Chinese Remainder Theorem (CRT)

Used to solve systems of simultaneous congruence equations.

Two types:
1. Two or more linear congruence equations in one variable but different moduli.
2. Two or more linear congruence equations in more than one variable but same modulus.

Theorem: Let \( m_1, m_2, \ldots, m_s \in \mathbb{Z}^{>0} \) be relatively prime integers. Then the system of congruences

\[
\begin{align*}
    x &\equiv a_1 \pmod{m_1}, \\
    x &\equiv a_2 \pmod{m_2}, \\
    &\quad \quad \ddots \\
    x &\equiv a_s \pmod{m_s}
\end{align*}
\]

has a unique solution modulo \( M = m_1 \cdot m_2 \cdot \cdots \cdot m_s \).

Idea of proof: Let \( M_k = \frac{M}{m_k} = m_1 \cdot m_2 \cdot \cdots \cdot m_{k-1} \cdot m_{k+1} \cdots m_s \) \((m_k \text{ omitted})\) and \((M_k, M_k) = 1\).

\( \Rightarrow \) \exists a modular inverse \( y_k \) of \( M_k \) mod \( m_k \), i.e.

\[ M_k y_k \equiv 1 \pmod{m_k}. \]

Solution of the system:

\[ x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_s M_s y_s. \]
Eg. Find solution for $x \equiv 1(2)$, $x \equiv 2(3)$,

$x \equiv 3(5)$.

$a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $m_1 = 2$, $m_2 = 3$, $m_3 = 5$.

$M = m_1 m_2 m_3 = 2 \times 3 \times 5 = 30$,

$M_1 = 15$, $M_2 = 20$, $M_3 = 18$.

$15y_1 \equiv 1(2)$, $20y_2 \equiv 1(3)$, $18y_3 \equiv 1(5)$

$y_1 = 1$, $y_2 = 1$, $y_3 = 1$.

Solve: $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \equiv m_1 m_2 m_3 = M$

$= 1 \cdot 15 \cdot 1 + 2 \cdot 20 \cdot 1 + 3 \cdot 1 \cdot 18 = 15 + 40 + 54 = 53$

$= 15 + 20 + 18$.

$y = \{53\} \mod 30$, hence $x \equiv [53] \mod 30$ is a solution.

$x \equiv 23(30)$ is a solution.

$23 \equiv 1(2)$; $23 \equiv 2(3)$; $23 \equiv 3(5)$.

Lemma: If $a, b \in \mathbb{Z}^+$, then the least positive residue of $2^a - 1$ modulo $2^b - 1$ is $2^x - 1,$

where $x$ is the least positive residue of $a \mod b$.

$[a \equiv x(b) = 2^x - 1 \equiv 2^a - 1 (2^{x^b} - 1)$.
By division algorithm, we have $a = bq + r$, where $r$ is the least positive residue of $a$ mod $b$; $0 \leq r \leq b$.

$$2^a - 1 = 2^b - 1 = (2^b - 1)(2^{a-b} + 2^{a-2b} + \ldots + 2 + 1) + (2^r - 1)$$

Eq.: $a = 3, b = 2; \quad 3 = 2 \cdot 1 + 1, \quad q = 1, \quad r = 1$.

$$(2^3 - 1) = (2^2 - 1)(2^1) + (2^1 - 1)$$

$4 = 3 \cdot 2 + 1 = 6 + 1$.

$$\Rightarrow 2^a - 1 \equiv (2^1)^b \mod (2^1 - 1).$$

Lemma: If $a$ and $b$ are positive integers, then the gcd of $2^a - 1$ and $2^b - 1$ is $2 - 1$.

$$(2^a - 1, 2^b - 1) = 2 - 1.$$ 

Pf: Use division algorithm and definition of gcd.

Theorem: The positive integers $2^a - 1$ and $2^b - 1$ are relatively prime if and only if $(a, b) = 1$. 
Example: Find the least positive residue of 1! + 2! + ... + 10! mod 23.

Answer:

4! = 24 ≡ 1 (23), 5! = 5 × 4! ≡ 5 × 1 (23)
6! ≡ 7 (23), 7! ≡ 3 (23), 8! ≡ 1 (23),
9! ≡ 9 (23), 10! = 3 × 2 = 6 (23), 10! ≡ 2 (23)

1! + 2! + ... + 10! ≡ 1 + 2 + 6 + 1 + 5 + 7 + 3 + 1 +
+ 9 * 2 (23)

≡ 33 (23) ≡ 10 (23)

5.1. Divisibility Test: Tests to decide when an integer n is divisible by another integer m.
- m = 2: Even numbers are divisible by 2.
  Unit digit ∈ \{0, 2, 4, 6, 8\}.
- m = 3: Sum of all digits should be divisible by 3.
- m = 5: Unit digit ∈ \{0, 5\}.
- m = 9: Sum of all digits in the number n should add up to a multiple of 9.
- m = 11: Sum of the two alternating sets of digits should be equal.
\[ e^8 \cdot 20468 \equiv 0 \ (2) \]

- \( m = 4 \): The last two digits of the number \( n \) should be divisible by 4.

\[ 20468 \equiv 0 \ (4) \quad \text{and} \quad 20362 \not\equiv 0 \ (4) \]

- \( m = 3 \): \[ 30651 \rightarrow 3 + 6 + 5 + 1 = 6, \ 3 \mid 6 \]

\[ \Rightarrow 30651 \equiv 0 \ (3) \]

- \( m = 9 \): \[ 654327 \rightarrow 6 + 5 + 4 + 3 + 2 + 7 = 27 \]

\[ 654327 \equiv 0 \ (9) \]

- \( m = 11 \): \[ 4573821 \rightarrow 4 + 5 + 7 + 3 + 8 + 2 + 1 = 30 \]

\[ 3 \mid 30, \ 9 \nmid 30 \]

\[ 4573821 \equiv 0 \ (3) \quad \text{and} \quad \not\equiv 0 \ (9) \]

- \( m = 11 \): \[ n = a_1, a_2, \ldots, a_k \]

\[ a_1 + a_3 + a_5 + \ldots = a_2 + a_4 + a_6 + \ldots \]

- \( m = 11 \): \[ 1 + 1 = 2, \ 11 \mid 121, \ 121 = 11 \times 11 \]

- \( m = 11 \): \[ 1, 0, 8, 6, 3, 2, 0, 0, 1, 5 \equiv 0 \ (1) \]

- \( m = 11 \): \[ 1 + 8 + 3 + 0 + 1 = 13, \ 1 + 6 + 2 + 0 + 5 = 13 \]
Simultaneous divisibility by 7, 11, 13:

\[ 7 \times 11 \times 13 = 1001 = 1000 + 1 \]

\[ 1000 \equiv -1 \mod 1001 \]

To test for simultaneous divisibility by 7, 11, 13:

1. Group the digits in the number into groups of three digits, starting from right (unit place).
2. Alternate sum of the groups (+ - + - ...)
3. This final alternate sum should be divisible by 7, 11, 13.

**Example:**

\[ \underline{2458456} \quad 456 - 458 + 2 = 0 \]

- 2\underline{458}\underline{456} \quad 7/0, 11/0, 13/0
- 2458\underline{456} \equiv 0 \begin{pmatrix} 4 \text{ } \\ 11 \text{ } \\ 13 \end{pmatrix}

\[ \underline{515970} \quad 970 - 515 = 455 \]

- 5\underline{159}\underline{70} \quad 11 \times 455
- 455 = 7 \times 65 = 7 \times 5 \times 13

\[ \underline{515970} \equiv 0 \begin{pmatrix} 7 \text{ } \\ 11 \text{ } \\ 13 \end{pmatrix} \]
Representation of Integers in Different Bases:

Decimal Integers Representation: \(0, 1, 2, \ldots, 9\)

\[ (1547)_{10} \text{ Base } 10 = 1 \times 10^3 + 5 \times 10^2 + 4 \times 10^1 + 7 \times 10^0 \]
\[ = 1000 + 500 + 40 + 7 = 1547 \]

Theorem: Let \( b \in \mathbb{Z}^+, \ b > 1 \). Then every positive integer \( n \) can be written uniquely in the form

\[ n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 \]

where \( 0 \leq a_i \leq b-1 \), \( a_k \neq 0 \)

Notation: \( n = (a_k, a_{k-1}, \ldots, a_1, a_0) \)\( b \)

For the proof, use division algorithm successively dividing \( n \) by \( b \):

\[ n = b q_0 + a_0 , \quad 0 \leq a_0 \leq b-1 \]
\[ q_0 = b q_1 + a_1 , \quad a \leq a_1 \leq b-1 \]

This ends with \( 0 \) as a quotient.
Example: $(541)_3$

\[541 = 3 \times 180 + 1\]
\[180 = 3 \times 60 + 0\]
\[60 = 3 \times 20 + 0\]
\[20 = 3 \times 6 + 2\]
\[6 = 3 \times 2 + 0\]

Stop when the quotient is < 6.

\[(541)_3 = (202001)_3\]

Left to right

\[2 \times 3^5 + 0 \times 3^4 + 2 \times 3^3 + 0 \times 3^2 + 0 \times 3^1 + 1 \times 3^0\]

\[= (2 \times 243) + 0 + (0 \times 27) + 0 + 0 + 1\]

\[= 486 + 54 + 1 = 541\]

Express $(11101101)_2$ as an integer.

\[(11101101)_2 \rightsquigarrow (237)_{10}\]

\[= (1 \times 2^7) + (1 \times 2^6) + (1 \times 2^5) + (0 \times 2^4) + (1 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0)\]

\[= 128 + 64 + 32 + 0 + 8 + 4 + 0 + 1\]

\[= 237\]
Base 16 → Hexadecimal or Hex
8 → Octal
0, 1, ... 9, A, B, C, D, E, F

\[ (A5BEC)_{16} \rightarrow (?)_{10} \]

\[ A \times 16^4 + B \times 16^3 + 5 \times 16^2 + E \times 16 + C \times 1 \]

\[ 10 \times 16^4 + 11 \times 16^3 + 5 \times 16^2 + 14 \times 16 + 12 \]

655360 + 49152 + 1280 + 64 + 12

Hex → Binary: Each hexadecimal digit corresponds to a four-digit block of 0s and 1s (binary expression).
\[ \text{Eq: } (ABCDEF)_{16} = (\_?\_)_2 \]
\[ = (1010101111001101111101111)_2 \]
\[ (\_?\_)_2 \rightarrow (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)_{16} \]

Binary \rightarrow Hexadecimal

Start with the binary expression. Group them into blocks of 4, use the corresponding hexadecimal digit for each block.

\[ \text{Eq: } (100110100000010111)_2 = (\_GAOB\_)_{16}. \]

\[ 9A0B \]

Divisibility Tests for Base \( b \) representation:

Theorem 1: If \( d | b \) and \( j, k \in \mathbb{Z}^+ \) with \( j < k \),
then \((a_k a_{k-1} \ldots a_{j+1} a_j a_{j-1} \ldots a_0)_b\) is divisible by \( d^j \) if and only if \((a_{j-1} \ldots a_{j+1} a_j a_{k-1} \ldots a_k)_b\) is divisible by \( d^k \).
Theorem 2: If \( d \mid b+1 \), then \( n = (a_k \ldots a_0)_b \) is divisible by \( d \) if and only if the sum of the digits \( a_k + a_{k-1} + \ldots + a + a_0 \) is divisible by \( d \).

\[ \text{ex}: \ (3E2A235)_6 \quad \text{Does 3 divide this?} \]

\[ b=16, \ d=3, \ b-1=15 \quad 2 \equiv 3 \mid 15 \]

\[ 3 + E + A + 2 + 3 + 5 = 3 + 14 + 10 + 2 + 3 + 5 = 37 \]
\[ 3 \mid 37, \text{ hence } 3 \mid (3E2A235)_6 \]

\[ \text{ex}: \text{ Find the highest power of } 2 \text{ dividing } (101111110)_2 \]

By Theorem 1, the power of 2 dividing this number = number of zeros at the end of its binary expression \( \Rightarrow 2^4 \text{ is the largest power of } 2 \).

Theorem 3: If \( d \mid b+1 \), then \( n = (a_k \ldots a_0)_b \) is divisible by \( d \) if and only if the alternating sum of digits is divisible by \( d \).

\[ \text{ex}: \ (1010000011)_2 \quad \text{divisible by 3?} \quad d=3, \ 3 \mid b+1 = 3 \]
\[ 1 - 0 + 1 - 0 + 0 - 0 + 0 + 1 - 1 = 2, \ 3 \nmid 2 \]

Hence given number is not divisible by 3.
Eq: Is $(101000100)_2$ divisible by 3?

$1-0+1-0+0-0+1-0+0 = 3$, yes.

5.5: Check Digits

Idea: To use congruences to check for errors in strings of digits. Typically used in error detection while transmission of number strings or in representing computer data.

Eq: Want to transmit a bit string

$x_1, x_2, \ldots, x_n$, $x_i$'s are 0 or 1.

Introduce a parity check $x_{n+1}$

$x_{n+1} = \sum_{i=1}^{n} x_i \mod 2$

$x_{n+1}$ → Parity check digit.
CHECK DIGITS

Eq. Want to transmit a bit string \( x_1 x_2 \ldots x_n \), \( x_i \)'s are 0 or 1.

Introduce a parity check bit \( x_{n+1} \):
\[
x_{n+1} = \sum_{i=1}^{2^n} x_i \quad (2)
\]

Send: \( x_1, x_2, \ldots, x_n \) \[\boxtimes\] 
Received: \( y_1, y_2, \ldots, y_n, y_{n+1} \)

Proper transmission \( \iff x_i = y_i \quad 1 \leq i \leq n \).

If \( \sum_{i=1}^{n} x_i \neq \sum_{i=1}^{n} y_i \), then signals an error.

Caution: However \( \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i \), (2) does not ensure error-free ness.

Eq. Suppose you receive the following bit string where the last one is the parity check bit. Has there been an error in transmission?

\[\begin{array}{cccccccc}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}\] Eight ones, \( \sum_{i=1}^{8} = 0 \) (2)

Since \( 8 \equiv 0 \pmod{2} \), the parity check bit should be zero, hence error in transmission.

Eq: Use of check digits to detect errors in passport number

Passport Number: \( n_1, n_2, n_3, n_4, n_5, n_6 \) (6-digit)
Introduce a 7th digit $x_7$ by defining

$$x_7 = 7x_1 + 3x_2 + x_3 + 7x_4 + 3x_5 + x_6$$

Last check digit $x_7$ is taken mod 10.

E.g.: 330011[8] To check validity, need to check whether

$$8 \equiv 7(3) + 3(3) + 0 + 7(0) + 3(1) + 1$$

$$21 + 9 + 3 + 1 = 34$$

34 $\equiv$ 4 (10); does not agree with check digit, hence an invalid passport.

**ISBN:** Identifying books by a unique number

ISBN - 10/13/15

ISBN - 10: Ten digits; the last one (10th digit) is a check digit.

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_9 & x_{10} \end{bmatrix} : x_{10} \text{ is a base 11 digit}$$

$x_1, \ldots, x_9$ are decimal digits

Base 11 digits: $(0, 1, 2, \ldots, 9, x)$

$$x_{10} = \sum_{i=1}^{10} x_i \mod 11$$
Example: 1) Suppose that an ISBN code has 10 digits and the eleventh digit is a check digit. Find the check digit if the number given is
\[ 2-1354001 \]

Use the above formula.

\[ 1 \cdot 2 + 2 \cdot 1 + 3 \cdot 1 + 4 \cdot 3 + 5 \cdot 5 + 6 \cdot 4 + 0 \cdot 0 + 0 \cdot 0 + 9 \cdot 1 \]

\[ = 2 + 2 + 3 + 12 + 25 + 24 + 9 \]

\[ = 77 \equiv 0 \pmod{11} \] Hence check digit is 0.

2) Is the ISBN code 0-404-50874-X valid where the 10th digit X is the check digit.

\[ 1 \cdot 0 + 2 \cdot 4 + 3 \cdot 0 + 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 0 + 7 \cdot 8 + 8 \cdot 7 + 9 \cdot 4 \]

\[ = 8 + 16 + 25 + 56 + 50 + 72 \]

\[ = 49 + 112 + 36 = 197 \]

\[ 197 \equiv 10 \pmod{11} \] Hence a valid ISBN code.
Eg: Find five consecutive integers and an integer n such that n! ends exactly with 74 zeroes, as does the other consecutive integers of n!, i.e., (n+1)! , (n+2)! , ... , (n+5)! should all end with exactly 74 zeroes.

Suppose n! ends exactly with 74 zeroes.

Then \( 100 \mid n! \). As there are more multiples of 2 than 5 in the integers \{1, 2, ..., m\}, we need only concern ourselves with the fact that \( 5^{74} \mid n! \).

Aim: To find an n such that

\[ 74 = \left[ \frac{n}{5} \right] + \left[ \frac{n}{5^2} \right] + \left[ \frac{n}{5^3} \right] \]

Eg. \( n = 300 \); \( \left[ \frac{n}{5} \right] = 60 \), \( \left[ \frac{300}{5^2} \right] = \left[ \frac{300}{25} \right] = 12 \)
\( \left[ \frac{300}{5^3} \right] = \left[ \frac{300}{125} \right] = 2 \); \( 60 + 12 + 2 = 74 \).

\( n = 200 \) does not work:
\( \left[ \frac{200}{5} \right] = 40 \), \( \left[ \frac{200}{25} \right] = 8 \)
\( 40 + 8 + 2 = 50 \).
Hence $300!$ ends with 74 zeroes; same is true for $301!, 302!, 303!, 304!$ all end 74 zeroes.

6.1: Congruences with practical and theoretical significance.

Wilson's Theorem: If $p$ is a prime, then

$$(p-1)! \equiv -1 \pmod{p}.$$ 

Proof: OK for $p=2$, since $\frac{1}{2} \equiv -1 \pmod{2}$.

Let $p$ be a prime $>2$ and let $a$ be an integer $s.t.$ $1 \leq a \leq p-1$. Then $a$ has a modular inverse $\overline{a} \pmod{p}$; i.e. since $(a,p)=1$

$$a \overline{a} \equiv 1 \pmod{p}.$$ 

Also the only positive integers $a < p$ s.t. $a^2 \equiv 1 \pmod{p}$ are 1 and $p-1$. The $(p-3)$ integers in $1 < a < p-1$ can be grouped into pairs $(a, \overline{a})$, where $\overline{a}$ is the modular inverse of $a \pmod{p}$. There are $\frac{(p-3)}{2}$ such pairs. The product of elements in any such pair is $\equiv 1 \pmod{p}$. Taking the product over all these pairs we get

$$2 \cdot 3 \cdot 4 \cdots (p-3)(p-2) \equiv 1 \pmod{p}.$$ 

Multiply both sides by $p$ and $(p-1)$ to get $p! = p-1 \pmod{p} \equiv -1 \pmod{p}.$
\[ p = 23, \quad p-1 = 22, \quad 22! = -1 \pmod{23} \]

\[ p = 7, \quad p-1 = 6, \quad 6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1 \]

\[ 6! = 30 \times 12 \times 2 = 360 \times 2 = 720 \]

\[ 720 \equiv -1 \pmod{7} \quad \text{as} \quad 7 \mid 721 \]

\[ 7 	imes 103 = 721. \]

**Theorem:** If \( n \) is a positive integer with \( n \geq 2 \) such that \( (n-1)! \equiv -1 \pmod{n} \), then \( n \) is a prime.

**Example:** \( n = 8 \), \( (8-1)! = 7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \)

\[ = 5040 \]

\[ 5040 - 1 = 5039 \text{ and } 8 \nmid 5039 \]