Math 445 Number Theory

September 26, 2008

A more powerful (read: faster) factoring algorithm: the Quadratic Sieve.

The starting point for the quadratic sieve is the boservation that if $n = ab$ is an odd composite number, then n is a difference of squares $n = ab = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$. Fermat used this to describe a factoring algorithm:

Starting with $a = \lfloor\sqrt{n}\rfloor\rfloor$, compute $(a+k)^2 - n = a_k$ for $k \in \mathbb{N}$ and look for a k with $a_k = b^2$ a perfect square, then $a+k-b|n$ and we have (probably) found a proper factor. This appraoch is fast if n has a factor close to $\sqrt{n}$, but in general (since a random number is more likely to have a small factor than one close to its sqaure root) this algorithm is slower than trial division.

Fermat;s idea was improved in the 1920's, by Kraitchik, whose instead proposed to find an a so that $a^2 \equiv b^2 \pmod{n}$ for some b, i.e., $n|a^2 - b^2 = (a-b)(a+b)$; the gcd of n with $a-b$ or $a+b$ is then likely to produce a proper factor. Kraitchik's idea was to start as with fermat, to compute $(a+k)^2 - n = a_k$, but instead to find a <u>collection</u> of k's,

$$k_1, \ldots k_r$$

so that $a_{k_1} \cdots a_{k_r} = b^2$ was a perfect square. Then $(a+k_1)\cdots(a+k_r) \equiv b^2 \pmod{n}$, and we may have found a proper factor of n. And the approach to finding the right a_i was to search for i so that $(a+i)^2 - n = a_i$ is a product of "small" primes. The idea is that with enough number, all of which are products of the same collection of small primes, we can eventually find some subset of them whose product is a square. A square has a prime factorization with all even exponents; while the exponent on each prime in the factorization of $a_{k_1} \cdots a_{k_r}$ is the sum of the exponents in the fatorization of each of the a_i. So we look for a_i's so that the sum of the exponents for each prime, summed over the i, is always even. The algorithm proceeds by choosing a bound B on the primes in a factorization we are willing to keep; the set of primes p less than or equal to B is called the *factor base* of the algorithm. We keep all a_k whose prime factorizations involve only primes in the factor base, and continue to collect a_i until we can find a subset of them whose product is a square. How do we find such a subset? Linear algebra!