Math 445 Number Theory

October 1, 2008

The Quadratic Sieve: the sieving process.

The sieving process involves looking at numbers $b = a^2 - n$ for a range of values of a, deciding when they are divisible by a small prime p, then replacing a with a/p if it is and moving on. But this amounts to deciding (quickly) when n is a square mod p, and for which values of a is $a^2 \equiv n$. Deciding if n is a square mod p can be done quickly (and note that if the answer is "no" then we needn't bother placing p in our facotr base: it will never play a role in a smooth number), using the technique of quadratic reciprocity, which we will esplore later. And if n is a square then there will be two values a_1, a_2 (since $x^2 \equiv n$ will have two solutions mod p) so that $p|a^2 - n \Leftrightarrow a \equiv a_1, a_2 \pmod{p}$, and we can find the a_i, for smallish p, by a brute force search. Then we know which $a^2 - n$ to divide by p; in our sequence they form two sets of subsequences which jump along by p, and we can quickly focus on just those terms that have a facotr of p to divide out. So in the end, the sieving process looks exactly like the prime sieve (we just start at different points and do it twice for each prime...).

For a complete change of topic (before coming back to look at quadratic residues $x^2 \equiv a \pmod{p}$), we will take a look at Pythagorean Triples:

Pythagorian triples: If $a^2 + b^2 = c^2$, then we call (a, b, c) a Pythagorean triple. Their connection to right triangles is well-known, and so it is of interest to know what the triples are! It is fairly straighforward to generate a lot of them (e,g, via $(n+1)^2 = n^2 + (2n+1)$, so any odd square $k^2 = 2n + 1$ can be used to build one). But to find them all takes a bit more work:

A Pythagorean triple (a, b, c) is *primitive* if the three numbers share no common factor. This is equivalent, in this case, to $(a, b) = (a, c) = (b, c) = 1$. Then by considering the equation mod 4, we can see that for a primitive triple, c must be odd, a (say) odd and b even. If we then write the equation as $b^2 = c^2 - a^2 = (c + a)(c - a)$, we find that we have factored b^2 in two different ways. Since $b, a + c$ and $a - c$ are all even, we can write $(b/2)^2 = [(c + a)/2]^2[(c - a)/2]^2$ But because $(c + a)/2 + (c - a)/2 = c$ and $(c + a)/2 - (c - a)/2 = b$, $\gcd((c + a)/2, (c - a)/2) = 1$. Then we can apply:

Proposition: If $(x, y) = 1$ and $xy = c^2$, then $x = u^2, y = v^2$ for some integers u, v .

Proof: next time