PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 117, Number 1, January 1993

THE NUMBER OF SOLUTIONS OF A CERTAIN QUADRATIC CONGRUENCE RELATED TO THE CLASS NUMBER OF $\mathbb{Q}(\sqrt{p})$

LE MAOHUA

(Communicated by William W. Adams)

ABSTRACT. Let p be an odd prime, and let k be a positive integer with $i \leq k \leq (p-1)/2$. In this note we give a formula for the number of solutions $(x_1, \ldots, x_k)$ of the congruence $x_1^2 + \cdots + x_k^2 \equiv 0 \pmod{p}$, $1 \leq x_1 < \cdots < x_k \leq (p-1)/2$.

Let p be an odd prime, and let h, ε (> 1) denote the class number and the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$, respectively. Let k be a positive integer with $1 \leq k \leq (p-1)/2$, and let N_k denote the number of solutions $(x_1, \ldots, x_k)$ of the congruence

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

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

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

where

$$a = \frac{1}{p-1}\left(1 + \sum_{k=1}^{(p-1)/2} (-1)^k N_k\right).$$

In [3, 4], Sun gave a formula for N_k when $k = 2, 3$, and 4. For example, he showed that

$$4N_2 = \begin{cases} p-1, & \text{if } p \equiv 1 \pmod{4}, \\ 0, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

$$48N_3 = \begin{cases} (p-1)(p-17), & \text{if } p \equiv 1 \pmod{8}, \\ (p-1)(p-11), & \text{if } p \equiv 3 \pmod{8}, \\ (p-1)(p-5), & \text{if } p \equiv 5 \pmod{8}, \\ (p-1)(p+1), & \text{if } p \equiv 7 \pmod{8}. \end{cases}$$

In this note we give a general formula for N_k as follows:

Received by the editors September 18, 1990 and, in revised form, May 6, 1991.
1991 *Mathematics Subject Classification.* Primary 11A10.

©1993 American Mathematical Society
0002-9939/93 $1.00 + $.25 per page

Theorem. *Let* $\Delta = \sqrt{(-1)^{(p-1)/2}p}$, *and let*

$$s_k = \frac{1}{2}\left(-1 + \left(\frac{k}{p}\right)\Delta\right), \qquad k = 1, \ldots, \frac{p-1}{2}, \tag{1}$$

where (k/p) *is the Legendre symbol. If*

$$\sigma_k = \frac{1}{2}(A_k + B_k\Delta), \qquad k = 1, \ldots, \frac{p-1}{2},$$

satisfy

$$\sigma_1 = s_1, \qquad k\sigma_k = s_1\sigma_{k-1} - s_2\sigma_{k-2} + \cdots + (-1)^{k-1}s_k, \tag{2}$$

then we have

$$N_k = \frac{1}{p}\left(\binom{(p-1)/2}{k} + \left(\frac{p-1}{2}\right)A_k\right). \tag{3}$$

By (1) and (2), we get

$$A_1 = -1,$$
$$A_2 = \tfrac{1}{4}(3 + (-1)^{(p-1)/2}p),$$
$$A_3 = -\tfrac{1}{8}(5 + (-1)^{(p-1)/2}p + (-1)^{(p-1)/2+(p^2-1)/8}2p),$$

and by (3), we obtain

$$N_2 = \tfrac{1}{8}(p-1)(1 + (-1)^{(p-1)/2}),$$
$$N_3 = \tfrac{1}{48}(p-1)(p - 8 - (-1)^{(p-1)/2}3 - (-1)^{(p-1)/2+(p^2-1)/8}6),$$

which agrees with Sun's evaluation. According to the theorem, we can determine N_k $(k = 1, \ldots, (p-1)/2)$ in a recursive manner so h can be computed algorithmically by means of Agoh's formula.

Proof of the Theorem. Let $\mathscr{M}, \mathscr{N}$ be the sets of quadratic residues and non-residues $\bmod p$, respectively, and let $\mathscr{M}_k, \mathscr{N}_k$ be the sets of all subsets of $\mathscr{M}, \mathscr{N}$ with k elements, respectively. Let ζ be a pth primitive root of unity, and let

$$\sigma_k = \sum_{\{i_1, \ldots, i_k\} \in \mathscr{M}_k} \zeta^{i_1 + \cdots + i_k}, \qquad k = 1, \ldots, \frac{p-1}{2}. \tag{4}$$

Since $\{\zeta^i | i \in \mathscr{M}\}$ represents $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\Delta))$, we see that σ_k $(k = 1, \ldots, (p-1)/2)$ are algebraic integers in $\mathbb{Q}(\Delta)$. Then we have

$$\sigma_k = \tfrac{1}{2}(A_k + B_k\Delta), \qquad A_k, B_k \in \mathbb{Z},\ A_k \equiv B_k \pmod 2. \tag{5}$$

Let

$$I_k = \sum_{\substack{\{i_1, \ldots, i_k\} \in \mathscr{M}_k \\ i_1 + \cdots + i_k \equiv 0 \pmod p}} \zeta^{i_1 + \cdots + i_k}, \qquad J_k = \sum_{\substack{\{i_1, \ldots, i_k\} \in \mathscr{M}_k \\ i_1 + \cdots + i_k \not\equiv 0 \pmod p}} \zeta^{i_1 + \cdots + i_k}. \tag{6}$$

Then $\sigma_k = I_k + J_k$, and $N_k = I_k$ since $1^2, 2^2, \ldots, ((p-1)/2)^2$ are all quadratic residues $\bmod p$. Moreover, we get from (6) that

$$J_k = \sum_{r=1}^{p-1} a_{kr}\zeta^r, \qquad a_{kr} \in \mathbb{Z},\ a_{kr} \geq 0,\ r = 1, \ldots, p-1,\ k = 1, \ldots, \frac{p-1}{2}. \tag{7}$$

As $\{(-1+\Delta)/2, (-1-\Delta)/2\}$ is an integral basis of $\mathbb{Q}(\Delta)$, there exist integers $b_k, \bar{b}_k$ $(k = 1, \ldots, (p-1)/2)$ such that

$$J_k = b_k\left(\frac{-1+\Delta}{2}\right) + \bar{b}_k\left(\frac{-1-\Delta}{2}\right), \qquad k = 1, \ldots, \frac{p-1}{2}. \tag{8}$$

By (6) and (8), we get

$$A_k = 2N_k - b_k - \bar{b}_k, \qquad k = 1, \ldots, \frac{p-1}{2}. \tag{9}$$

On the other hand, by the well-known evaluation of the Gaussian sum, we have

$$\sum_{i\in\mathscr{M}} \zeta^i = \frac{-1+\Delta}{2}, \qquad \sum_{j\in\mathscr{N}} \zeta^j = \frac{-1-\Delta}{2}. \tag{10}$$

Since $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ are linearly independent over $\mathbb{Q}$, we see from (7), (8), and (10) that

$$a_{kr} = \begin{cases} b_k, & \text{if } r \in \mathscr{M}, \\ \bar{b}_k, & \text{if } r \in \mathscr{N}, \end{cases} \qquad k = 1, \ldots, \frac{p-1}{2}.$$

Recalling that $a_{kr} \geq 0$, we have

$$N_k + \left(\frac{p-1}{2}\right)(b_k + \bar{b}_k) = |\mathscr{M}_k| = \binom{(p-1)/2}{k}, \qquad k = 1, \ldots, \frac{p-1}{2}, \tag{11}$$

by (5). Combining (9) and (11) yields (3).

Let

$$s_k = \sum_{i\in\mathscr{M}} \zeta^{ki}, \qquad k = 1, \ldots, \frac{p-1}{2}.$$

Then s_k $(k = 1, \ldots, (p-1)/2)$ satisfy (1) by (10). Thus, by Newton's relations between the coefficients of a polynomial and the sums of powers of its zeros, σ_k $(k = 1, \ldots, (p-1)/2)$ satisfy (2). The proof is complete.

Remark. On applying Waring's formula (cf. [2, Formula 1.76]), we have an explicit formula for σ_k:

$$\sigma_k = \sum_{\substack{n_1+2n_2+\cdots+kn_k=k \\ n_i\geq 0,\ i=1,\ldots,k}} (-1)^{n_2+n_4+\cdots+n_{2[k/2]}} \prod_{i=1}^{k} \frac{s_i^{n_i}}{n_i!\, i^{n_i}}.$$

References

1. T. Agoh, *A note on unit and class number of real quadratic fields*, Acta Math. Sinica (N.S.) **5** (1989), 281–288.
2. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
3. 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 (Zirao Kexue Ban) **27** (1990), 260–264. (Chinese)
4. ——, *On the number of solutions of* $\sum_{i=1}^{k} x_i^2 \equiv 0 \pmod{p}$ $(1 \leq x_1 < \cdots < x_k \leq (p-1)/2)$, Adv. in Math. (Beijing) **19** (1990), 501–502.

RESEARCH DEPARTMENT, CHANGSHA RAILWAY INSTITUTE, CHANGSHA, HUNAN, PEOPLE'S REPUBLIC OF CHINA