Math 571

Taught by Tom Weston
Scribed by Ben Burns

UMass Amherst

Spring 2022

Contents

1 First Exam

Covers through today

- Discrete Logs
- Diffie-Hellman Key Exchange
- Shanks Algorithm
- RSA
- Factorization (p-1 method, trial division, difference of squares)

Example 1. Fiven a few explicity congruences $c_i \equiv a_i^2 \pmod{n}$ explain how you can find a factor of n

Practice exam by Thursday

Format of Exam: Around 4 questions, 2 proof, 2 computation, no calculator

2 Factorization by difference of squares

(1) Find lots of congruences $a_1^2 \equiv c_i \pmod{n}$ with c_i product of small primes. Fix small number B, and require all prime factors $p \leqslant B$
(2) Elimination: Find a subset of these congruences which multiply to give $x^2 \equiv y^2 \pmod{n}$ ($\mathbb{F}_2$ linear algebra)
(3) Compute $\gcd(x \pm y, n)$, hope its a proper factors of n

Review finding kernel, Gaussian Elimination $\mathbb{F}_2$, book of (2)

Algorithm: Find numbers a such that $a^2 \pmod{n}$ is a product of small primes

$m = \lfloor \sqrt{n} \rfloor + 1$. Try $a = m, m+1, m+2, \cdots, a^2 \pmod{n} = a^2 - n$.

This is relatively small since $a \approx \sqrt{n}$, so has a better chance of factoring into small primes

$Q(x) = x^2 - n$

Looking at $x = m, m+1, m+2$, we find $x^2 \equiv Q(x) \pmod{n}$, where $x^2 = a_i$ and $Q(x) = c_i$.

Problem: Given n, a, how do you determine if $Q(a) = a^2 - n$ is a product of small primes without factoring?

Remark 2. Roughly half of primes will never be factors of $Q(a)$

Why? Suppose $p | Q(a)$ for some a. Then $p | a^2 - n \implies a^2 \equiv n \pmod{p} \implies n$ is a square mod p.

Fix odd prime p

Definition 3. Given $t \in \mathbb{F}_p$ such that $t \neq 0$, we say t is a quadratic residue mod p if $\exists s \in \mathbb{F}_p$ such that $s \equiv s^2 \pmod{p}$

For example, $p = 11$

"Squares are always squares" - :D

There are always exactly $\frac{p-1}{2}$ squares and $\frac{p-1}{2}$ non-squares

Definition 4 (Legendre Symbol)**.** $\left(\frac{t}{p}\right) = +1$ if t square mod p, -1 if t non-square, 0 if $t = 0 \pmod{p}$.

Remark 5. The quadratic resides of $\mathbb{F}_p$ are the even powers of any generator g.

Fix a generator $g \in \mathbb{F}_p$. Fix $t \in \mathbb{F}_p$. Write $t = g^e$ for some e s.t $0 \leqslant e \leqslant p-1$. If e is even then $t = (g^{e/2})^2 \implies \left(\frac{t}{p}\right) = 1$. Since this already gives $(p-1)/2$ squares for $e = 0, 2, 4, \ldots p-3$, so it follows that e odd $\implies \left(\frac{t}{p}\right) = -1$.

Definition 6 (Properties of Legendre Symbol)**.** (1) $\left(\frac{t}{p}\right) \equiv t^{\frac{p-1}{2}} \pmod{p}$

(2) $\left(\frac{st}{p}\right) = \left(\frac{s}{p}\right)\left(\frac{t}{p}\right)$

(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$ if $p \equiv 1 \pmod{4}$, -1 is $p \equiv 3 \pmod{4}$

Proof:
(1) FLT for squares, polynomial counting argument for non-squares
(2) right side of (1) is multplicative, so left side has to be as well
(3)

Definition 7 (Quadratic Reciprocity Law)**.** Let p, q be distinct odd positive primes. Then $\left(\frac{p}{q}\right) = \frac{q}{p}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Equivalently, if either p or q is congruent to 1 mod 4, then the reciprocity holds. Else, they are negations.

Definition 8 (Quadratic Sieve)**.** brr