Math 445 Number Theory

September 29, 2008

The Quadratic Sieve: speeding it up.

Our setup: n (odd) composite. $a = \lfloor\sqrt{n}\rfloor$, $(a+k)^2 - n = a_k$, and we collect the a_k which completely factor into primes in our factor base consisting of primes $\leq B$, our bound.

To find a product of a_i's which is a square, Brillhart and Morrison in the 1970's introduced some linear algebra. Each a_k that we keep is completely determined by the vector of exponents $(\epsilon_1, \ldots, \epsilon_r)$ from its prime factorization $a_k = p_1^{\epsilon_1} \cdots p_r^{\epsilon_r}$ over our factor base, so we can work with these vectors. Our goal is a product of a_i with all exponents even; so what we want is a sum of these exponent vectors with all entries of the sum even. Since we are only interested in even versus odd, we can make a further simplification and keep only this parity information, setting $\eta_i = \epsilon_i \pmod 2$, and using the vector $(\eta_1, \ldots \eta_r)$. Then what we seek is a collection of a_i's so that their mod 2 exponent vectors $(\eta_1, \ldots \eta_r)$ sum, mod 2, to the 0-vector. If we think of these vectors as lying in the vector space $\mathbb{Z}_2^r$, what we are looking for is a linear dependence among the mod 2 exponent vectors. Such a dependence leads directly to a collection of a_i (those corresponding to the vectors in the dependence with coefficient 1) whose product is a square.

But! We know that $r+1$ vectors in an r-dimensional space (like $\mathbb{Z}_2^r$) <u>must</u> be linearly dependent! this tells us how many a_i's we must find the factor completely over our factor base before we can find a dependency; we need one more a_i than the number of primes in our factor base. Then we can find the linear dependency by arranging our mod 2 exponent vectors as the columns of a matrix, and (by row reduction!) compute the nullspace of the matrix. (Row reduction works perfectly fine over $\mathbb{Z}_2$, since it is a field.) This significantly speeds up finding the product of a_i's which is a square.

In-class example: factoring $n = 3920053$.

The final speedup for this process is to make finding the a_i that completely factor over the factor base more efficient. This is due to Carl Pomerance, in the early 1980's. The idea is to adapt the Sieve of Eratosthenes, which looks for primes, to instead look for number that factor into small primes. So instead of circling the smallest untouched number (which is the next prime p) and crossing off the multiples of that prime - this crosses off precisely what we are looking for! - we divide in place every number that is a multiple of p by p. The idea is that If we repeatedly cycle through the list, dividing multiples of 2 by 2 (i.e., every other number), then every multiple of 4 by <u>another</u> 2 (i.e., every 4th number), and divide all multiples of 3 by 3, etc., the numbers which are products of small primes will be reduced to 1, telling us <u>precisely</u> where they are!