CS4390/5390 Fall 2013
Shirley Moore, Instructor
November 7 Class and Homework 5 (due Thursday, November 14)

Quadratic Residues and Quadratic Sieve Factorization

Exercise 6.13. (Homework) Similar to the CFRAC algorithm, for the quadratic sieve algorithm, we will need to try to find a product of factorizations such that the powers of the primes in the product are all even. Formulate the linear algebra problem that can be solved to accomplish this.

Definition 6.12. *b* is a *quadratic residue* modulo *m* if *b* is relatively prime to *m* and there exists an integer *t* such that $b \equiv t^2 (\mathrm{mod}\ m)$.

Exercise 6.14. (a) Find the quadratic residues for *m* =7.

(b) Find the quadratic residues for *m* = 11.

(c) What do you observe?

Theorem 6.13. For any prime modulus $p > 2$: (a) Exactly $(p - 1)/2$ elements of the reduced residue system modulo *p* are quadratic residues,
(b) Euler's Criterion: The integer *b* is a quadratic residue modulo *p* if and only if $b^{(p-1/2)} \equiv 1 (\mathrm{mod}\ p)$, and (c) If *p* does not divide $b = cd$, then *b* is a quadratic residue if and only if either *c* and *d* are both quadratic residues or neither is a quadratic residue.

Euler's Criterion enables us to easily test whether an integer *b* is a quadratic residue for a prime *p*. For some algorithms (such as quadratic sieve), we need to generate primes for which a given *b* is a quadratic residue. By Theorem 6.13(c), if we know the status of all prime factors of *b*, we can easily determine if *b* is a quadratic residue, and thus we need only consider prime *b*.

Exercise 6.15 (Homework). Write a function that takes inputs *b* and *p* and determines whether or not *b* is a quadratic residue for *p*. Use your function to write a program that, given N and M, outputs a row for each prime *b* less than or equal to N containing all the primes less than or equal to M for which *b* is a quadratic residue.

Quadratic Sieve Algorithm

Similar to other factorization algorithms we have studied, the quadratic sieve algorithm tries to find X and Y such that $X^2 \equiv Y^2 (\text{mod } n)$, where *n* is the number we are trying to factor. If we can do this, then there is a 50-50 chance that $\gcd(X - Y, n)$ is a nontrivial factor of *n*. The quadratic sieve method finds a set of numbers that can be factored as a product of primes from a specially chosen factor base. Similar to CFRAC, it then tries to find a product of the factorizations in which all of the primes have even powers. We choose the factor base $B = \{p_1, p_2, \ldots, p_k\}$ such that $2 \in B$ and for each odd $p_i \in B$, *n* is a quadratic residue for p_i. Now pick x_k near $\sqrt{n}$ and try to factor $y_k = x_k^2 - n$. Then try to find a product of the factorizations with all prime factors having even powers.

Exercise 6.16. (Homework) Consider the number *n* = 16843009. Using a factor base consisting of 2 plus the four smallest odd primes for which *n* is a quadratic residue, factor *n* by finding the first six factorable y_k greater than $\sqrt{n}$.

B = { }

x_k	y_k	**Factorization of** y_k

Exercise 6.17 (Homework). (a) (Required for graduate students. Optional/extra credit for undergraduates). Show that by restricting the factor base to primes for which *n* is a quadratic residue, we are guaranteed to find all useful factorizations of the y_k. (b) Argue why using such a restricted factor base makes the quadratic sieve algorithm fast.