Lecture 14 Difference of squares method §3.6–3.7.2.

Last time Algorithms to factor $N = pq$

1. Exhaustive search — general purpose, slow
2. Pollard's $(p-1)$ method — fast if $p-1$ or $q-1$ is $\log(N)$-smooth, not general purpose
3. Difference of squares method — general purpose

Key Fact $N = a^2 - b^2 = (a-b)(a+b)$

So $a^2 \equiv b^2 \pmod N \Rightarrow (a+b)(a-b) \equiv 0 \pmod N$

$\Rightarrow \gcd(a-b, N) = p$ or q or N

If $\gcd(a-b, N) \neq N$, we factor N.

So we need a strategy to find solutions to $a^2 \equiv b^2 \bmod N$

Pick a s.t. $\sqrt{N} < a < \sqrt{2N}$, so

$0 \leq a^2 - N < N$.

Can factor $a^2 - N$ into $p_1^{e_1} \cdots p_r^{e_r}$. If all e_i's are even then $a^2 - N = \left(p_1^{e_1/2} \cdots p_r^{e_r/2}\right)^2$.

Of course, we were trying to factor N, but N not smooth $\Rightarrow$ hard to factor.

Pick B & look at $a^2 - N$ only if it is B-smooth, otherwise throw it out.

Recall

Def An integer n is B-smooth if all prime factors of n are $\leq B$.

Suppose $p_1, \ldots, p_r$ are all primes $\leq B$.

Then each B-smooth number has a factorization

$$a_1^2 - N = p_1^{e_{11}} \cdots p_r^{e_{r1}}$$

$$a_2^2 - N = p_1^{e_{12}} \cdots p_r^{e_{r2}}$$

$$\vdots$$

Now we want to find a product of these s.t. $(a_{i_1}^2 - N) \cdots (a_{i_k}^2 - N) = p_1^{2f_1} \cdots p_r^{2f_r}$ has all exponents even.

Since multiplication $\rightsquigarrow$ addition of exponent vectors, we are looking for coefficients s.t.

$$\vec{e}_i = (e_{i1}, \ldots, e_{ir})$$

$$\sum \varepsilon_i \vec{e}_i \equiv (0, \ldots, 0) \bmod 2.$$

We are looking for a linear dependence in an r-dim'l vector space $\Rightarrow$ guaranteed if we have at least r+1 vectors.

Then $(a_{i_1} \cdots a_{i_k})^2 \equiv (p_1^{f_1} \cdots p_r^{f_r})^2 \mod N$.

So we can compute $\gcd(N, a_{i_1} \cdots a_{i_k} + p_1^{f_1} \cdots p_r^{f_r})$

& if we are lucky, we factor N.

Three steps

(1) Relation building - find a_i s.t. $a_i^2 \equiv c_i$ w/ c_i B-Smooth

(2) elimination $\rightsquigarrow$ find a product $\prod a_{i_j}^2 \equiv d$ w/ $d = p_1^{2f_1} \cdots p_r^{2f_r}$.

(3) GCD computation.

(1) is the most interesting & slowest step though (2) is also nontrivial when r is large. Can just use Gaussian elimination.

Ex $N = 221$, $\sqrt{N} < 15, \ldots, 21 < \sqrt{2N}$

$B = 7$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ $r = 4$.

Step 1

Find B-smooth numbers

$15^2 - 221 = 2^2$

$16^2 - 221 = 35 = 5 \cdot 7$

$17^2 - 221 = 68 = 2^2 \cdot 17$

$18^2 - 221 = 103$

$19^2 - 221 = 140 = 2^2 \cdot 5 \cdot 7$

$20^2 - 221 = 179$

$21^2 - 221 = 220 = 2^2 \cdot 11$

So:

$15^2 \equiv 2^2$ $\quad e_1 = (0,0,0)$

$16^2 \equiv 5 \cdot 7$ $\quad e_2 = (0,1,1)$

$19^2 \equiv 2^2 \cdot 5 \cdot 7$ $\quad e_3 = (0,1,1)$

$e_1 = \vec{0}$

$e_2 + e_3 = \vec{0}$

$15^2 \equiv 2^2$

$(16 \cdot 19)^2 \equiv (2 \cdot 5 \cdot 7)^2$.

$15 - 2 = 13$

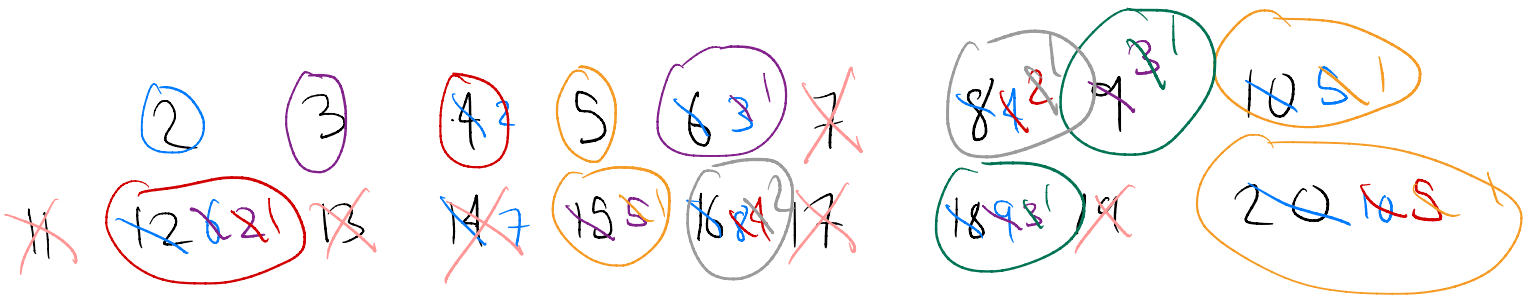
$304 - 70 = 234$

$\gcd(234, 221) = \gcd(221, 13) = 13.$

$\Rightarrow) \; 221 = 13 \cdot 17.$

Quadratic Sieve

To find numbers such that $x^2 - N$ is B-Smooth, we use a sieve method. First imagine we were looking for all 5-smooth numbers:



B-smooth Sieve

- Write out numbers in a range
- Look at first unclassified #,
  - if current value > B, cross it off this one isn't B-smooth
  - if current value = 1, select it, it is B-smooth
  - if current value is between 1 & B, this # is a prime power of a prime < B. If current value is p & orig value is p^k, divide every p^kth number by p. Also select p^k as a B-smooth #.

We want to do this same process except with the output of $F(t) = t^2 - N$.

List out the values of $F(t)$.

For each p^t, want to locate the t s.t. $F(t) \equiv 0 \pmod{p^k}$.

There will either be 0 or 2 $t \in \mathbb{Z}/p^k$ s.t. $F(t) = 0 \pmod{p^k}$. If there are 0, none of the $F(t)$ are divisible by p & no need to do any divisions. If there are two solutions, say α & β, then the entries $F(\alpha + ip^k)$ & $F(\beta + ip^k)$ need to be divided by p. See the book for an example!