# MATH/CMSC 456 :: UPDATED COURSE INFO

**Instructor:** Gorjan Alagic (galagic@umd.edu)

**Guest instructor:** Carl Miller (camiller@umd.edu), ATL 3100K

**Textbook:** *Introduction to Modern Cryptography*, Katz and Lindell;

Current readings:

**Feb 25:** pp. 285-297

**Feb 27:** pp. 302-324 (skip subsections 8.2.2 and 8.2.5)

---

**Webpage:** alagic.org/cmsc-456-cryptography-spring-2020/

**Piazza:** piazza.com/umd/spring2020/cmsc456

**ELMS:** active, slides and reading posted there, **homework 3 due midnight Thursday.**

**Gradescope:** active, access through ELMS.

---

**TAs** (Our spot: shared open area across from **AVW 4166**)

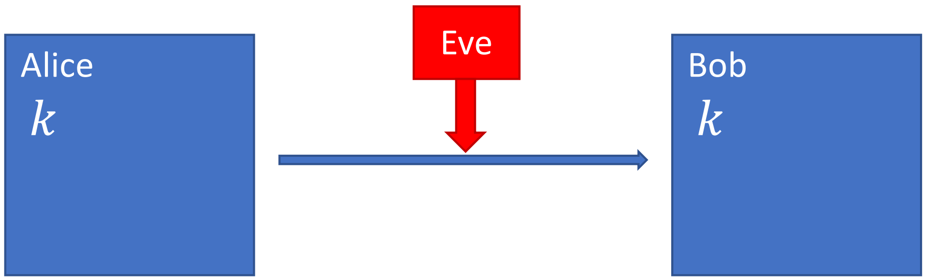
- Elijah Grubb (egrubb@cs.umd.edu) 11am-12pm TuTh (AVW);
- Justin Hontz (jhontz@terpmail.umd.edu) 1pm-2pm MW (AVW);

**Additional help:**

- Chen Bai (cbai1@terpmail.umd.edu) 3:30-5:30pm Tu (2115 ATL – inside **JQI**)
- Bibhusa Rawal (bibhusa@terpmail.umd.edu) 3:30-5:30pm Th (2115 ATL – inside **JQI**)

# RECAP: Secret-key vs. Public-key cryptography

A MAC (Message Authentication Code) is an example of **secret-key cryptography**.



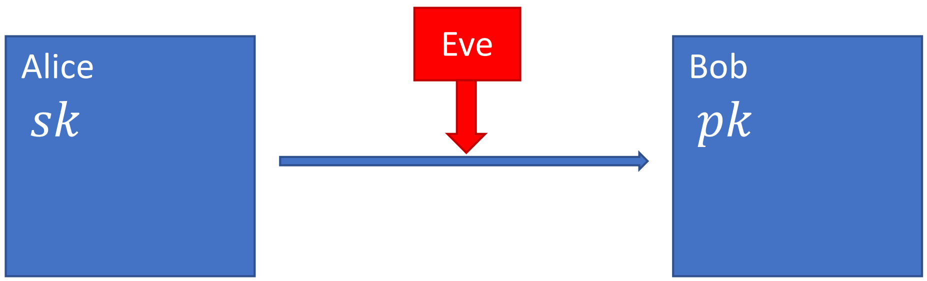

Alice uses the secret key **k** to authenticate a message, which is then verified by Bob.

**Limitations:**

- Alice & Bob have to find a way to exchange the key **k** secretly.
- Any party that can verify an authentication code can also forge one!

# RECAP: Secret-key vs. Public-key cryptography

In **public-key cryptography,** Alice creates a public key (*pk*) and a secret key (*sk*).




The public key is broadcast – anyone can know it.

**Desired properties:**

- Alice can sign a message in such way that her signature can be verified, **but not forged,** using *pk*.
- Anyone who has *pk* can encrypt, **but not decrypt**, a message to Alice.

We always want to make our protocol computationally easy to carry out, and computationally difficult for an adversary to break.

# COMPUTATIONALLY DIFFICULT PROBLEMS

Classical (non-quantum) cryptography relies on the assumption that certain computational problems are hard.

Example from February 13th: **Collision-resistance for keyed hash-function.**

$$\begin{tikzcd} x \arrow[dr, "\mathcal{H}^s"'] & & x' \arrow[dl, "\mathcal{H}^s"] \\ & y & \end{tikzcd}$$

We assume that, given randomly chosen $s$, it is hard to find a collision for $\mathcal{H}^s$.

Properties of this problem:

- It is easy to **describe**. (Just specify the hash function – e.g., SHA3.)
- It is easy to **check** a valid answer.
- We believe that it is hard to **find** a valid answer.

# COMPUTATIONALLY DIFFICULT PROBLEMS

How about factoring numbers?

**Problem:** Suppose that n is a positive integer (expressed as a string of bits). Express n as

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_r,$$

where each $p_i$ is prime (i.e., has no factors other than 1 and itself).

It is easy to check a factorization (in time less than a polynomial function of the number of bits).
However, no polynomial-time, non-quantum algorithm for factoring numbers is currently known.

**The Plan:**

1. Do a detailed study of some basic number theory.
2. Build a public-key cryptosystem based on the hardness of factoring.

# MODULAR ARITHMETIC: Notation & Examples

# ARITHMETIC: THE BEGINNING

Let $\mathbb{Z}$ denote the set of all integers.

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

For any $n, q \in \mathbb{Z}$ with $q \neq 0$, the expression

$$[n \bmod q]$$

denotes the remainder of $n$ after division by $q$.
(Always, $0 \leq [n \bmod q] < q$.)

> *"Consider thyself to be dead, and to have completed thy life up to the present time; and live according to nature the **remainder** which is allowed thee."*
> *- Marcus Aurelius*

**Examples:** $[2459 \bmod 100] = 59.$
$[(-4) \bmod 7] = 3.$

# ARITHMETIC: THE BEGINNING

Let $\mathbb{Z}_q$ denote the set.

$$\mathbb{Z}_q = \{0,1,2,3,\dots,q-1\}$$

For any $a, b \in \mathbb{Z}_q$, the elements

$$[(a+b) \bmod q]$$
$$[(a \cdot b) \bmod q]$$

are also elements of $\mathbb{Z}_q$.

**Example:** $[(31 \cdot 8) \bmod 100] = [248 \bmod 100] = 48.$

*Alternative notation*:

If $n, m$ are integers, then

$$n = m \bmod q$$

means

$$[n \; mod \; q] = [m \; mod \; q].$$

## ARITHMETIC: THE BEGINNING

Also, for any $a \in \mathbb{Z}_q$ and $n > 0$, the integer

$$[a^n \bmod q]$$

is an element of $\mathbb{Z}_q$.

**Trick:** When carrying out multiple operations, you can mod out as you go.

$$\begin{gathered}[(2 \cdot 3 \cdot 4 \cdot 4) \bmod 5] \\ = [(6 \cdot 16) \bmod 5] \\ = [(1 \cdot 1) \bmod 5] \\ = \mathbf{1}\end{gathered}$$

# TWO EXERCISES (no calculators!)

**#1:** Compute $[(21 \cdot 33 \cdot 495 \cdot 433) \bmod 10]$.

$$[(21 \cdot 33 \cdot 495 \cdot 433) \bmod 10]$$
$$= [(1 \cdot 3 \cdot 5 \cdot 3) \bmod 10]$$
$$=[(45) \bmod 10] = \mathbf{5}.$$

**#2:** Compute $[(2^{101}) \bmod 7]$.

$$([2^i \bmod 7]) = (2,4,1,2,4,1,2,4,1 \ldots)$$

The 101st term in this sequence is **4**.

To show this answer more formally:

$$[2^{101} \bmod 7] = [2^{99} \cdot 2^2 \bmod 7] = [2^{3 \cdot 33} \cdot 2^2 \bmod 7]$$
$$= [(8)^{33} \cdot 4 \bmod 7] = [1^{33} \cdot 4 \bmod 7] = 4.$$

# ADDITION AND MULTIPLICATION IN $\mathbb{Z}_q$

Let $f: \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ be the function defined by $f(a) = [(a + 4)\ mod\ 9]$.

$$f(0) = 4$$
$$f(1) = 5$$
$$f(2) = 6$$
$$f(3) = 7$$
$$f(4) = 8$$
$$f(5) = 0$$
$$f(6) = 1$$
$$f(7) = 2$$
$$f(8) = 3$$

## ADDITION AND MULTIPLICATION IN $\mathbb{Z}_q$

Let $f: \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ be the function defined by $f(a) = [(a + 5)\ mod\ 9]$.

$$f(0) = 5$$
$$f(1) = 6$$
$$f(2) = 7$$
$$f(3) = 8$$
$$f(4) = 0$$
$$f(5) = 1$$
$$f(6) = 2$$
$$f(7) = 3$$
$$f(8) = 4$$

## ADDITION AND MULTIPLICATION IN $\mathbb{Z}_q$

Let $f: \mathbb{Z}_9 \to \mathbb{Z}_9$ be the function defined by $f(a) = [(4a) \ mod \ 9]$.

$$f(0) = 0$$
$$f(1) = 4$$
$$f(2) = 8$$
$$f(3) = 3$$
$$f(4) = 7$$
$$f(5) = 2$$
$$f(6) = 6$$
$$f(7) = 1$$
$$f(8) = 5$$

# ADDITION AND MULTIPLICATION IN $\mathbb{Z}_q$

Let $f: \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ be the function defined by $f(a) = [(5a)\ mod\ 9]$.

$f(0) = 0$
$f(1) = 5$
$f(2) = 1$
$f(3) = 6$
$f(4) = 2$
$f(5) = 7$
$f(6) = 3$
$f(7) = 8$
$f(8) = 4$

*Note: No repeats! Why?*

The map $\mathrm{g}: \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ defined by $\mathrm{g(a)} = [(2\mathrm{a}) \bmod 9]$ satisfies

$$\begin{aligned} g(f(a)) &= [2 \cdot 5 \cdot a \bmod 9] \\ &= [1 \cdot a \bmod 9] \\ &= a. \end{aligned}$$

That means f is a **one-to-one function**.

Since $[2 \cdot 5 \bmod 9] = 1$, we say that 2 is the **multiplicative inverse** of 5 mod 9. We write:

$$2 = 5^{-1} \bmod 9.$$

# ADDITION AND MULTIPLICATION IN $\mathbb{Z}_q$

Let $f: \mathbb{Z}_9 \to \mathbb{Z}_9$ be the function defined by $f(a) = [(3a) \; mod \; 9]$.

$f(0) = 0$

$f(1) = 3$

$f(2) = 6$

$f(3) = 0$

$f(4) = 3$

$f(5) = 6$

$f(6) = 0$

$f(7) = 3$

$f(8) = 6$

This is <u>not</u> a one-to-one function.

**Q:** When is multiplication one-to-one?

# EXPONENTIATION IN $\mathbb{Z}_q$

Let $f: \{0,1,2, \dots\} \rightarrow \mathbb{Z}_9$ be the function defined by $f(a) = [2^a \ mod\ 9]$.

$f(0) = 1$
$f(1) = 2$
$f(2) = 4$
$f(3) = 8$
$f(4) = 7$
$f(5) = 5$
$f(6) = 1$ ⟵ Repeat.
$f(7) = 2$
$f(8) = 4$
$\dots$

This is a periodic function.
$f(a + 6) = f(a)$.

## EXPONENTIATION IN $\mathbb{Z}_q$

Let $f: \{0,1,2, \ldots\} \rightarrow \mathbb{Z}_9$ be the function defined by $f(a) = [6^a \; mod \; 9]$.

$f(0) = 1$
$f(1) = 6$
$f(2) = 0$
$f(3) = 0$
$f(4) = 0$
$f(5) = 0$
$f(6) = 0$
$f(7) = 0$
$f(8) = 0$
$\ldots$

This is **not** a periodic function.

Why is exponentiation periodic for some bases and not for others?

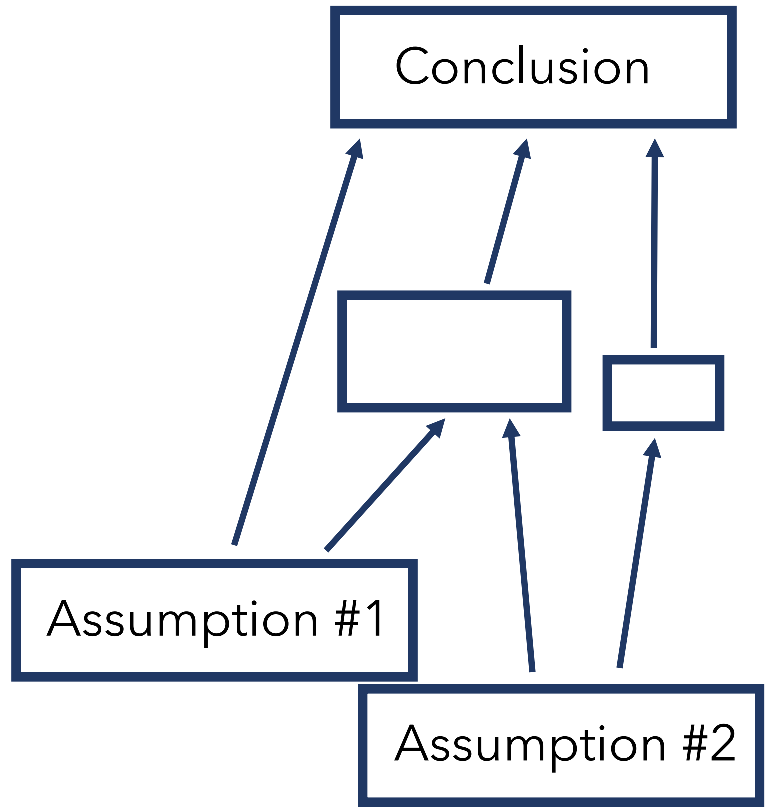
# MODULAR ARITHMETIC: Proofs

# COMMENTS ABOUT PROOFS

A proof is a series of **deductions** based on clearly stated **assumptions.**

Everything must be justified, unless it's an assumption, or it's obvious.

What's obvious? If in doubt, ask.

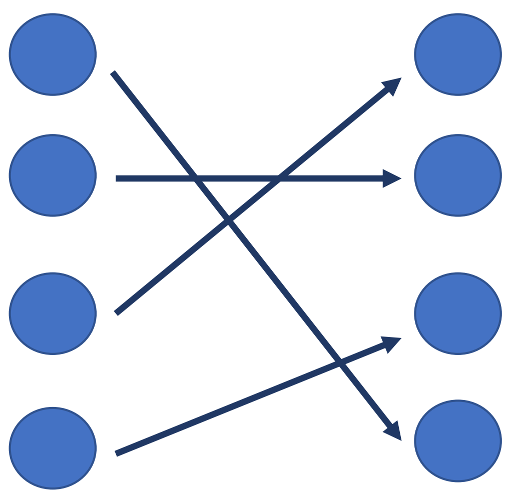


# A PROPOSITION ABOUT MULTIPLICATIVE INVERSES

**Proposition:** Let $q$ be a positive integer. Let $a$ be an element of $\mathbb{Z}_q$, and suppose that $a$ has a multiplicative inverse in $\mathbb{Z}_q$. Then, the function $f: \mathbb{Z}_q \to \mathbb{Z}_q$ defined by

$$f(x) = [ax \bmod q]$$

is a one-to-one function.



# A PROPOSITION ABOUT MULTIPLICATIVE INVERSES

**Proposition:** Let $q$ be a positive integer. Let $a$ be an element of $\mathbb{Z}_q$, and suppose that $a$ has a multiplicative inverse in $\mathbb{Z}_q$. Then, the function $f: \mathbb{Z}_q \to \mathbb{Z}_q$ defined by

$$f(x) = [ax \bmod q]$$

is a one-to-one function.

**Proof:** Let $x, y$ be elements of $\mathbb{Z}_q$ such that $f(x) = f(y)$.

Then,

$$[ax \bmod q] = [ay \bmod q],$$

and therefore,

$$[a^{-1}ax \bmod q] = [a^{-1}ay \bmod q],$$

which implies (by the definition of multiplicative inverse) that $x = y$.

Thus, the only way that the equation $f(x) = f(y)$ can occur is if x and y are equal. We conclude that $f$ is a one-to-one function. $\square$

# ANOTHER PROPOSITION ABOUT MULTIPLICATIVE INVERSES

**Proposition:** Let $q$ be a positive integer. Let $a$ be an element of $\mathbb{Z}_q$ such that the function $f: \mathbb{Z}_q \rightarrow \mathbb{Z}_q$ defined by

$$f(x) = [ax \bmod q]$$

is a one-to-one function. Then, $a$ has a multiplicative inverse in $\mathbb{Z}_q$.

**Proof:** Suppose, for the sake of contradiction, that $a$ does **not** have a multiplicative inverse.

Then, there is no $x$ such that $f(x) = 1$. But, this means that the function $f$ maps $\mathbb{Z}_q$ (which has $q$ elements) into the set

$$\{0,2,3,4,5,6, \ldots q-1\},$$

which has only $(q-1)$ elements.

Since f is a one-to-one function, this is a contradiction. We conclude that $a$ must have a multiplicative inverse in $\mathbb{Z}_q$. $\square$

# A FUNDAMENTAL PROPOSITION

**Question:** Which elements of $\mathbb{Z}_q$ have multiplicative inverses?

The next proposition will eventually help us to answer that question.

**More terminology:**

We say that one integer $n$ **divides** another integer $m$ if there exists an integer $\mathrm{c}$ such that $m = nc$.

If $a, b$ are positive integers, then the **greatest common divisor** of $a, b$ (denoted "$\mathrm{gcd}(a, b)$") is the largest integer that divides both.

# A FUNDAMENTAL PROPOSITION

**Proposition:** Let $a, b$ be positive integers. Then, there exist integers $x, y$ such that

$$ax + by = \gcd(a, b).$$

**Proof:** Let $d$ be the smallest positive integer in the set $S = \{ax + by \mid x, y \in \mathbb{Z}\}$.

Let $r = [a \bmod d]$. Then, $a = nd + r$ for some $n \in \mathbb{Z}$.

Since $d = ax + by$, we have

$$r = a - n(ax + by) = a(1 - nx) - b(ny),$$

which means that $r$ is in $S$.

Since $0 \leq r < d$ and we assumed that $d$ is the smallest positive element of S, we conclude that $r = 0$ and thus $d$ divides $a$. Similar reasoning shows that $d$ divides $b$.

Therefore, $d$ is a common divisor of $a, b$.

On the other hand, $d$ must be divisible by $\gcd(a, b)$ (since $\gcd(a, b)$ divides every element of $S$), and so $d \geq \gcd(a, b)$. We conclude that $d$ is itself the greatest common divisor of $a, b$. This completes the proof. $\square$

## A CRITERION FOR MULTIPLICATIVE INVERSES

**Corollary:** Let $q$ be a positive integer. Let $a \in \mathbb{Z}_q$ be such that

$$\gcd(a, q) = 1.$$

Then, $a$ has a multiplicative inverse in $\mathbb{Z}_q$.

**Proof:** By the previous proposition, find $x, y \in \mathbb{Z}$ such that

$$ax + qy = 1.$$

Then,

$$ax = 1 \bmod q. \qquad \square$$

(Exercise: Prove the converse of this statement.)

# COMMENTS ABOUT COMPUTATION

We consider an operation to be efficient if it takes time that is polynomial in the **length** of its input.

(If the input is a sequence of integers, then its length is, approximately, the number of bits needed to represent those integers in base 2.)

So, addition is efficient:

$$\begin{array}{r} 1\,1\,1\,0\,1\,1\,0\,0\,0\,1 \\ +\,1\,0\,0\,0\,0\,1\,0\,1\,1\,0 \\ \hline 1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1 \end{array}$$

So are multiplication and mod.

Can multiplicative inverses be computed efficiently?

**Yes** – Euclid's algorithm. See appendix B.1.2.

## SUMMING UP

We reviewed the concept of **public-key cryptography.**

We did experiments with **modular arithmetic** ($\mathbb{Z}_q$) and noted patterns.

We did some model proofs dealing with the **multiplicative structure** of $\mathbb{Z}_q$.

Coming up: We'll look more at the exponential function for $\mathbb{Z}_q$.