Modular Arithmetic

Definition:

- Let $n \in \mathbb{N}, a \in \mathbb{Z}$, we define $a \bmod n$ to be the remainder when a is divided by n.

Exercise:

a) $10 \bmod 4 = 2$ ← Since $\frac{10}{4} = 2$ w/ remainder of 2
b) $18 \bmod 3 = 0$
c) $-8 \bmod 6 = 4$ ← Since $x = qn + r$, $-8 = (-2 \cdot 6) + r$, $r = 4$
d) $10 \bmod 1 = 0$ ← anything mod 1 is always 0

- a, b are **congruent modulo n**, written $a \equiv b \pmod{n}$, if $n|(a - b)$
- Equivalently, $a \equiv b \pmod{n}$ IFF $a \bmod n = b \bmod n$

Modular Equivalences

- Let a, b and n be integers and suppose $n > 1$. The following statements are all equivalent:
  - $n|(a - b)$
  - $a \equiv b \pmod{n}$
  - $a = b + kn$ for some integer k
  - $a \bmod n = b \bmod n$

Exercise:

True or false?

a) $154 \equiv 56 \pmod{11}$

$11|(154-56) \Leftrightarrow 11|98$ False

b) $7 \equiv -9 \pmod{8}$

$8|(7-(-9)) \Leftrightarrow 8|16$ True

Exercise:

Find x such that $12 \equiv x \pmod{5}$.

$5|(12-x)$, $\therefore x$ is any of $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$

Exercise:

If $m \equiv 0 \pmod{2}$, what can we say about m?

$2|(m-0)$, $\therefore m$ is an even number.

Theorem (Congruence Arithmetic):

- Let $n \in \mathbb{N}, a, b, c, d \in \mathbb{Z}$, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then:
  1) $(a + b) \equiv (c + d) \pmod{n}$;
  2) $(a - c) \equiv (c - d) (md\ n)$;
  3) $ab \equiv cd \pmod{n}$;
  4) $a^m \equiv c^m \pmod{n}\ \forall m \in \mathbb{N}$;

Proof:

$n \mid (a-c) \Rightarrow a - c = np,\ p \in \mathbb{Z}$

$n \mid (b-d) \Rightarrow b - d = nq,\ q \in \mathbb{Z}$

(1) $a + b = (np + c) + (nq + d) = n(p+q) + c + d$

$(a+b) \pmod n \equiv [\underbrace{n(p+q)}_{\text{mod } n \to 0} + c + d] \pmod n$

$\equiv (c+d) \pmod n$

(2) $a - b = (np + c) - (nq + d) = n(p-q) + (c-d)$

$(a-b) \pmod n \equiv [\underbrace{n(p-q)}_{\text{mod } n \to 0} + (c-d)] \pmod n$

$\equiv (c-d) \pmod n$

(3) $ab = (np + c)(nq + d) = n^2pq + npd + nqc + cd$

$= n(npq + pd + qc) + cd$

$ab \pmod n \equiv [\cancel{n(npq + pd + qc)} + cd] \pmod n$

$\equiv cd \pmod n$

(4) Induction

a) $m = 1$

$a^1 \equiv c^1 \pmod n$ ✓

b) Suppose $a^k \equiv c^k \pmod n$. Prove $a^{k+1} \equiv c^{k+1} \pmod n$

$a^{k+1} = a^k \cdot a$ and $c^{k+1} = c^k \cdot c$.

So by (3) $a^k \cdot a \equiv c^k \cdot c \pmod n \Rightarrow a^{k+1} \equiv c^{k+1} \pmod n$

$\therefore a^m \equiv c^m \pmod n \ \forall m \in \mathbb{N}$

Exercise:

a) Given that $2064 = 1715 + 349$, find $2064 \pmod{17}$

b) Given that $713064 = 803 \cdot 888$, find $713064 \pmod{8}$

c) Find x such that $3^9 \equiv x \pmod{5}$

a) $(a+b) \equiv (c+d) \pmod{n}$

$1715 \equiv 15 \pmod{17}$ since $17 \mid (1715 - 15)$ and,

$349 \equiv 9 \pmod{17}$ since $17 \mid (349 - 9)$.

$(1715 + 349) \equiv (15 + 9) \pmod{17}$.

$2064 \equiv 7 \pmod{17}$ since $17 \mid (2064 - 7)$ □

b) $ab \equiv cd \pmod{n}$

$803 \equiv 3 \pmod{8}$ and $888 \equiv 0 \pmod{8}$

$713064 \pmod{8} \equiv (803 \cdot 888) \equiv (3 \cdot 0) \pmod{8} \equiv 0 \pmod{8}$

c) $ab \equiv cd \pmod{n}$

$3^9 = 3^4 \cdot 3^4 \cdot 3 = 81 \cdot 81 \cdot 3$

$81 \equiv 1 \pmod{5}$

$81 \cdot 81 \cdot 3 \pmod{5} \equiv 1 \cdot 1 \cdot 3 \pmod{5} \equiv 3 \pmod{5}$

$\therefore x = 3$

Exercise:

Find the remainder when 7^8 is divided by 16.

$a^m \equiv c^m \pmod{n} \; \forall \; m \in \mathbb{Z}$

?

$7^8 = (7^4)^2$

$(7^4)^2 \bmod 16 = (7^4 \bmod 16)^2 \bmod 16$

$= (2401 \bmod 16)^2 \bmod 16$

$= (1)^2 \bmod 16$ (because $\frac{2401}{16} = 150 \text{ r } 1$)

$= 1 \bmod 16$

Theorem (Cancellation Law):

- Let $n \in \mathbb{Z}, a, b, c \in \mathbb{Z}$
- If $\gcd(a, n) = 1$ and $ab = ac (mod\ n)$, then $b \equiv c\ (mod\ n)$.

Proof:

$$ab \equiv ac \pmod n$$
$$(ab - ac) \equiv 0 \pmod n$$
$$a(b-c) \equiv 0 \pmod n$$

$\Rightarrow a(b-c) \equiv kn$ for some $k \in \mathbb{Z}$ but a and n are coprime by ⊛, so the factor of n on LHS is contained in $(b-c)$. Hence,

$$(b-c) \equiv 0 \pmod n$$
$$b \equiv c \pmod n$$

- NOTE: ⊛ is essential.

Counterexample:

$$60 \equiv 90 \pmod{15}$$
$$10 \cdot 6 \equiv 10 \cdot 9 \pmod{15}, \text{ but}$$
$$6 \not\equiv 9 \pmod{15}$$

Since 10 and 15 are not coprime, the cancellation law does not apply.

Exercise:

Given $10904 \equiv 32\ (mod\ 9)$, find the smallest $x \in \mathbb{N}$ such that $x \equiv 1363\ (mod\ 9)$.

$10904 = 1363 \cdot 8$

$8 \cdot 1363 \equiv 8 \cdot 4 \pmod 9$

$1363 \equiv 4 \pmod 9$ (Since 8 and 9 are coprime)

$\therefore x = 4$ ($4 < 9$, so there are no smaller congruence > 0)

Congruence Classes modulo n

- The quotient-remainder theorem gives us the following:

Fact:

- Let $n \in \mathbb{Z}$.
- Every integer $x \in \mathbb{Z}$ is congruent modulo n to exactly one element in $\{0, 1, 2, \dots, n-1\}$
- This allows us to group integers according to their remainders after dividing by n.

Definition:

- Let $n \in \mathbb{N}$.
- The **congruence class (residue)** of $a \in \mathbb{Z}$ *modulo* n is the set $[a] = \{x \in \mathbb{Z} : x \equiv a \ (mod\ n)\}$.

Exercise:

Write the congruence classes for $n = 4$. How many of them are there?

$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$ (since $4 \bmod 4 = 0$)
$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$ (since $5 \bmod 4 = 1$)
$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\}$ (since $-6 \bmod 4 = 2$)
$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\}$ (since $-5 \bmod 4 = 3$)

Note: $\underset{x}{-5} \bmod \underset{n}{4} = \underset{r}{3}$

$x = qn + r$

Theorem:

- Let $n \in \mathbb{N}$. There are exactly n distinct congruence classes: $[0], [1], \dots, [n-1]$.

Proof:

First, show that no two of $0, 1, \dots, n-1$ are congruent modulo n.
Let $0 \leq a < b < n, a, b \in \mathbb{N}$.
Then $b - a \in \mathbb{N}$ and $b - a < n$.
Thus, $n \nmid (b - a)$, so $b \not\equiv a \ (mod\ n)$.
Therefore, no two of $0, 1, \dots, n-1$ are congruent, and we have that $[0], [1], \dots, [n-1]$ are all distinct residues.

Next, show that every $x \in \mathbb{Z}$ is in one of these residues.
The Quotient-Remainder Theorem gives $x = nq + r, 0 \leq r < n$.
So, $r \in \{0, 1, \dots, n-1\}$, and $x - r = nq \Rightarrow x \equiv r \ (mod\ n)$.
Therefore, every $x \in \mathbb{Z}$ is in one of $[0], [1], \dots, [n-1]$.

Definition:

- Let $n \in \mathbb{N}$. The complete set of residues modulo n is the set.

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

Exercise:
$\mathbb{Z}_3 = \{[0], [1], [2]\}$.
In $\mathbb{Z}_3$, we have
$[4] = [1]; [-1] = [2]; [30] = [0]$

Exercise:
In $\mathbb{Z}_n$,

a) $[0] \cup [1] \cup \dots \cup [n-1] = \mathbb{Z}$
b) $[0] \cap [1] \cap \dots \cap [n-1] = \emptyset$

↑ No two elements are the same.

Operations on $\mathbb{Z}_n$

- We want to define addition and multiplication on $\mathbb{Z}_n$.
- Since different numbers can give the same residue, we must be careful with the definitions.

Theorem:

- Let $n \in \mathbb{N}$.
  The operation $+$:

$$[a] + [b] = [a + b]$$

is well-defined addition on $\mathbb{Z}_n$, i.e. if $[a] = [c]$ and $[b] = [d]$, then $[a + b] = [c + d]$.

Similarly, the operation $\cdot$:

$$[a][b] = [ab]$$

is well-defined multiplication on $\mathbb{Z}_n$, i.e. if $[a] = [c]$ and $[b] = [d]$, then $[ab] = [cd]$.

Proof:

$[a] = [c] \Rightarrow a \equiv c \ (mod\ n) \Rightarrow \exists\, k_1 \in \mathbb{Z} \ni a = c + k_1 \cdot n$
$[b] = [d] \Rightarrow b \equiv d \ (mod\ n) \Rightarrow \exists\, k_2 \in \mathbb{Z} \ni b \equiv d + k_2 \cdot n$

$a + b = (c + k_1 n) + (d + k_2 n) = c + d + n(k_1 + k_2)$
$\Rightarrow (a + b) \equiv (c + d) \ (mod\ n)$
$\therefore [a + b] = [c + d]$

$ab = (c + k_1 n)(d + k_2 n) = cd + n(k_2 c + k_1 d + n k_1 k_2)$
$\Rightarrow ab \equiv cd \ (mod\ n)$
$\therefore [ab] = [cd]$

Exercise:

Write addition and multiplication tables for $\mathbb{Z}_3$.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\swarrow [2]+[1] = 2+1 \pmod 3 = 0$

$\leftarrow [2]+[2] = 2+2 \pmod 3 = 1$

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$\leftarrow [2]\cdot[1] = 2\cdot 1 \pmod 3 = 2$

$\leftarrow [2]\cdot[2] = 2\cdot 2 \pmod 3 = 1$

Properties of $\mathbb{Z}_n$

1) $+$ and $\cdot$ are closed (binary) operations.
2) $+$ and $\cdot$ are commutative
3) $+$ and $\cdot$ are associative
4) $\cdot$ is distributive over $+$
5) Identities are [0] under $+$, [1] under $\cdot$
6) The additive inverse of $[x]$ is $[n-x]$
7) Multiplicative inverses exist only for $x \ni \gcd(x,n) = 1$

Theorem:

- If a and n are coprime, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \ (mod\ n)$.
- We call b the multiplicative inverse of a *modulo* n.
- b is unique modulo n.
- We write $b = a^{-1} (mod\ n)$.

Proof:

Consider the set $\{0, a, 2a, 3a, \dots, (n-1)a\}$.
If we can show that there are all distinct modulo n, then exactly one of them is equal to $1 \ (mod\ n)$.
Suppose the contrary: $\exists\ c, d \in \mathbb{N} \cup \{0\}, c, d < n \ni ca \equiv da \ (mod\ n), c \neq d$.
Then $(c-d)a \equiv 0 \ (mod\ n)$, so $\exists\ k \in \mathbb{Z} \ni (c-d)a = kn$.
But a and n are coprime, so $n|(c-d)$.
This is a contradiction, since c and d are distinct nonnegative integers less than n.

Exercise:

Find a multiplicative inverse of $43x$ *modulo* 60.

Given the theorem $ab \equiv 1 \pmod{n} \Rightarrow b = a^{-1} \pmod{n}$

Let $n = 60$, $b = 43$, $a = x$,

We need $x \in \mathbb{N} \ni 43x \equiv 1 \pmod{60}$

Notice that $43x$ must have a last digit of 1, since 60 is a multiple of 10. So any x such that $43x$ ends in 1 has last digit 7.

i.e. $61 \bmod 60 = 1$, $43 \cdot 7 = 301$ ← one option,
$43 \cdot 17 = 731$ ← another option

The possibilities are 7, 17, 27, 37, 47, 57,

$43 \cdot 7 = 301 \equiv 1 \pmod{60}$

$\therefore 43^{-1} = 7 \pmod{60}$

Exercise:

Find $3^{-1} (mod\ 40)$.

We need $x \in \mathbb{N} \ni 3x \equiv 1 \pmod{40}$ where $3^{-1} = x \pmod{40}$

$10 | 40 \rightarrow 3x$ must end in 1

$3 \cdot 7 = 21 \rightarrow x$ must end in 7

possibilities are 7, 17, 27, 37, 47.

$3 \cdot 7 = 21 \equiv 21 \pmod{40}$

$3 \cdot 17 = 51 \equiv 11 \pmod{40}$

$3 \cdot 27 = 81 \equiv 1 \pmod{40}$

$\therefore 3^{-1} = 27 \pmod{40}$

Application: Cryptography

- Cryptography is the study of methods for sending secrete messages.
- There are many techniques for encryption and decryption, one of which is **public-key cryptography**.
- The method uses big prime numbers and modular arithmetic.
- **RSA** is one such public-key method.

RSA

1) Choose 2 large primes p, q.
2) Choose $e \in \mathbb{Z}$ that is coprime with $(p-1)(q-1)$.
3) Choose $d \in \mathbb{Z} \ni ed \equiv 1\ (mod\ (p-1)(q-1))$.
4) The public key is (e, pq). This is available to everyone for encryption.
5) The private key is (d, pq). This is available only to those who the send wants to be able to decrypt.

Encryption Step:

- Let the message to be encrypted be $M \in \mathbb{Z}, 0 \leq M < pq$ (a computer uses binary code for everything, so encrypting integers is sufficient).
- The encrypted message is $C = M^e\ (mod\ pq)$.

Decryption Step:

- M is received by $M = C^d\ (mod\ pq)$.

- We will not see the proof.
- p and q are chosen to be several hundred digits long each, making it impossible for a computer to finds the factors $(p-1)(q-1)$ in reasonable time.
- We will see some examples with small primes.

Example:

Let $A = 1, B = 2, \ldots, Z = 26$, public key (3, 55). Encrypt and decrypt the message "HEY."

A: Given pub. key (e, pq), $pq = 55 \Rightarrow p = 5, q = 11$, $e = 3$ which is coprime with $(5-1)(11-1) = 40$.

$\gcd(3, 40) = 1$

Unencrypted method $H = 8$, $E = 5$, $Y = 25$.

Encryption: $C = M^e \pmod{pq}$

$8^3 = 64 \cdot 8 \equiv 9 \cdot 8 \pmod{55} = 72 \pmod{55} \equiv 17 \pmod{55}$

$5^3 = 125 \equiv 15 \pmod{55}$

$25^3 = 125 \cdot 125 \pmod{55} \equiv 15 \cdot 15 \pmod{55} = 225 \pmod{55} \equiv 5 \pmod{55}$

The encrypted message is 17, 15, 5

Decryption: $M = C^d \pmod{pq}$ or the inverse

From a previous example, $3^{-1} \pmod{40} = 27$.

$17^{27} = 289^{13} \cdot 17 \equiv 14^{13} \cdot 17 \pmod{55} = 196^6 \cdot 14 \cdot 17 \pmod{55} = 196^6 \cdot 238 \pmod{55}$

$\equiv 31^6 \cdot 18 \pmod{55} = 961^3 \cdot 18 \pmod{55} \equiv 26^3 \cdot 18 \pmod{55}$

$= 676 \cdot 468 \pmod{55} \equiv 16 \cdot 28 \pmod{55} = 448 \pmod{55}$

$\equiv 8 \pmod{55}$

So the decrypted 17 is 8, the original "H".

Similarly, 15 decrypts to 5, and 5 decrypts to 25.

Exercise:

Decrypt the message 41 83 36 that was encrypted with public key (5, 91).

$91 \quad pq = 91 \Rightarrow e = 5,\ p = 7,\ q = 13$

$7 \quad 13 \quad (13-1)(7-1) = 72$

$d = 5^{-1} \pmod{72} \leftarrow d \text{ s.t. } 5d \equiv 1 \pmod{72}$