6. Quadratic congruences.

A. Ushakov

MA503, October 12, 2022

Contents

Today we consider quadratic congruences

$$\mathrm{ax}^2 + \mathrm{bx} + \mathrm{c} \equiv_{\mathrm{n}} 0$$

and their applications in cryptography. We show that a congruence $ax^2 + bx + c \equiv_n 0$ can be reduced to a congruence $x^2 \equiv_n d$ and discuss two related algorithmic problems.

(Decision problem) For a given $x^2 \equiv_n d$ decide if it has a solution, or not.

(Search problem) For a given $x^2 \equiv_n d$ find its solutions.

Both problems can be solved efficiently (in polynomial time) if n is prime. Both problems do not have polynomial time solutions if n is not prime. Security of several cryptographic primitives relies on computational hardness of these problems.

- Finding all zeros of $x^2 \equiv_p a$.
- Quadratic congruence $x^2 \equiv_{pq} a$.
- Finding all zeros of $x^2 \equiv_{pq} a$.
- Remote coin flipping. Example. Security.
- General quadratic congruence.
- Quadratic residues.
- Quadratic residues modulo p and primitive roots.
- Euler's criterion.
- Legendre symbol.
- Quadratic reciprocity law.
- Quadratic residues modulo a prime p.
- Quadratic residues modulo a composite n.
- Goldwasser–Micali cryptosystem. Example.

Finding zeros of $x^2 \equiv_p a$

Consider a congruence $x^2 \equiv_p a$, where p and a are given, and x is unknown. E.g.,

- $x^2 \equiv_7 2$ has solutions ± 3, denoted $\sqrt{2}$ mod 7.
- $x^2 \equiv_{21} 16$ has solutions $\pm 4, \pm 10$, denoted $\sqrt{16}$ mod 21.

Suppose that p is prime and $a \in U_p$. We can solve $x^2 \equiv_p a$ depending on p.

$p \equiv_4 3$ *and* x *is a solution of* $x^2 \equiv_p a \quad \Rightarrow \quad x = \pm a^{(p+1)/4}$.

Indeed, $x^2 = \left(a^{(p+1)/4}\right)^2 = a^{(p+1)/2} \equiv_p (\alpha^2)^{(p+1)/2} \equiv_p \alpha^{p+1} \equiv_p \alpha^{p-1}\alpha^2 \equiv_p a$.

$p \equiv_8 5$ *and* x *is a solution of* $x^2 \equiv_p a \quad \Rightarrow \quad$ *either* $x \equiv_p \pm a^{\frac{p+3}{8}}$ *or* $x \equiv_p \pm a^{\frac{p+3}{8}} 2^{\frac{p-1}{4}}$.

$p \equiv_8 1 \quad \Rightarrow \quad$ x *can found using Tonelli (randomized) algorithm.*

Thus, there are efficient algorithms to compute $\sqrt{a}$ modulo any prime p.

(*We always assume that* a *is a unit modulo* n.)

Finding zeros of $x^2 \equiv_p a$: examples

Find $\sqrt{13}$ *modulo* 43.

Since $43 \equiv_4 3$,

- compute $\pm a^{(p+1)/4} = \pm 13^{11} \equiv_{43} \pm 23$.
- check that $x = \pm 23$ satisfy $x^2 \equiv_{43} 13$ (they do).

Find $\sqrt{28}$ *modulo* 37.

Since $37 \equiv_8 5$,

- Compute $x = \pm a^{\frac{p+3}{8}} = \pm 28^5 \equiv_{37} \pm 3$.
- Check that $x = \pm 3$ satisfy $x^2 \equiv_{37} 28$ (they do not).
- Compute $x = \pm a^{\frac{p+3}{8}} 2^{\frac{p-1}{4}} = \pm 28^5 2^9 \equiv_{37} \pm 19$.
- Check that $x = \pm 19$ satisfy $x^2 \equiv_{37} 28$ (they do).

Quadratic congruence $x^2 \equiv_{pq} a$

Proposition

p is an odd prime $\quad\Rightarrow\quad x^2 \equiv_p a$ has no solutions or two solutions $\pm s$.

- By Lagrange theorem $x^2 - a = 0$ has at most 2 zeros in the field $\mathbb{Z}_p$.
- Furthermore, if s is a solution, then $-s \not\equiv_p s$ is a solution too.

Proposition

p, q distinct odd primes $\quad\Rightarrow\quad x^2 \equiv_{pq} a$ has either 0 or 4 solutions.

$$x^2 \equiv_{pq} a \quad\Leftrightarrow\quad \begin{cases} x^2 \equiv_p a \\ x^2 \equiv_q a \end{cases}$$

- Assume that $x^2 \equiv_{pq} a$ has a solution.
- Then $x^2 \equiv_p a$ has two solutions $x \equiv_p \pm s$,
- and $x^2 \equiv_q a$ has two solutions $x \equiv_q \pm t$.

Finally, using Chinese remainder theorem to solve four systems

$$\begin{cases} x \equiv_p \pm s \\ x \equiv_q \pm t \end{cases}$$

we get four distinct solutions of the form $\{\alpha_1, -\alpha_1, \alpha_2, -\alpha_2\}$.

Finding all zeros of $x^2 \equiv_{pq} a$

Here we prove that the problem of finding all zeros of $x^2 \equiv_{pq} a$ is as hard as factorization of $n = pq$.

(If we can find all zeros, then we can find p, q)

$$\begin{array}{l} \textit{p, q are distinct odd primes} \\ \pm\alpha_1, \pm\alpha_2 \textit{ the solutions of } x^2 \equiv_{pq} a \end{array} \quad \Rightarrow \quad \gcd(n, \alpha_1 - \alpha_2) = p \textit{ or } q.$$

$$\begin{aligned} \alpha_1^2 \equiv_n a \text{ and } \alpha_2^2 \equiv_n a \quad &\Rightarrow \quad 0 \equiv_n \alpha_1^2 - \alpha_2^2 = (\alpha_1 - \alpha_2)(\alpha_1 + \alpha_2) \\ &\Rightarrow \quad n \mid (\alpha_1 - \alpha_2)(\alpha_1 + \alpha_2). \end{aligned}$$

But $\pm\alpha_1, \pm\alpha_2$ are **distinct modulo** n and, hence,

$$n \nmid \alpha_1 - \alpha_2 \quad \text{and} \quad n \nmid \alpha_1 + \alpha_2$$

Hence, one of the primes, say p, divides $\alpha_1 - \alpha_2$ and q divides $\alpha_1 + \alpha_2$. Therefore,

$$\gcd(n, \alpha_1 - \alpha_2) = p < n.$$

If we can find p, q, then we can find all zeros for $x^2 \equiv_{pq} a$.

Because we can solve the system

$$\begin{cases} x^2 \equiv_p a \\ x^2 \equiv_q a \end{cases}$$

Since factorization for numbers of the form pq is computationally hard, the problem to find all solutions of $x^2 \equiv_n a$ is hard.

Protocol for remote coin flipping

Consider a simple game of 2 people, Alice and Bob. Alice throws a fair coin and if

- the coin lands **heads up** then Alice wins;
- the coin lands **tails up** then Bob wins.

This game is easy to play if Alice and Bob are in the same place. But what if Alice is in US and Bob in is Europe and they use a phone line for communication? In such a setting they can use the following protocol.

- **Alice** chooses large distinct primes p and q satisfying $p \equiv_4 q \equiv_4 3$.
- **Alice** computes $n = pq$ and sends n to Bob.
- **Bob** chooses a random $1 \leq \alpha_1 \leq n-1$ such that $\gcd(\alpha_1, n) = 1$.
- **Bob** sends $a = \alpha_1^2 \ \% \ n$ to Alice.
- **Alice** finds all solutions of $x^2 \equiv_n a$ by solving modulo p and q

  $$\begin{cases} x^2 \equiv_p a \\ x^2 \equiv_q a \end{cases} \quad \Rightarrow \quad \begin{cases} x \equiv_p \pm a^{(p+1)/4}, \\ x \equiv_q \pm a^{(q+1)/4}. \end{cases}$$

  That gives four systems of linear congruences. Using CRT, Alice finds four solutions $\pm\alpha_1$, $\pm\alpha_2$ and sends a random solution $z \in \{\pm\alpha_1, \pm\alpha_2\}$ to Bob.
- **Bob** checks if $z = \pm\alpha_1$ and, if so, he announces Alice a winner. Otherwise Bob computes p and q (he can do that efficiently when $z \neq \pm\alpha_1$), announces himself a winner, and sends p, q to Alice as a proof.

Protocol for remote coin flipping: example

- **Alice** chooses $p = 43$ and $q = 71$, and send $n = 43 \cdot 71 = 3053$ to Bob.
- **Bob** chooses random $x = 192$ and sends $a = 192^2\%3053 = 228$ to Alice.
- **Alice** solves $x^2 \equiv_{43} 228 \equiv_{43} 13$ by computing the power

  $$13^{(p+1)/4} = 13^{11} \equiv_{43} 20.$$

  and gets ± 20. **Alice** solves $x^2 \equiv_{71} 228 \equiv_{43} 15$ by computing the power

  $$15^{(q+1)/4} = 15^{18} \equiv_{71} 21$$

  and get ± 21. Then she solves fours systems of linear congruences

  $$\begin{cases} x \equiv_{43} 20 \\ x \equiv_{71} 21 \end{cases} \quad \begin{cases} x \equiv_{43} -20 \\ x \equiv_{71} 21 \end{cases} \quad \begin{cases} x \equiv_{43} 20 \\ x \equiv_{71} -21 \end{cases} \quad \begin{cases} x \equiv_{43} -20 \\ x \equiv_{71} -21 \end{cases}$$

  Solving each subsystem she finds 4 solutions of $x^2 \equiv_{3053} 228$:

  $$x \equiv_{3053} 192,\ 2861,\ 1399,\ 1654.$$

  Note that $-192 \equiv_{3053} 2861$ and $-1399 \equiv_{3053} 1654$. Assume that Alice chooses $z = 1399$ and sends it to Bob.
- Bob compares Alice's choice 1399 with his original number $1399 \equiv \pm 192$? and since comparison fails he announces himself a winner. To prove that he is indeed a winner he computes $\gcd(3053, 1399 - 192) = \gcd(3053, 1207) = 71$ and sends 71 and $3053/71 = 43$ to Alice.

Protocol for remote coin flipping: security

If Bob announces himself a winner, he has to prove that by showing prime factors of n.

- It does not give Bob any new information if he receives $z = \pm\alpha_1$ (recall that he generated α_1 himself). In that case Bob has to factor n, which is computationally hard.
- If $z \neq \pm\alpha_1$, then $z = \pm\alpha_2$. In that case Bob has all four solutions $\{\pm\alpha_1, \pm\alpha_2\}$ and can compute prime factors of n by computing $\gcd(\alpha_1 \pm \alpha_2, n)$.

Theorem

Dishonest Bob can not cheat (efficiently) in the coin flipping protocol unless he can (efficiently) solve the integer factorization problem for n.

General quadratic congruence

A **quadratic congruence** *is an expression of the form* $ax^2 + bx + c \equiv_p 0$.

(Quadratic formula, $p \neq 2$ and $a \not\equiv_p 0$)

If x is a solution of $ax^2 + bx + c \equiv_p 0$, then $x = \frac{1}{2a}\left(-b + \sqrt{b^2 - 4ac}\right)$.

$$\begin{aligned} ax^2 + bx + c \equiv_p 0 \quad &\Leftrightarrow \quad x^2 + \tfrac{b}{a}x + \tfrac{c}{a} \equiv_p 0 \\ &\Leftrightarrow \quad \left(x + \tfrac{b}{2a}\right)^2 + \tfrac{c}{a} - \tfrac{b^2}{4a^2} \equiv_p 0 \\ &\Leftrightarrow \quad \left(x + \tfrac{b}{2a}\right)^2 \equiv_p \tfrac{b^2}{4a^2} - \tfrac{c}{a}. \end{aligned}$$

Hence, to solve a quadratic congruence, we can solve a congruence $y^2 \equiv_n d$, where $d = \frac{b^2}{4a^2} - \frac{c}{a}$ for y and then subtract $\frac{b}{2a}$, i.e., compute

$$\sqrt{\tfrac{b^2}{4a^2} - \tfrac{c}{a}} - \tfrac{b}{2a} = \tfrac{1}{2a}\left(\sqrt{b^2 - 4ac} - b\right).$$

(It is important that we can divide by 2 and by a modulo p in computations above.)

Quadratic residues

Definition

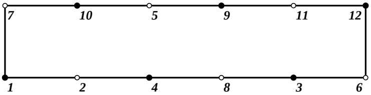
A unit $a \in \mathbb{Z}$ modulo $n \in \mathbb{N}$ is called a **quadratic residue** of n if $x^2 \equiv_n a$ has a solution. Otherwise, it is called a **quadratic nonresidue** of n.

$$\mathrm{Q_n} = \left\{ \mathrm{a} \in \mathrm{U_n} \;\middle|\; \mathrm{x}^2 \equiv_\mathrm{n} \mathrm{a} \text{ has a solution} \right\} \text{ – the set of all residues of } n.$$

For instance, to find all quadratic residues of 13 we compute squares of units $1, \ldots, 6$:

$$\begin{array}{lcll}
1^2 \equiv_{13} 1 & \Rightarrow & \sqrt{1} = 1 \text{ or } 12 & \text{mod } 13 \\
2^2 \equiv_{13} 4 & \Rightarrow & \sqrt{4} = 2 \text{ or } 11 & \text{mod } 13 \\
3^2 \equiv_{13} 9 & \Rightarrow & \sqrt{9} = 3 \text{ or } 10 & \text{mod } 13 \\
4^2 \equiv_{13} 3 & \Rightarrow & \sqrt{3} = 4 \text{ or } 9 & \text{mod } 13 \\
5^2 \equiv_{13} 12 & \Rightarrow & \sqrt{12} = 5 \text{ or } 8 & \text{mod } 13 \\
6^2 \equiv_{13} 10 & \Rightarrow & \sqrt{10} = 6 \text{ or } 7 & \text{mod } 13
\end{array}$$

We do not need to compute squares of $7, \ldots, 12$, they are the same. Therefore $1, 3, 4, 9, 10, 12$ are quadratic residues of 13.



$r = 2$ is a primitive root of 13. Consider the graph of powers of 2. The quadratic residues of 13 have black dots and nonresidues have white dots.

Observe that **every second power of r is a residue**. This is true for every odd prime p.

Quadratic residues modulo p and primitive roots

Lemma

Let p be an odd prime. Let r be a primitive root of p and $a \equiv_p r^k$.
Then a is a quadratic residue of p $\Leftrightarrow$ k is even.

$$\begin{aligned} a \text{ is a quadratic residue} \quad &\Leftrightarrow \quad x^2 \equiv_p a \text{ is satisfied for some } x = r^i \\ &\Leftrightarrow \quad r^{2i} \equiv_p r^k \\ &\Leftrightarrow \quad 2i \equiv_{p-1} k \\ &\Leftrightarrow \quad \gcd(2, p-1) = 2 \text{ divides } k \\ &\Leftrightarrow \quad k \text{ is even.} \end{aligned}$$

± 1 are the only solutions of $x^2 \equiv_p 1$.

(a) $a \equiv_p r^k \quad \Rightarrow \quad a^{(p-1)/2} \equiv_p \pm 1;$

(b) $a \equiv_p r^k$ *and k is even* $\quad \Rightarrow \quad a^{(p-1)/2} \equiv_p 1;$

(c) $a \equiv_p r^k$ *and k is odd* $\quad \Rightarrow \quad a^{(p-1)/2} \equiv_p -1.$

(a) $(a^{(p-1)/2})^2 = a^{p-1} \equiv_p 1$ and, hence, $a^{(p-1)/2}$ is a solution of $x^2 \equiv_p 1$.

(b) $k = 2j \quad \Rightarrow \quad a^{(p-1)/2} \equiv_p (r^{2j})^{(p-1)/2} \equiv_p r^{j(p-1)} \equiv_p (r^{p-1})^j \equiv_p 1^j = 1.$

(c) $k = 2j+1 \quad \Rightarrow \quad a^{(p-1)/2} \equiv_p (r^{2j+1})^{(p-1)/2} \equiv_p r^{j(p-1)+(p-1)/2} \equiv_p r^{(p-1)/2} \equiv_p -1.$

Quadratic residues modulo p: Euler's criterion

The next theorem gives an easy way to check if a is a quadratic residue of p.

Theorem (Euler's criterion)

Let p be an odd prime and $\gcd(p, a) = 1$. *Then*

(EC1) $a \in Q_p \quad \Leftrightarrow \quad a^{(p-1)/2} \equiv_p 1.$

(EC2) $a \notin Q_p \quad \Leftrightarrow \quad a^{(p-1)/2} \equiv_p -1.$

Example. Use Euler's criterion to check if 2 *is a quadratic residue modulo* 7.

2 is a quadratic residue modulo 7, because $2^{\frac{7-1}{2}} \equiv_7 1$.

Example. Use Euler's criterion to check if 3 *is a quadratic residue modulo* 17.

3 is a quadratic nonresidue modulo 17, because $3^{\frac{17-1}{2}} \equiv_{17} -1$.

Legendre symbol

Definition

Let p be an odd prime and $a \in \mathbb{Z}$. The **Legendre symbol (a/p)** is defined by

$$(a/p) = \begin{cases} 0 & \text{if } a \text{ is not a unit modulo } p; \\ 1 & \text{if } a \text{ is a quadratic residue of } p; \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Legendre symbol is just a piece of notation. It is introduced for convenience!

(Easy properties of the Legendre symbol)

(1) $(1/p) = 1.$

(2) $(a^2/p) = 1.$

(3) $(a/p) = a^{(p-1)/2}.$

(4) $(ab/p) = (a/p)(b/p).$

(5) $(-1/p) = -1^{(p-1)/2} = \begin{cases} \mathit{1} & \textit{if } p \equiv_4 1; \\ \textit{-1} & \textit{if } p \equiv_4 3. \end{cases}$

Proposition

- $(Q_n, \cdot)$ *is a group.*
- $a \mapsto (a/p)$ *is a homomorphism from* U_p *to* $(\{-1, 1\}, \cdot)$.

Quadratic reciprocity law - 1

Theorem (Quadratic reciprocity law)

Let p and q be distinct odd primes. Then

$$(p/q) = \begin{cases} (q/p) & \textit{if } p \equiv_4 1 \textit{ or } q \equiv_4 1; \\ -(q/p) & \textit{if } p \equiv_4 3 \textit{ and } q \equiv_4 3. \end{cases}$$

Observe that the theorem does not cover the symbol $(2, q)$.

Example. Compute $(29/53)$.

$(29/53) = (53/29) = (24/29) = (6/29) = (2/29)(3/29) = -1 \cdot (29/3) = -(2/3) = 1.$

Example. Compute $(-46/17)$.

$(-46/17) = (-63/17) = (9/17)(-7/17) = (10/17) = (2/17)(5/17) = 1 \cdot (17/5) = (2/5) = -1.$

Quadratic reciprocity law - 2

The next statement claims that $2 \in Q_p$ if and only if $p \equiv_8 1$ or $p \equiv_8 7$.

Theorem (Square roots of 2 modulo p)

Let p be an odd prime, then

$$(2/p) = \begin{cases} 1 & \textit{if } p \equiv_8 1 \textit{ or } p \equiv_8 7, \\ -1 & \textit{if } p \equiv_8 3 \textit{ or } p \equiv_8 5. \end{cases}$$

Example. Use quadratic reciprocity law to decide if 2 *is a quadratic residue modulo* 17.

$17 \equiv_8 1 \quad \Rightarrow \quad (2/17) = 1 \quad \Rightarrow$ 2 is a quadratic residue modulo 17.

Example. Use quadratic reciprocity law to decide if 2 *is a quadratic residue modulo* 43.

$43 \equiv_8 3 \quad \Rightarrow \quad (2/43) = -1 \quad \Rightarrow$ 2 is not a quadratic residue modulo 43.

Quadratic residues modulo prime powers

Theorem

$a \in Q_{p^s} \quad \Leftrightarrow \quad a \in Q_p$ *for an odd prime* p.

Theorem

Let a be an odd integer. The following holds.

- *a is a quadratic residue modulo* 2.
- *a is a quadratic residue modulo* $4 \quad \Leftrightarrow \quad a \equiv_4 1$.
- *a is a quadratic residue modulo* $2^s \quad \Leftrightarrow \quad a \equiv_8 1$. □

Quadratic residues modulo general composite numbers

Let $n = p_1^{a_1} \dots p_m^{a_m}$ and $a \in U_n$.

Theorem

a is a quadratic residue of n $\Leftrightarrow$ a is a quadratic residue of $p_i^{a_i}$ for each $1 \le i \le m$.

Example. *Decide if $a = 6$ is a quadratic residue of 65.*

$$x^2 \equiv_{65} 6 \;\Leftrightarrow\; \begin{cases} x^2 \equiv_5 6 & \text{has a solution because } (6/5) = (1/5) = 1 \\ x^2 \equiv_{13} 6 & \text{has no solutions because } (6/13) = (2/13)(3/13) = -1(13/3) = -(1/3) = -1. \end{cases}$$

Hence, $a = 6$ is not a quadratic residue of $n = 65$.

Example. *Decide if $a = 108$ is a quadratic residue of 143.*

$$x^2 \equiv_{143} 108 \;\Leftrightarrow\; \begin{cases} x^2 \equiv_{11} 108 & \text{has a solution because } (108/11) = (9/11) = 1 \\ x^2 \equiv_{13} 108 & \text{has a solution because } (108/13) = (4/13) = 1. \end{cases}$$

Hence, $a = 108$ is a quadratic residue of $n = 143 = 11 \cdot 13$.

Example. *Decide if $a = 106$ is a quadratic residue of 143.*

$$x^2 \equiv_{143} 106 \;\Leftrightarrow\; \begin{cases} x^2 \equiv_{11} 106 & \text{has no solutions because } (106/11) = (7/11) = -(11/7) = -(4/7) = -1 \\ x^2 \equiv_{13} 106 & \text{has no solutions because } (106/13) = (2/13) = -1. \end{cases}$$

Hence, $a = 106$ is not a quadratic residue of $n = 143$.

In general, the problem to decide if a is a quadratic residue of a composite n is **computationally hard***!*

It is easy only if we know prime factorization of n.

Goldwasser–Micali cryptosystem

Goal: Bob wants to encrypt and send Alice one bit m (called ***plaintext****).*

Key generation (performed by Alice):

- Choose randomly two distinct prime numbers p and q.
- Compute $n = pq$ called **public modulus**.
- Choose a random integer a such that $(a/p) = (a/q) = -1$.

Finally, Alice publishes the numbers n and a, together called **Alice's public key**.

Encryption (performed by Bob):

- Choose a random $1 < r < n$ and use (n, a) to compute

$$c = \begin{cases} r^2 \,\%n & \text{if } m = 0, \\ ar^2 \,\%n & \text{if } m = 1. \end{cases}$$

The number c (called **ciphertext**) is then sent to Alice.

Decryption (performed by Alice):

- Alice computes (c/p) and $m = \begin{cases} 0 & \text{if } (c/p) = 1, \\ 1 & \text{if } (c/p) = -1. \end{cases}$

By design, $m = 0 \quad \Leftrightarrow \quad (c/p) = 1$. Hence, Alice recovers the original value of m.

Goldwasser–Micali cryptosystem

Goal: Bob wants to encrypt and send Alice one bit m (called ***plaintext****).*

Key generation (performed by Alice):

- Choose randomly two distinct prime numbers p and q.
- Compute $n = pq$ called **public modulus**.
- Choose a random integer a such that $(a/p) = (a/q) = -1$.

Finally, Alice publishes the numbers n and a, together called **Alice's public key**.

Encryption (performed by Bob):

- Choose a random $1 < r < n$ and use (n, a) to compute

$$c = \begin{cases} r^2 \,\%n & \text{if } m = 0, \\ ar^2 \,\%n & \text{if } m = 1. \end{cases}$$

The number c (called **ciphertext**) is then sent to Alice.

Decryption (performed by Alice):

- Alice computes (c/p) and $m = \begin{cases} 0 & \text{if } (c/p) = 1, \\ 1 & \text{if } (c/p) = -1. \end{cases}$

By design, $m = 0 \quad \Leftrightarrow \quad (c/p) = 1$. Hence, Alice recovers the original value of m.

Goldwasser–Micali cryptosystem

Goal: Bob wants to encrypt and send Alice one bit m (called ***plaintext****).*

Key generation (performed by Alice):

- Choose randomly two distinct prime numbers p and q.
- Compute $n = pq$ called **public modulus**.
- Choose a random integer a such that $(a/p) = (a/q) = -1$.

Finally, Alice publishes the numbers n and a, together called **Alice's public key**.

Encryption (performed by Bob):

- Choose a random $1 < r < n$ and use (n, a) to compute

$$c = \begin{cases} r^2 \,\%n & \text{if } m = 0, \\ ar^2 \,\%n & \text{if } m = 1. \end{cases}$$

The number c (called **ciphertext**) is then sent to Alice.

Decryption (performed by Alice):

- Alice computes (c/p) and $m = \begin{cases} 0 & \text{if } (c/p) = 1, \\ 1 & \text{if } (c/p) = -1. \end{cases}$

By design, $m = 0 \iff (c/p) = 1$. Hence, Alice recovers the original value of m.

Goldwasser–Micali cryptosystem

Goal: Bob wants to encrypt and send Alice one bit m (called ***plaintext****).*

Key generation (performed by Alice):

- Choose randomly two distinct prime numbers p and q.
- Compute $n = pq$ called **public modulus**.
- Choose a random integer a such that $(a/p) = (a/q) = -1$.

Finally, Alice publishes the numbers n and a, together called **Alice's public key**.

Encryption (performed by Bob):

- Choose a random $1 < r < n$ and use (n, a) to compute

$$c = \begin{cases} r^2 \,\%n & \text{if } m = 0, \\ ar^2 \,\%n & \text{if } m = 1. \end{cases}$$

The number c (called **ciphertext**) is then sent to Alice.

Decryption (performed by Alice):

- Alice computes (c/p) and $m = \begin{cases} 0 & \text{if } (c/p) = 1, \\ 1 & \text{if } (c/p) = -1. \end{cases}$

By design, $m = 0 \quad \Leftrightarrow \quad (c/p) = 1$. Hence, Alice recovers the original value of m.

Goldwasser–Micali cryptosystem (worked out example)

Key generation

- Choose random primes $p = 7$, $q = 13$.
- We can choose $a = 5$ because $(5/7) = (5/13) = -1$.

Encryption: To encrypt $m = 1$ Bob

- picks a random $r = 11$
- sends $5 \cdot 11^2 \equiv_{91} 59 = c$ to Alice.

Decryption: To decrypt the message Alice computes $(59/7) = (5/7) = (7/5) = (2/5) = -1$ and, hence, $m = 1$.

Goldwasser–Micali cryptosystem is an example of a **probabilistic encryption** *because the same message m has many different ciphers (defined by the choice of r).*

E.g., in the example above, Bob could generate $r = 2$ in which case he'd get the cipher $c = 20$.

Goldwasser–Micali cryptosystem: basic security

By design, a passive eavesdropper obtains two public values: n and c. Furthermore,

$$\begin{aligned} m = 0 \quad &\Leftrightarrow \quad x^2 \equiv_n c \text{ has a solution} \\ &\Leftrightarrow \quad c \text{ is a quadratic residue modulo } n = pq. \end{aligned}$$

Hence, security of the Goldwasser–Micali cryptosystem relies on computational hardness of the problem to decide if a is a quadratic residue of n, or not.

Goldwasser–Micali cryptosystem: message expansion

The Goldwasser–Micali public key cryptosystem is not practical, because each bit of the plaintext is encrypted with a number modulo N. For it to be secure, it is necessary that Eve be unable to factor the number $N = pq$, so in practice N should be (at least) a 1000-bit number. Thus, if Alice wants to send k bits of plaintext to Bob, her ciphertext will be $1000k$ bits long. Thus the Goldwasswer–Micali public key cryptosystem has a **message expansion** ratio of 1000, since the ciphertext is 1000 times as long as the plaintext. In general, the Goldwasswer–Micali public key cryptosystem expands a message by a factor of $log_2(N)$. There are other probabilistic public key cryptosystems whose message expansion is much smaller.