Lectures 22 and 23

Algorithmic Number Theory

(Silvio Micali, Jeff Wu)

1 Review: Number Theory and Notation

Here we review some basic concepts in number theory.

- $\mathbb{Z}_n$: the additive group of integers modulo n.
- Two integers a, b are relatively prime if $\gcd(a, b) = 1$.
- $\mathbb{Z}_n^*$: the multiplicative group of integers less than n and relatively prime to n. Every element $a \in \mathbb{Z}_n^*$ has an inverse that is easy to compute. (Because, since $\gcd(a, n) = 1$, we know that there exist integers x and y such that $ax+ny = 1$, so that $ax = 1 \mod n$; thus, $x \equiv a^{-1} \mod n$. We can find x using the Extended Euclidean Algorithm.)
- $\mathbb{Z}_p^*$: a special case of $\mathbb{Z}_n^*$ where $n = p$ is a prime. $\mathbb{Z}_p^*$ is a cyclic group of order $p - 1$ (See Dana Angluin's notes for the proof.) This means that there exists an element $g \in \mathbb{Z}_p^*$ such that $\mathbb{Z}_p^* = \{g, g^2, \ldots, g^{p-1}\}$. For instance, 2 is a generator of $\mathbb{Z}_{11}^*$. We have:

$$\mathbb{Z}_{11}^* = \{2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10,\ 2^6 = 9,\ 2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 1\}$$

- Fermat's Little Theorem states that $a^{p-1} \equiv 1 \mod p$ for all $a \in \mathbb{Z}_p^*$. (For example, note that $2^{10} = 1 \mod 11$ in $\mathbb{Z}_{11}^*$ above is a consequence of Fermat's Little theorem).
- $\phi(n)$: The Euler totient function is defined by $\phi(n) := |\mathbb{Z}_n^*|$. Equivalently, $\phi(n)$ is the number of integers between 1 and n that are relatively prime to n.
- When p is prime, all integers between 1 and $p-1$ are relatively prime to p. Thus, $\phi(p) = p-1$.
- If p^k is a prime power, then all integers between 1 and p^k are relatively prime to p^k except $p, 2p, 3p, \ldots, p^{k-1}p$. Thus $\phi(p^k) = p^k - p^{k-1}$.

2 Modular exponentiation

Problem: "Given a, x, and n, efficiently compute $a^x \mod n$."

An obvious (naive) approach is to repeatedly multiply by a, and then take the remainder modulo n:

1. Set $y = 1$
2. Repeat x times: $y = y \cdot a$
3. Return $y \mod n$

This number y gets extremely large. To avoid this, we can simply use properties of modular arithmetic:

1. Set $y = 1$
2. Repeat x times: $y = (y \cdot a) \bmod n$
3. Return y

However, this still requires x multiplications. Can we do better?

The answer is (of course) yes! We will use a well-known trick called repeated squaring. The important observation is that squaring a number doubles the exponent. That is, $(a^k)^2 = a^{2k}$. This means that $(a^{(2^i)})^2 = a^{2 \cdot 2^i} = a^{(2^{i+1})}$. So by repeatedly squaring, we can obtain $a^{(2^i)}$ in only i multiplications. Thus if x is a power of 2, we can obtain a^x in only $\log(x)$ multiplications.

But if x is not a power of two, we can write it as a sum of powers of 2 in the following manner: $x = \sum_{i=1}^{k} b_i 2^i$ where $b_k b_{k-1} \dots b_0$ is the binary representation of x. Here, $k = \lfloor \log_2(x) \rfloor$. This means

$$a^x = a^{\sum_{i=1}^{k} b_i 2^i} = \prod_{i=1}^{k} a^{b_i 2^i} = \prod_{i=1}^{k} \left(a^{(2^i)} \right)^{b_i}.$$

This is simply the product of the $a^{(2^i)}$ for i where $b_i = 1$. All of this analysis holds modulo n, as well.

So we have the following algorithm, which uses $O(k) = O(\log x)$ multiplications:

1. First make a matrix so that $A[i] = a^{(2^i)}$.
   i. Set $A[0] = a$.
   ii. For $i = 1, \dots, k$: $A[i] = (A[i-1])^2 \bmod n$
2. Obtain the binary representation $b_k b_{k-1} \dots b_0$ of x.
3. Let $y = 1$
4. For $i = 1, \dots, k$: If $b_i = 1$, set $y = (A[i] \cdot y) \bmod n$
5. Return y

3 Quadratic residues modulo p

We can define a quadratic residue modulo p as follows:

Definition 1 *We say that a is a* quadratic residue *(or simply* square*) modulo p if there exists $x \in \mathbb{Z}_p^*$ such that $a \equiv x^2 \bmod p$.*

Note that $\mathbb{Z}_p^*$ has a generator g. Thus, we can write any $x \in \mathbb{Z}_p^*$ as $x = g^k$. Not only that, but the set $\{g^1, \dots, g^{p-1}\}$ is precisely $\{1, \dots, p-1\}$, the set of elements of $\mathbb{Z}_p^*$.

3.1 Deciding if a number is a quadratic residue modulo p

Problem: "Given (a, p), decide if a is a quadratic residue modulo p."

Let's first suppose we have a generator g. Which of the elements of $\mathbb{Z}_p^*$ are quadratic residues? There is a very simple answer. We'll assume $p > 2$, so it is odd.

We know that the set of elements is $\{g^1, \ldots, g^{p-1}\}$. Thus the set of squares is simply the elements of the sequence $g^2, g^4, \ldots, g^{2p-2}$. However, we are counting elements twice. By Fermat's little theorem, $g^{p-1} \equiv 1 \bmod p$. So the sequence was equivalent to $g^2, g^4, \ldots, g^{p-3}, g^0, g^2, \ldots, g^{p-3}, g^0$. From this, we see that the set of squares is simply $\{g^2, g^4, \ldots, g^{p-3}, g^{p-1} = g^0\}$.

So we have shown that the quadratic residues modulo p are precisely the even powers of g. That is, a is a square modulo p if and only if $a = g^{2k}$ for some k.

Note that this also shows that every quadratic residue $a = x^2 \in \mathbb{Z}_p^*$ has two square roots (which are $+x$ and $-x$). And precisely half the elements of $\mathbb{Z}_p^*$ are quadratic residues.

This gives an immediate approach to the problem posed: Compute $\log_g(a) \bmod p$ and check if the result is even. Unfortunately, we don't know of any algorithms for efficiently computing discrete logarithms. (In fact, we believe that doing so is hard!)

What can we do when the main road is blocked? We find another road! In this case, we can use *Euler's Criterion*.

Proposition 2 (Euler's criterion) *The element a is a square modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Moreover, a is not a square modulo p if and only if $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.*

Proof: If a is a square modulo p, then $a \equiv x^2 \bmod p$ for some $x \in \mathbb{Z}_p^*$. Let g be a generator of $\mathbb{Z}_p^*$ and write $x = g^k$ for some $k \in [p-1]$. Then $a = g^{2k}$, and we can write:

$$a^{\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv (g^{p-1})^k \equiv 1^k \equiv 1 \bmod p \ .$$

For the other direction, suppose a is *not* a square modulo p. Then write $a = g^{2k+1}$, so that

$$a^{\frac{p-1}{2}} \equiv g^{(2k+1)(\frac{p-1}{2})} \equiv (g^{p-1})^k g^{\frac{p-1}{2}} \equiv 1 \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \bmod p \ .$$

To conclude the proof, we need to show is that $g^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Recall that g is a generator of $\mathbb{Z}_p^*$, which has $p-1$ elements. Hence, $g, g^2, \ldots, g^{\frac{p-1}{2}}, \ldots, g^{p-1}$ must *all* be *distinct* elements of $\mathbb{Z}_p^*$. In particular, $g^{\frac{p-1}{2}} \not\equiv g^{p-1} \equiv 1 \bmod p$. (Where $g^{p-1} \equiv 1 \bmod p$ follows from Fermat's Little Theorem.)

But $g^{\frac{p-1}{2}}$ is a square root of $g^{p-1} \equiv 1 \bmod p$. As we showed above, this square root is not 1. Since $\mathbb{Z}_p$ is a field, there are only two square roots of unity: $+1$ and -1. Thus, we must have $g^{\frac{p-1}{2}} \equiv -1 \bmod p$. □

In summary, if p is prime, we can efficiently decide whether a given a is a square modulo p.

3.2 Finding square roots modulo p

Problem: "Given (a, p), find a square root of a modulo p."

We assume that p is a prime such that $p \equiv 3 \bmod 4$ and that a is a square modulo p. Since a is a square modulo p, Euler's Criterion tells us that

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p \ .$$

Writing $p = 3 + 4k$ for some integer k, we obtain

$$\begin{aligned} a^{\frac{2+4k}{2}} &\equiv 1 \bmod p \\ a^{2k+1} &\equiv 1 \bmod p \\ a^{2k+2} &\equiv a \bmod p \\ (a^{k+1})^2 &\equiv a \bmod p \ . \end{aligned}$$

We deduce that $\sqrt{a} \equiv a^{k+1} \bmod p$, provided $p = 3 + 4k$, for some integer k. See Dana Angluin's notes (chapters 20 and 21) for general (randomized polynomial time) procedures to find a square root of a modulo p for any odd prime p.

4 Quadratic residues modulo n (composite)

The definition of a quadratic residue modulo a composite number n remains the same:

Definition 3 *We say that a is a* quadratic residue *(or simply* square*) modulo n if there exists $x \in \mathbb{Z}_p^*$ such that $a \equiv x^2 \bmod n$.*