CPSC 467b: Cryptography and Computer Security

Lecture 13

Michael J. Fischer

Department of Computer Science
Yale University

February 22, 2010

Quadratic residues modulo n

An integer b is said to be a *square root modulo n* of an integer a if

$$b^2 \equiv a \pmod{n}.$$

a is called a *quadratic residue (or perfect square) modulo n* if has a square root modulo n.

Quadratic residues in $\mathbf{Z}_n^*$

If $a, b \in \mathbf{Z}_n$ and $b^2 \equiv a \pmod{n}$, then

$$b \in \mathbf{Z}_n^* \text{ iff } a \in \mathbf{Z}_n^*.$$

Why?

Quadratic residues in $\mathbf{Z}_n^*$

If $a, b \in \mathbf{Z}_n$ and $b^2 \equiv a \pmod{n}$, then

$$b \in \mathbf{Z}_n^* \text{ iff } a \in \mathbf{Z}_n^*.$$

Why? Because

$$\gcd(b, n) = 1 \text{ iff } \gcd(a, n) = 1$$

This follows from the fact that $b^2 = a + un$ for some u, so if p is a prime divisor of n, then

$$p \mid b \text{ iff } p \mid a.$$

Quadratic residues in $\mathbf{Z}_n^*$

If $a, b \in \mathbf{Z}_n$ and $b^2 \equiv a \pmod{n}$, then

$$b \in \mathbf{Z}_n^* \text{ iff } a \in \mathbf{Z}_n^*.$$

Why? Because

$$\gcd(b, n) = 1 \text{ iff } \gcd(a, n) = 1$$

This follows from the fact that $b^2 = a + un$ for some u, so if p is a prime divisor of n, then

$$p \mid b \text{ iff } p \mid a.$$

Henceforth, we will generally assume that all quadratic residues and square roots under discussion are in $\mathbf{Z}_n^*$.

QR_n and QNR_n

We partition $\mathbf{Z}_n^*$ into two parts.

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

QR_n is the *set of quadratic residues* modulo n.

QNR_n is the *set of quadratic non-residues* modulo n.

For $a \in \mathrm{QR}_n$, we sometimes write

$$\sqrt{a} = \{b \in \mathbf{Z}_n^* \mid b^2 \equiv a \pmod{n}\},$$

the *set of square roots* of a modulo n.

Quadratic residues in $\mathbf{Z}_{15}^*$

The following table shows all elements of $\mathbf{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and their squares.

a		$a^2 \bmod 15$
1		1
2		4
4		1
7		4
8	$= -7$	4
11	$= -4$	1
13	$= -2$	4
14	$= -1$	1

Thus, $\mathrm{QR}_{15} = \{1, 4\}$ and $\mathrm{QNR}_{15} = \{2, 7, 8, 11, 13, 14\}$.

Quadratic residues modulo a prime

We next look at the case where $n = p$ is an odd prime.

Fact

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.

In other words, if $a \in \mathrm{QR}_p$

1. $|\sqrt{a}| = 2$.
2. $|\mathrm{QR}_n| = |\mathbf{Z}_p^*|/2$.

Quadratic residues in $\mathbf{Z}_{11}^*$

The following table shows all elements $b \in \mathbf{Z}_{11}^*$ and their squares.

b	b^2 mod 11
1	1
2	4
3	9
4	5
5	3

b	$-b$	b^2 mod 11
6	-5	3
7	-4	5
8	-3	9
9	-2	4
10	-1	1

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

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.
- Hence, $p \mid c^2 - b^2$, so $p \mid (c - b)(c + b)$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.
- Hence, $p \mid c^2 - b^2$, so $p \mid (c-b)(c+b)$.
- Since p is prime, then either $p \mid (c-b)$ or $p \mid (c+b)$ (or both).

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.
- Hence, $p \mid c^2 - b^2$, so $p \mid (c - b)(c + b)$.
- Since p is prime, then either $p \mid (c - b)$ or $p \mid (c + b)$ (or both).
- If $p \mid (c - b)$, then $c \equiv b \pmod{p}$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.
- Hence, $p \mid c^2 - b^2$, so $p \mid (c - b)(c + b)$.
- Since p is prime, then either $p \mid (c - b)$ or $p \mid (c + b)$ (or both).
- If $p \mid (c - b)$, then $c \equiv b \pmod{p}$.
- If $p \mid (c + b)$, then $c \equiv -b \pmod{p}$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.
- Hence, $p \mid c^2 - b^2$, so $p \mid (c-b)(c+b)$.
- Since p is prime, then either $p \mid (c-b)$ or $p \mid (c+b)$ (or both).
- If $p \mid (c-b)$, then $c \equiv b \pmod{p}$.
- If $p \mid (c+b)$, then $c \equiv -b \pmod{p}$.
- Hence, $c = \pm b$, so $\sqrt{a} = \{b, -b\}$, and $|\sqrt{a}| = 2$.

Proof that $|\sqrt{a}| = 2$ modulo a prime

We show that $|\sqrt{a}| = 2$ for $a \in \mathrm{QR}_p$.

- Let $a \in \mathrm{QR}_p$. It must have a square root $b \in \mathbf{Z}_p^*$.
- Consider $-b \in \mathbf{Z}_p$. $-b \in \sqrt{a}$ since $(-b)^2 \equiv b^2 \equiv a \pmod{p}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$.
- Hence, b and $-b$ are distinct elements of $\sqrt{a}$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.
- Hence, $p \mid c^2 - b^2$, so $p \mid (c - b)(c + b)$.
- Since p is prime, then either $p \mid (c - b)$ or $p \mid (c + b)$ (or both).
- If $p \mid (c - b)$, then $c \equiv b \pmod{p}$.
- If $p \mid (c + b)$, then $c \equiv -b \pmod{p}$.
- Hence, $c = \pm b$, so $\sqrt{a} = \{b, -b\}$, and $|\sqrt{a}| = 2$.
- Finally, since each $b \in \mathbf{Z}_p^*$ is the square root of exactly one element of QR_p, it must be that $|\mathrm{QR}_p| = \frac{1}{2}|\mathbf{Z}_p^*|$ as desired.

Quadratic residues modulo pq

We now turn to the case where $n = pq$ is the product of distinct odd primes.

Fact

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.

In other words, if $a \in \mathrm{QR}_n$

1. $|\sqrt{a}| = 4$.
2. $|\mathrm{QR}_n| = |\mathbf{Z}_n^*|/4$.

Proof that $|\sqrt{a}| = 4$ modulo pq

We show that $|\sqrt{a}| = 4$ for $a \in \mathrm{QR}_n$.

Proof that $|\sqrt{a}| = 4$ modulo pq

We show that $|\sqrt{a}| = 4$ for $a \in \mathrm{QR}_n$.

- Let $a \in \mathrm{QR}_n$. Then $b^2 \equiv a \pmod{n}$ for some $b \in \mathbf{Z}_n^*$,

Proof that $|\sqrt{a}| = 4$ modulo pq

We show that $|\sqrt{a}| = 4$ for $a \in \mathrm{QR}_n$.

- Let $a \in \mathrm{QR}_n$. Then $b^2 \equiv a \pmod{n}$ for some $b \in \mathbf{Z}_n^*$,
- Then $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$.

Proof that $|\sqrt{a}| = 4$ modulo pq

We show that $|\sqrt{a}| = 4$ for $a \in \mathrm{QR}_n$.

- Let $a \in \mathrm{QR}_n$. Then $b^2 \equiv a \pmod{n}$ for some $b \in \mathbf{Z}_n^*$,
- Then $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$.
- Therefore, b is a square root of a modulo both p and q.

Proof that $|\sqrt{a}| = 4$ modulo pq

We show that $|\sqrt{a}| = 4$ for $a \in \mathrm{QR}_n$.

- Let $a \in \mathrm{QR}_n$. Then $b^2 \equiv a \pmod{n}$ for some $b \in \mathbf{Z}_n^*$,
- Then $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$.
- Therefore, b is a square root of a modulo both p and q.
- Conversely, if $b_p \in \sqrt{a} \pmod{p}$ and $b_q \in \sqrt{a} \pmod{q}$, 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 $a \pmod{n}$.

Proof that $|\sqrt{a}| = 4$ modulo pq

We show that $|\sqrt{a}| = 4$ for $a \in \mathrm{QR}_n$.

- Let $a \in \mathrm{QR}_n$. Then $b^2 \equiv a \pmod{n}$ for some $b \in \mathbf{Z}_n^*$,
- Then $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$.
- Therefore, b is a square root of a modulo both p and q.
- Conversely, if $b_p \in \sqrt{a} \pmod{p}$ and $b_q \in \sqrt{a} \pmod{q}$, 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 by the Chinese remainder theorem that a has four distinct square roots mod n.

Proof that $|\sqrt{a}| = 4$ modulo pq

We show that $|\sqrt{a}| = 4$ for $a \in \mathrm{QR}_n$.

- Let $a \in \mathrm{QR}_n$. Then $b^2 \equiv a \pmod{n}$ for some $b \in \mathbf{Z}_n^*$,
- Then $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$.
- Therefore, b is a square root of a modulo both p and q.
- Conversely, if $b_p \in \sqrt{a} \pmod{p}$ and $b_q \in \sqrt{a} \pmod{q}$, 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 by the Chinese remainder theorem that a has four distinct square roots mod n.
- Finally, since each $b \in \mathbf{Z}_n^*$ is the square root of exactly one element of QR_n, it must be that $|\mathrm{QR}_n| = \frac{1}{4}|\mathbf{Z}_n^*|$ as desired.

Testing for membership in QR_p

Theorem (Euler Criterion)

An integer a is a non-trivial[a] quadratic residue modulo a prime p iff

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

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

Proof in forward direction.

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. □

Proof of Euler Criterion

Proof in reverse direction.

Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Clearly $a \not\equiv 0 \pmod{p}$. We find a square root b of a modulo p.

□

Proof of Euler Criterion

Proof in reverse direction.

Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Clearly $a \not\equiv 0 \pmod{p}$. We find a square root b of a 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

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

□

Proof of Euler Criterion

Proof in reverse direction.

Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Clearly $a \not\equiv 0 \pmod{p}$. We find a square root b of a 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

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

Since g is a primitive root, $(p-1) | \ell$. Hence, $2|k$ and $k/2$ is an integer.

$\square$

Proof of Euler Criterion

Proof in reverse direction.

Suppose $a^{(p-1)/2} \equiv 1 \pmod p$. Clearly $a \not\equiv 0 \pmod p$. We find a square root b of a 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

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

Since g is a primitive root, $(p-1) \mid \ell$. Hence, $2|k$ 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 non-trivial square root of a modulo p, as desired. $\square$

Finding square roots modulo prime $p \equiv 3 \pmod 4$

The Euler criterion lets us test membership in QR_p for prime p, but it doesn't tell us how to find square roots. They are easily found in the special case when $p \equiv 3 \pmod 4$.

Theorem

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.

$p + 1$ is divisible by 4, so $(p + 1)/4$ is an integer. Then

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

by the Euler Criterion. □

Finding square roots for general primes

We now present an algorithm due to D. Shanks[1] that finds square roots of quadratic residues modulo any odd prime p.

It bears a strong resemblance to the algorithm presented in lecture 11 for factoring the RSA modulus given both the encryption and decryption exponents.

Let p be an odd prime. Write $\phi(p) = p - 1 = 2^s t$, where t is odd. (Recall: s is $\#$ trailing 0's in the binary expansion of $p - 1$.)

Because p is odd, $p - 1$ is even, so $s \geq 1$.

[1] 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.

A special case

In the special case when $s = 1$, then $p - 1 = 2t$, 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 $p \equiv 3 \pmod 4$.

This is exactly the case that we handled above.

Overall structure of Shank's algorithm

Let $p - 1 = 2^s t$ be as above, where p is an odd prime.

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 $x^2 \equiv a \pmod{p}$.

Shanks's algorithm

Let s, t satisfy $p - 1 = 2^s t$ and t odd.
Let $u \in \mathrm{QNR}_p$.
$k = s$
$z = u^t \bmod p$
$x = a^{(t+1)/2} \bmod p$
$b = a^t \bmod p$
while $(b \not\equiv 1 \pmod{p})$ $\{$
    let m be the least integer with $b^{2^m} \equiv 1 \pmod{p}$
    $t = z^{2^{k-m-1}} \bmod p$
    $z = t^2 \bmod p$
    $b = bz \bmod p$
    $x = xt \bmod p$
    $k = m$
$\}$
return x

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

Loop invariant

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 $a \pmod{p}$.

Termination proof

The algorithm terminates after at most s iterations of the loop.

To see why, we look at the orders[2] 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, $k = s$, 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 $\mathrm{ord}(z) \mid 2^s$. 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, $\mathrm{ord}(z) = 2^s$.

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

Termination proof (cont.)

Still on the first iteration, $b = a^t \pmod{p}$ and $k = s$.

Since a is a quadratic residue,

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

by the Euler Criterion. Hence, $\mathrm{ord}(b) \mid 2^{s-1}$.

It follows that $\mathrm{ord}(b) \leq 2^{s-1} < 2^s$.
Since $\mathrm{ord}(z) = 2^s$, we have $\mathrm{ord}(b) < \mathrm{ord}(z) = 2^s = 2^k$.

Termination proof (cont.)

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

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

Line 10 sets $z = t^2$, so $\text{ord}(z) = \text{ord}(t)/2 = 2^m$.

After line 11, $\text{ord}(b) < 2^m$. 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 $\text{ord}(b) < \text{ord}(z) = 2^k$ is maintained. Moreover, $\text{ord}(b)$ is reduced at each iteration, so the loop must terminate after at most s iterations. $\square$

Quadratic residues modulo $n = pq$

Let $n = pq$, p, q distinct odd primes.

We divide the numbers in $\mathbf{Z}_n^*$ into four classes depending on their membership in QR_p and QR_q.[3]

- Let $Q_n^{11} = \{a \in \mathbf{Z}_n^* \mid a \in \mathrm{QR}_p \cap \mathrm{QR}_q\}$.
- Let $Q_n^{10} = \{a \in \mathbf{Z}_n^* \mid a \in \mathrm{QR}_p \cap \mathrm{QNR}_q\}$.
- Let $Q_n^{01} = \{a \in \mathbf{Z}_n^* \mid a \in \mathrm{QNR}_p \cap \mathrm{QR}_q\}$.
- Let $Q_n^{00} = \{a \in \mathbf{Z}_n^* \mid a \in \mathrm{QNR}_p \cap \mathrm{QNR}_q\}$.

Under these definitions,

$$\mathrm{QR}_n = Q_n^{11}$$

$$\mathrm{QNR}_n = Q_n^{00} \cup Q_n^{01} \cup Q_n^{10}$$

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

Quadratic residuosity problem

Definition (Quadratic residuosity problem)

The *quadratic residuosity problem* is to decide, given $a \in Q_n^{00} \cup Q_n^{11}$, whether or not $a \in \mathrm{QR}_n$.

Fact

There is no known feasible algorithm for solving the quadratic residuosity problem that gives the correct answer significantly more than 1/2 the time for uniformly distributed random $a \in Q_n^{00} \cup Q_n^{11}$.

Goldwasser-Micali probabilistic cryptosystem

The Goldwasser-Micali cryptosystem is based on the assumed hardness of the quadratic residuosity problem.

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 $\mathcal{M} = \{0, 1\}$. (Single bits!)

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 $c = a \bmod n \in Q_n^{11}$.
If $m = 1$, then $c = ay \bmod n \in Q_n^{00}$.

Hence, the problem of finding m given c is equivalent to the problem of testing if $c \in \mathrm{QR}_n$, given that $c \in Q_n^{00} \cup Q_n^{11}$.

Decryption in Goldwasser-Micali encryption

Bob, knowing the private key p, can use the Euler Criterion to quickly determine whether or not $c \in \mathrm{QR}_p$ and hence whether $c \in Q_n^{11}$ or $c \in Q_n^{00}$, thereby determining m.

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 is just the quadratic residuosity problem, assuming the ciphertexts are uniformly distributed.

One can 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 $m = 1$. If the messages are also uniformly distributed, then any element of $Q_n^{00} \cup Q_n^{11}$ is equally likely to be the ciphertext.