Lecture Notes 15

61 Quadratic Residues, 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 $\mathrm{QNR}_n = \mathbf{Z}_n^* - \mathrm{QR}_n$.

62 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. ■

63 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, $\mathrm{sq}()$ is a 4-to-1 function, and $|\mathrm{QR}_n| = \frac{1}{4}|\mathbf{Z}_n^*|$ as desired. ∎

64 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, 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. ∎

65 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 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 $0 \pmod{p}$.

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

Let p be an odd prime. Let s and t be unique integers such that $p - 1 = 2^s t$ and t is odd. (Note that s is simply the number of trailing 0's in the binary expansion of $p - 1$, and t is what remains when $p - 1$ is shifted right by s places.) Because p is odd, $p - 1$ is even, so $s \geq 1$.

In the special case when $s = 1$, $p - 1 = 2t$, so $p = 2t + 1$. Writing the odd number t as $2\ell + 1$ for some integer ℓ, we have $p = 2(2\ell + 1) + 1 = 4\ell + 3$, so $p \equiv 3 \pmod 4$. But this is exactly the special that we considered in Section 65.

We now present an algorithm that works to find square roots of quadratic residues modulo any odd prime p. Algorithm 66.1, due to D. Shanks[2], bears a strong resemblance to Algorithm 56.1 for factoring the RSA modulus given both the encryption and decryption exponents.

Let p, s, t be as above. Assume $a \in \mathrm{QR}_p$ is a quadratic residue and $u \in \mathrm{QNR}_p$ is a quadratic non-residue. (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 $a \pmod p$.

1. Let s, t satisfy $p = 2^s t$ and t odd.
2. Let $u \in \mathrm{QNR}_p$.
3. $k = s$
4. $z = u^t \bmod p$
5. $x = a^{(t+1)/2} \bmod p$
6. $b = a^t \bmod p$
7. while ($b \not\equiv 1 \pmod p$) {
8.   let m be the least integer with $b^{2^m} \equiv 1 \pmod p$
9. $t = z^{2^{k-m-1}} \bmod p$
10. $z = t^2 \bmod p$
11. $b = bz \bmod p$
12. $x = xt \bmod p$
13. $k = m$
14. }
15. return x

Figure 66.1: Shank's algorithm for finding a square root of $a \pmod n$.

The congruence $x^2 \equiv ab \pmod p$ is easily shown to be a loop invariant. It's clearly true initially since $x^2 \equiv a^{t+1}$ and $b \equiv a^t \pmod p$. Each time through the loop, a is unchanged, b gets multiplied by t^2 (lines 10 and 11), and x gets multiplied by t (line 12); hence the invariant remains true regardless of the value of t. If the program terminates, we have $b \equiv 1 \pmod p$, so $x^2 \equiv a$, and x is a square root of $a \pmod p$.

To see why it terminates after at most s 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 $\mathrm{ord}(b) < \mathrm{ord}(z) = 2^k$.

---

[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.

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

On the first iteration, $k = s$, and $z \equiv u^t \pmod{p}$. We argue that $\mathrm{ord}(z) = 2^s$. Clearly

$$z^{2^s} \equiv u^{2^s t} \equiv u^{p-1} \equiv 1 \pmod{p},$$

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

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

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

Now, on each iteration, line 8 sets $m = \mathrm{ord}(b)$ and line 9 sets $t = z^{2^{k-m-1}} \bmod p$, 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 $-1 \pmod{p}$, so their product (the new value of b) raised to that same power is $(-1)^2 \equiv 1$. 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 s iterations.

67 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 element of Q_n^{11} is equally likely to be chosen as the ciphertext c in case $m = 0$, and every element of Q_n^{00} is equally likely to be chosen as the ciphertext c 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.

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