YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security

Notes 13 (rev. 1)
Professor M. J. Fischer *October 18, 2005*

Lecture Notes 13

1 Quadratic Residues

1.1 Squares and square roots

An integer a is called a *quadratic residue (or perfect square) modulo* n if $a \equiv b^2 \pmod{n}$ for some integer b. Such a b is said to be a *square root* of a modulo n. We let

$$\mathrm{QR}_n = \{a \in \mathbf{Z}_n^* \mid a \text{ is a quadratic residue modulo } n\}.$$

be the set of quadratic residues in $\mathbf{Z}_n^*$, and we denote the set of non-quadratic residues in $\mathbf{Z}_n^*$ by $\mathrm{QNR}_n = \mathbf{Z}_n^* - \mathrm{QR}_n$.

1.2 Square roots modulo a prime

Claim 1 *For an odd prime p, every $a \in QR_p$ has exactly two square roots in $\mathbf{Z}_p^*$, and exactly 1/2 of the elements of $\mathbf{Z}_p^*$ are quadratic residues.*

For example, take $p = 11$. The following table shows all of the elements of $\mathbf{Z}_{11}^*$ and their squares.

a	$a^2 \bmod 11$
1	1
2	4
3	9
4	5
5	3
$6 = -5$	3
$7 = -4$	5
$8 = -3$	9
$9 = -2$	4
$10 = -1$	1

Thus, we see that $\mathrm{QR}_{11} = \{1, 3, 4, 5, 9\}$ and $\mathrm{QNR}_{11} = \{2, 6, 7, 8, 10\}$.

Proof: We now prove Claim 1. Consider the mapping $\mathrm{sq} : \mathbf{Z}_p^* \to \mathrm{QR}_p$ defined by $b \mapsto b^2 \bmod p$. We show that this is a 2-to-1 mapping from $\mathbf{Z}_p^*$ onto QR_p.

Let $a \in \mathrm{QR}_p$, and let $b^2 \equiv a \pmod{p}$ be a square root of a. Then $-b$ is also a square root of a, and $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$. Hence, a has at least two distinct square roots $\pmod{n}$. Now let c be any square root of a.

$$c^2 \equiv a \equiv b^2 \pmod{p}.$$

Then $p \mid c^2 - b^2$, so $p \mid (c - b)(c + b)$. Since p is prime, then either $p \mid (c - b)$, in which case $c \equiv b \pmod{p}$, or $p \mid (c + b)$, in which case $c \equiv -b \pmod{p}$. Hence $c \equiv \pm b \pmod{p}$. Since c was an arbitrary square root of a, it follows that $\pm b$ are the only two square roots of a. Hence, $\mathrm{sq}()$ is a 2-to-1 function, and $|\mathrm{QR}_p| = \frac{1}{2}|\mathbf{Z}_p^*|$ as desired. ■

1.3 Square roots modulo the product of two primes

Claim 2 *Let $n = pq$ for p, q distinct odd primes. Then every $a \in QR_n$ has exactly four square roots in $\mathbf{Z}_n^*$, and exactly 1/4 of the elements of $\mathbf{Z}_n^*$ are quadratic residues.*

Proof: Consider the mapping $\mathrm{sq} : \mathbf{Z}_n^* \to \mathrm{QR}_n$ defined by $b \mapsto b^2 \bmod n$. We show that this is a 4-to-1 mapping from $\mathbf{Z}_n^*$ onto QR_n.

Let $a \in \mathrm{QR}_n$ and let $b^2 \equiv a \pmod n$ be a square root of a. Then also $b^2 \equiv a \pmod p$ and $b^2 \equiv a \pmod q$, so b is a square root of $a \pmod p$ and b is a square root of $a \pmod q$. Conversely, if b_p is a square root of $a \pmod p$ and b_q is a square root of $a \pmod q$, then by the Chinese Remainder theorem, the unique number $b \in \mathbf{Z}_n^*$ such that $b \equiv b_p \pmod p$ and $b \equiv b_q \pmod q$ is a square root of $a \pmod n$. Since a has two square roots mod p and two square roots mod q, it follows that a has four square roots mod n. Thus, sq() is a 4-to-1 function, and $|\mathrm{QR}_n| = \frac{1}{4}|\mathbf{Z}_n^*|$ as desired. ∎

1.4 Euler criterion

There is a simple test due to Euler for whether a number is in QR_p for p prime.

Claim 3 *(Euler Criterion): An integer a is a non-trivial*[1] *quadratic residue modulo p iff*

$$a^{(p-1)/2} \equiv 1 \pmod p.$$

Proof: Let $a \equiv b^2 \pmod p$ for some $b \not\equiv 0 \pmod p$. Then

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod p$$

by Euler's theorem.

For the other direction, suppose $a^{(p-1)/2} \equiv 1 \pmod p$. Let g be a primitive root of p, and choose k so that $a \equiv g^k \pmod p$. Then

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

Because g is a primitive root, $g^\ell \equiv 1 \pmod p$ implies that ℓ is a multiple of $p-1$ for any ℓ. Taking $\ell = (p-1)k/2$, we have that $p - 1 \mid (p-1)k/2$, from which we conclude that $2|k$. Hence, $k/2$ is an integer, and $b = g^{k/2} \not\equiv 0 \pmod p$ is a square root of a, so a is a non-trivial quadratic residue modulo p. ∎

1.5 Finding square roots

The Euler criterion lets us test membership in QR_p for prime p, but it doesn't tell us how to find square roots. In case $p \equiv 3 \pmod 4$, there is an easy algorithm for finding the square roots of any member of QR_p.

Claim 4 *Let $p \equiv 3 \pmod 4$, $a \in \mathrm{QR}_p$. Then $b = a^{(p+1)/4}$ is a square root of $a \pmod p$.*

Proof: Under the assumptions of the claim, $p + 1$ is divisible by 4, so $(p + 1)/4$ is an integer. Then

$$b^2 \equiv (a^{(p+1)/4})^2 \equiv a^{(p+1)/2} \equiv a^{1+(p-1)/2} \equiv a \cdot a^{(p-1)/2} \equiv a \cdot 1 \equiv a \pmod p$$

by the Euler Criterion (Claim 3). ∎

[1] A non-trivial quadratic residue is one that is not equivalent to $0 \pmod p$.

2 QR Probabilistic Cryptosystem

Let $n = pq$, p, q distinct odd primes. We can divide the numbers in $\mathbf{Z}_n^*$ into four classes depending on their membership in QR_p and QR_q.[2] Let Q_n^{11} be those numbers that are quadratic residues mod both p and q; let Q_n^{10} be those numbers that are quadratic residues mod p but not mod q; let Q_n^{01} be those numbers that are quadratic residues mod q but not mod p; and let Q_n^{00} be those numbers that are neither quadratic residues mod p nor mod q. Under these definitions, $Q_n^{11} = \mathrm{QR}_n$ and $Q_n^{00} \cup Q_n^{01} \cup Q_n^{10} = \mathrm{QNR}_n$.

Fact Given $a \in Q_n^{00} \cup Q_n^{11}$, there is no known feasible algorithm for determining whether or not $a \in \mathrm{QR}_n$ that gives the correct answer significantly more than 1/2 the time.

The Goldwasser-Micali cryptosystem is based on this fact. The public key consist of a pair $e = (n, y)$, where $n = pq$ for distinct odd primes p, q, and $y \in Q_n^{00}$. The private key consists of p. The message space is $\mathcal{M} = \{0, 1\}$.

To encrypt $m \in \mathcal{M}$, Alice chooses a random $a \in \mathrm{QR}_n$. She does this by choosing a random member of $\mathbf{Z}_n^*$ and squaring it. If $m = 0$, then $c = a \bmod n$. If $m = 1$, then $c = ay \bmod n$. The ciphertext is c.

It is easily shown that if $m = 0$, then $c \in Q_n^{11}$, and if $m = 1$, then $c \in Q_n^{00}$. One can also show that every $a \in Q_n^{11}$ is equally likely to be chosen as the ciphertext in case $m = 0$, and every $a \in Q_n^{00}$ is equally likely to be chosen as the ciphertext in case $m = 1$. Eve's problem of determining whether c encrypts 0 or 1 is the same as the problem of distinguishing between membership in Q_n^{00} and Q_n^{11}, which by the above fact is believed to be hard. Anyone knowing the private key p, however, can use the Euler Criterion to quickly determine whether or not c is a quadratic residue mod p and hence whether $c \in Q_n^{11}$ or $c \in Q_n^{00}$, thereby determining m.

3 Legendre Symbol

Let p be an odd prime, a an integer. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is a number in $\{-1, 0, +1\}$, defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a non-trivial quadratic residue modulo } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \\ -1 & \text{if } a \text{ is } \textit{not} \text{ a quadratic residue modulo } p \end{cases}$$

By the Euler Criterion (see Claim 3), we have

Theorem 1 *Let p be an odd prime. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} \pmod{p}$$

Note that this theorem holds even when $p \mid a$.

The Legendre symbol satisfies the following *multiplicative property*:

Fact Let p be an odd prime. Then

$$\left(\frac{a_1 a_2}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)$$

[2] To be strictly formal, we classify $a \in \mathbf{Z}_n^*$ according to whether or not $(a \bmod p) \in \mathrm{QR}_p$ and whether or not $(a \bmod q) \in \mathrm{QR}_q$.

Not surprisingly, if a_1 and a_2 are both non-trivial quadratic residues, then so is $a_1 a_2$. This shows that the fact is true for the case that

$$\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = 1.$$

More surprising is the case when neither a_1 nor a_2 are quadratic residues, so

$$\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = -1.$$

In this case, the above fact says that the product $a_1 a_2$ *is* a quadratic residue since

$$\left(\frac{a_1 a_2}{p}\right) = (-1)(-1) = 1.$$

Here's a way to see this. Let g be a primitive root of p. Write $a_1 \equiv g^{k_1} \pmod{p}$ and $a_2 \equiv g^{k_2} \pmod{p}$. Since a_1 and a_2 are not quadratic residues, it must be the case that k_1 and k_2 are both odd; otherwise $g^{k_1/2}$ would be a square root of a_1, or $g^{k_2/2}$ would be a square root of a_2. But then $k_1 + k_2$ is even since the sum of any two odd numbers is always even. Hence, $g^{(k_1+k_2)/2}$ is a square root of $a_1 a_2 \equiv g^{k_1+k_2} \pmod{p}$, so $a_1 a_2$ is a quadratic residue.