CSC110 Lecture 17: Modular Arithmetic

David Liu, Department of Computer Science

*Navigation tip for web slides: press **?** to see keyboard navigation controls.*

Announcements & Today's plan

- Assignment 3 has been posted—please start early!
  - Check out the A3 FAQ (+ corrections)
  - Additional TA office hours
  - Review advice on academic integrity
- PythonTA survey 1

Joonho's last class 🥲

Finishing up the Extended Euclidean Algorithm

Today you'll learn to...

1. Define modular equivalence.
2. State and prove some properties of modular equivalence.
3. Translate between a proof of existence and an algorithm.
4. Define the terms order and Euler totient function and state properties of these term.

Modular Arithmetic

Definition

Let $a, b, n \in \mathbb{Z}$, and assume $n \neq 0$. We say that a **is equivalent to** b **modulo** n when $n \mid a - b$. In this case, we write $a \equiv b \pmod{n}$.

Examples:

$$10 \equiv 1 \pmod{3}$$

$$10 \equiv 601 \pmod{3}$$

$$10 \equiv -2 \pmod{3}$$

Modular equivalence and remainders

Warning: $a \equiv b \pmod{n}$ does NOT mean that b is the remainder when a is divided by n.

But...

Theorem. Let $a, b, n \in \mathbb{Z}$ and assume $n \neq 0$. Then $a \equiv b \pmod{n}$ if and only if $a \,\%\, n = b \,\%\, n$.

Modular equivalence and arithmetic operations

For all $a, b, c, d, n \in \mathbb{Z}$, if $n \neq 0$ and $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then:

1. $a + b \equiv c + d \pmod{n}$
2. $a - b \equiv c - d \pmod{n}$
3. $ab \equiv cd \pmod{n}$

Example: Proof of 1 ($a + b \equiv c + d \pmod{n}$)

Let $a, b, c, d, n \in \mathbb{Z}$. Assume that:

- $n \neq 0$
- $a \equiv c \pmod{n}$, i.e., $\exists k_1 \in \mathbb{Z},\ c - a = k_1 n$
- $b \equiv d \pmod{n}$, i.e., $\exists k_2 \in \mathbb{Z},\ d - b = k_2 n$

We want to prove that $a + b \equiv c + d \pmod{n}$, i.e.,
$\exists k_3 \in \mathbb{Z},\ (c + d) - (a + b) = k_3 n.$

(rough work)

Given: the two equations

$$c - a = k_1 n$$
$$d - b = k_2 n$$

Want: the equation

$$(c + d) - (a + b) = \_\_\_\_ n$$

Let $k_3 = k_1 + k_2$.

Then we can prove $(c + d) - (a + b) = k_3 n$ with a calculation:

$$\begin{aligned}(c + d) - (a + b) &= (c - a) + (d - b) \\ &= k_1 n + k_2 n \\ &= (k_1 + k_2) n \\ &= k_3 n\end{aligned}$$

Exercise 1: Modular arithmetic practice

You proved this statement in Question 3 of the exercise:

$$\forall a, b, c \in \mathbb{Z},\ \forall n \in \mathbb{Z}^+,\ a \equiv b \pmod{n} \Rightarrow ca \equiv cb \pmod{n}$$

What about the converse?

$$\forall a, b, c \in \mathbb{Z},\ \forall n \in \mathbb{Z}^+,\ ca \equiv cb \pmod{n} \Rightarrow a \equiv b \pmod{n}$$

In other words, can we “divide by c” in modular equivalence?

Let $n = 12$. Let $a = 3$, $b = 6$, and $c = 4$. Then:

- $ca = 12 \equiv 0 \pmod{12}$
- $cb = 24 \equiv 0 \pmod{12}$
- But $a \not\equiv b \pmod{12}$

What is division?

In normal arithmetic, division relies on taking reciprocals:

$$\frac{a}{b} = a \times b^{-1}$$

What is division?

What's the equivalent of a reciprocal in modular arithmetic?

$$10 \times 5 \equiv 1 \pmod{7}$$

$$10 \times \ldots \equiv 1 \pmod{15}$$

Theorem (Modular inverse theorem).

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $\gcd(a, n) = 1$, then there exists $p \in \mathbb{Z}$ such that $ap \equiv 1 \pmod{n}$.

We call this p a **modular inverse of a modulo n**.

Proof of the Modular inverse theorem

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Assume $\gcd(a, n) = 1$. We want to prove that there exists $p \in \mathbb{Z}$ such that $ap \equiv 1 \pmod{n}$.

By the **GCD Characterization theorem**, there exist $p, q \in \mathbb{Z}$ such that

$$1 = pa + qn$$

Rearranging, we have $1 - pa = qn$, and so by the definition of divisibility $n \mid 1 - pa$.

Then by the definition of modular equivalence, $pa \equiv 1 \pmod{n}$.

Theorem. (Modular division)

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. If $\gcd(a, n) = 1$, then for all $b \in \mathbb{Z}$, there exists $k \in \mathbb{Z}$ such that $ak \equiv b \pmod{n}$.

Exercise 2: Modular division

Modular exponentiation and order

Consider:

2^k	$2^k \,\%\, 7$
2^0	$2^0 \,\%\, 7 = 1$
2^1	$2^1 \,\%\, 7 = 2$
2^2	$2^2 \,\%\, 7 = 4$
2^3	$2^3 \,\%\, 7 = 1$
2^4	$2^4 \,\%\, 7 = 2$
2^5	$2^5 \,\%\, 7 = 4$
2^6	$2^6 \,\%\, 7 = 1$

The powers of 2 modulo 7 enter a cycle of length 3:

- 1, 2, 4, 1, 2, 4, 1, 2, 4, ...

What about other bases $a \in \{0, 1, \ldots, 6\}$? ($2^k$, 3^k, etc.)

Base a	Cycle length
0	1
1	1
2	3
3	6
4	3
5	6
6	2

order (cycle length)

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. We define the **order of a modulo n** to be the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$, when such a number exists.

We denote the order of a modulo n as $\mathrm{ord}_n(a)$.

For example, $\mathrm{ord}_7(2) = 3$ and $\mathrm{ord}_7(3) = 6$.

Consider $\mathbf{ord}_{17}(a)$—notice anything?

Base a	$\mathrm{ord}_{17}(a)$
0	1
1	1
2	8
3	16
4	4
5	16
6	16
7	16
8	8

Base a	$\mathrm{ord}_{17}(a)$
9	8
10	16
11	16
12	16
13	4
14	16
15	8
16	2

It seems that $\mathrm{ord}_{17}(a)$ is always a factor of 16...

Fermat's Little Theorem.

Let $p, a \in \mathbb{Z}$ and assume p is prime and that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

How can we extend this to non-prime numbers?

The **Euler totient function** (or **Euler phi function**) is defined as:

$$\varphi : \mathbb{Z}^+ \to \mathbb{N}$$

$$\varphi(n) = \left|\left\{a \mid a \in \{1, \ldots, n-1\} \text{ and } \gcd(a, n) = 1\right\}\right|$$

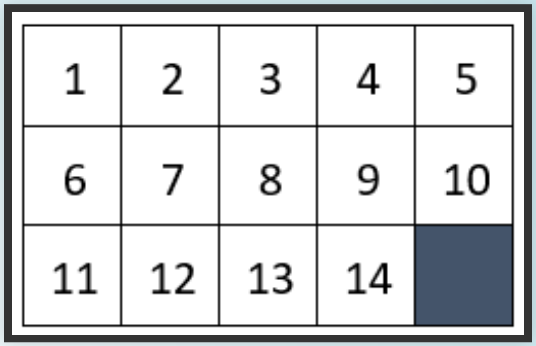
Examples

- $\varphi(5) = 4 \quad (\{1, 2, 3, 4\})$
- $\varphi(17) = 16 \quad (\{1, 2, \ldots, 16\})$
- For any prime number p, $\varphi(p) = p - 1 \quad (\{1, 2, \ldots, p - 1\})$

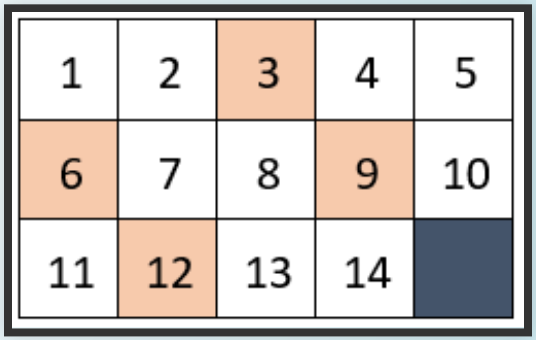
- $\varphi(6) = 2 \quad (\{1, 5\})$
- $\varphi(15) = 8 \quad (\{1, 2, 4, 7, 8, 11, 13, 14\})$

$\varphi(15)$

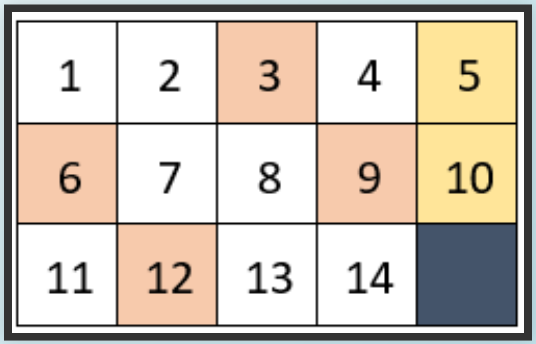
1. Start with $15 - 1 = 14$ numbers.



2. Remove the multiples of 3: $14 - 4 = 10$.



3. Remove the multiples of 5: $10 - 2 = 8$.



$\varphi(pq)$

Theorem. For all prime numbers $p, q \in \mathbb{Z}^+$, $\varphi(pq) = (p-1)(q-1)$.

Proof sketch.

- Start with $pq - 1$ numbers ($\{1, 2, \ldots, pq-1\}$).
- Remove the $(q-1)$ multiples of p.
  - $(pq-1) - (q-1)$
- Remove the $(p-1)$ multiples of q.
  - $(pq-1) - (q-1) - (p-1)$

The remaining count is:

$$\begin{aligned}(pq-1) - (q-1) - (p-1) &= pq - q - p + 1 \\ &= (p-1)(q-1)\end{aligned}$$

Generalizing Fermat's Little Theorem

Fermat's Little Theorem.
Let $p, a \in \mathbb{Z}$ and assume p is prime and that $p \nmid a$.
Then $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Theorem.
Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, and assume $\gcd(a, n) = 1$.
Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

We'll use Euler's Theorem next week in our study of cryptographic algorithms, so stay tuned!

Summary

Today you learned to...

1. Define modular equivalence.
2. State and prove some properties of modular equivalence.
3. Translate between a proof of existence and an algorithm.
4. Define the terms order and Euler totient function and state properties of these term.

Homework

- Readings:
  - From today: 7.4, 7.5
  - Next week: Chapter 8
- Work on Assignment 3
- Prep 7 to be posted after class today

Good luck with your MAT137 test!