YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security | Notes 12 (rev. 1)
Professor M. J. Fischer | *October 17, 2006*

Lecture Notes 12

62 Square Roots Modulo the Product of Two Primes

Claim 1 *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. ■

63 Euler Criterion

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

Claim 2 *(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, as desired.

For the other direction, suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Clearly $a \not\equiv 0 \pmod{p}$. We show that a is a quadratic residue by finding a square root b modulo p.

Let g be a primitive root of p. Choose k so that $a \equiv g^k \pmod{p}$, and let $\ell = (p-1)k/2$. Then

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

Because g is a primitive root, $g^\ell \equiv 1 \pmod{p}$ implies that ℓ is a multiple of $p-1$. Hence, $(p-1) \mid (p-1)k/2$, from which we conclude that $2|k$ and $k/2$ is an integer. Let $b = g^{k/2}$. Then $b^2 \equiv g^k \equiv a \pmod{p}$, so b is a square root of a modulo p, as desired. ■

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

64 Finding Square Roots Modulo Special Primes

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 3 *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 2). ■

65 Shank's Algorithm for Finding Square Roots Modulo Odd Primes

Let p be an odd prime. It can be written uniquely as $p = 2^n q + 1$, where n and q are integers and q is odd. (Note that n is simply the number of trailing 0's in the binary expansion of p, and q is what results when p is shifted right by n places.) Because p is odd, $p-1$ is even, so $n \geq 1$. Section 64 treats the special case where $n = 1$. We now present an algorithm due to D. Shanks[2] that works for all n.

Let p, n, q be as above. Assume a is a quadratic residue and u is a quadratic non-residue modulo p. (We can easily find u by choosing random elements of $\mathbf{Z}_p^*$ and applying the Euler Criterion.) The goal is to find x such that $x^2 \equiv a \pmod p$.

Shank's Algorithm
Input: Odd prime p, quadratic residue $a \in \mathrm{QR}_p$.
Output: A square root of $a \pmod p$.

Let n, q satisfy $p = 2^n q$ and q odd.
Let u be a quadratic non-residue modulo p.
$k = n$
$z = u^q$
$x = a^{(q+1)/2}$
$b = a^q$
while ($b \not\equiv 1 \pmod p$) {
  let m be the least integer with $b^{2^m} \equiv 1 \pmod p$
  $t = z^{2^{k-m-1}}$
  $z = t^2$
  $b = bz$
  $x = xt$
  $k = m$
}
return x

[2] Shanks's algorithm appeared in his paper, "Five number-theoretic algorithms", in Proceedings of the Second Manitoba Conference on Numerical Mathematics, Congressus Numerantium, No. VII, 1973, 51–70. Our treatment is taken from the paper by Jan-Christoph Schlage-Puchta", "On Shank's Algorithm for Modular Square Roots", *Applied Mathematics E-Notes, 5* (2005), 84–88.

The congruence $x^2 \equiv ab \pmod{p}$ is easily shown to be a loop invariant. Hence, if the program terminates, x is a square root of a.

To see why it terminates after at most n iterations of the loop, we look at the orders[3] of b and z $\pmod{p}$ at the start of each loop iteration (before line 8) and show that $\mathrm{ord}(b) < \mathrm{ord}(z) = 2^k$.

On the first iteration, $k = n$, $z = u^q$, and $\mathrm{ord}(z) = 2^n$. Clearly

$$z^{2^n} \equiv u^{2^n q} \equiv u^{p-1} \equiv 1 \pmod{p},$$

so $\mathrm{ord}(z) \mid 2^n$. By the Euler Criterion, since u is a non-residue, we have

$$z^{2^{n-1}} \equiv u^{2^{n-1}q} \equiv u^{(p-1)/2} \not\equiv 1 \pmod{p}.$$

Hence, $\mathrm{ord}(z) = 2^n$. Using similar reasoning, since a is a quadratic residue, $b^{2^{n-1}} \equiv 1 \pmod{p}$, so $\mathrm{ord}(b) \mid 2^{n-1}$. It follows that $\mathrm{ord}(b) < \mathrm{ord}(z) = 2^n \pmod{p}$.

Now, on each iteration, line 8 sets $m = \mathrm{ord}(b)$ and line 9 sets $t = z^{2^{k-m-1}}$, so

$$\mathrm{ord}(t) = \mathrm{ord}(z)/2^{k-m-1} = 2^k/2^{k-m-1} = 2^{m+1}.$$

Line 10 sets $z = t^2$, so $\mathrm{ord}(z) = \mathrm{ord}(t)/2 = 2^m$. After line 11, $\mathrm{ord}(b) < 2^m$. This because the old value of b and the new value of z both have order 2^m. Hence, both of those numbers raised to the power 2^{m-1} are -1, so their product (the new value of b) raised to that same power is $(-1)^2 = 1$. Line 13 sets $k = m$ in preparation for the next iteration, and the loop invariant $\mathrm{ord}(b) < \mathrm{ord}(z) = 2^k$ is maintained. Moreover, $\mathrm{ord}(b)$ is reduced at each iteration, so the loop must terminate after at most n iterations.

66 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.[4] 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

[3] Recall that the order of an element g modulo p is the least integer k such that $g^k \equiv 1 \pmod{p}$.

[4] 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 $(a \bmod q) \in \mathrm{QR}_q$.

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.

67 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 2), 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 $p \,|\, a$.

The Legendre symbol satisfies the following *multiplicative property*:

Fact Let p be an odd prime. Then

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

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.