Math 115 Professor K. A. Ribet

Take-home Exam, due April 7, 1994

Let p be a prime number greater than 3. Let N_p be the number of solutions to $y^2 = x^3 - x$ in $\mathbf{F}_p$.

1. Show that $N_p = p + \sum_{a \in \mathbf{F}_p} \left(\frac{a^3 - a}{p} \right)$.

2. Prove that $N_p = p$ if $p \equiv 3 \pmod 4$.

3. Suppose from now on that $p \equiv 1 \bmod 4$. Recall from class that p may be written in the form $r^2 + s^2$ where r and s are integers, cf. Proposition 8.3.1 of the text. Since p is odd, r and s cannot have the same parity—we will suppose that r is odd and that s is *even*. Show that r and s are then determined up to sign. (This is a restatement of problem 12 on page 106 of the book.)

4. While I'm at it, let me assign problem 13 on page 106. This came up in class.

5. Let $E = p - N_p = -\sum_{a \in \mathbf{F}_p} \left(\frac{a^3 - a}{p} \right) = -\sum_{a \in \mathbf{F}_p} \left(\frac{a - a^3}{p} \right)$; we think of E as an error term. Here is a table giving the value of E for twenty-one small primes p:

p	13	17	29	37	41	53	61	73	89	97	101	109	113	137	149	157	173	181	193	197	229
E	6	2	−10	−2	10	14	−10	−6	10	18	−2	6	−14	−22	14	22	−26	−18	−14	−2	30

6. Calculate r and s for a fair number of the twenty-one primes p which appear in the table. Following in the 1814 footsteps of Gauss, conjecture a rule which determines E in terms of r and s. For example, decide what E ought to be when $p = 144169 = (315)^2 + (212)^2$.

7. Let χ be a character of order 4 on $\mathbf{F}_p^*$, so that χ^2 is the quadratic symbol $\left(\frac{\cdot}{p}\right)$. Show that $E = -2 \operatorname{Re} J$, where $J = J(\chi, \chi^2)$. Check this general formula by calculating E and J explicitly in the case where $p = 5$ and χ is the character mapping 2 to i.

8. Regard J as an element of $\mathbf{Z}[i]$. Show that $J + 1$ is divisible by $(2 + 2i)$. (See page 168 of the book if you get stuck.)

9. Suppose that $J = \alpha + i\beta$ where α and β are integers. Explain why α is odd, β is even, $\alpha + \beta + 1$ is divisible by 4 and $\alpha^2 + \beta^2 = p$. Recapitulate what you have learned in the form of a rule for calculating N_p when p is congruent to 1 mod 4.