Math 445 Number Theory

October 15, 2004

Some computations: our basic facts are

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$ if p,q distinct odd primes, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, and $\left(\frac{a+pk}{p}\right) = \left(\frac{a}{p}\right)$.

With these we can, in principle, decide for any prime p and $(a,p)=1$ if $x^2 \equiv a \pmod{p}$ has a solution. And the fun part is that, in the last of these facts, we can choose something equivalent to a mod p in any way we want, which can lead to some very different computations of the same result!

$\left(\frac{619}{1229}\right)$: $\left(\frac{619}{1229}\right)\left(\frac{1229}{619}\right) = (-1)^{\frac{619-1}{2}\frac{1229-1}{2}} = (-1)^{309\cdot 614} = 1$, so $\left(\frac{619}{1229}\right) = \left(\frac{1229}{619}\right) = \left(\frac{1238-9}{619}\right) = \left(\frac{-9+619\cdot 2}{619}\right) = \left(\frac{-9}{619}\right) = \left(\frac{(-1)(3)^2}{619}\right) = \left(\frac{-1}{619}\right)(\left(\frac{3}{619}\right))^2 = \left(\frac{-1}{619}\right) = (-1)^{309} = -1$ so $\left(\frac{619}{1229}\right) = -1$, so $x^2 \equiv 619 \pmod{1229}$ has no solutions.

$\left(\frac{617}{1229}\right)$: $\left(\frac{617}{1229}\right)\left(\frac{1229}{617}\right) = (-1)^{\frac{617-1}{2}\frac{1229-1}{2}} = (-1)^{308\cdot 614} = 1$, so $\left(\frac{617}{1229}\right) = \left(\frac{1229}{617}\right) = \left(\frac{1234-5}{617}\right) = \left(\frac{-5+617\cdot 2}{617}\right) == \left(\frac{-5}{617}\right) = \left(\frac{(-1)(5)}{617}\right) = \left(\frac{-1}{617}\right)\left(\frac{5}{617}\right)$. Now, $\left(\frac{-1}{617}\right) = (-1)^{\frac{617-1}{2}} = (-1)^{308} = 1$, so $\left(\frac{617}{1229}\right) = \left(\frac{1229}{617}\right) = \left(\frac{5}{617}\right)$

$\left(\frac{5}{617}\right)\left(\frac{617}{5}\right) = (-1)^{308\cdot 2} = 1$, so $\left(\frac{5}{617}\right) = \left(\frac{617}{5}\right) = \left(\frac{5\cdot 123+2}{5}\right) = \left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1 \pmod{5}$, so $\left(\frac{617}{1229}\right) = \left(\frac{5}{617}\right) = \left(\frac{2}{5}\right) = -1$, so $x^2 \equiv 617 \pmod{1229}$ also has no solutons.

$\left(\frac{223}{617}\right)$: Check that they are prime! Then: $\left(\frac{223}{617}\right)\left(\frac{617}{223}\right) = (-1)^{\frac{617-1}{2}\frac{223-1}{2}} = (-1)^{308\cdot 111} = 1$, so $\left(\frac{223}{617}\right) = \left(\frac{617}{223}\right) = \left(\frac{669-52}{23}\right) = \left(\frac{223\cdot 3-52}{223}\right) = \left(\frac{-52}{223}\right) = \left(\frac{(-1)(2)^2(13)}{223}\right) = \left(\frac{-1}{223}\right)(\left(\frac{2}{223}\right))^2\left(\frac{13}{223}\right) = \left(\frac{-1}{223}\right)\left(\frac{13}{223}\right)$. But $\left(\frac{-1}{223}\right) = (-1)^{\frac{223-1}{2}} = (-1)^{111} = -1$, and $\left(\frac{13}{223}\right)\left(\frac{223}{13}\right) = (-1)^{\frac{13-1}{2}\frac{223-1}{2}} = (-1)^{6\cdot 111} = 1$, so $\left(\frac{13}{223}\right) = \left(\frac{223}{13}\right) = \left(\frac{260-37}{13}\right) = \left(\frac{-37}{13}\right) = \left(\frac{-37+39}{13}\right) = \left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = (-1)^{21} = -1$, so $\left(\frac{223}{617}\right) = \left(\frac{-52}{223}\right) = (-1)\left(\frac{13}{223}\right) = (-1)\left(\frac{2}{13}\right) = (-1)(-1) = 1$, so $x^2 \equiv 223 \pmod{617}$ has a solution.

$\left(\frac{555}{1663}\right)$: $555 = 5\cdot 111 = 5\cdot 3\cdot 37$, so $\left(\frac{555}{1663}\right) = \left(\frac{5}{1663}\right)\left(\frac{3}{1663}\right)\left(\frac{37}{1663}\right)$ And we can compute:

$\left(\frac{5}{1663}\right) = (-1)^{\frac{1663-1}{2}\frac{5-1}{2}}\left(\frac{1663}{5}\right) = (-1)^{831\cdot 2}\left(\frac{1663}{5}\right) = \left(\frac{1663}{5}\right) = \left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} = 3^2 = 9 \equiv -1 \pmod{5}$, so $\left(\frac{5}{1663}\right) = -1$.

$\left(\frac{3}{1663}\right) = (-1)^{\frac{1663-1}{2}\frac{3-1}{2}}\left(\frac{1663}{3}\right) = (-1)^{831\cdot 1}\left(\frac{1663}{3}\right) = (-1)\left(\frac{1663}{3}\right) = (-1)\left(\frac{3\cdot 554+1}{3}\right) = (-1)\left(\frac{1}{3}\right) = (-1)(1)^{\frac{3-1}{2}} = -1$

$\left(\frac{37}{1663}\right) = (-1)^{831\cdot 18}\left(\frac{1663}{37}\right) = \left(\frac{1663}{37}\right) = \left(\frac{1663-1350}{37}\right) = \left(\frac{313}{37}\right) = \left(\frac{313-370}{37}\right) = \left(\frac{-57}{37}\right) = \left(\frac{-57+74}{37}\right) = \left(\frac{17}{37}\right) = (-1)^{\frac{17-1}{2}\frac{37-1}{2}}\left(\frac{37}{17}\right) = (-1)^{8\cdot 18}\left(\frac{37}{17}\right) = \left(\frac{37}{17}\right) = \left(\frac{37-34}{17}\right) = \left(\frac{3}{17}\right) = (-1)^{1\cdot 8}\left(\frac{17}{3}\right) = \left(\frac{17}{3}\right) = \left(\frac{17-18}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = (-1)^1 = -1$.

So, putting them together, $\left(\frac{555}{1663}\right) = \left(\frac{5}{1663}\right)\left(\frac{3}{1663}\right)\left(\frac{37}{1663}\right) = (-1)(-1)(-1) = -1$, so $x^2 \equiv 555 \pmod{1663}$ has no solutions.