COMS BC3262: Introduction to Cryptography

Lecture 12: Number Theory

Copyright © 2026 Barnard College

March 2, 2026

Office Hours

Office hours:

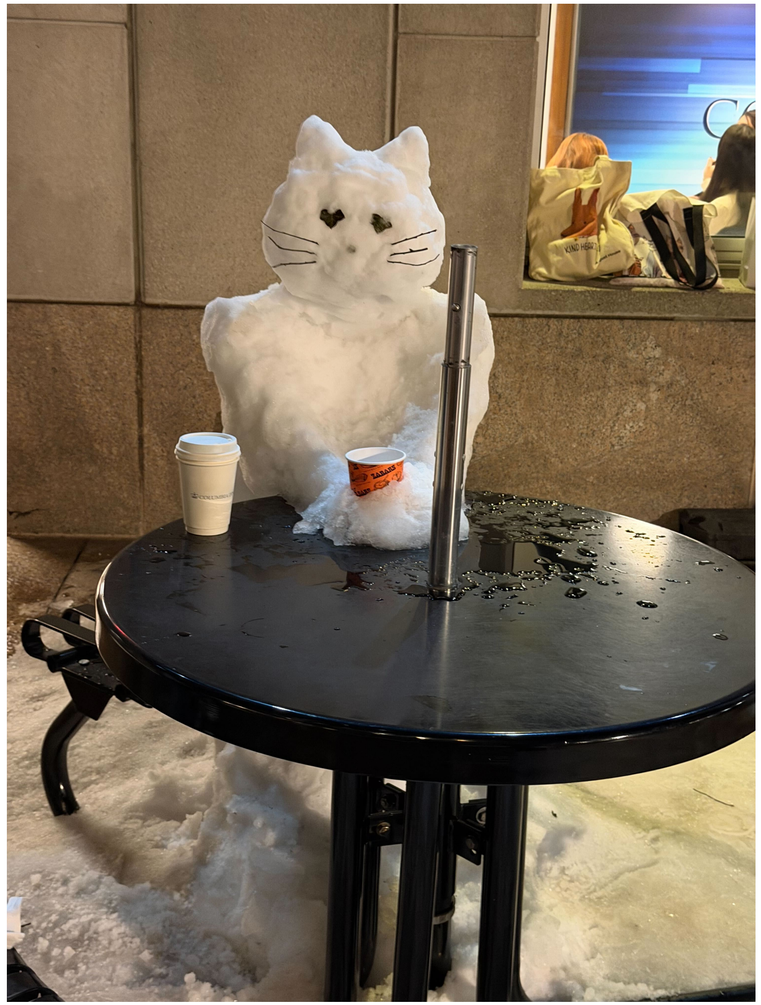
- **Eysa**: Mondays 3-5, Milstein 512
- **Mark**: Tuesdays 6:30-8:30, Milstein 503

Midterm

- There will be an **in-class written midterm** on **Wednesday, March 11**
- You may bring a single letter-sized reference sheet (double-sided)
  - You will be expected to submit your reference sheet along with your exam
- Exam is closed note, no technology, no collaboration
- *Exam will not cover any material introduced after last lecture (Lecture 11)*
- Next week Monday (March 9) will be a review session
  - Come with questions!
  - Lecture may end early if we run out of questions

Problem Sets

- PS 2 grades are out!
  - If you notice a mistake in the grading, please let me know by March 14
  - Regrades for PS 2 will be closed after that date!
- PS 3 is due Thursday, March 5
  - We will go over solutions the following Monday



3262 students very happy PS 2 was graded so quickly

Problem Set 2

- 45 points possible, scored out of 40 points
    - Question 1 was worth 15 + 5 points
- Highest grade was a 43 (more than one person got a 43, and a few more got 42, 41, and 40. Nice!)
- Median was a 37, mean was a 34.3
    - Vast majority got full points on questions 2, 3, and 4 (worth 25 points)

Today's Lecture

- Comments and Motivation
- Basics of Number Theory
- Groups

A Quick Disclaimer

- In this course, we are not going to go very in-depth in number theory
    - Our focus will be on basics that are needed for cryptography
    - We are definitely not doing this topic justice!
        - Those interested are encouraged to take relevant courses in the math department
- There are certain proofs in today's lecture I included for completeness but we are not going to spend much time on

Notes about Computational Efficiency

- Recall that runtime is defined in terms of the length of the input
  - We typically set our input length as the security parameter n
    - If our secret key is n-bits, that's 2^n possible keys
- We care about whether there exists an efficient algorithm for certain tasks
- On input N, an integer N is represented by a string of length $\log_2 N$
  - Therefore, a loop like "for 1 to N" is *not* efficient (e.g., if $N = 2^{100}$ the input length is 100 but looping 2^{100} times is not efficient)
  - To be efficient, it needs to run in time polynomial in the length of the input, which for integer N is $\log N$

Basic Number Theory

Primes and Divisibility

We'll discuss the integers $\mathbb{Z}$ (but will have the naturals $\mathbb{N}$ in mind)

- For $a, b \in \mathbb{Z}$, we say that a divides b and write $a \mid b$ if $\exists c \in \mathbb{Z}$ such that $b = ac$

- If $a \mid b$ and a is positive, then we say a is a divisor of b

- A positive integer $p > 1$ is prime if the only divisors of p are $\{1, p\}$

- A positive integer $N > 1$ is composite if it is not prime

Primes and Divisibility

The fundamental theorem of arithmetic:

Every positive integer $N > 1$ can be expressed as a product of primes in a unique way (up to ordering), i.e., $N = \Pi_i p_i^{e_i}$ where p_i is prime and $e_i \geq 1$

Note: This does not necessarily hold in arbitrary rings

Primes and Divisibility

- For $a, b \in \mathbb{N}$, there exists unique $q, r \in \mathbb{N}$ such that $a = qb + r$ and $r < b$
- The greatest common divisor of $a, b \in \mathbb{N}$ is the largest $c \in \mathbb{N}$ such that $c \mid a$ and $c \mid b$, which we denote as $c = \gcd(a, b)$
  - Example, $\gcd(12,30) = 6$
- $\gcd(a, b)$ can be expressed as $aX + bY$ for $X, Y \in \mathbb{Z}$,
  - It is the smallest positive integer that can be expressed this way
  - Example: $6 = 12 \cdot (-2) + 30 \cdot 1$
- If $\gcd(a, b) = 1$, we say that a and b are co-prime

Primes and Divisibility

- The Euclidian algorithm computes $\gcd(a, b)$ in polynomial time
- The extended Euclidian algorithm computes $\gcd(a, b), X, Y$ in polynomial time

Primes and Divisibility

Claim: If $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$. Thus, if p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Example: Consider $c = 3$, $a = 5$, and $b = 6$

$3 \mid 5 \cdot 6$ and $\gcd(3,5) = 1$, and it is indeed true $3 \mid 6$

Primes and Divisibility

Claim: If $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$. Thus, if p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof: (part 1)

- Since $c \mid ab$, there exists an integer d such that $ab = cd$
- Since $\gcd(a, c) = 1$, there exist $X, Y \in \mathbb{Z}$ such that $1 = aX + cY$
- By multiplying both sides by b we get that

$$b = abX + cbY = cdX + cbY = c \cdot (dX + bY)$$

- Since $dX + bY$ is an integer, we conclude that $c \mid b$

Primes and Divisibility

Claim: If $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$. Thus, if p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof: (part 2)

- For the second part, let p be a prime and assume that $p \mid ab$.
- Consider the two cases:
  - If $p \mid a$, then we're done :)
  - If $p \nmid a$, then it holds that $\gcd(a, p) = 1$. Hence, $p \mid b$ by the first part of the claim

Primes and Divisibility

Claim: If $a \mid N$, $b \mid N$, and $\gcd(a, b) = 1$, then $ab \mid N$

Example: Consider $a = 3$, $b = 5$, and $N = 30$

$3 \mid 30$, $5 \mid 30$, and $\gcd(3,5) = 1$, and indeed $15 \mid 30$

Primes and Divisibility

Claim: If $a \mid N$, $b \mid N$, and $\gcd(a, b) = 1$, then $ab \mid N$

Proof:

- Since $a \mid N$, there exists an integer c such that $ac = N$
- Since $b \mid N$, there exists an integer d such that $bd = N$
- Since $\gcd(a, b) = 1$, there exists $X, Y \in \mathbb{Z}$ such that $1 = aX + nY$
- Multiplying both sides by N we get

$$N = aXN + bYN = aXbd + bYac = ab \cdot (dX + cY)$$

- Therefore, $ab \mid N$

Modular Arithmetic

Definition: Let $a, b, N \in \mathbb{Z}$ and $N > 1$

- $a = b \mod N$ if $N \mid (a - b)$ (also denoted as $a \equiv b \mod N$)
  - a and b are congruent modulo N
- We denote $[a \mod N]$ the unique $r \in \{0, \ldots, N-1\}$ such that $a = r \mod N$

Examples:

- $7 = 22 \mod 15$
- $1 = 14581 \mod 2$

Modular Arithmetic

Definition: Let $a, b, N \in \mathbb{Z}$ and $N > 1$. $a = b \mod N$ if $N \mid (a - b)$ (also denoted as $a \equiv b \mod N$)

Congruence $\mod N$ is an equivalence relation

- **Reflexive**: $a = a \mod N$
  - $N \mid (a - a) = 0$ since $N \cdot 0 = 0$
- **Symmetric**: $a = b \mod N$ implies $b = a \mod N$
  - If $\exists u$ such that $N \cdot u = a - b$, then $N \cdot (-u) = b - a$
- **Transitive**: If $a = b \mod N$ and $b = c \mod N$, then $a = c \mod N$
  - If $\exists u, v$ such that $N \cdot u = a - b$ and $N \cdot v = b - c$, then

$$N \cdot (u + v) = N \cdot u + N \cdot v = a - b + b - c = a - c$$

Modular Arithmetic: Addition and Multiplication

Congruence $\mod N$ respects addition and multiplication

- If $a = a' \mod N$ and $b = b' \mod N$ then
  - **Addition**: $(a + b) = (a' + b') \mod N$
  - **Multiplication**: $a \cdot b = a' \cdot b' \mod$

Modular Arithmetic: Addition and Multiplication

Examples:

- What is $7 \cdot 8 \mod 5$?

$$(7 \mod 5) \cdot (8 \mod 5) \mod 5 = 2 \cdot 3 \mod 5 = 6 \mod 5 = 1$$

- What is $[1093028 \cdot 190301 \mod 100]$?

$$\begin{aligned} 1093028 \cdot 190301 \mod 100 \\ &= [1093028 \mod 100] \cdot [190301 \mod 100] \mod 100 \\ &= 28 \cdot 1 \mod 100 \\ &= 28 \mod \end{aligned}$$

Modular Arithmetic: Division

Congruence $\mod N$ does *not* respect division

- Example: For $N = 24$, we have $3 \cdot 2 = 6 = 15 \cdot 2 \mod 24$, but $3 \neq 15 \mod 24$

Modular Arithmetic: Division

Definition: b is invertible $\mod N$ if there exists c such that $bc = 1 \mod N$. In this case, we denote the multiplicative inverse of b in $\{0,\ldots,N-1\}$ as b^{-1}.

If $ab = cb \mod N$ and b is invertible $\mod N$,

then $(ab) \cdot b^{-1} = (cb) \cdot b^{-1} \mod N$. Therefore, $a = c \mod N$

Claim: Let $b \geq 1$ and $N > 1$. Then b is invertible $\mod N$ gif $\gcd(b, N) = 1$.

Groups

Groups

Definition: A group is a set $\mathbb{G}$ along with a binary operation $\circ$ satisfying

- **Closure**: $\forall g, h \in \mathbb{G}$, it holds that $g \circ h \in \mathbb{G}$
- **Identity element**: $\exists 1_{\mathbb{G}} \in \mathbb{G}$ such that $\forall g$ it holds that $g \circ 1_{\mathbb{G}} = 1_{\mathbb{G}} \circ g = g$
- **Inverse element**: $\forall g \, \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1} \circ g = 1_{\mathbb{G}}$
- **Associativity**: $\forall g_1, g_2, g_3 \in \mathbb{G}$ it holds that $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

Groups

Definition: A group is a set $\mathbb{G}$ along with a binary operation $\circ$ satisfying

- **Closure**: $\forall g, h \in \mathbb{G}$, it holds that $g \circ h \in \mathbb{G}$
- **Identity element**: $\exists 1_{\mathbb{G}} \in \mathbb{G}$ such that $\forall g$ it holds that $g \circ 1_{\mathbb{G}} = 1_{\mathbb{G}} \circ g = g$
- **Inverse element**: $\forall g \, \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1} \circ g = 1_{\mathbb{G}}$
- **Associativity**: $\forall g_1, g_2, g_3 \in \mathbb{G}$ it holds that $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

- Denote by $|\mathbb{G}|$ the cardinality of $\mathbb{G}$. If $\mathbb{G}$ is finite, this is the number of elements.
- $|\mathbb{G}|$ is the order of $(\mathbb{G}, \circ)$
- $(\mathbb{G}, \circ)$ is commutative (Abelian) if $\forall g, h \in \mathbb{G}$ it holds that $g \circ h = h \circ g$
- $(\mathbb{H}, \circ)$ is a sub-group of $(\mathbb{G}, \circ)$ if $(\mathbb{H}, \circ)$ is a group and $\mathbb{H} \subseteq \mathbb{G}$

Groups

Definition: A group is a set $\mathbb{G}$ along with a binary operation $\circ$ satisfying

- **Closure**: $\forall g, h \in \mathbb{G}$, it holds that $g \circ h \in \mathbb{G}$
- **Identity element**: $\exists 1_{\mathbb{G}} \in \mathbb{G}$ such that $\forall g$ it holds that $g \circ 1_{\mathbb{G}} = 1_{\mathbb{G}} \circ g = g$
- **Inverse element**: $\forall g \, \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1} \circ g = 1_{\mathbb{G}}$
- **Associativity**: $\forall g_1, g_2, g_3 \in \mathbb{G}$ it holds that $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

- Is $(\mathbb{Z}, +)$ a group?
- Is $(\mathbb{Z}, \cdot)$ a group?
- Is $(\mathbb{R}, +)$ a group?
- Is $(\mathbb{R}, \cdot)$ a group?
- Is $(\mathbb{R}^*, \cdot)$ a group, where $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$?

Group Exponentiation

Given $g \in \mathbb{G}$, we can consider applying the group operation on g multiple times: $((g \circ g) \circ g \ldots) \circ g$

- This is called group exponentiation
- In multiplicative notation we write $g^m = g \cdot \ldots \cdot g$
  - Not to be confused with integer multiplication/exponentiation
- We define $g^0 = 1$ and $g^{-m} = (g^{-1})^m$
- $g^{m_1} \cdot g^{m_2} = g^{m_1+m_2}$
- If $\mathbb{G}$ is commutative, then $(gh)^m = g^m \cdot h^m$

Groups

Theorem: Let $\mathbb{G}$ be a finite group of order $m = |\mathbb{G}|$. Then, for every $a \in \mathbb{G}$, it holds that $a^m = 1$

Corollary: Let $\mathbb{G}$ be a finite group of order $m = |\mathbb{G}| > 1$. Then, for every $g \in \mathbb{G}$ and every integer x it holds that $g^x = g^{[x \bmod m]}$

Groups

Theorem: Let $\mathbb{G}$ be a finite group of order $m = |\mathbb{G}|$. Then, for every $a \in \mathbb{G}$, it holds that $a^m = 1$

Corollary: Let $\mathbb{G}$ be a finite group of order $m = |\mathbb{G}| > 1$. Then, for every $g \in \mathbb{G}$ and every integer x it holds that $g^x = g^{[x \bmod m]}$

In general, if you want to exponentiate, it helps to figure out the order of the group first and then perform modular reduction

The Group $(\mathbb{Z}_N, +)$

The group $(\mathbb{Z}_N, +)$ for $N > 1$

- Consider the set $\mathbb{Z}_N = \{0, \ldots, N-1\}$ with the operation addition $\bmod N$
- **Closure**: By definition, for $a, b \in \mathbb{Z}_N$, it holds that $[a + b \bmod N] \in \mathbb{Z}$
- The **identity** element is $[0 \bmod N]$
- The (additive) **inverse** of $a \in \mathbb{Z}_N$ is $[N - a \bmod N]$
- Associativity and commutativity follow from these properties in the integers

The Group $\mathbb{Z}_N^*$

- Is $(\mathbb{Z}_N, \cdot\ )$ a group?
  - No! Not every element has an inverse
  - For example, 2 is not invertible in $\mathbb{Z}_4$
- What are the invertible elements in $\mathbb{Z}_{10}$?

$$\mathbb{Z}_{10} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$$

The Group $\mathbb{Z}_N^*$

- Is $(\mathbb{Z}_N, \cdot\,)$ a group?
  - No! Not every element has an inverse
  - For example, 2 is not invertible in $\mathbb{Z}_4$
- What are the invertible elements in $\mathbb{Z}_{10}$?

$$\mathbb{Z}_{10} = \{\cancel{0}, 1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9\}$$

The Group $\mathbb{Z}_N^*$

- For $N > 1$, define $\mathbb{Z}_N^* = \{a \in \{1,\ldots,N-1\} \mid \gcd(a,N) = 1\}$ with the group operation $ab = [ab \bmod N]$
- $\mathbb{Z}_N^*$ is a commutative group
  - **Closure**: If $a, b \in \mathbb{Z}_N^*$, then $[ab \bmod N]$ has inverse $[b^{-1}a^{-1} \bmod N]$
  - **Identity**: 1 is the identity element
  - **Inverse**: If $a \in \mathbb{Z}_N^*$, i.e., $\gcd(a,N) = 1$, then $Xa + YN = 1$ and $a^{-1} = [X \bmod N]$
  - **Associativity** and **commutativity** follow from these properties in the integers

The Group $\mathbb{Z}_N^*$

Euler's phi function / Euler's totient function: $\phi(N)$ is the order of $\mathbb{Z}_N^*$

e.g., $\phi(N) = |\mathbb{Z}_N^*|$

- How large many elements are in $\mathbb{Z}_N^*$?

The Group $\mathbb{Z}_N^*$

How large many elements are in $\mathbb{Z}_N^*$?

- Consider $N = p$ is a prime
  - Every $a \in \{1,\ldots,p-1\}$ is co-prime to p
  - $\phi(p) = p - 1$
- Consider $N = pq$, where p and q are primes
  - Every $a \in \{1,\ldots,N-1\}$ is not co-prime to N if it is either $p \mid a$ or $q \mid a$
  - There are $q - 1$ elements divisible by p : $p,\ 2p,\ 3p,\ \ldots,\ (q-1)p$
  - There are $p - 1$ elements divisible by q : $q,\ 2q,\ 3q,\ \ldots,\ (p-1)q$
  - $\phi(N) = N - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$

The Group $\mathbb{Z}_N^*$

Theorem: Let $N = \Pi_i p_i^{e_i}$, where p_i are distinct primes and $e_i \geq 1$. Then

$$\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$$

The Group $\mathbb{Z}_N^*$

Corollary: Let $N > 1$ and let $a \in \mathbb{Z}_N^*$. Then $a^{\phi(N)} = 1 \mod N$

If $N = p$ is prime and $a \in \{1,\ldots,p-1\}$ then $a^{p-1} = 1 \mod p$

Next Time

- Today
  - Number Theory
- Wednesday
  - More Number Theory!
  - RSA
  - DL