Math 445 Number Theory

October 5, 2008

We wish to prove:

Conjecture: A prime p is a sum of two squares $\Leftrightarrow$ ($p = 2$ or) $p \equiv 1 \pmod 4$.

It turns out that what is really relevant to the discussion is under what circumstances the equation $x^2 \equiv -1 \pmod p$ has a solution! And for this, we need:

Theorem: If p is prime, the equation $x^2 \equiv -1 \pmod p$ has a solution $\Leftrightarrow$ $p = 2$ or $p \equiv 1 \pmod 4$.

Checking this for $p = 2$ is quick ($x = 1$ works), and so we need to show that (1) if $p \equiv 1 \pmod 4$ then $x^2 \equiv -1 \pmod p$ has a solution, and (2) if $p \equiv 3 \pmod 4$ then $x^2 \equiv -1 \pmod p$ has no solution.

To see the first, since $p - 1 = 4k$ for some k, we have, since there is a primitive root of 1 mod p, a c such that $c^{p-1} = c^{4k} \equiv 1$ but $c^{2k} \not\equiv 1$, so (by Euler) $c^{2k} \equiv -1$. But then setting $x = c^k$, we then have $x^2 = (c^k)^2 = c^{2k} \equiv -1$, giving us our desired solution.
The second case is really rather quick. If, by way of contradiction, we have $x^2 \equiv -1 \pmod p$, then since by FLT $x^{p-1} \equiv 1 \pmod p$, we have, mod p,

$$1 \equiv x^{p-1} = x^{(4k+3)-1} = x^{4k+2} = x^{2(2k+1)} = (x^2)^{2k+1} \equiv (-1)^{2k+1} = -1$$

so $1 \equiv -1 \pmod p$. i.e., $p|2$, which is absurd.

With this in hand, we can show:

Proposition: If $n = a^2 + b^2$, $p|n$, and $p \equiv 3 \pmod 4$, then $p|a$ and $p|b$.

If not, then either $p \not| a$ or $p \not| b$, say $p \not| a$. Then $(a, p) = 1$, so there is a z with $az \equiv 1 \pmod p$. But then since $p|n$, $p|a^2 + b^2$, so $a^2 + b^2 \equiv 0 \pmod p$. Then $1 + (bz)^2 = (az)^2 + (bz)^2 = z^2(a^2 + b^2) \equiv z^2 0 = 0 \pmod p$, so $x = bz$ satisfies $x^2 + 1 \equiv 0 \pmod p$, i.e., $x^2 \equiv -1 \pmod p$, a contradication. So $p|a$ and $p|b$.

(*) This means that $p^2|a^2$ and $p^2|b^2$, so $p^2|a^2 + b^2 = n$, and $(n/p^2) = (a/p)^2 + (b/p)^2$. This will be very significant shortly!