Lecture 7

1 More on Chinese Remaindering

Let $N = pq$, where p, q are distinct primes. We saw last time the notion of *Chinese remaindering*, whereby we can view $x \in \mathbb{Z}_N^*$ as $(x_p, x_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. We also saw how this representation might speed up multiplication in $\mathbb{Z}_N^*$. But it can also speed up exponentiation. For completeness, we state the following results:

Fact 1 *Let N, p, q as above. Let $\leftrightarrow$ denote the "Chinese remaindering" representation of an element in $\mathbb{Z}_N^*$ as discussed above. Then:*

- *If $x \leftrightarrow (x_p, x_q)$ and $y \leftrightarrow (y_p, y_q)$ then $xy \leftrightarrow (x_p y_p \bmod p, x_q y_q \bmod q)$ (Note that computation in the left half of the tuple is always done in $\mathbb{Z}_p^*$ and computation in the right half of the tuple in always done in $\mathbb{Z}_q^*$, so the notation "$\bmod p$", "$\bmod q$" is redundant. From now on, we omit it.)*
- *If $x \leftrightarrow (x_p, x_q)$ then $x^{-1} \leftrightarrow (x_p^{-1}, x_q^{-1})$.*
- *If $x \leftrightarrow (x_p, x_q)$ and k is an integer, then $x^k \leftrightarrow (x_p^k, x_q^k)$.*

These facts can speed up computations. As an example, consider computing $4^{1056} \bmod 15$. Since $15 = 3 \cdot 5$, we can represent 4 as $(1, 4)$. Then $4^{1056} = (1^{1056}, 4^{1056}) = (1, (-1)^{1056}) = (1, 1)$. To get our final answer, we now just need to convert $(1, 1)$ back to an element of $\mathbb{Z}_{15}^*$. We gave a technique for doing this last time, but here we can observe that $1 \in \mathbb{Z}_{15}^*$ has the property that $1 = 1 \bmod 3$ and $1 = 1 \bmod 5$! So our final answer is 1.

We will see below that Chinese remaindering is also a powerful theoretical tool, enabling us to easily prove many useful theorems.

2 Quadratic Residues

The notion of *quadratic residues* pops up very often in cryptography. An element $a \in \mathbb{Z}_k^*$ is a quadratic residue if and only if it is a square; i.e., if there is an element $x \in \mathbb{Z}_k^*$ such that $x^2 = a \bmod k$. We begin by looking at the case $k = p$, where p is an odd prime. It is a fact that every element in $\mathbb{Z}_p^*$ has either no square roots (i.e., is not a quadratic residue) or has exactly two, distinct square roots, and we now state and prove this formally.

Lemma 1 *For $p \geq 3$ an odd prime, every element $a \in \mathbb{Z}_p^*$ has either no square roots or two distinct square roots in $\mathbb{Z}_p^*$.*

Proof Let $a \in \mathbb{Z}_p^*$. If a has no square roots, we are done. Otherwise, let x be a square root of a. Note that $-x$ is also a square root of a (why?). On the other hand, x and $-x$ are distinct modulo p (this is why we require that $p \neq 2$), so a has at least two square roots. Can there be more? Well, let y be another square root of a. Then $x^2 = y^2$ and thus $x^2 - y^2 = 0$. Algebra gives: $(x-y)(x+y) = 0$. But this has the two solutions $y = \pm x$ (important note: this makes use of the fact that the equation $wz = 0 \bmod p$ has solutions only if $w = 0$ or $z = 0$, or both. This is true when p is prime but is *not* true if p is composite, as we will see below). ■

This lemma also gives us a count of how many quadratic residues there are in $\mathbb{Z}_p^*$. Since every square maps to two, distinct elements of the group, exactly half of the elements of $\mathbb{Z}_p^*$ must be squares (i.e., there are $(p-1)/2$ squares).

We now consider the case $k = N$, where $N = pq$ is a product of two, distinct (odd) primes. How many square roots can elements $a \in \mathbb{Z}_N^*$ have now? We show that each element has either no square roots or exactly *four* distinct square roots.

Theorem 1 *Let $N = pq$ as above. Then an element $a \in \mathbb{Z}_N^*$ has either no square roots or four distinct square roots in $\mathbb{Z}_N^*$.*

Proof If $a \in \mathbb{Z}_N^*$ has no square roots, we are done. So, assume a has at least one square root x. Using Chinese remaindering, let $a \leftrightarrow (a_p, a_q)$ and $x \leftrightarrow (x_p, x_q)$. Since $x^2 = a$, it must be the case that $x_p^2 = a_p \bmod p$ and $x_q^2 = a_q \bmod q$ (by Fact 1). But then a has three more square roots: $(-x_p, x_q)$, $(x_p, -x_q)$, and $(-x_p, -x_q)$ (and these are all distinct, as argued above for the case p prime). Finally, if a had another square root (y_p, y_q) then $y_p^2 = a_p \bmod p$ and $y_q^2 = a_q \bmod q$ so that $y_p = \pm x_p$ and $y_q = \pm x_q$ (as argued above for the case p prime). So these four square roots are the *only* square roots of a. ■

Define $\mathcal{QR}_N$ as the set of quadratic residues in $\mathbb{Z}_N^*$. Note that the theorem above implies that exactly $1/4$ of the elements in $\mathbb{Z}_N^*$ are quadratic residues; or $|\mathcal{QR}_N| = |\mathbb{Z}_N^*|/4$.

(As an aside, note why the proof that there are only two square roots given in the case of $\mathbb{Z}_p^*$, p prime, fails here. In particular, it is not the case that if $xy = 0 \bmod N$ then either $x = 0$ or $y = 0$. As an easy counterexample, note that, for any a, b we have [using representations]: $(a, 0) \cdot (0, b) = (0, 0) = 0$. Also, $pq = 0 \bmod N$ although $p, q \neq 0 \bmod N$.)

It is the case that square roots modulo a prime p can be computed in polynomial-time (we may discuss how to do this later in the semester). This allows efficient calculation of square roots modulo N *if* the factors of N are known (by application of the Chinese remainder theorem and Fact 1). We will see below that square roots *cannot* be computed in polynomial time modulo N when the factorization of N is not known, unless factoring can be done in polynomial time.

2.1 Legendre and Jacobi Symbols

Notation has developed for dealing with quadratic residues in modular groups. For elements in $\mathbb{Z}_p^*$ (p prime), define the Legendre symbol as follows:

$$\mathcal{L}_p(y) = \begin{cases} +1 & \text{if } y \text{ is a quadratic residue modulo } p \\ -1 & \text{otherwise.} \end{cases}$$