Math 115 Professor Kenneth A. Ribet

Homework assignment #13
Due December 1, 2006

1. Let p and q be distinct odd primes. Set $q^* := (-1)^{(q-1)/2} q$, so that q^* is q if $q \equiv 1 \bmod 4$ and $-q$ otherwise. Show that the main theorem of quadratic reciprocity may be expressed as the equality

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

In particular, conclude that $\left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right)$ for $p \geq 5$. Hence -3 is a square mod p if and only if $p \equiv 1 \bmod 3$.

2. Let p be an odd prime. Recall that we showed on November 15 that there is a generator mod p^n for each $n \geq 1$. How many generators are there? Also, suppose that g is a generator mod p^n. How many integers are there mod p^{n+1} that lift g? Among the lifts, how many of the lifts are generators mod p^{n+1}. (This question is mostly a review of my lecture.)

2bis. Again a review: Grant the fact that there is a generator mod p^n whenever p is an odd prime and n is a positive integer. Using this fact, present a characterization of those integers $m \geq 1$ for which there is a generator mod m. (By definition, a generator is an integer g prime to m such that each integer prime to m is congruent mod m to a power of g.)

3. Show that the equation $165x^2 - 21y^2 = 19$ has no integral solutions.

4. Suppose that a is an integer. Show that there are integers x and y such that $y^2 = x^2 - a^3$.

5. Now here's a problem that I don't know the answer to. As background, one can ask (as a Fermat-type problem) whether it's possible for three different perfect nth powers to be in arithmetic progression. For $n = 2$, this is indeed possible; for example, 1, 25 and 49 form an arithmetic progression. If $a = 1$, $b = 7$ and $c = 5$, we then have $a^2 + b^2 = 2c^2$. A theorem (proved soon after FLT was proved) is that there are no non-trivial solutions to $a^n + b^n = 2c^n$ for $n > 2$. This theorem was known for $n < 31$ (I think) by the 1950s. The cases $n = 3$ and $n = 4$ went back centuries. (The whole story is parallel to the tale of FLT.)

For the case $n = 4$, Legendre proved the stronger theorem that there are no non-trivial solutions to $a^4 + b^4 = 2c^2$. More precisely: if a, b and c are non-zero integers that satisfy the equation, then $a^2 = b^2$ and $c^2 = a^4 = b^4$. The homework problem (which is maybe hard!) is to prove Legendre's theorem by some variant of Fermat's method of descent (as I presented it in class). The proof is old and elementary, so I'm hoping that we can reconstruct it!

Happy Thanksgiving to All!