MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 211
JULY 1995, PAGES 1319–1331

A RECURSIVE METHOD TO CALCULATE THE NUMBER OF SOLUTIONS OF QUADRATIC EQUATIONS OVER FINITE FIELDS

KENICHI IYANAGA

ABSTRACT. The number $S_m(\alpha)$ of solutions of the quadratic equation

$$x_1^2 + x_2^2 + \cdots + x_m^2 = \alpha \quad (x_i^2 \neq \pm x_j^2 \quad \text{for } i \neq j)$$

for given m, with α and x_i belonging to a finite field, is studied and a recursive method to compute $S_m(\alpha)$ is established.

INTRODUCTION

Given a finite field $\mathbb{F}_q$ ($q = p^n$, p: odd prime), the estimation of the number of solutions of the quadratic equation in the abstract ($x_i \in \mathbb{F}^*$) is reduced to the study of certain vectors $\boldsymbol{\mu}_m$, and a recursive method to calculate this number is established. When $q = p$, the latter computation may be applied to calculate the number N_m of solutions of the congruence

$$x_1^2 + \cdots + x_m^2 \equiv 0 \pmod{p}, \quad 1 \leq x_1 < \cdots < x_m \leq \frac{p-1}{2}.$$

The number N_m is known to be related to the class number of $\mathbb{Q}(\sqrt{p})$ (Agoh [1]), and an algorithm, different from ours, to calculate it is given by Maohua [3] (see also Sun [4, 5]).

1. PREPARATORY LEMMAS AND PROPOSITION

1.1. In this section we shall establish three lemmas and a proposition, which will be used to prove Theorem 1. The latter gives an algorithm for computing the number of solutions of the quadratic equation specified in the abstract.

Given an odd prime number p and $q = p^n$, we let $\mathbb{F} = \mathbb{F}_q$ and set

$$\mathbb{F}^2 = \{x^2 | x \in \mathbb{F}^*\}.$$

We also set, for $\xi \in \mathbb{F}^*$,

$$(1) \qquad \nu_\xi = \frac{1}{2}\left(1 + \left(\frac{\xi}{q}\right)\right), \qquad \nu'_\xi = \frac{1}{2}\left(1 - \left(\frac{\xi}{q}\right)\right).$$

Received by the editor May 26, 1993 and, in revised form, December 16, 1993 and June 10, 1994.

1991 *Mathematics Subject Classification.* Primary 11E25, 11R29, 11Y16.

Key words and phrases. Quadratic equations over a finite field, number of solutions, algorithm.

The author extends his gratitude to Professors H. Wada and N. Adachi for their most valuable advice.

Lemma 1. *Given* $\xi, \eta \in \mathbb{F}^*$, *we have*

$$\text{(i)} \qquad \nu_\xi + \nu'_\xi = 1, \quad \nu_\xi \nu'_\xi = 0, \quad \nu_\xi^2 = \nu_\xi, \quad (\nu'_\xi)^2 = \nu'_\xi,$$

$$\text{(ii)} \qquad 2\nu_\xi \nu_\eta = \nu_\xi + \nu_\eta + \nu_{\xi\eta} - 1,$$

$$\text{(iii)} \qquad 2\nu'_\xi \nu'_\eta = \nu'_\xi + \nu'_\eta - \nu'_{\xi\eta}.$$

Proof. Assertion (i) follows directly from the definition. Since

$$\left(\frac{\xi}{q}\right) = 2\nu_\xi - 1,$$

we have

$$\left(\frac{\xi\eta}{q}\right) = 2\nu_{\xi\eta} - 1 = (2\nu_\xi - 1)(2\nu_\eta - 1),$$

which implies (ii). Similarly, since

$$\left(\frac{\xi}{q}\right) = 1 - 2\nu'_\xi,$$

(iii) follows from

$$\left(\frac{\xi\eta}{q}\right) = 1 - 2\nu'_{\xi\eta} = (1 - 2\nu'_\xi)(1 - 2\nu'_\eta). \quad \square$$

It is convenient to introduce the following notation:

$$\rho = \begin{cases} \dfrac{q-1}{4} & \text{if } \nu_{-1} = 1, \\ \dfrac{q-3}{4} & \text{if } \nu_{-1} = 0. \end{cases} \tag{2}$$

We note that

$$\frac{q-1}{4} = \rho + \frac{\nu'_{-1}}{2}. \tag{3}$$

1.2. Given α, β, γ belonging to $\mathbb{F}$, we set

$$\Lambda^{(\alpha)}_{\beta,\gamma} = \{(x, y) \in \mathbb{F}^2 \times \mathbb{F}^2 | \alpha x + \beta y = \gamma, y = 1 \text{ if } \beta = 0\} \tag{4}$$

and

$$\lambda^{(\alpha)}_{\beta,\gamma} = \sharp\Lambda^{(\alpha)}_{\beta,\gamma}, \qquad \lambda_{\beta,\gamma} = \lambda^{(1)}_{\beta,\gamma}. \tag{5}$$

These numbers will be used in the algorithm described in Theorem 1.

The following relations are easily deduced from the definitions:

$$\lambda^{(\alpha)}_{\beta,\gamma} = \lambda^{(1)}_{\alpha^{-1}\beta,\alpha^{-1}\gamma} \qquad (\alpha \in \mathbb{F}^*), \tag{6}$$

$$\lambda_{\xi^2\beta,\eta^2\gamma} = \lambda_{\beta,\gamma} \qquad (\xi, \eta \in \mathbb{F}^*), \tag{7}$$

$$\lambda^{(0)}_{00} = 2\rho + \nu'_{-1}, \ \lambda^{(0)}_{\beta,0} = \lambda^{(0)}_{0,\gamma} = 0, \ \lambda^{(0)}_{\beta,\gamma} = (2\rho + \nu'_{-1})\nu_{\beta\gamma} \quad (\beta, \gamma \in \mathbb{F}^*), \tag{8}$$

$$\lambda_{0,0} = 0, \quad \lambda_{\beta,0} = (2\rho + \nu'_{-1})\nu_{-\beta}, \quad \lambda_{0,\gamma} = \nu_\gamma \qquad (\beta, \gamma \in \mathbb{F}^*). \tag{9}$$

Given $\beta, \gamma \in \mathbb{F}^*$, it is known that $\lambda_{\beta,\gamma}$ may be computed by using Jacobi sums [2]. In the following, we shall show that group-theoretical considerations can be used to compute $\lambda_{\beta,\gamma}$.

1.3. We set, for a given $\alpha \in \mathbb{F}^*$,

$$A_\alpha = \left\{X \in M_2(\mathbb{F}) | X \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix} X \right\}$$

and

$$A_\alpha^* = A_\alpha \cap GL_2(\mathbb{F}), \qquad A_\alpha^1 = A_\alpha \cap SL_2(\mathbb{F}).$$

We have

$$A_\alpha = \left\{ \begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix} | x, y \in \mathbb{F} \right\}.$$

Lemma 2. *The following sequence is exact*:

$$1 \to A_\alpha^1 \to A_\alpha^* \overset{\det}{\to} \mathbb{F}^* \to 1.$$

Proof. It is sufficient to show, for a given $\beta \in \mathbb{F}^*$, that there exist $x, y \in \mathbb{F}^*$ satisfying $x^2 - \alpha y^2 = \beta$ or, equivalently, $x^2 = \alpha y^2 + \beta$. We now have

$$\sharp\{x^2 | x \in \mathbb{F}\} = \sharp\{\alpha y^2 + \beta | y \in \mathbb{F}\} = \frac{q+1}{2},$$

whence

$$\{x^2 | x \in \mathbb{F}\} \cap \{\alpha y^2 + \beta | y \in \mathbb{F}\} \neq \varnothing,$$

which implies Lemma 2.

Lemma 3. *Given* $\alpha \in \mathbb{F}^*$, *we have*

(i) $$\sharp A_\alpha^* = (q-1)(q+1-2\nu_\alpha),$$

(ii) $$\sharp A_\alpha^1 = q + 1 - 2\nu_\alpha.$$

Proof. We have

$$A_\alpha^* = A_\alpha - \left\{ \begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix} | x^2 - \alpha y^2 = 0 \right\},$$

whence we readily obtain (i). The second assertion (ii) then follows from Lemma 2. □

Proposition 1. *Given* $\alpha, \beta, \gamma \in \mathbb{F}^*$, *we have*

(i) $$4\lambda_{\beta,\gamma} = q + 1 - 2(\nu_{-\beta} + \nu_\gamma + \nu_{\beta\gamma}),$$

(ii) $$\lambda_{\beta,\gamma}^{(\alpha)} = \begin{cases} \rho - \nu_{-1}\nu_{\alpha\beta} & (\nu_{\beta\gamma} = 1), \\ \rho + \nu'_{-1}\nu'_{\alpha\gamma} & (\nu_{\beta\gamma} = 0). \end{cases}$$

Proof. Since

$$\begin{aligned} \sharp A_{-\beta}^1 &= \sharp\{(x, y) \in \mathbb{F} \times \mathbb{F} | x^2 + \beta y^2 = 1\} \\ &= \sharp\{(x, y) \in \mathbb{F} \times \mathbb{F} | x^2 + \beta y^2 = \gamma\} \\ &= 4\lambda_{\beta,\gamma} + \sharp\{(x, y) \in \mathbb{F} \times \mathbb{F} | x^2 + \beta y^2 = \gamma, xy = 0\}, \end{aligned}$$

the first claim (i) follows from Lemma 3(ii). We have

$$\begin{aligned} \lambda_{\beta,\gamma}^{(\alpha)} &= \lambda_{\alpha^{-1}\beta, \alpha^{-1}\gamma} \\ &= \frac{q+1}{4} - \frac{1}{2}(\nu_{-\alpha^{-1}\beta} + \nu_{\alpha^{-1}\gamma} + \nu_{\beta\gamma}) \\ &= \frac{q-1}{4} + \frac{1}{2} - \frac{1}{2}(\nu_{-\alpha\beta} + \nu_{\alpha\gamma} + \nu_{\beta\gamma}) \\ &= \rho + \frac{1}{2}(1 + \nu'_{-1} - \nu_{-\alpha\beta} - \nu_{\alpha\gamma} - \nu_{\beta\gamma}). \end{aligned}$$

If $\nu_{\beta\gamma} = 1$, we have

$$\lambda^{(\alpha)}_{\beta,\gamma} = \rho + \frac{1}{2}(1 - \nu_{-1} - \nu_{-\alpha\beta} - \nu_{\alpha\gamma})$$
$$= \rho + \frac{1}{2}(1 - \nu_{-1} - \nu_{-\alpha\beta} - \nu_{\alpha\beta}).$$

Whence, by Lemma 1(ii), we obtain

$$\lambda^{(\alpha)}_{\beta,\gamma} = \rho - \nu_{-1}\nu_{\alpha\beta}.$$

If, on the other hand, $\nu_{\beta\gamma} = 0$, we have

$$\lambda^{(\alpha)}_{\beta,\gamma} = \rho + \frac{1}{2}(1 + \nu'_{-1} - \nu_{-\alpha\beta} - \nu_{\alpha\gamma})$$
$$= \rho + \frac{1}{2}(\nu'_{-1} - \nu'_{-\alpha\gamma} + \nu'_{\alpha\gamma}),$$

whence, by Lemma 1(iii),

$$\lambda^{(\alpha)}_{\beta,\gamma} = \rho + \nu'_{-1}\nu'_{\alpha\gamma}. \quad \square$$

2. A RECURSIVE METHOD TO COMPUTE THE NUMBER OF SOLUTIONS OF CERTAIN QUADRATIC EQUATIONS

2.1. Given $\alpha \in \mathbb{F}$ and m $(1 \le m \le (1 + \nu'_{-1})\frac{q-1}{4})$, we set

$$S_m(\alpha) = \sharp\left\{(x_1, \dots, x_m) | x_i \in \mathbb{F}^*, \sum_{i=1}^{m} x_i^2 = \alpha, x_i^2 \ne \pm x_j^2 \ (i \ne j)\right\}. \tag{10}$$

In order to compute this number, we consider the following set:

$$M^{(\beta)}_{m,\alpha} = \left\{(J, x) | J \subseteq \mathbb{F}^2, J\text{: irreducible}, x \in J, \sharp J = m, \beta x + \sum_{y \in J - \{x\}} y = \alpha\right\}, \tag{11}$$

where $\beta \in \mathbb{F}$ and J is defined to be *irreducible* if and only if it does not contain any pair $\{z, -z\}$. Further, we set

$$M_{m,\alpha} = \left\{J \subseteq \mathbb{F}^2 | J\text{: irreducible}, \sharp J = m, \sum_{x \in J} x = \alpha\right\}, \tag{12}$$

$$\mu^{(\beta)}_{m,\alpha} = \sharp M^{(\beta)}_{m,\alpha}, \ \mu_{m,\alpha} = \sharp M_{m,\alpha}. \tag{13}$$

We have

$$\mu^{(\beta\xi^2)}_{m,\alpha\eta^2} = \mu^{(\beta)}_{m,\alpha} \qquad (\xi, \eta \in \mathbb{F}^*), \tag{14}$$

$$\mu^{(1)}_{m,\alpha} = m\mu_{m,\alpha}, \tag{15}$$

$$S_m(\alpha) = 2^m m! \mu_{m,\alpha}. \tag{16}$$

2.2. Now fix an element $r \in \mathbb{F}^*$ such that $\nu_r = 0$ and consider the following vectors $(\beta \in \mathbb{F},\ 1 \le m \le (1+\nu'_{-1})\frac{q-1}{4})$:

$$\boldsymbol{\mu}_m^{(\beta)} = (\mu_{m,0}^{(\beta)},\ \mu_{m,1}^{(\beta)},\ \mu_{m,r}^{(\beta)}), \tag{17}$$

$$\boldsymbol{\mu}_m = (\mu_{m,0},\ \mu_{m,1},\ \mu_{m,r}). \tag{18}$$

Since $S_m(\alpha)$ equals either $S_m(0)$, $S_m(1)$ or $S_m(r)$, the problem of computing $S_m(\alpha)$ is, by virtue of (16), reduced to the computation of the vectors $\boldsymbol{\mu}_m$.

2.3. Given an element $\beta \in \mathbb{F}$ and a fixed element $r \in \mathbb{F}^*$ such that $\nu_r = 0$, we shall introduce here a matrix $L^{(\beta)}$ which will be used to compute $\boldsymbol{\mu}_m$:

$$L^{(\beta)} = \begin{pmatrix} \lambda_{0,0}^{(\beta)} & \lambda_{0,1}^{(\beta)} & \lambda_{0,r}^{(\beta)} \\ \lambda_{1,0}^{(\beta)} & \lambda_{1,1}^{(\beta)} & \lambda_{1,r}^{(\beta)} \\ \lambda_{r,0}^{(\beta)} & \lambda_{r,1}^{(\beta)} & \lambda_{r,r}^{(\beta)} \end{pmatrix}. \tag{19}$$

The following proposition follows easily from (8), (9) and Proposition 1 (ii).

Proposition 2. *We have*

(i) $$L^{(0)} = (2\rho + \nu'_{-1})E_3.$$

For $\beta \in \mathbb{F}^*$,

(ii) $$L^{(\beta)} = \begin{pmatrix} 0 & \nu_\beta & \nu'_\beta \\ (2\rho+\nu'_{-1})\nu_{-\beta} & \rho - \nu_{-1}\nu_\beta & \rho + \nu'_{-1}\nu_\beta \\ (2\rho+\nu'_{-1})\nu'_{-\beta} & \rho + \nu'_{-1}\nu'_\beta & \rho - \nu_{-1}\nu'_\beta \end{pmatrix}.$$

Theorem 1. *Given* $\xi \in \mathbb{F}^*$, *set*

$$\nu_\xi = \frac{1}{2}\left(1 + \left(\frac{\xi}{q}\right)\right), \qquad \nu'_\xi = \frac{1}{2}\left(1 - \left(\frac{\xi}{q}\right)\right).$$

Also, given $\alpha \in \mathbb{F}$ *and* $1 \le m \le (1+\nu'_{-1})\frac{q-1}{4}$, *set*

$$S_m(\alpha) = \sharp\left\{(x_1,\ \dots,\ x_m) \middle| x_i \in \mathbb{F}^*,\ \sum_{i=1}^m x_i^2 = \alpha,\ x_i^2 \ne \pm x_j^2\ (i \ne j)\right\},$$

and let $\boldsymbol{\mu}_m^{(\beta)} = (\mu_{m,0}^{(\beta)},\ \mu_{m,1}^{(\beta)},\ \mu_{m,r}^{(\beta)})$ *and* $\boldsymbol{\mu}_m = (\mu_{m,0},\ \mu_{m,1},\ \mu_{m,r})$ *be the vectors defined by* (17) *and* (18) $(\beta \in \mathbb{F},\ \nu_r = 0,\ r \in \mathbb{F}^*)$, *and let* $L^{(\beta)}$ *be the matrix defined by* (19). *We then have*

(i) $$S_m(\alpha) = 2^m m! \mu_{m,\alpha} \qquad (\alpha = 0,\ 1,\ r),$$

(ii) $$\boldsymbol{\mu}_m^{(1)} = m\boldsymbol{\mu}_m,$$

(iii) $$\boldsymbol{\mu}_1^{(\beta)} = (0,\ \nu_\beta,\ \nu'_\beta)\ (\beta \ne 0), \qquad \boldsymbol{\mu}_1^{(0)} = \left(\frac{q-1}{2},\ 0,\ 0\right),$$

(iv) $$\boldsymbol{\mu}_m^{(\beta)} = \boldsymbol{\mu}_{m-1}L^{(\beta)} - \boldsymbol{\mu}_{m-1}^{(\beta+1)} - \nu_{-1}\boldsymbol{\mu}_{m-1}^{(\beta-1)} \qquad (1 < m).$$

Proof. The first three statements (i), (ii) and (iii) are clear from the definitions (see (15), (16)); the fourth, (iv), is equivalent to

$$\mu_{m,\alpha}^{(\beta)} = \mu_{m-1,0}\lambda_{0,\alpha}^{(\beta)} + \mu_{m-1,1}\lambda_{1,\alpha}^{(\beta)} + \mu_{m-1,r}\lambda_{r,\alpha}^{(\beta)} - \mu_{m-1,\alpha}^{(\beta+1)} - \nu_{-1}\mu_{m-1,\alpha}^{(\beta-1)}.$$

In order to prove the above, suppose we are given $(J, x) \in M_{m,\alpha}^{(\beta)}$ with $J = \{x, y_1, \dots, y_{m-1}\}$ satisfying

$$\beta x + \sum_{i=1}^{m-1} y_i = \alpha.$$

Then, the set $J' = \{y_1, \dots, y_{m-1}\}$ belongs to $M_{m-1, \alpha-\beta x}$. We have

$$\alpha - \beta x = 0 \text{ or } \alpha - \beta x = y^2 \text{ or } \alpha - \beta x = rz^2 \qquad (y, z \in \mathbb{F}^*),$$

and accordingly,

$$(J', (x, 1)) \in M_{m-1,0} \times \Lambda_{0,\alpha}^{(\beta)}, \ (y^{-2}J', (x, y^2)) \in M_{m-1,1} \times \Lambda_{1,\alpha}^{(\beta)}$$

or

$$(z^{-2}J', (x, z^2)) \in M_{m-1,r} \times \Lambda_{r,\alpha}^{(\beta)},$$

where

$$wJ' = \{wy_1, \dots, wy_{m-1}\} \ (w \in \mathbb{F}^*).$$

Conversely, given

$$(x, y) \in \Lambda_{\gamma,\alpha}^{(\beta)} \qquad (\gamma = 0, 1, r; \ y = 1 \text{ if } \gamma = 0),$$

and $J' = \{y_1, \dots, h_{m-1}\}$ belonging to $M_{m-1,\gamma}$, we have

$$(\{x, yy_1, \dots, yy_{m-1}\}, x) \in M_{m,\alpha}^{(\beta)}$$

unless

$$x = \pm yy_j \quad \text{for some } j \ (1 \le j \le m-1)$$

($x = -yy_j$ may occur only when $\nu_{-1} = 1$). Let us set $J = \{x, yy_1, \dots, yy_{m-1}\}$. If $x = yy_j$, then $J = \{yy_1, \dots, yy_{m-1}\}$, and we have

$$(\beta + 1)yy_j + \sum_{k \neq j} yy_k = \alpha,$$

whence $(J, yy_j) \in M_{m-1,\alpha}^{(\beta+1)}$. If, on the other hand, $x = -yy_j$ $(\nu_{-1} = 1)$, then

$$(\beta - 1)x + \sum_{k \neq j} y_k = \alpha,$$

and we have

$$(\{x, yy_1, \dots, yy_{j-1}, yy_{j+1}, \dots, yy_{m-1}\}, x) \in M_{m-1,\alpha}^{(\beta-1)}.$$

Combining the above, we obtain (iv). This completes the proof. □

Specifically, for $1 < m \le (1 + \nu'_{-1})\frac{q-1}{4}$, we obtain the following:

$$\begin{aligned}\boldsymbol{\mu}_m^{(0)} &= \boldsymbol{\mu}_{m-1}L^{(0)} - \boldsymbol{\mu}_{m-1}^{(1)} - \nu_{-1}\boldsymbol{\mu}_{m-1}^{(-1)} \\ &= (2\rho + \nu'_{-1})\boldsymbol{\mu}_{m-1} - (m-1)\boldsymbol{\mu}_{m-1} - \nu_{-1}(m-1)\boldsymbol{\mu}_{m-1},\end{aligned}$$

whence

$$\boldsymbol{\mu}_m^{(0)} = (2\rho + \nu'_{-1} - (m-1)(1 + \nu_{-1}))\boldsymbol{\mu}_{m-1}. \tag{20}$$

2.4. We set $(1 + \nu'_{-1})\frac{q-1}{4} = \kappa$. Given $1 \le m \le \kappa$, we have

$$\sharp\{J \subset \mathbb{F}^2 | J\text{: irreducible}, \ \sharp J = m\} = \begin{cases} 2^m \binom{\kappa}{m} & \text{if } \nu_{-1} = 1, \\ \binom{\kappa}{m} & \text{if } \nu_{-1} = 0. \end{cases}$$

Hence, we have

$$\mu_{m,0}^{(\beta)} + \frac{q-1}{2}(\mu_{m,1}^{(\beta)} + \mu_{m,r}^{(\beta)}) = \begin{cases} 2^m m\binom{\kappa}{m} & \text{if } \nu_{-1} = 1, \\ m\binom{\kappa}{m} & \text{if } \nu_{-1} = 0. \end{cases} \tag{21}$$

In particular, we have

$$\mu_{m,0} + \frac{q-1}{2}(\mu_{m,1} + \mu_{m,r}) = \begin{cases} 2^m \binom{\kappa}{m} & \text{if } \nu_{-1} = 1, \\ \binom{\kappa}{m} & \text{if } \nu_{-1} = 0. \end{cases} \tag{22}$$

For $m = \kappa$, we have

$$\mu_{\kappa,0} + \frac{q-1}{2}(\mu_{\kappa,1} + \mu_{\kappa,r}) = \begin{cases} 2^\kappa & \text{if } \nu_{-1} = 1, \\ 1 & \text{if } \nu_{-1} = 0. \end{cases} \tag{23}$$

When $q = 3$, we have $\kappa = 1$ and $\boldsymbol{\mu}_\kappa = \boldsymbol{\mu}_1 = (0, 1, 0)$; whereas when $\nu_{-1} = 0$ and $q > 3$, we have $\frac{q-1}{2} > 1$ and therefore $\boldsymbol{\mu}_\kappa = (1, 0, 0)$.

2.5. We now compute $\boldsymbol{\mu}_2$ and $\boldsymbol{\mu}_3$. We have

$$\begin{aligned} 2\boldsymbol{\mu}_2 &= \boldsymbol{\mu}_2^{(1)} \\ &= \boldsymbol{\mu}_1 L^{(1)} - \boldsymbol{\mu}_1^{(2)} - \nu_{-1}\boldsymbol{\mu}_1^{(0)} \\ &= (0, 1, 0)\begin{pmatrix} 0 & 1 & 0 \\ 2\rho\nu_{-1} & \rho - \nu_{-1} & \rho + \nu'_{-1} \\ (2\rho+1)\nu'_{-1} & \rho & \rho \end{pmatrix} - (0, \nu_2, \nu'_2) \\ &\quad - \nu_{-1}(2\rho + \nu'_{-1})(1, 0, 0) \\ &= (0, \rho - \nu_{-1} - \nu_2, \rho + \nu'_{-1} - \nu'_2) \\ &= (0, \rho - \nu_{-1} - \nu_2, \rho - \nu_{-1} + \nu_2). \end{aligned}$$

Whence, we obtain

$$2\boldsymbol{\mu}_2 = (0, \rho - \nu_{-1} - \nu_2, \rho - \nu_{-1} + \nu_2). \tag{24}$$

We also have

$$\begin{aligned} 3\boldsymbol{\mu}_3 &= \boldsymbol{\mu}_3^{(1)} \\ &= \boldsymbol{\mu}_2 L^{(1)} - \boldsymbol{\mu}_2^{(2)} - \nu_{-1}\boldsymbol{\mu}_2^{(0)}, \\ \boldsymbol{\mu}_2^{(2)} &= \boldsymbol{\mu}_1 L^{(2)} - \boldsymbol{\mu}_1^{(3)} - \nu_{-1}\boldsymbol{\mu}_1^{(1)} \\ &= (0, 1, 0)L^{(2)} - (0, \nu_3, \nu'_3) - (0, \nu_{-1}, 0). \end{aligned}$$

By Proposition 2 (ii), we have

$$\boldsymbol{\mu}_2^{(2)} = ((2\rho + \nu'_{-1})\nu_{-2}, \rho - \nu_{-1} - \nu_3 - \nu_{-1}\nu_2, \rho - \nu'_3 + \nu'_{-1}\nu_2),$$

and, by the remark made following the proof of Theorem 1,

$$\nu_{-1}\boldsymbol{\mu}_2^{(0)} = \nu_{-1}(2\rho + \nu'_{-1} - 1 - \nu_{-1})\boldsymbol{\mu}_1 = 2\nu_{-1}(\rho - 1)\boldsymbol{\mu}_1,$$

and therefore,

$$\begin{aligned} 6\boldsymbol{\mu}_3 = (&2\rho^2 + (1 - 3\nu_{-1} - 4\nu_{-1}\nu_2 - 4\nu_{-2} + 2\nu_2)\rho + \nu'_{-1}(\nu_2 - 2\nu_{-2}), \\ &2\rho^2 - (2 + 7\nu_{-1})\rho + 7\nu_{-1} + 3\nu_{-1}\nu_2 + 2\nu_3, \\ &2\rho^2 - (1 + 3\nu_{-1})\rho + 2\nu'_3 - 3\nu'_{-1}\nu_2). \end{aligned}$$

Lemma 1 implies that

$$2\nu_{-1}\nu_2 = \nu_{-1} + \nu_2 + \nu_{-2} - 1\,,$$

whence

$$3\boldsymbol{\mu}_3 = \left(\rho^2 + \left(\frac{3}{2} - \frac{5}{2}\nu_{-1} - 3\nu_{-2}\right)\rho + \nu'_{-1}\left(\frac{\nu_2}{2} - \nu_{-2}\right),\right.$$
$$\tag{25} \rho^2 - \left(1 + \frac{7}{2}\nu_{-1}\right)\rho + \frac{7}{2}\nu_{-1} + \frac{3}{2}\nu_{-1}\nu_2 + \nu_3\,,$$
$$\left.\rho^2 - \left(\frac{1}{2} + \frac{3}{2}\nu_{-1}\right)\rho + \left(\nu'_3 - \frac{3}{2}\nu'_{-1}\nu_2\right)\right).$$

2.6. We note here that some of the classical formulas concerning quadratic residues can be obtained from the formulas (24) and (25) describing $\boldsymbol{\mu}_2$ and $\boldsymbol{\mu}_3$. The formula (24) for $\boldsymbol{\mu}_2$ leads to

$$\tag{26} \rho \equiv \nu_{-1} + \nu_2 \pmod 2,$$

or, equivalently,

$$\nu_2 \equiv \begin{cases} \dfrac{q-5}{4} \pmod 2 & \text{if } \left(\dfrac{-1}{q}\right) = 1, \\ \dfrac{q-3}{4} \pmod 2 & \text{if } \left(\dfrac{-1}{q}\right) = -1; \end{cases}$$

the latter implies the classical formula

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}.$$

(The above formula for $q = p$, may also be deduced from computing the number of solutions of $x_1^2 + x_2^2 \equiv 4 \pmod p$, as shown by Kenneth S. Williams [6].)

The formula (25) describing $\boldsymbol{\mu}_3$, on the other hand, implies

$$\tag{27} \rho^2 + \left(\frac{3}{2} - \frac{5}{2}\nu_{-1}\right)\rho + \nu'_{-1}\left(\frac{\nu_2}{2} - \nu_{-2}\right) \equiv 0 \pmod 3,$$

$$\tag{28} \rho^2 - \left(1 + \frac{7}{2}\nu_{-1}\right)\rho + \frac{7}{2}\nu_{-1} + \frac{3}{2}\nu_{-1}\nu_2 + \nu_3 \equiv 0 \pmod 3,$$

$$\tag{29} \rho^2 - \left(\frac{1}{2} + \frac{3}{2}\nu_{-1}\right)\rho + \left(\nu'_3 - \frac{3}{2}\nu'_{-1}\nu_2\right) \equiv 0 \pmod 3.$$

When $\nu_{-1} = 1$, it follows from the formulas (27) and (29) that

$$\rho^2 - \rho \equiv \rho^2 - 2\rho + \nu'_3 \equiv 0 \pmod 3,$$

whence

$$\tag{30} \rho \equiv \nu'_3 \pmod 3.$$

When, on the other hand, $\nu_{-1} = 0$, it follows from formula (28) that

$$\tag{31} \rho^2 - \rho + \nu_3 \equiv 0 \pmod 3.$$

Combining the congruences (30) and (31), we obtain the following special case of the law of quadratic reciprocity:

$$\left(\frac{3}{q}\right)\left(\frac{q}{3}\right) = (-1)^{\frac{q-1}{2}\frac{3-1}{2}}.$$

2.7. We now illustrate how Theorem 1 may be used to compute the vectors $\boldsymbol{\mu}_m$ by looking at an example: $q = p = 17$. In this case, we have

$$\rho = 4, \quad \nu_{-1} = 1, \quad \nu_{\pm 2} = 1, \quad \nu_{\pm 3} = 0.$$

We use the general formulas derived above to compute $\boldsymbol{\mu}_1$, $\boldsymbol{\mu}_2$, and $\boldsymbol{\mu}_3$:

$$\boldsymbol{\mu}_1 = (0, 1, 0) \quad \text{(Theorem 1(iii))}.$$

Now, by virtue of (24), we have

$$\boldsymbol{\mu}_2 = \frac{1}{2}(0, \rho - \nu_{-1} - \nu_2, \rho - \nu_{-1} + \nu_2) = \frac{1}{2}(0, 2, 4) = (0, 1, 2).$$

By (25), we have

$$\begin{aligned}\boldsymbol{\mu}_3 = \frac{1}{3}\Bigg(&\rho^2 + \left(\frac{3}{2} - \frac{5}{2}\nu_{-1} - 3\nu_{-2}\right)\rho + \nu'_{-1}\left(\frac{\nu_2}{2} - \nu_{-2}\right), \\ &\rho^2 - \left(1 + \frac{7}{2}\nu_{-1}\right)\rho + \frac{7}{2}\nu_{-1} + \frac{3}{2}\nu_{-1}\nu_2 + \nu_3, \\ &\rho^2 - \left(\frac{1}{2} + \frac{3}{2}\nu_{-1}\right)\rho + \left(\nu'_3 - \frac{3}{2}\nu'_{-1}\nu_2\right)\Bigg) \\ = \frac{1}{3}&(0, 3, 9) = (0, 1, 3).\end{aligned}$$

Also,

$$\begin{aligned} 4\boldsymbol{\mu}_4 &= \boldsymbol{\mu}_4^{(1)} \\ &= \boldsymbol{\mu}_3 L^{(1)} - \boldsymbol{\mu}_3^{(2)} - \nu_{-1}\boldsymbol{\mu}_3^{(0)}, \\ \boldsymbol{\mu}_3^{(2)} &= \boldsymbol{\mu}_2 L^{(2)} - \boldsymbol{\mu}_2^{(3)} - \nu_{-1}\boldsymbol{\mu}_2^{(1)}, \\ \boldsymbol{\mu}_2^{(3)} &= \boldsymbol{\mu}_1 L^{(3)} - \boldsymbol{\mu}_1^{(4)} - \nu_{-1}\boldsymbol{\mu}_1^{(2)}, \end{aligned}$$

and

$$L^{(1)} = L^{(2)} = \begin{pmatrix} 0 & 1 & 0 \\ 2\rho & \rho - 1 & \rho \\ 0 & \rho & \rho \end{pmatrix},$$

$$L^{(3)} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & \rho & \rho \\ 2\rho & \rho & \rho - 1 \end{pmatrix},$$

and therefore,

$$\begin{aligned} \boldsymbol{\mu}_2^{(3)} &= (0, 1, 0)L^{(3)} - (0, 1, 0) - (0, 1, 0) \\ &= (0, \rho - 2, \rho) \\ &= (0, 2, 4), \\ \boldsymbol{\mu}_3^{(2)} &= \boldsymbol{\mu}_2 L^{(2)} - \boldsymbol{\mu}_2^{(3)} - 2\boldsymbol{\mu}_2 \\ &= (0, 1, 2)L^{(2)} - (0, 2, 4) - (0, 2, 4) \\ &= (2\rho, 3\rho - 5, 3\rho - 8) \\ &= (8, 7, 4). \end{aligned}$$

We have, by (20),

$$\begin{aligned}\boldsymbol{\mu}_3^{(0)} &= (2\rho + \nu'_{-1} - 2(1+\nu_{-1}))\boldsymbol{\mu}_2 \\ &= (2\rho - 4)(0, 1, 2) \\ &= (0, 4, 8),\end{aligned}$$

so that

$$\begin{aligned}\boldsymbol{\mu}_4 &= \frac{1}{4}((0, 1, 3)L^{(1)} - (8, 7, 4) - (0, 4, 8)) \\ &= \frac{1}{4}(2\rho - 8, 4\rho - 12, 4\rho - 12) \\ &= \frac{1}{4}(0, 4, 4) = (0, 1, 1).\end{aligned}$$

3. Computation of $\mathbb{N}_m$

3.1. We set, for an integer $m \geq 1$ and $\alpha \in \mathbb{F}$,

(32) $$\Omega_{m,\alpha} = \left\{ J \subseteq \mathbb{F}^2 \mid \sharp J = m, \sum_{x \in J} x = \alpha \right\},$$

(33) $$N_{m,\alpha} = \sharp\Omega_{m,\alpha}, \qquad N_m = N_{m,0},$$

(34) $$\mathbb{N}_m = (N_{m,0}, N_{m,1}, N_{m,r}) \qquad (\nu_r = 0).$$

When $\mathbb{F} = \mathbb{F}_p$, the number N_m is the number of solutions of the congruence

(35) $$x_1^2 + \cdots + x_m^2 \equiv 0 \pmod p \qquad \left(1 \leq x_1 < \cdots < x_m \leq \frac{p-1}{2}\right).$$

Agoh [1] proved that, if $p \equiv 1 \pmod 4$, then

(36) $$\varepsilon^h = \sqrt{pa^2 - 1} + a\sqrt{p},$$

where $h, \varepsilon\ (> 1)$ stand for the class number and the fundamental unit of $\mathbb{Q}(\sqrt{p})$, respectively, and

(37) $$a = \frac{1}{p-1}\left(1 + \sum_{m=1}^{\frac{p-1}{2}} (-1)^m N_m\right).$$

In [4, 5] Sun gave a formula for N_m when $m = 2, 3$ and 4. Maohua showed in [3] that

$$N_m = \frac{1}{p}\left(\binom{\frac{p-1}{2}}{m} + \frac{p-1}{2}A_m\right),$$

where A_m is determined recursively by means of the following formulas:

$$\sigma_m = \frac{1}{2}(A_m + B_m\Delta), \qquad \Delta = \sqrt{(-1)^{\frac{p-1}{2}}p},$$

$$s_m = \frac{1}{2}\left(-1 + \left(\frac{m}{p}\right)\Delta\right),$$

$$\sigma_1 = s_1, \qquad m\sigma_m = s_1\sigma_{m-1} - s_2\sigma_{m-2} + \cdots + (-1)^{m-1}s_m.$$

We have the following

Theorem 2. *Given* $1 \le m \le \frac{q-1}{2}$ *and* $\alpha \in \mathbb{F}$, *set*

$$N_{m,\alpha} = \sharp\left\{J \subseteq \mathbb{F}^2 | \sharp J = m,\ \sum_{x\in J} x = \alpha\right\}.$$

Choosing $r \in \mathbb{F}^*$ *such that* $\nu_r = 0$, *set*

$$\mathbb{N}_m = (N_{m,0},\ N_{m,1},\ N_{m,r}).$$

Let $\boldsymbol{\mu}_k$ $(0 \le k \le \rho)$ *be the vector given by* (18) *and let* ρ *be as in* (2) (*we set* $\boldsymbol{\mu}_0 = (1, 0, 0)$). *We then have*:

(i) $$\text{If } \nu_{-1} = 0, \quad \text{then } \mathbb{N}_m = \boldsymbol{\mu}_m;$$

(ii) $$\text{if } \nu_{-1} = 1, \quad \text{then } \mathbb{N}_m = \mathbb{N}_{2\rho-m} \text{ (we set } \mathbb{N}_0 = \boldsymbol{\mu}_0).$$

If $\nu_{-1} = 1$ *and* $1 \le m \le \rho$, *we have*

(iii) $$\mathbb{N}_m = \sum_{k=0}^{[\frac{m}{2}]} \binom{\rho - m + 2k}{k} \boldsymbol{\mu}_{m-2k}.$$

Proof. If $\nu_{-1} = 0$, it is obvious that $\mathbb{N}_m = \boldsymbol{\mu}_m$.

Suppose $\nu_{-1} = 1$. Then

$$\sum_{x\in\mathbb{F}^2} x = 0, \qquad \sharp\mathbb{F}^2 = 2\rho,$$

and therefore $\mathbb{N}_m = \mathbb{N}_{2\rho-m}$ holds. Suppose, further, that $1 \le m \le \rho$. Denote the canonical projection from $\mathbb{F}^2$ onto $\mathbb{F}^2/\{\pm 1\}$ by π. Suppose $J \in N_{m,\alpha}$. We have

$$J = J_0 \cup -J_0 \cup J_1, \qquad \pi(J_0) \cap \pi(J_1) = \varnothing,$$

where

$$J_1 \in M_{m-2k,\alpha} \qquad (k = \sharp J_0,\ J_1 = \varnothing \text{ if } m = 2k).$$

Conversely, suppose we are given $0 \le k \le [\frac{m}{2}]$ and $J_1 \in M_{m-2k,\alpha}$ (if $m = 2k$ we set $J_1 = \varnothing$). Since $m \le \rho + k$, we have $k \le \rho - m + 2k$ and therefore we may choose $J_0 \subseteq \mathbb{F}^2$ such that $\sharp J_0 = k$, $\pi(J_0) \cap \pi(J_1) = \varnothing$; the set $J = J_0 \cup -J_0 \cup J_1$ then belongs to $N_{m,\alpha}$. Combining the above, we obtain Theorem 2. □

3.2. We now use Theorem 2 to compute $\mathbb{N}_m$ $(m = 2, 3)$ $(\mathbb{N}_1 = (0, 1, 0))$:

$$\mathbb{N}_2 = \begin{cases} \boldsymbol{\mu}_2 & \text{if } \nu_{-1} = 0, \\ \boldsymbol{\mu}_0 & \text{if } q = 5, \\ \boldsymbol{\mu}_2 + \rho\boldsymbol{\mu}_0 & \text{if } 5 < q \text{ and } \nu_{-1} = 1. \end{cases}$$

Therefore, when $1 < \rho$ $(5 < q)$, we have

(38) $$\mathbb{N}_2 = \boldsymbol{\mu}_2 + \nu_{-1}\rho\boldsymbol{\mu}_0.$$

We also have

$$\mathbb{N}_3 = \begin{cases} \boldsymbol{\mu}_3 & \text{if } \nu_{-1} = 0, \\ \boldsymbol{\mu}_1 & \text{if } q = 9, \\ \boldsymbol{\mu}_3 + (\rho - 1)\boldsymbol{\mu}_1 & \text{if } 9 < q \text{ and } \nu_{-1} = 1. \end{cases}$$

Hence, when $11 \le q$, we have

$$\mathbb{N}_3 = \boldsymbol{\mu}_3 + \nu_{-1}(\rho - 1)\boldsymbol{\mu}_1. \tag{39}$$

Now using the formulas (23) and (29) describing $\boldsymbol{\mu}_2$ and $\boldsymbol{\mu}_3$, we obtain:
When $5 < q$,

$$\mathbb{N}_2 = \left(\nu_{-1}\rho, \frac{\rho - \nu_{-1} - \nu_2}{2}, \frac{\rho - \nu_{-1} + \nu_2}{2}\right);$$

when $11 < q$,

$$\begin{aligned}\mathbb{N}_3 = \Bigg(&\frac{\rho^2}{3} + \left(\frac{1}{2} - \frac{5}{6}\nu_{-1} - \nu_{-2}\right)\rho + \nu'_{-1}\left(\frac{\nu_2}{6} - \frac{\nu_{-2}}{3}\right), \\ &\frac{\rho^2}{3} - \left(\frac{1}{3} + \frac{\nu_{-1}}{6}\right)\rho + \frac{\nu_{-1}}{6} + \frac{\nu_{-1}\nu_2}{2} + \frac{\nu_3}{3}, \\ &\frac{\rho^2}{3} - \left(\frac{1}{6} + \frac{\nu_{-1}}{2}\right)\rho + \frac{\nu'_3}{3} - \frac{\nu'_{-1}\nu_2}{2}\Bigg).\end{aligned}$$

We have, therefore, the following formulas, which contain expressions for $8N_2$ and $48N_3$ agreeing with Sun's results [4, 5]:

$$8\mathbb{N}_2 = \begin{cases} (2(q-1), q-9, q-1) & \text{if } q \equiv 1 \pmod 8, \\ (0, q-3, q-3) & \text{if } q \equiv 3 \pmod 8, \\ (2(q-1), q-5, q-5) & \text{if } q \equiv 5 \pmod 8, \\ (0, q-7, q+1) & \text{if } q \equiv 7 \text{ (mod)}; \end{cases}$$

$$48\mathbb{N}_3 = \begin{cases} ((q-1)(q-17), (q-1)(q-7) + 32 + 16\nu_3, \\ \qquad (q-1)(q-9) + 16\nu'_3) & \text{if } q \equiv 1 \pmod 8, \\ ((q-1)(q-11), (q-3)(q-7) + 16\nu_3, \\ \qquad (q-3)(q-5) + 16\nu'_3) & \text{if } q \equiv 3 \pmod 8, \\ ((q-1)(q-5), (q-3)(q-5) + 16\nu_3, \\ \qquad (q-1)(q-9) + 16\nu'_3) & \text{if } q \equiv 5 \pmod 8, \\ ((q-1)(q+1), (q-3)(q-7) + 16\nu_3, \\ \qquad (q+1)(q-9) + 16\nu'_3) & \text{if } q \equiv 7 \pmod 8. \end{cases}$$

3.3. We now show how Theorem 2 can be used by looking at an example: $q = p = 17$. We have $\rho = 4$, $\nu_{-1} = 1$. We also have $\boldsymbol{\mu}_0 = (1, 0, 0)$, $\boldsymbol{\mu}_1 = (0, 1, 0)$. As shown in 2.7, we have

$$\boldsymbol{\mu}_2 = (0, 1, 2), \quad \boldsymbol{\mu}_3 = (0, 1, 3), \quad \boldsymbol{\mu}_4 = (0, 1, 1).$$

Hence, by Theorem 2, we have

$$\begin{gathered}\mathbb{N}_1 = \boldsymbol{\mu}_1 = (0, 1, 0), \quad \mathbb{N}_2 = \boldsymbol{\mu}_2 + \rho\boldsymbol{\mu}_0 = (4, 1, 2), \\ \mathbb{N}_3 = \boldsymbol{\mu}_3 + (\rho - 1)\boldsymbol{\mu}_1 = (0, 4, 3), \\ \mathbb{N}_4 = \boldsymbol{\mu}_4 + (\rho - 2)\boldsymbol{\mu}_2 + \binom{\rho}{2}\boldsymbol{\mu}_0 = (6, 3, 5), \\ \mathbb{N}_5 = \mathbb{N}_3, \quad \mathbb{N}_6 = \mathbb{N}_2, \quad \mathbb{N}_7 = \mathbb{N}_1, \quad \mathbb{N}_8 = \mathbb{N}_0 = \boldsymbol{\mu}_0.\end{gathered}$$

We can now compute a given in (37):

$$a = \frac{1}{p-1}\left(1 + \sum_{m=1}^{\frac{p-1}{2}} (-1)^m N_m\right)$$
$$= \frac{1}{16}(1 - 0 + 4 - 0 + 6 - 0 + 4 - 0 + 1)$$
$$= 1.$$

Whence, by virtue of Agoh's result (cf. (36)), we have

$$\varepsilon^h = \sqrt{17-1} + \sqrt{17} = 4 + \sqrt{17}.$$

It is well known that the class number h of $\mathbb{Q}(\sqrt{17})$ is 1, and that $\varepsilon = 4+\sqrt{17}$ is a fundamental unit of the latter real quadratic number field.

Bibliography

1. T. Agoh, *A note on unit and class number of real quadratic fields*, Acta Math. Sinica (N.S.) **5** (1989), 281–288.
2. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, Berlin and New York, 1982.
3. L. Maohua, *The number of solutions of a certain quadratic congruence related to the class number of* $\mathbb{Q}(\sqrt{p})$, Proc. Amer. Math. Soc. **117** (1993), 1–3.
4. Q. Sun, *On the number of solutions of* $\sum_{i=1}^{k} x_i^2 \equiv 0 \pmod p$ *and the class number of* $\mathbb{Q}(\sqrt{p})$, Sichuan Daxue Xuebao **27** (1990), 260–264.
5. ——, *On the number of solutions of* $\sum_{i=1}^{k} x_i^2 \equiv 0 \pmod p$ $(1 \le x_1 < \cdots < x_k \le (p-1)/2)$, Adv. in Math. (Beijing) **19** (1990), 501–502.
6. K. S. Williams, *The quadratic character of* $2 \bmod p$, Math. Mag. **49** (1976), 89–90.

Department of Mathematics, Tokyo University of Mercantile Marine, Kotoku, Etchujima 2-1-6, Tokyo, Japan