

**The number of solutions of  $X^p + Y^q = 1$   
in certain finite fields**

Marko J. Moisio

*Dedicated to Ilkka Virtanen on the occasion of his 60th birthday*

**Abstract**

Moisio, Marko J. (2004). The number of solutions of  $X^p + Y^q = 1$  in certain finite fields. In *Contributions to Management Science, Mathematics and Modelling. Essays in Honour of Professor Ilkka Virtanen*. Acta Wasaensia No. 122, 125–130. Eds Matti Laaksonen and Seppo Pynnönen.

We derive a formula from which one can compute the number of solutions of  $X^p + Y^q = 1$  in certain finite fields.

*Marko J. Moisio*, Department of Mathematics and Statistics, University of Vaasa, P.O. Box 700, FIN-65101 Vaasa, Finland.

**Key words:** Equations over finite fields, Jacobi sums, Gauss sums.

*Mathematics Subject Classification (2000):* 11T06; 11T23; 11T24; 11T71.

**1. Introduction**

A classical problem in number theory is the determination of the number of solutions of polynomial equations  $f(X, Y) = 0$  over finite fields. It is known that this is a very difficult problem in general. In this paper we study polynomial equations  $X^p + Y^q = 1$  with  $p, q$  satisfying certain conditions and obtain a formula from which we can calculate the number of the solutions of them. This problem is important also in coding theory, since it is known that one can construct good error-correcting codes based on the polynomial equations having many solutions with respect to the size of the finite field over which the polynomials are defined.

**2. The formula**

Let  $p$  and  $q$  be two distinct odd prime numbers and denote  $N = pq$ . We shall

assume that the index of  $\langle 2 \rangle$  in  $\mathbb{Z}_N^*$  [ $\mathbb{Z}_N^* : \langle 2 \rangle$ ] = 2 and  $k = \phi(N)/2$ . Let  $K$  be a field with  $2^k$  elements and  $E_l$  the extension of  $K$  with  $2^{kl}$  elements. Let  $f(X, Y) = X^p + Y^q - 1 \in K[X, Y]$ . Let  $N(l)$  denote the number of solutions of  $f(X, Y) = 0$  in  $E_l^2$ . In a forthcoming paper (Moisio and Väänänen, to appear) we proved, as a special case of Theorem 1 of that article, that

If  $\mathbb{Z}_p^* = \langle 2 \rangle$  and  $\mathbb{Z}_q^* = \langle 2 \rangle$  then

$$(1) \quad N(l) = 2^{kl} - \frac{(p-1)(q-1)}{2}(\alpha^l + \bar{\alpha}^l),$$

where

$$\alpha = 2^{h-1}(a + b\sqrt{-pq}),$$

and  $(a, b)$  is a solution of the Diophantine equation

$$a^2 + pqb^2 = 2^{k-2h+2}$$

satisfying  $a \equiv 2^{k-h+1} \pmod{p}$ ,  $a \equiv 1 \pmod{2}$ , and

$$h = \min\left\{S_2\left(\frac{2^k-1}{pq}\right), k - S_2\left(\frac{2^k-1}{pq}\right)\right\}$$

where  $S_2(j)$  denotes the digit sum in binary expansion of  $j \in \mathbb{Z}_+$ . We remark that the Diophantine equation can be solved with a very fast, in fact  $\mathcal{O}(k)$ , algorithm introduced in Hardy, Muskat, and Williams (1990).

The aim of this article is to present a simple proof of (1) by following the classical method of A. Weil appeared in his famous paper (Weil 1949), where he expressed the number of solutions of

$$a_1x^{m_1} + \cdots + a_kx^{m_k} = 1$$

in terms of so-called Jacobi sums, and furthermore in terms of so-called Gauss sums. After that we use our knowledge of the Gauss sums appearing in the consideration of the equation  $f(X, Y) = 0$ . We remark that the method used in Moisio and Väänänen was totally different from the method we are using in this article.

Let  $\chi$  be the generator of the group of multiplicative characters of  $E_l^*$ , i.e.

$$\begin{aligned} \chi : E_l^* &\longrightarrow \mathbb{C}, \\ \chi(ab) &= \chi(a)\chi(b) \quad \forall a, b \in E_l^*, \\ \widehat{E}_l^* &= \langle \chi \rangle . \end{aligned}$$

We extend every character to  $E_l$  by defining  $\chi^j(0) = 0$  if  $0 < j < 2^{kl} - 1$  and  $\chi^0(0) = 1$ .

**Lemma 1.** *Let  $\lambda \in \widehat{E}_l^*$ ,  $\text{ord}(\lambda) = t$  and  $a \in E_l$ . Then the number of solutions of  $X^t = a$  in  $E_l$  is given by*

$$S_l(X^t = a) = \sum_{j=0}^{t-1} \lambda^j(a).$$

*Proof.* If  $a = 0$  the equality is obvious. Let  $\gamma$  be a primitive element of  $E_l$  and let  $a = \gamma^k$ . Now  $\gamma^{ti} = a$  iff  $ti \equiv k \pmod{2^{kl} - 1}$ . The congruence has exactly  $t$  solutions if  $t \mid k$  and no solutions if  $t \nmid k$ . The claim follows now by noting that the sum is a geometric sum.

Let  $\lambda, \psi \in \widehat{E}_l^*$ ,  $\text{ord}(\lambda) = p$ ,  $\text{ord}(\psi) = q$ . Now, by Lemma 1, we have

$$\begin{aligned} N(l) &= \sum_{\substack{a, b \in E_l \\ a+b=1}} S_l(X^p = a) S_l(Y^q = b) \\ &= \sum_{a+b=1} \left( \sum_{i=0}^{p-1} \lambda^i(a) \right) \left( \sum_{j=0}^{q-1} \psi^j(b) \right) \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \left( \sum_{a+b=1} \lambda^i(a) \psi^j(b) \right) \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} J(\lambda^i, \psi^j). \end{aligned}$$

Here  $J(\lambda^i, \psi^j)$  is a Jacobi sum with the following properties (see Lidl and Niederreiter 1984 for a proof):

$$\begin{aligned} J(\lambda^0, \psi^0) &= 2^{kl}, \\ J(\lambda^0, \psi^j) &= J(\lambda^i, \psi^0) = 0 \text{ if } i, j \neq 0, \\ J(\lambda^i, \psi^j) &= -1 \text{ if } \lambda^i \psi^j = \chi_0 \text{ and } i, j \neq 0, \end{aligned}$$

where  $\chi_0$  is the trivial character.

**Lemma 2.** *Let  $0 \leq i \leq p-1$  and  $0 \leq j \leq q-1$ . Then  $\lambda^i \psi^j = \chi_0$  if and only if  $i = j = 0$ .*

*Proof.* If  $\lambda^i \psi^j = \chi_0$  then  $\lambda^i \in \langle \psi \rangle \cap \langle \lambda \rangle =: H$ . Since  $\gcd(p, q) = 1$  we have  $H = \langle \chi_0 \rangle$ . If  $i = j = 0$  then obviously  $\lambda^i \psi^j = \chi_0$ .

As a consequence,

$$N(l) = 2^{kl} + \sum_{i=1}^{p-1} \sum_{j=1}^{q-1} J(\lambda^i, \psi^j).$$

Let  $G(\eta)$  denote the Gauss sum,

$$G(\eta) = \sum_{a \in E_l^*} (-1)^{\text{Tr}(a)} \eta(a),$$

where  $\eta \in \widehat{E_l^*}$  and  $\text{Tr}(a) = a + a^2 + a^{2^2} + \dots + a^{2^{kl-1}}$ . Gauss sums have the following properties (see Lidl and Niederreiter 1984 for a proof):

$$\begin{aligned} |G(\eta)| &= 2^{kl/2} \text{ if } \eta \neq \chi_0, \\ J(\lambda^i, \psi^j) &= \frac{G(\lambda^i)G(\psi^j)}{G(\lambda^i \psi^j)} \text{ if } \lambda^i \psi^j \neq \chi_0. \end{aligned}$$

Now we have

$$J(\lambda^i, \psi^j) = G(\lambda^i)G(\psi^j)G(\lambda^{-i}\psi^{-j})/2^{kl}.$$

In Moisio (1998) we proved in an elementary way that

$$G(\lambda^i) = (-1)^{l-1} 2^{kl/2}, \quad G(\psi^j) = -2^{kl/2}.$$

Thus

$$J(\lambda^i, \psi^j) = (-1)^l G(\lambda^{-i}\psi^{-j}),$$

and we have

$$N(l) = 2^{kl} + (-1)^l \sum_{i=1}^{p-1} \sum_{j=1}^{q-1} G(\lambda^{-i}\psi^{-j}).$$

It is known (see Lidl and Niederreiter) that the value of  $G(\eta^t)$  depends only on the 2-cyclotomic coset of  $t$  modulo order of  $\eta$ . It is easy to see (cf. Moisio 1998) that  $\{0, \pm 1, p, q\}$  is a complete set of representatives of 2-cyclotomic cosets modulo  $pq$ .

**Lemma 3.**

$$G(\lambda^{-i}\psi^{-j}) = G(\chi^{\pm\frac{2^{kl}-1}{pq}}) \forall 1 \leq i \leq p-1, 1 \leq j \leq q-1,$$

and the sign is + for exactly  $(p-1)(q-1)/2$  pairs  $(i, j)$ .

*Proof.* Let  $\lambda = \chi^{\frac{2^{kl}-1}{p}}$  and  $\psi = \chi^{\frac{2^{kl}-1}{q}}$ . Now  $\lambda^{-i}\psi^{-j} = \chi^{-\frac{2^{kl}-1}{pq}(qi+pj)}$ . It is impossible to have  $qi + pj \equiv p2^s \pmod{pq}$  for some  $s$  since otherwise  $qi \equiv 0 \pmod{p}$  or  $p \mid i$ . Similarly it is impossible to have  $qi + pj \equiv q2^s \pmod{pq}$ . Thus  $qi + pj \equiv \pm 2^s \pmod{pq}$  for some  $s$ . If  $qi + pj \equiv \pm 2^s \pmod{pq}$  then  $q(p-i) + p(q-j) \equiv \mp 2^s \pmod{pq}$  proving the claim.

As a consequence

$$N(l) = 2^{kl} + (-1)^l \frac{(p-1)(q-1)}{2} \left( G(\chi^{\frac{2^{kl}-1}{pq}}) + G(\chi^{-\frac{2^{kl}-1}{pq}}) \right).$$

It follows from a deep theorem of Hasse and Davenport (see Lidl and Niederreiter 1984 for a proof) that

$$G(\chi^{\pm\frac{2^{kl}-1}{pq}}) = (-1)^{l-1} G(\sigma^{\pm\frac{2^k-1}{pq}})^l,$$

where  $\sigma$  is a generator of  $\widehat{K^*}$ . Thus,

$$N(l) = 2^{kl} - \frac{(p-1)(q-1)}{2} \left( G(\sigma^{\frac{2^k-1}{pq}})^l + G(\sigma^{-\frac{2^k-1}{pq}})^l \right).$$

We proved in Moisiso (1998) (see also van der Vlugt 1995) that

$$G(\sigma^{\frac{2^k-1}{pq}}) = \alpha$$

and so we have proved (1).

**Example 1.** The number of solutions of  $X^5 + Y^3 = 1$  in a field with  $2^{4l}$  elements is

$$N(l) = 2^{4l} - 4(\alpha^l + \bar{\alpha}^l),$$

where  $\alpha = 1 + \sqrt{-15}$ .

**Example 2.** The number of solutions of  $X^{1061} + Y^{1019} = 1$  in a field with  $2^{539540l}$  elements is

$$N(l) = 2^{539540l} - 539540(\alpha^l + \bar{\alpha}^l),$$

where

$$\alpha = 2^{269465}(a + b\sqrt{-1081159})$$

and

$$a = 15653893922452223679962310974017897281057358424919897563343594574939868921335590498498507507,$$

$$b = 60856290986390583356597858041834034244827604359378785044754804982717456405470460677418905.$$

## References

- Hardy, K., J.B. Muskat & K.S. Williams (1990). A deterministic algorithm for solving  $n = fu^2 + gv^2$  in coprime integers  $u$  and  $v$ . *Math. Comp.* 55, 327–343.
- Lidl, R. & H. Niederreiter (1984). *Finite Fields*. Cambridge: Cambridge Univ. Press.
- Moisio, M. (1998). Exponential sums, Gauss sums and cyclic codes, Dissertation. *Acta Univ. Oul. A* 306.
- Moisio, M. & K. Väänänen. A comparison of the number of rational places of certain function fields to the Hasse-Weil bounds. To appear in *Applicable Algebra in Engineering, Communication and Computing*.
- van der Vlugt, M. (1995). Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes. *J. Number Theory* 55, 145–159.
- Weil, A. (1949). Numbers of solutions of equations in finite fields. *Bull. of American Math. Society* 14, 497–508.