CMSC/Math 456: Cryptography (Fall 2022)

Lecture 28

Daniel Gottesman

Administrative

Problem set #9 due tonight at midnight.

Final exam: Monday, Dec. 19, 1:30-3:30 PM, here (IRB 0318)

- Will be open book again (textbook, lecture notes)
- Students taking the final at ADS: Remember to book with them soon.
- Today (last lecture): Review for final
- Topics covered: Everything up to (and including) post-quantum cryptography

Course evaluations are now available to fill out.

The last 15 minutes of class will be reserved for course evaluations.

Office hours: I will hold an extended office hour next week, from 10:30 AM-12:30 AM Tuesday Dec. 13.

A list of topics covered in the course is available on the course website.

This class is being recorded

Modular Arithmetic Summary

- Elements of $\mathbb{Z}_N^*$
- Euclid's algorithm
- Groups
- Modular exponentiation and order
- Chinese remainder theorem

Elements of $\mathbb{Z}_{21}^*$

Let us work through the structure of $\mathbb{Z}_{21}^*$ in detail.

First: What are the elements of $\mathbb{Z}_{21}^*$?

> Recall: the $*$ indicates that we are talking only about the elements that have a multiplicative inverse — those that are relatively prime to 21.

$$\mathbb{Z}_{21}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$$

The number of elements of $\mathbb{Z}_{21}^*$ is $\varphi(21) = 12$.

> Recall: $\varphi(N)$ is the number of numbers that are relatively prime to N. When p is prime, $\varphi(p) = p - 1$. When N=pq with p and q prime, $\varphi(N) = (p-1)(q-1)$.

Non-Elements of $\mathbb{Z}_{21}^*$

What are *not* elements of $\mathbb{Z}_{21}^*$?

Multiples of 3 and 7, specifically 0, 3, 6, 7, 9, 12, 14, 15, 18.

Why not?

These have no multiplicative inverses. For instance, consider $6i \bmod 21$:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
6i	0	6	12	18	3	9	15	0	6	12	18	3	9	15	0	6	12	18	3	9	15

Nothing can be multiplied by 6 to give 1: 6 has no multiplicative inverse. This also means that division by 6 doesn't make sense in general mod 21.

Multiplicative Inverses

The elements of $\mathbb{Z}_{21}^*$ *do* have multiplicative inverses mod 21.

Example: The multiplicative inverse of 8 mod 21 is 8:

$$8 \cdot 8 = 64 = 1 \bmod 21$$

But note that if we are working mod 15, then the inverse of 8 is 2:

$$8 \cdot 2 = 16 = 1 \bmod 15$$

and 8 doesn't have a multiplicative inverse mod 10.

Dividing by 8 is equivalent to multiplying by its inverse:

$$11/8 = 11 \cdot 8 = 4 \bmod 21$$
$$11/8 = 11 \cdot 2 = 7 \bmod 15$$

We can find inverses using Euclid's algorithm.

Euclid's Algorithm Summary

Euclid's algorithm finds the GCD (greatest common divisor) of two numbers. An extension (sometimes called the extended Euclidean algorithm) finds coefficients X and Y such that

$$Xa + Yb = \gcd(a, b)$$

It works by subtracting multiples of the smaller number from the larger number and then continually updating and repeating the process.

It has many uses, including finding the GCD of two numbers or finding multiplicative inverses.

Euclid's Algorithm

Let $r_0 = a$ and $r_1 = b$. Assume $a > b$.

$i = 1, X_0 = 1, Y_0 = 0, X_1 = 0, Y_1 = 1$

Repeat:

$$r_{i+1} = r_{i-1} \bmod r_i$$

$$m_i = \lfloor r_{i-1}/r_i \rfloor$$

$$X_{i+1} = X_{i-1} - m_i X_i$$

$$Y_{i+1} = Y_{i-1} - m_i Y_i$$

$$i = i + 1$$

Until $r_i = 0$

Output:

$$\gcd(a, b) = r_{i-1}$$

$$X = X_{i-1}, Y = Y_{i-1}$$

This class is being recorded

Example:

$r_0 = 21, r_1 = 8$

$r_2 = 5,$
$X_2 = 1, Y_2 = -2$

$r_3 = 3,$
$X_3 = -1, Y_3 = 3$

$r_4 = 2,$
$X_4 = 2, Y_4 = -5$

$r_5 = 1,$
$X_5 = -3, Y_5 = 8$

$r_6 = 0$

$\gcd(21,8) = 1,$
$1 = -3 \cdot 21 + 8 \cdot 8$

Euclid's Algorithm

Let $r_0 = a$ and $r_1 = b$. Assume $a > b$.

$i = 1, X_0 = 1, Y_0 = 0, X_1 = 0, Y_1 = 1$

Repeat:

$$r_{i+1} = r_{i-1} \bmod r_i$$

$$m_i = \lfloor r_{i-1}/r_i \rfloor$$

$$X_{i+1} = X_{i-1} - m_i X_i$$

$$Y_{i+1} = Y_{i-1} - m_i Y_i$$

$$i = i + 1$$

Until $r_i = 0$

Output:

$$\gcd(a, b) = r_{i-1}$$

$$X = X_{i-1}, Y = Y_{i-1}$$

This class is being recorded

Example:

$r_0 = 21, r_1 = 8$

$r_2 = 5,$
$X_2 = 1, Y_2 = -2$

$r_3 = 3,$
$X_3 = -1, Y_3 = 3$

$r_4 = 2,$
$X_4 = 2, Y_4 = -5$

$r_5 = 1,$
$X_5 = -3, Y_5 = 8$

$r_6 = 0$

$\gcd(21,8) = 1,$
$1 = -3 \cdot 21 + 8 \cdot 8$

$8^{-1} \bmod 21$

Group Theory Summary

Definition: A group $(G, *)$ is a set G of elements along with a binary operation $* : G \times G \rightarrow G$ with the following properties:

1. Closure: $g * h \in G$ when $g, h \in G$.
2. Associativity: $\forall g, h, k \in G, (g * h) * k = g * (h * k)$.
3. Identity: $\exists e \in G$ such that $\forall g \in G, e * g = g * e = g$.
4. Inverses: $\forall g \in G, \exists g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

A subgroup H of G, written $H \leq G$ is a subset of G which is also a group. The order $|G|$ of a finite group G is the number of elements.

A set S generates a group G if all elements of G can be written as products of elements of S. A group that can be generated by just one element is cyclic.

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

$\mathbb{Z}_{21}^*$ as a Group

$\mathbb{Z}_{21}^*$ (or any $\mathbb{Z}_N^*$) is a group with multiplication as the group operation:

- Multiplication is closed: $a, b \in \mathbb{Z}_{21} \Rightarrow ab \bmod 21 \in \mathbb{Z}_{21}$.
- Associative: $(ab)c = a(bc) \bmod 21$.
- Identity is 1: $a \cdot 1 = 1 \cdot a = a$.
- Inverses: This is why we used $\mathbb{Z}_{21}^*$ instead of $\mathbb{Z}_{21}$.

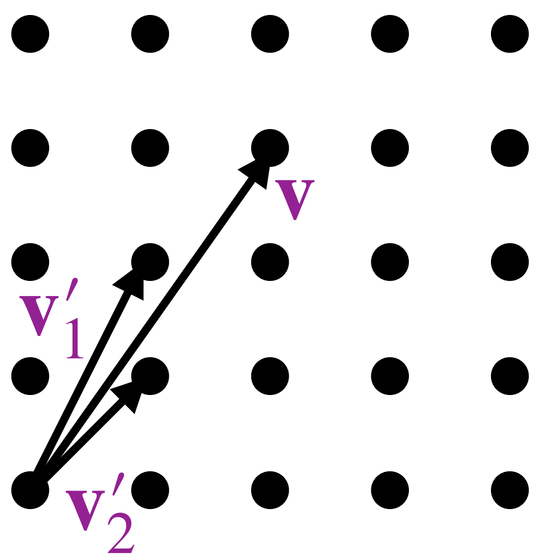
Note that $\mathbb{Z}_{21}$ under multiplication would satisfy all conditions but the last one.

$\mathbb{Z}_{21}$ is a group as well, but only when the group operation is addition rather than multiplication.

Lattice as a Group

A lattice is a group under addition of vectors.

$$L = \left\{ \sum_i s_i \mathbf{v}_i \,\middle|\, s_i \in \mathbb{Z} \right\}$$

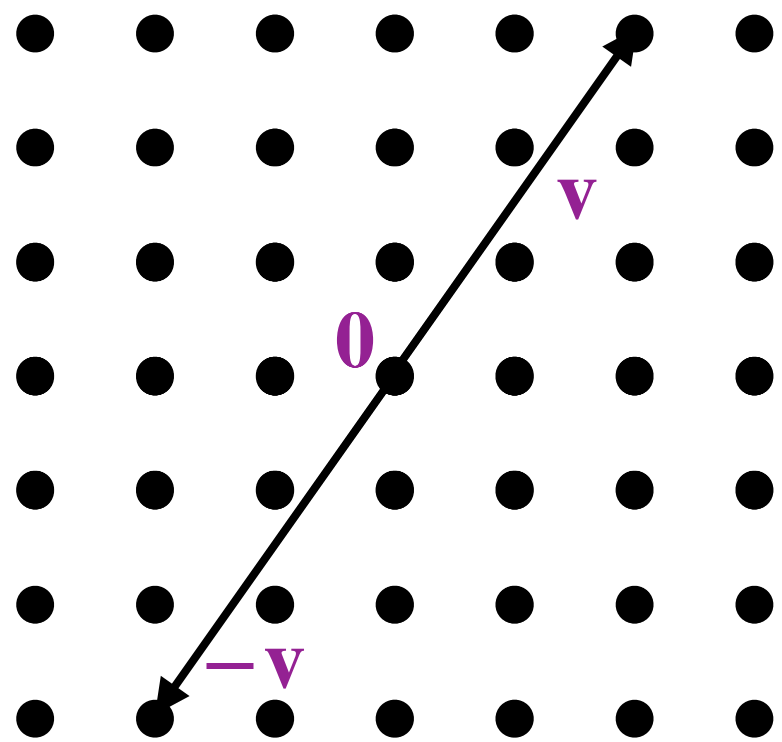


Closure: If $\mathbf{v}'_1$ and $\mathbf{v}'_2$ are in the lattice, then $\mathbf{v} = \mathbf{v}'_1 + \mathbf{v}'_2$ is also in the lattice.

Associativity: Addition is associative: $(\mathbf{v} + \mathbf{w}) + \mathbf{x} = \mathbf{v} + (\mathbf{w} + \mathbf{x})$.

Identity: The origin, $\mathbf{0}$ vector is in the lattice, and $\mathbf{v} + \mathbf{0} = \mathbf{v}$.

Inverse: If $\mathbf{v}$ is in the lattice, $-\mathbf{v}$ is in the lattice, and $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.



This class is being recorded

Modular Exponentiation

$x^a \bmod N$ can be computed efficiently (i.e., in a time polynomial in log x, log a, and log N) using repeated squaring.

Modular exponentials satisfy all the usual properties of exponentials. For instance:

$$x^a x^b = x^{a+b} \bmod N$$
$$(x^a)^b = x^{ab} \bmod N$$
$$x^a y^a = (xy)^a \bmod N$$
$$x^{-a} = 1/(x^a) \bmod N$$

Let us calculate the order of elements in $\mathbb{Z}_{21}^*$ under modular exponentiation. Lagrange's Theorem tells us all orders must be factors of $|\mathbb{Z}_{21}^*| = \varphi(21) = 12$.

Recall: The order of x mod N is the smallest integer r>0 such that $x^r = 1 \bmod N$.

Orders in $\mathbb{Z}_{21}^*$

This class is being recorded

Orders in $\mathbb{Z}_{21}^*$

$1^1 = 1 \bmod 21$ Order of 1 is 1.

This class is being recorded

Orders in $\mathbb{Z}_{21}^*$

$1^1 = 1 \bmod 21$ Order of 1 is 1.

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 11,\ 2^6 = 1 \bmod 21$

Order of 2 is 6.

Orders in $\mathbb{Z}_{21}^*$

$1^1 = 1 \bmod 21$ Order of 1 is 1.

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 11,\ 2^6 = 1 \bmod 21$

Order of 2 is 6.

$4^1 = 4,\ 4^2 = 16,\ 4^3 = 1 \bmod 21$ Order of 4 is 3.

Orders in $\mathbb{Z}_{21}^*$

$1^1 = 1 \bmod 21$ Order of 1 is 1.

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 11,\ 2^6 = 1 \bmod 21$

Order of 2 is 6.

$4^1 = 4,\ 4^2 = 16,\ 4^3 = 1 \bmod 21$ Order of 4 is 3.

But note: $2^2 = 4 \bmod 21$ and 2 has order 6.

Therefore, $4^3 = (2^2)^3 = 2^6 \bmod 21$.

We can deduce the order of 4 by looking at the powers of 2.

Orders in $\mathbb{Z}_{21}^*$

$1^1 = 1 \bmod 21$ Order of 1 is 1.

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 11,\ 2^6 = 1 \bmod 21$

Order of 2 is 6.

$4^1 = 4,\ 4^2 = 16,\ 4^3 = 1 \bmod 21$ Order of 4 is 3.

But note: $2^2 = 4 \bmod 21$ and 2 has order 6.

Therefore, $4^3 = (2^2)^3 = 2^6 \bmod 21$.

We can deduce the order of 4 by looking at the powers of 2.

More generally,

$$\mathrm{ord}(g^j) = \mathrm{ord}(g) / \gcd(j, \mathrm{ord}(g))$$

E.g., if j and ord(g) are relatively prime, then $\mathrm{ord}(g^j) = \mathrm{ord}(g)$.

Orders Continued

$$5^1 = 5,\ 5^2 = 4,\ 5^3 = 20,\ 5^4 = 16,\ 5^5 = 17,\ 5^6 = 1 \bmod 21$$

Order of 5 is 6.

We can also conclude that the order of 17 is 6 as well, and the order of 20 is 2.

$$10^1 = 10,\ 10^2 = 16,\ 10^3 = 13,\ 10^4 = 4,\ 10^5 = 19,\ 10^6 = 1 \bmod 21$$

Order of 10 is 6.

From this and the previous slide, we conclude that 11 and 19 also have order 6, that 8 and 13 have order 2, and that 16 has order 3.

Cyclic Subgroups of $\mathbb{Z}_{21}^*$

The results of the previous page also tell us the subgroup structure of $\mathbb{Z}_{21}^*$:

3 cyclic subgroups of order 6:

$\{1,2,4,8,11,16\}$ $\{1,4,5,16,17,20\}$ $\{1,4,10,13,16,19\}$

1 cyclic subgroup of order 3:

$\{1,4,16\}$

3 cyclic subgroups of order 2:

$\{1,8\}$ $\{1,13\}$ $\{1,20\}$

1 cyclic subgroup of order 1:

$\{1\}$

Note that $\mathbb{Z}_{21}^*$ is not cyclic; it doesn't have to be since 21 is not prime. But when p is prime, $\mathbb{Z}_p^*$ is cyclic.

Chinese Remainder Theorem

Chinese remainder theorem: When a, b relatively prime,

$$x = x_a \bmod a$$
$$x = x_b \bmod b$$

have unique solution x mod ab.

Algorithm:

Run Euclid's algorithm to find X and Y such that

$$aX + bY = 1$$

Then

$$x = x_b a X + x_a b Y$$

Example: $a = 3, b = 7, x_a = 2, x_b = 1$

$$x = 2 \bmod 3$$
$$x = 1 \bmod 7$$

Euclid's algorithm:

$$3 * (-2) + 7 * 1 = 1$$

$X = -2, Y = 1$

Then

$$x = 1 * 3 * (-2) + 2 * 7 * 1$$
$$= -6 + 14 = 8 \bmod 21$$