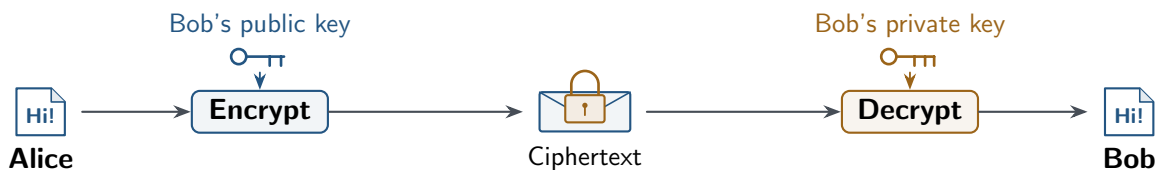


Lecture 13: Modular Arithmetic and RSA

Lecturer and scribe: Karthik Gajulapalli



Public-key encryption: anyone can encrypt for Bob; only Bob can decrypt.

1 Operations Modulo N

Fix an integer $N \geq 2$. We say that two integers A and B are **equal modulo N** , and write

$$A \equiv B \pmod{N} \iff N \mid (A - B).$$

This is also written $A = B \pmod{N}$. It means that A and B differ by an integer multiple of N , or equivalently that they have the same remainder when divided by N .

The expression $A \bmod N$ denotes the unique integer r such that

$$A = qN + r \quad \text{for some } q \in \mathbb{Z}, \quad 0 \leq r < N.$$

The remainder is always nonnegative, even when A is negative.

1.1 Examples with Modulus Five

Remainder	Explanation
$-2 \bmod 5 = 3$	$-2 = (-1) \cdot 5 + 3$
$18 \bmod 5 = 3$	$18 = 3 \cdot 5 + 3$
$10 \bmod 5 = 0$	$10 = 2 \cdot 5 + 0$
$-14 \bmod 5 = 1$	$-14 = (-3) \cdot 5 + 1$

For instance, $-2 \equiv 18 \pmod{5}$, because their difference is -20 , a multiple of 5. Both have remainder 3.

1.2 The Set of Residues

We work with the set

$$\mathbb{Z}_N = \{0, 1, \dots, N-1\}.$$

For example, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Addition and multiplication in $\mathbb{Z}_N$ mean the ordinary integer operation followed by reduction:

$$3 + 4 \equiv 2 \pmod{5}, \quad 3 \cdot 4 \equiv 2 \pmod{5}.$$

We now show that reducing before an operation gives the same result as reducing afterward.

2 Adding and Multiplying Modulo N

If we only want the answer modulo N , **we do not need to compute the full integer result first**. We can reduce the inputs, add or multiply their remainders, and reduce again after every step. The following identities justify this shortcut.

2.1 Addition

For all integers a, b ,

$$(a + b) \bmod N = ((a \bmod N) + (b \bmod N)) \bmod N.$$

Proof. Write $a = qN + r$ and $b = sN + t$, where $0 \leq r, t < N$. Then $r = a \bmod N$, $t = b \bmod N$, and

$$a + b = (q + s)N + (r + t).$$

The integers $a + b$ and $r + t$ differ by a multiple of N , so they have the same remainder modulo N . $\square$

For example, with $N = 5$, reduce the inputs before adding:

$$(18 + (-14)) \bmod 5 = (3 + 1) \bmod 5 = 4.$$

The final reduction is necessary: $4 + 4 = 8$, but $(4 + 4) \bmod 5 = 3$.

2.2 Multiplication

For all integers a, b ,

$$ab \bmod N = ((a \bmod N)(b \bmod N)) \bmod N.$$

Proof. With the same notation $a = qN + r$ and $b = sN + t$,

$$ab = (qN + r)(sN + t) = (qsN + qt + sr)N + rt.$$

Thus ab and rt differ by a multiple of N , so their remainders are equal. $\square$

For example, reduce the factors before multiplying:

$$(18 \cdot (-14)) \bmod 5 = (3 \cdot 1) \bmod 5 = 3.$$

We only multiply the small remainders 3 and 1; computing the original product is unnecessary.

These identities also say that if $a \equiv a' \pmod{N}$ and $b \equiv b' \pmod{N}$, then

$$a + b \equiv a' + b' \pmod{N}, \quad ab \equiv a'b' \pmod{N}.$$

These identities apply repeatedly: in any expression built from additions and multiplications, **we can work entirely with remainders, reducing after every operation**. The final remainder is unchanged.

3 Two Algorithms We Already Know

3.1 We Can Do Fast Exponentiation

The multiplication identity lets us use the fast-exponentiation algorithm from Lecture 7 to compute $a^k \bmod N$. Reduce the base first, and reduce after every multiplication and squaring. Each reduction preserves the final answer.

For example, to compute $18^{13} \bmod 5$, first replace 18 by 3. Repeated squaring gives

$$3^2 \equiv 4, \quad 3^4 \equiv 4^2 \equiv 1, \quad 3^8 \equiv 1 \pmod{5}.$$

Since $13 = 8 + 4 + 1$,

$$18^{13} \equiv 3^{13} = 3^8 \cdot 3^4 \cdot 3 \equiv 1 \cdot 1 \cdot 3 \equiv 3 \pmod{5}.$$

For a positive exponent k , the algorithm uses $O(\log(k+1))$ modular multiplications. The stored residues are always less than N , and a temporary product of two residues is less than N^2 . We do not have to construct the full integer a^k .

3.2 We Can Compute GCDs

The remainder operation also drives Euclid's algorithm from Lecture 12. If $a = qN + r$, then

$$\gcd(a, N) = \gcd(N, r), \quad r = a \bmod N.$$

To see why, a common divisor of a, N divides $a - qN = r$. Conversely, a common divisor of N, r divides $qN + r = a$. The pairs therefore have exactly the same common divisors.

For example,

$$\begin{aligned} \gcd(18, 5) &= \gcd(5, 3) \\ &= \gcd(3, 2) \\ &= \gcd(2, 1) = 1. \end{aligned}$$

Repeated division computes the gcd efficiently. Recall **Bézout's identity from Lecture 12**: extended Euclid gives integers u, v satisfying

$$au + Nv = \gcd(a, N).$$

We will use this identity to determine exactly which residues have multiplicative inverses.

The two tools we will use. Fast exponentiation computes powers modulo N . Euclid computes $\gcd(a, N)$, and extended Euclid supplies coefficients in a Bézout identity.

4 Multiplicative Inverses

What plays the role of $1/a$ in modular arithmetic? Modulo 5, we have $2 \cdot 3 \equiv 1$. Thus multiplying by 3 undoes multiplication by 2.

Definition. For $a \in \mathbb{Z}_N$, a **multiplicative inverse** of a is an element $b \in \mathbb{Z}_N$ satisfying

$$ab \equiv 1 \pmod{N}.$$

When an inverse exists, we denote it by a^{-1} . This is an inverse modulo N , not an ordinary rational reciprocal.

4.1 Every Element Modulo Five

$a \in \mathbb{Z}_5$	Inverse	Verification or reason
0	None	$0b \equiv 0$ for every b
1	1	$1 \cdot 1 \equiv 1 \pmod{5}$
2	3	$2 \cdot 3 = 6 \equiv 1 \pmod{5}$
3	2	$3 \cdot 2 = 6 \equiv 1 \pmod{5}$
4	4	$4 \cdot 4 = 16 \equiv 1 \pmod{5}$

Every nonzero element has an inverse. Does this happen for every modulus?

4.2 Every Element Modulo Ten

$a \in \mathbb{Z}_{10}$	Inverse	Verification or reason
0	None	Every product is 0 modulo 10
1	1	$1 \cdot 1 \equiv 1 \pmod{10}$
2	None	Every product is even
3	7	$3 \cdot 7 = 21 \equiv 1 \pmod{10}$
4	None	Every product is even
5	None	Every product is 0 or 5 modulo 10
6	None	Every product is even
7	3	$7 \cdot 3 = 21 \equiv 1 \pmod{10}$
8	None	Every product is even
9	9	$9 \cdot 9 = 81 \equiv 1 \pmod{10}$

An even integer cannot be congruent to 1 modulo 10: subtracting any multiple of 10 preserves parity. Thus the even entries really have no inverse, and 5 fails for the separate reason shown above.

5 Which Elements Have Inverses?

Define the set of invertible residues by

$$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : a \text{ has a multiplicative inverse modulo } N\}.$$

These elements are also called **units**. Our examples give

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}, \quad \mathbb{Z}_{10}^* = \{1, 3, 7, 9\}.$$

The star selects elements that have inverses. For a composite modulus, being nonzero is not enough.

Claim 1 (The inverse criterion). *For $a \in \mathbb{Z}_N$, a^{-1} exists exactly when $\gcd(a, N) = 1$.*

Proof. If an inverse exists, the gcd is 1. Suppose $ab \equiv 1 \pmod{N}$. Then $ab - 1 = kN$ for some integer k , so

$$ab - kN = 1.$$

Every common divisor of a and N therefore divides 1. It follows that $\gcd(a, N) = 1$.

If the gcd is 1, an inverse exists. By Bézout's identity from Lecture 12, there are integers u, v such that

$$au + Nv = 1.$$

Reducing modulo N gives $au \equiv 1 \pmod{N}$. Therefore $b = u \bmod N$ is an inverse of a in $\mathbb{Z}_N$. $\square$

Consequently, we can describe the same set as

$$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}.$$

This proof gives an algorithm: run extended Euclid on (a, N) . If the gcd is 1, reduce the coefficient of a modulo N . For example,

$$1 = 3 \cdot 7 - 2 \cdot 10 \implies 7^{-1} \equiv 3 \pmod{10}.$$

5.1 Uniqueness and Cancellation

If b and c are both inverses of a , then

$$b \equiv b(ac) \equiv (ba)c \equiv c \pmod{N}.$$

Because $b, c \in \mathbb{Z}_N$, they are equal. So the inverse is unique as an element of $\mathbb{Z}_N$.

If $ax \equiv ay \pmod{N}$ and $a \in \mathbb{Z}_N^*$, multiplication by a^{-1} gives $x \equiv y \pmod{N}$. We will use this cancellation rule below. Without an inverse, cancellation may fail: modulo 10, $2 \cdot 1 \equiv 2 \cdot 6$, although $1 \not\equiv 6$.

6 Question 1: How Many Elements Are Invertible?

Definition: Euler's totient function. The number of invertible residues modulo N is

$$\varphi(N) = |\mathbb{Z}_N^*| = |\{a \in \{0, \dots, N-1\} : \gcd(a, N) = 1\}|.$$

Thus $\varphi(N)$ counts residues coprime to N . In particular, $\varphi(5) = 4$ and $\varphi(10) = 4$.

6.1 When the Modulus Is Prime

Claim 2. If p is prime, then $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ and $\varphi(p) = p-1$.

Proof. The only positive divisors of p are 1 and p . If $1 \leq a \leq p-1$, then $p \nmid a$, so $\gcd(a, p) = 1$. All $p-1$ nonzero residues therefore have inverses. The residue 0 does not: $\gcd(0, p) = p > 1$. $\square$

6.2 A Product of Two Distinct Primes

Let p, q be *distinct* primes and $N = pq$. A residue has a common divisor greater than 1 with N exactly when it is divisible by p or q . Among $0, 1, \dots, pq-1$,

- there are q multiples of p : $0, p, 2p, \dots, (q-1)p$;
- there are p multiples of q : $0, q, 2q, \dots, (p-1)q$;
- only 0 is in both lists, since a multiple of both distinct primes is a multiple of pq .

Subtract the two lists from all pq residues, then add back the single residue counted twice. This proves

$$|\mathbb{Z}_{pq}^*| = \varphi(pq) = pq - q - p + 1 = (p-1)(q-1).$$

For example, $10 = 2 \cdot 5$ gives $\varphi(10) = (2-1)(5-1) = 4$.

Extra: The General Formula

If $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of N , with distinct primes p_i and positive exponents α_i , then

$$\varphi(N) = N \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1).$$

We state this formula as an extra; the two-prime case is all we need for RSA. For instance, $\varphi(12) = 12(1 - 1/2)(1 - 1/3) = 4$.

7 Multiplication Permutes the Invertible Elements

7.1 Observation 1: Closure Under Multiplication

If $a, b \in \mathbb{Z}_N^*$, then $(ab) \bmod N \in \mathbb{Z}_N^*$. Indeed, if a^{-1} and b^{-1} are their inverses, then

$$(ab)(a^{-1}b^{-1}) \equiv (aa^{-1})(bb^{-1}) \equiv 1 \pmod{N}.$$

Thus a product of invertible elements is invertible. The element 1 is invertible, and the inverse of an invertible element is itself invertible. Together with associativity of modular multiplication, these facts say that $\mathbb{Z}_N^*$ is a **multiplicative group**. We will use the concrete inverse and closure properties just proved.

7.2 Multiplying the Entire Set by One Element

Fix $x \in \mathbb{Z}_N^*$. We claim that

$$\boxed{x\mathbb{Z}_N^* = \mathbb{Z}_N^*}, \quad x\mathbb{Z}_N^* := \{(xu) \bmod N : u \in \mathbb{Z}_N^*\}.$$

For $x = 7$ and $N = 10$, the calculation is

u	1	3	7	9
$7u \bmod 10$	7	1	9	3

Thus $7\mathbb{Z}_{10}^* = \{7, 1, 9, 3\} = \{1, 3, 7, 9\} = \mathbb{Z}_{10}^*$. The same elements appear in a different order.

7.3 Why the Map Is a Bijection

Consider

$$f_x : \mathbb{Z}_N^* \longrightarrow \mathbb{Z}_N^*, \quad f_x(u) = (xu) \bmod N.$$

Closure proves that every output lies in the claimed codomain.

One-to-one. Suppose $f_x(u) = f_x(v)$. Then $xu \equiv xv \pmod{N}$. Multiplying by x^{-1} gives $u \equiv v \pmod{N}$. Since $u, v \in \mathbb{Z}_N^*$, this means $u = v$.

Onto. Given $w \in \mathbb{Z}_N^*$, take $u = (x^{-1}w) \bmod N$. Closure gives $u \in \mathbb{Z}_N^*$, and $f_x(u) = w$, since $x(x^{-1}w) \equiv w \pmod{N}$.

Comment. Closure and the one-to-one proof already imply that f_x is onto: closure makes f_x a map from the *finite* set $\mathbb{Z}_N^*$ to itself, and an injective map from a finite set to itself is automatically surjective. Thus the direct construction above is an alternative way to see surjectivity.

Therefore f_x is a bijection, with inverse $f_{x^{-1}}$. Multiplication by x permutes the invertible residues. The assumption $x \in \mathbb{Z}_N^*$ is essential to this argument.

8 Euler's Theorem and Fermat's Little Theorem

Claim 3 (Euler's theorem). *If $\gcd(x, N) = 1$, then*

$$x^{\varphi(N)} \equiv 1 \pmod{N}.$$

Proof. List the invertible residues as $u_1, \dots, u_r$, where $r = \varphi(N)$. By the bijection just proved, multiplying by x permutes this list modulo N . Hence the product of the entries is unchanged modulo N :

$$(xu_1)(xu_2) \cdots (xu_r) \equiv u_1 u_2 \cdots u_r \pmod{N}.$$

Let $P = u_1 u_2 \cdots u_r$. Collecting the r copies of x gives

$$x^r P \equiv P \pmod{N}.$$

Every factor in P is invertible, so closure tells us that $P \bmod N$ is invertible. Multiplying both sides by its inverse cancels P and gives $x^r \equiv 1 \pmod{N}$. $\square$

The coprimality hypothesis is what puts x in $\mathbb{Z}_N^*$ and makes the permutation argument work.

8.1 The Special Case of a Prime Modulus

If p is prime, then $\varphi(p) = p - 1$. Euler's theorem therefore gives **Fermat's little theorem**:

$$\boxed{p \nmid x \implies x^{p-1} \equiv 1 \pmod{p}.$$

For example, $2^4 = 16 \equiv 1 \pmod{5}$. An equivalent version is $x^p \equiv x \pmod{p}$ for every integer x : multiply the displayed congruence by x when $p \nmid x$; when $p \mid x$, both sides are zero modulo p .

8.2 Testing Euler's Theorem on $\mathbb{Z}_{10}^*$

We found $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ and $\varphi(10) = 4$. Euler's theorem predicts that the fourth power of every element is 1 modulo 10:

x	1	3	7	9
x^4	1	81	2401	6561
$x^4 \bmod 10$	1	1	1	1

In particular, the earlier permutation by 7 leads to $7^4 \equiv 1 \pmod{10}$. The modulus 10 is composite, so this is an application of Euler's theorem. For comparison, $2 \notin \mathbb{Z}_{10}^*$ and $2^4 \equiv 6 \pmod{10}$, not 1.

9 RSA for Coprime Messages

RSA is a public-key construction: a receiver publishes an encryption key and retains a private decryption key. Both operations are modular exponentiation. In this lecture, we make the explicit promise

$$m \in \mathbb{Z}_N^*, \quad \text{equivalently } 0 \leq m < N \text{ and } \gcd(m, N) = 1.$$

The sender can check this promise using Euclid's algorithm.

9.1 Key Generation

1. Choose distinct odd primes p, q and compute $N = pq$.
2. Compute $\varphi(N) = (p - 1)(q - 1)$.
3. Choose an integer e with $1 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$.
4. Use extended Euclid to find $d = e^{-1} \bmod \varphi(N)$, with $1 \leq d < \varphi(N)$. Thus $ed = 1 + k\varphi(N)$ for an integer $k \geq 1$.
5. Publish (N, e) . Keep d and the factors p, q private.

The exponent e has an inverse modulo $\varphi(N)$ by the inverse criterion. Notice the two moduli: N is used for messages and ciphertexts, while $\varphi(N)$ is used to choose inverse exponents.

9.2 Encryption, Decryption, and Correctness

The sender computes $c = m^e \bmod N$. The receiver computes $c^d \bmod N$. Both calculations use fast exponentiation. Closure ensures that $c \in \mathbb{Z}_N^*$, since it is a power of the invertible element m .

Why does decryption recover m ? Since $c \equiv m^e \pmod{N}$,

$$\begin{aligned} c^d &\equiv (m^e)^d = m^{ed} \\ &= m^{1+k\varphi(N)} = m(m^{\varphi(N)})^k \\ &\equiv m \cdot 1^k = m \pmod{N}. \end{aligned}$$

The last line uses Euler's theorem, which applies because the message is promised to be coprime to N . Both m and the decryption output are in $\mathbb{Z}_N$, so this congruence means they are exactly the same integer.

Extended Euclid supplies the inverse exponent, and fast exponentiation computes the two powers efficiently. Knowing p, q lets the receiver compute $\varphi(N)$; anyone who learns these factors can also recover d by the same method.

10 A Worked RSA Example

Choose $p = 11$, $q = 17$, giving

$$N = 187, \quad \varphi(N) = (11 - 1)(17 - 1) = 160.$$

Take $e = 7$. Extended Euclid gives

$$160 = 22 \cdot 7 + 6, \quad 7 = 6 + 1,$$

so

$$1 = 7 - (160 - 22 \cdot 7) = 23 \cdot 7 - 160.$$

Thus $d = 23$, with $ed = 161 = 1 + 160$. The public key is $(187, 7)$, and the private exponent is 23.

10.1 Encrypt $m = 42$

The message satisfies the promise: $\gcd(42, 187) = 1$. Using the fast-exponentiation method we already know,

$$42^2 \equiv 81, \quad 42^4 \equiv 16 \pmod{187}.$$

Since $7 = 4 + 2 + 1$,

$$c \equiv 42^7 \equiv 16 \cdot 81 \cdot 42 \equiv 174 \cdot 42 \equiv 15 \pmod{187}.$$

The ciphertext is 15.

10.2 Decrypt $c = 15$

Repeated squaring gives the following residues modulo 187:

Power	15^1	15^2	15^4	15^8	15^{16}
Residue	15	38	135	86	103

Since $23 = 16 + 4 + 2 + 1$,

$$\begin{aligned} 15^{23} &\equiv 103 \cdot 135 \cdot 38 \cdot 15 \\ &\equiv 67 \cdot 38 \cdot 15 \\ &\equiv 115 \cdot 15 \equiv 42 \pmod{187}. \end{aligned}$$

This recovers the original message. Euler's theorem explains why: $42^{160} \equiv 1 \pmod{187}$, so $42^{161} \equiv 42 \pmod{187}$.

Homework: Removing the Promise

In homework, we will prove that the assumption $\gcd(m, N) = 1$ can be removed altogether. With the same RSA key construction, decryption recovers every message $m \in \mathbb{Z}_N$, including messages that share a factor with N . The proof in this lecture establishes correctness under the coprime-message promise; the general case is left for homework.