent to $\mathrm{Tr}_4^q(a) \neq 0$. ∎

REMARK 7.4. In the case of r odd Theorem 7.3 follows also from [3, Thm. 3] proved by using different methods.

8. A proof for the value distribution of a Kloosterman sum, $q = 3^r$. The aim of this section is to give a fairly elementary proof for Theorem 6.4. Let $q = 3^r$, and let $c \in \mathbb{F}_q^*$. Let $k(c) := k_1(c)$ and let $\mathcal{X}$ be the elliptic curve over $\mathbb{F}_q$ defined by

$$\mathcal{X}: \ y^2 + cy + xy = x^3.$$

LEMMA 8.1.

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 + k(c) \quad \textit{and} \quad k(c) \equiv -1 \pmod 3.$$

Proof. Choose $p = m = 3$, and combine Theorem 5.1 and Corollary 6.2 to get

$$|\mathcal{X}(\mathbb{F}_q)| = 3P(1,c) = q + 1 + k(c). \ ∎$$

LEMMA 8.2. *$\mathcal{X}$ is isomorphic over $\mathbb{F}_q$ to $\mathcal{X}' : y^2 = x^3 + x^2 - c$.*

Proof. Complete the square to get the equation of $\mathcal{X}$ in the form

$$(y + x + c)^2 = x^3 + (x + c)^2.$$

Then substitute $y \mapsto y - x - c$, $x \mapsto x - c$ to get

$$y^2 = x^3 + x^2 - c^3,$$

and then substitute $x \mapsto x^3$, $y \mapsto y^3$ to obtain

$$(y^2 - x^3 - x^2 - c)^3 = 0. \ ∎$$

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$. Starting from the long Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

of the equation of $\mathcal{E}$, it is easy to see (see e.g. [19, p. 10]) that the equation of $\mathcal{E}$ can be given in the form

$$y^2 = x^3 + ax^2 + cx + d.$$

If $a \neq 0$ the substitution $x \mapsto x + e$ with $e = c/a$ yields the equation

$$y^2 = x^3 + ax^2 + e^3 + ae^2 + ce + d,$$

and therefore we may assume that the equation of $\mathcal{E}$ is one of the following:

(i) $y^2 = x^3 + ax^2 + b$,
(ii) $y^2 = x^3 + cx + b$,

for some $a, b, c \in \mathbb{F}_q$. Since $\mathcal{E}$ is smooth we must have $ab \neq 0$ in case (i), and $c \neq 0$ in case (ii).

The j-invariant of $\mathcal{E}$ is given by

$$j(\mathcal{E}) = \begin{cases} -a^3/b & \text{in case (i)}, \\ 0 & \text{in case (ii)}. \end{cases}$$

LEMMA 8.3. *Let $|\mathcal{E}(\mathbb{F}_q)| = q+1+t$. The following three conditions are equivalent*:

(1) *$\mathcal{E}$ is supersingular*,
(2) $j(\mathcal{E}) = 0$,
(3) $3 \mid t$.

Proof. See [19, pp. 75, 121]. ■

Assume next that $\mathcal{E}$ is ordinary (i.e. non-supersingular). We may now assume that $\mathcal{E}$ is defined by

$$\mathcal{E}: \ y^2 = x^3 + ax^2 + b.$$

LEMMA 8.4. *If a is a square in $\mathbb{F}_q^*$ then $\mathcal{E}$ is isomorphic over $\mathbb{F}_q$ to*

$$\mathcal{X}': \ y^2 = x^3 + x^2 + b/a^3,$$

and $|\mathcal{E}(\mathbb{F}_q)| = q+1+t$ for some integer t with $t \equiv -1 \pmod 3$.

If a is not a square, then $|\mathcal{E}(\mathbb{F}_q)| = 2(q+1) - |\mathcal{X}'(\mathbb{F}_q)|$, and $|\mathcal{E}(\mathbb{F}_q)| = q+1+t$ for some integer t with $t \equiv 1 \pmod 3$.

Proof. If $a = c^2$ for some $c \in \mathbb{F}_q^*$, the substitution $x \mapsto ax$, $y \mapsto c^3 y$ yields the equation $y^2 = x^3 + x^2 + b/a^3$. Assume next that a is not a square. Let η be the quadratic character of $\mathbb{F}_q$ with $\eta(0) = 0$. The number of solutions N of $y^2 = x^3 + ax^2 + b$ in $\mathbb{F}_q^2$ is

$$N = \sum_{x \in \mathbb{F}_q} (1 + \eta(x^3 + ax^2 + b)) = q + \sum_{x \in \mathbb{F}_q} \eta(x^3 + ax^2 + b).$$

Now substitute $x \mapsto ax$ to obtain

$$N = q + \eta(a) \sum_{x \in \mathbb{F}_q} \eta(x^3 + x^2 + b/a^3) = q - \sum_{x \in \mathbb{F}_q} \eta(x^3 + x^2 + b/a^3),$$

and so

$$|\mathcal{E}(\mathbb{F}_q)| = N + 1 = q + 1 - (|\mathcal{X}'(\mathbb{F}_q)| - (q+1)).$$

The remaining assertions follow immediately from Lemmas 8.2 and 8.1. ■

Proof of Theorem 6.4. Let $t \equiv -1 \pmod 3$ be an integer belonging to the interval $(-2\sqrt{q}, 2\sqrt{q})$. By Theorem 8.5 below there exist exactly $H(t^2 - 4q)$ pairwise non-isomorphic elliptic curves $\mathcal{E}$ with $|\mathcal{E}(\mathbb{F}_q)| = q+1+t$, and by Lemma 8.3 each of them is ordinary. Now, by Lemma 8.4 each $\mathcal{E}$ is isomorphic over $\mathbb{F}_q$ to $\mathcal{X}' : y^2 = x^3 + x + c$ for some $c \in \mathbb{F}_q^*$, and finally Lemmas 8.2 and 8.1 conclude the proof. ■

THEOREM 8.5 ([8, 17]). *The number $M(t)$ of isomorphism classes of elliptic curves over $\mathbb{F}_q$ having $q+1+t$ points with* $\gcd(q,t)=1$ *is given by*

$$M(t) = \begin{cases} H(t^2-4q) & \text{if } t^2 < 4q, \\ 0 & \text{otherwise.} \end{cases}$$

REMARK 8.6. Yet another proof of Theorem 6.4, which uses fairly advanced methods, is given in [9].

References

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

[2] —, *A note on exponential sums*, Pacific J. Math. 30 (1969), 35–37.

[3] P. Charpin, T. Helleseth and V. Zinoviev, *The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd*, J. Combin. Theory Ser. A 114 (2007), 322–338.

[4] S. D. Cohen, *Gauss sums and a sieve for generators of Galois fields*, Publ. Math. Debrecen 56 (2000), 293–312.

[5] —, *Explicit theorems on generator polynomials*, Finite Fields Appl. 11 (2005), 337–357.

[6] S. D. Cohen and S. Huczynska, *Primitive free quartics with specified norm and trace*, Acta Arith. 109 (2003), 359–385.

[7] P. Deligne, *Applications de la formule des traces aux sommes trigonométriques*, in: SGA $4\frac{1}{2}$, Lecture Notes in Math. 569, Springer, Berlin, 1977, 168–232.

[8] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197–272.

[9] G. van der Geer and M. van der Vlugt, *Artin–Schreier curves and codes*, J. Algebra 139 (1991), 256–272.

[10] S. Huczynska and S. D. Cohen, *Primitive free cubics with specified norm and trace*, Trans. Amer. Math. Soc. 355 (2003), 3099–3116.

[11] N. M. Katz, *Estimates for Soto–Andrade sums*, J. Reine Angew. Math. 438 (1993), 143–161.

[12] N. M. Katz et R. Livné, *Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3*, C. R. Acad. Sci. Paris Sér. I Math. 309 (1989), 723–726.

[13] G. Lachaud and J. Wolfmann, *The weights of orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory 36 (1990), 686–692.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1997.

[15] M. Moisio, *On the number of rational points on some families of Fermat curves over finite fields*, Finite Fields Appl. 13 (2007), 546–562.

[16] M. Rosen, *Number Theory in Function Fields*, Springer, New York, 2002.

[17] R. Schoof, *Non-singular plane cubic curves over finite fields*, J. Combin. Theory Ser. A 46 (1987), 183–211.

[18] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp. 219 (1997), 1195–1212.

[19] L. C. Washington, *Elliptic Curves. Number Theory and Cryptography*, Chapman and Hall/CRC, Boca Raton, 2003.

[20] J. L. Yucas, *Irreducible polynomials over finite fields with prescribed trace/prescribed constant term*, Finite Fields Appl. 12 (2006), 211–221.

Department of Mathematics and Statistics
University of Vaasa
P.O. Box 700
FIN-65101 Vaasa, Finland
E-mail: mamo@uwasa.fi

Received on 23.7.2007
and in revised form on 20.11.2007 (5481)