1. Introduction

THE NUMBER OF SOLUTIONS OF THE CONGRUENCE $y^2 \equiv x^4 - a \pmod{p}$

by Surjit SINGH and A. R. RAJWADE

1. INTRODUCTION

The object of this paper is to prove the following theorem.

THEOREM. *Let a be an integer not divisible by a given prime p. Then the number of solutions of the congruence $y^2 \equiv x^4 - a \pmod{p}$ is*

$$\begin{cases} p - 1 \text{ if } p \equiv 3 \pmod{4}. \\ p - (a/\pi)_4\,\bar{\pi} - (a/\bar{\pi})_4\,\pi - 1 \text{ if } p \equiv 1 \pmod{4}. \end{cases}$$

where $(\frac{\cdot\cdot}{\cdot\cdot})_4$ is the biquadratic residue symbol and $p = \pi\bar{\pi}$ is the factorization of p in the ring $Z[i]$ of the Gaussian integers, π and $\bar{\pi}$ being both normalized $\equiv 1 \pmod{(2(1+i))}$.

Morlaye shows (see [4] Proposition 1) that if N is the number of solutions of the congruence $y^2 \equiv x^3 - ax \pmod{p}$ and N' the number of solution of the congruence $y^2 \equiv x^4 - a \pmod{p}$ then $N = N' + 1$. This is a short proposition for the case $p \equiv 1\ (4)$ and so our theorem gets the number of solutions of

$$y^2 \equiv x^3 - ax \pmod{p}$$

by yet another elementary method. This latter equation: $y^2 = x^3 - ax$ is the elliptic curve with complex multiplication by $\sqrt{-1}$. (See also a remark by Swinnerton-Dyer in [1]). A proof of the latter result is also given in [2] and [5]. These proofs, however, are not elementary.

We note here that both N and N' can be computed trivially for the case $p \equiv 3\ (4)$.

To get N we proceed as follows:

Case 1. a is a quadratic non-residue mod p. Then corresponding to $y = 0$, there exist only one x viz $x = 0$ satisfying

$$y^2 \equiv x(x^2 - a) \pmod{p}$$

since $x^2 - a \equiv 0\,(p)$ is not solvable. This gives one solution (0, 0). Let now $x = \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, be a complete non-zero residue system mod p. Of $x^3 - ax$ and $(-x)^3 - a(-x) = -(x^3 - ax)$ one is a quadratic residue and the other a non-residue since -1 is a non-residue, p being $\equiv 3\,(4)$. Hence as x takes the values $\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, $x^3 - ax$ becomes a quadratic residue $\frac{p-1}{2}$ times (perhaps with repetitions) and a non-residue $\frac{p-1}{2}$ times. Each time it is a quadratic residue, we get 2 solutions. Hence there exist $p - 1$ solutions, and together with (0, 0) gives p solutions as required.

Case 2. a is a quadratic residue mod p, that is there exists an x_0 such that $x_0^2 \equiv a \pmod{p}$. Then corresponding to $y = 0$ there exist 3 solutions, $(0, 0), (x_0, 0), (-x_0, 0)$. Let now $x = \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, but $\neq \pm x_0$ (or 0) (all together $p - 3$ values). As above $x^3 - ax$ becomes a quadratic residue exactly $\frac{p-3}{2}$ times and so there exists $p - 3$ solutions, which together with $(0, 0), (\pm x_0, 0)$ gives p solutions as required. To get N' we note that in this case the biquadratic residues of p are the same as quadratic residues. Hence the congruence can be written as

$$y^2 \equiv x^2 - a \pmod{p}$$

or

$$(x+y)(x-y) \equiv a \pmod{p}$$

or

$$u.v \equiv a \pmod{p}$$

which has $p - 1$ solutions as required. For the case $p \equiv 1 \pmod 4$ we shall use results from cyclotomy for the factorization $p - 1 = 4f$.

2. The congruence $y^2 \equiv (x^4 - a) \pmod{p}$

Let $\left(\frac{t}{p}\right)$ be the Legendre symbol. The number of solutions of $y^2 \equiv x^4 - a \pmod{p}$ equals $\sum_x \left[1 + \left(\frac{x^4-a}{p}\right)\right] = p + \sum_x \left(\frac{x^4-a}{p}\right) = p + S$. To get S we define first the biquadratic character χ as follows: