Math 445 Number Theory

October 22, 2004

Since the Jacobi symbol has essentially the same properties as the Legendre symbol, we can compute them in essentially the same way; extract factors of 2 from the top (and -1), and use reciprocity to compute the rest. The advantage: we don't need to factor the top any further, any odd number will work fine.

Example: $\left(\frac{2225}{3333}\right) = \left(\frac{3333}{2225}\right)(-1)^{1666\cdot 1112} = \left(\frac{2225+1108}{2225}\right) = \left(\frac{2^2\cdot 277}{2225}\right) = (\left(\frac{2}{2225}\right))^2\left(\frac{277}{2225}\right) = \left(\frac{2225}{277}\right)(-1)^{1112\cdot 138} = \left(\frac{277\cdot 9+182}{277}\right) = \left(\frac{182}{277}\right) = \left(\frac{2}{277}\right)\left(\frac{91}{277}\right) = (-1)^{\frac{277^2-1}{8}}\left(\frac{277}{91}\right)(-1)^{138\cdot 45} = (-1)^{9591}\left(\frac{91\cdot 3+4}{91}\right) = (-1)\left(\frac{4}{91}\right) = (-1)(\left(\frac{2}{91}\right))^2 = -1$

One basic result coming from reciprocity: for a fixed (odd) a, we can determine for which primes p the equation $x^2 \equiv a \pmod p$ will have solutions.

$1 = \left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{\frac{p-1}{2}\frac{a-1}{2}}$ is determined by $\left(\frac{p}{a}\right)$ (which only depends on p mod a) and (if $a \equiv 3 \pmod 4$) on p mod 4 (to determine the parity of $\frac{p-1}{2}\frac{a-1}{2}$ - if $a \equiv 1 \pmod 4$ it is always even). So $\left(\frac{a}{p}\right)$ depends on p mod a and on p mod 4 (when $a \equiv 3 \pmod 4$), so it depends at most on p mod $4a$ (by the Chinese Remainder Theorem). So the primes for which $x^2 \equiv a \pmod p$ have solutions fall *precisely* into certain equivalence classes mod a or $4a$, depending upon a. If we include even values for a, then we need to extract 2's, and the result will depend upon p mod 8 (for the $\left(\frac{2}{p}\right)$'s) and, at worst, on p mod $a/2$, and so it still depends at most on p mod $4a$.

A brief interlude: we know that there are infinitely many primes. But how are they distributed? For example, $\sum_{n=1}^{\infty}\frac{1}{n}$ diverges, but $\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6} < \infty$. So how about $\sum_{p \text{ prime}}\frac{1}{p}$? We will show that this sum diverges, so that we know that, in some sense, primes are more common than perfect squares....

To show this, pick a positive number N, and let $p_1,\dots p_k$ be the primes $\leq N$. Then let $A = \sum_{i_1,\dots i_k=0}^{\infty}\frac{1}{p_1^{i_1}\cdots p_k^{i_k}} = (\sum_{i_1=0}^{\infty}(\frac{1}{p_1})^{i_1})\cdots(\sum_{i_k=0}^{\infty}(\frac{1}{p_k})^{i_k}) = \frac{1}{1-\frac{1}{p_1}}\cdots\frac{1}{1-\frac{1}{p_k}} = \frac{p_1}{p_1-1}\cdots\frac{p_k}{p_k-1}$.
But the initial sum includes all denomenators $\leq N$, since every $k \leq N$ is a product of primes $\leq N$, i.e, is a product of the primes $p_1,\dots,p_k$. So $A \geq \sum_{n=1}^{N}\frac{1}{n} \geq \int_1^N \frac{1}{x}\,dx = \ln(N)$ by the integral test. So $\frac{p_1}{p_1-1}\cdots\frac{p_k}{p_k-1} \geq \ln(N)$. Taking logs of both sides, we have
$\sum_{i=1}^{k}\ln(\frac{p_i}{p_i-1}) = \sum_{i=1}^{k}\ln(1+\frac{1}{p_i-1}) \geq \ln(\ln(N))$. But from power series we know that for $|x|<1$, $\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots \leq x$ (since it is an alternating series with terms decreasing to 0 (or, if you prefer, by using $\frac{1}{1+x} \leq 1$ and integrating from 1 to x)), so $\sum_{i=1}^{k}\frac{1}{p_i-1}) \geq \sum_{i=1}^{k}\ln(1+\frac{1}{p_i-1} \geq \ln(\ln(N))$. But $\frac{1}{p_i-1} \leq \frac{p_i+2}{p_i^2} = \frac{1}{p_i} + \frac{2}{p_i^2}$ (since $(p_i-1)(p_i+2) = p_i^2 + p_1 - 2 \geq p_i^2$), so $\sum_{i=1}^{k}\frac{1}{p_i} + \frac{2}{p_i^2} \geq \sum i = 1^k \frac{1}{p_i-1}) \geq \ln(\ln(N))$. So
$\sum_{i=1}^{k}\frac{1}{p_i} \geq \ln(\ln(N)) - \sum_{i=1}^{k}\frac{2}{p_i^2} \geq \ln(\ln(N)) - \sum_{i=1}^{\infty}\frac{2}{n^2} = \ln(\ln(N)) - \frac{\pi^2}{3} \geq \ln(\ln(N)) - 4$. So the sum of the reciprocals of the primes $\leq N$ is $\geq \ln(\ln(N)) - 4$. Since $\ln(\ln(N))$ tends to ∞ as $N \to \infty$ (albeit very slowly), the sum of the reciprocals of the primes diverges.

It is in fact true that as $n \to \infty$, $(\sum_{p \text{ prime}, p\leq n}\frac{1}{p}) - \ln(\ln(n))$ converges to a finite constant M, known as the *Meissel-Mertens constant*. It's value is, approximately, 0.26149721284764278... .