Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 20 (1974)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE NUMBER OF SOLUTIONS OF THE CONGRUENCE $y^2 \equiv x^4 – a(mod \quad p)$
Autor: Singh, Surjit / Rajwade, A. R.
Kapitel: 2. The congruence $y^2 \equiv (x^4 —a)\quad (mod \quad p)$
DOI: https://doi.org/10.5169/seals-46910

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:

Let g be a primitive root mod p. Then for any integer $m\ (\neq 0)$ there exists a positive integer v such that $m \equiv g^v\ (p)$. We put $\chi(m) = (i)^v$ where $i = \sqrt{-1}$ and put $\chi(0) = 0$. This defines χ. We now have

$$S = \sum_y [1 + \chi(y) + \chi^2(y) + \chi^3(y)] \left(\frac{y-a}{p}\right)$$
$$= \sum_y \chi(y) \left(\frac{y-a}{p}\right) + \sum_y \chi^2(y) \left(\frac{y-a}{p}\right) + \sum_y \chi^3(y) \left(\frac{y-a}{p}\right).$$

Setting $y = -az$ we get:

$$S = \left(\frac{-a}{p}\right) \left[\sum_{all\ z} \chi(-a)\chi(z) \left(\frac{z+1}{p}\right) + \sum_{all\ z} \chi^2(-a)\chi^2(z) \left(\frac{z+1}{p}\right) + \sum_{all\ z} \overline{\chi(-a)}\ \overline{\chi(z)} \left(\frac{z+1}{p}\right)\right],$$

since $\chi^3(m) = \overline{\chi(m)}$ for all integers m.
Now we look at the sum

$$\sum \chi(z) \left(\frac{z+1}{p}\right).$$

This equals

$$\sum_{z+1\ =\ square} \chi(z) - \sum_{z+1\ =\ not\ square} \chi(z).$$

But

$$0 = \sum_{z+1\ =\ square} \chi(z) + \sum_{z+1\ \neq\ square} \chi(z) + \chi(-1).$$

Therefore

$$\sum_{z+1\ =\ square\ not\ zero} \chi(z) = \tfrac{1}{2} \sum_{u \neq o} \chi(u^2-1) = \tfrac{1}{2} \sum_{u \neq o} \chi(u+1)\chi(u-1)$$
$$= \tfrac{1}{2} \left[\sum_{all\ u} \chi(u+1)\chi(u-1) - \chi(-1)\right].$$

Now put $u = 2v + 1$.
Therefore $\sum_{z+1\ =\ square\ not\ zero} \chi(z) = \tfrac{1}{2} \left[\chi(4) \sum_{all\ v} \chi(v)\chi(v+1) - \chi(-1)\right].$

Hence $\sum_{all\ z} \chi(z) \left(\frac{z+1}{p}\right) = \chi(4) \sum_{all\ v} \chi(v)\chi(v+1).$

Similarly for χ^2 and $\bar{\chi}$ and therefore we get

$$S = \left(\frac{-a}{p}\right) \left[\chi(-4a) \sum_{all\ v} \chi(v)\chi(v+1) + \bar{\chi}(-4a) \sum_{all\ v} \bar{\chi}(v)\bar{\chi}(v+1) + \chi^2(-4a) \sum_{all\ v} \chi^2(v)\chi^2(v+1)\right].$$