Chinese Remainder Theorem

Michael Levin

Computer Science Department, Higher School of Economics

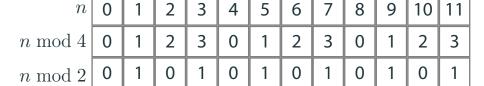
Outline

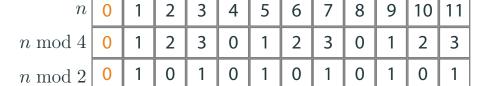
Remainders

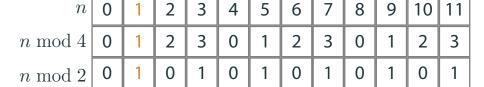
Chinese Remainder Theorem

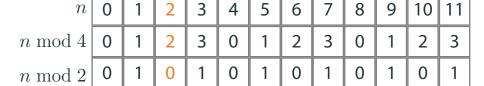
Remainders

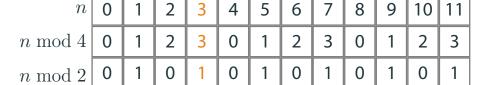
- Properties of remainders
- When remainder modulo \boldsymbol{a} defines remainder modulo \boldsymbol{b}
- When remainders modulo \boldsymbol{a} and \boldsymbol{b} are independent

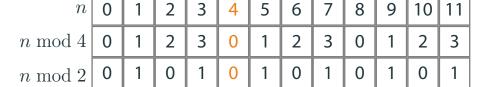


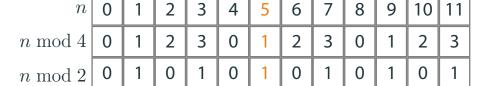




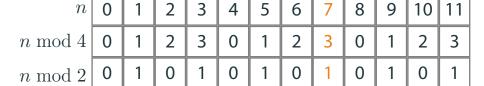




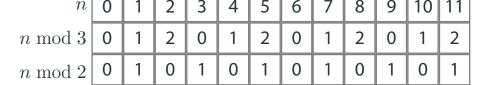




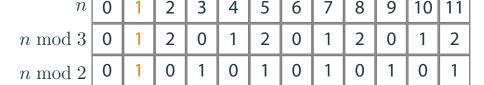




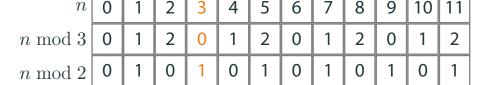
- $n \mod 4$ defines $n \mod 2$!
- Indeed, if $n_1\equiv n_2 \bmod 4$, then $4\mid (n_1-n_2)$, so $2\mid (n_1-n_2)$ and $n_1\equiv n_2 \bmod 2$

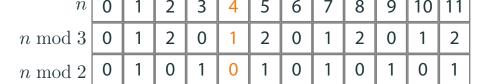


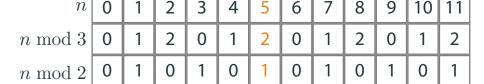














- $n \mod 3$ doesn't define $n \mod 2$
- All pairs of remainders are possible
- One remainder doesn't give information about another

• Divisibility by 2: the last digit is even

- Divisibility by 2: the last digit is even
- Divisibility by 5: the last digit is 0 or 5 (5 divides the last digit)

- Divisibility by 2: the last digit is even
- Divisibility by 5: the last digit is 0 or 5 (5 divides the last digit)
- The last digit is the remainder after division of $n \ \mbox{by} \ 10$

- Divisibility by 2: the last digit is even
- Divisibility by 5: the last digit is 0 or 5 (5 divides the last digit)
- The last digit is the remainder after division of $n \ \mbox{by} \ 10$
- $10 = 2 \cdot 5$

- Divisibility by 2: the last digit is even
- Divisibility by 5: the last digit is 0 or 5 (5 divides the last digit)
- The last digit is the remainder after division of $n \ \mbox{by} \ 10$
- $10 = 2 \cdot 5$
- Divisibility by 3: the sum of digits is divisible
 by 3 is not determined just by the last digit

Remainders

Lemma

If n_1 and n_2 have the same remainders modulo b and $a \mid b$, then n_1 and n_2 have the same remainders modulo a.

Proof

•
$$n_1 \equiv n_2 \bmod b \Rightarrow b \mid (n_1 - n_2)$$

Proof

•
$$n_1 \equiv n_2 \mod b \Rightarrow b \mid (n_1 - n_2)$$

•
$$b \mid (n_1 - n_2), a \mid b \Rightarrow a \mid (n_1 - n_2)$$

Proof

•
$$n_1 \equiv n_2 \mod b \Rightarrow b \mid (n_1 - n_2)$$

•
$$b \mid (n_1 - n_2), a \mid b \Rightarrow a \mid (n_1 - n_2)$$

•
$$a \mid (n_1 - n_2) \Rightarrow n_1 \equiv n_2 \bmod a$$

Problem

If $n \equiv 1 \mod 6$, then what can be $n \mod 4$?

- If n is even, then the remainder modulo 6 can be only 0,2 or 4

- If n is even, then the remainder modulo 6 can be only 0,2 or 4
- So n is odd, and $n \mod 4$ can be either 1 or 3

- If n is even, then the remainder modulo 6 can be only 0,2 or 4
- So n is odd, and $n \mod 4$ can be either 1 or 3
- If n = 1, then $n \equiv 1 \mod 6$ and $n \equiv 1 \mod 4$

- If n is even, then the remainder modulo 6 can be only 0,2 or 4
- So n is odd, and $n \mod 4$ can be either 1 or 3
- If n = 1, then $n \equiv 1 \mod 6$ and $n \equiv 1 \mod 4$
- If n=7, then $n\equiv 1 \bmod 6$ and $n\equiv 3 \bmod 4$

- If n is even, then the remainder modulo 6 can be only 0,2 or 4
- So n is odd, and $n \mod 4$ can be either 1 or 3
- If n = 1, then $n \equiv 1 \mod 6$ and $n \equiv 1 \mod 4$
- If n = 7, then $n \equiv 1 \mod 6$ and $n \equiv 3 \mod 4$
- So $n \mod 4$ can be either 1 or 3

- Remainders modulo 4 and 6 are dependent
- This is because 2 is their common divisor
- In general, if $d\mid a$ and $d\mid b$, then remainders modulo a and b are dependent
- It turns out that if $\mathrm{GCD}(a,b)=1$, then the remainders modulo a and b are independent

— see the next video

Outline

Remainders

Chinese Remainder Theorem

Chinese Remainder Theorem

Theorem

If $\operatorname{GCD}(a,b)=1$, then for any remainder r_a modulo a and any remainder r_b modulo b there exists integer n, such that $n\equiv r_a\pmod a$ and $n\equiv r_b\pmod b$. If n_1 and n_2 are two such integers, then $n_1\equiv n_2\pmod ab$.

In Other Words

Consider all ab remainders modulo ab:

$$0, 1, 2, \ldots, ab-1$$

Every such remainder r corresponds to a pair of remainders (r_a, r_b) :

$$r \equiv r_a \mod a, r \equiv r_b \mod b$$

Claim: if we consider pairs corresponding to each r, then each of the possible ab pairs (r_a, r_b) appears exactly once.

First, let us prove that if n_1 and n_2 correspond to the same pair (r_a, r_b) , then $n_1 \equiv n_2 \mod ab$:

• $n_1 \equiv r_a \equiv n_2 \pmod{a}$

First, let us prove that if n_1 and n_2 correspond to the same pair (r_a, r_b) , then $n_1 \equiv n_2 \bmod ab$:

- $n_1 \equiv r_a \equiv n_2 \pmod{a}$
- $n_1 \equiv n_2 \pmod{a} \Rightarrow a \mid (n_1 n_2)$

First, let us prove that if n_1 and n_2 correspond to the same pair (r_a, r_b) , then $n_1 \equiv n_2 \mod ab$:

- $n_1 \equiv r_a \equiv n_2 \pmod{a}$
- $n_1 \equiv n_2 \pmod{a} \Rightarrow a \mid (n_1 n_2)$
- Similarly, $b \mid (n_1 n_2)$

First, let us prove that if n_1 and n_2 correspond to the same pair (r_a, r_b) , then $n_1 \equiv n_2 \mod ab$:

- $n_1 \equiv r_a \equiv n_2 \pmod{a}$
- $n_1 \equiv n_2 \pmod{a} \Rightarrow a \mid (n_1 n_2)$
- Similarly, $b \mid (n_1 n_2)$
- a and b are coprime and both divide (n_1-n_2) , so $ab \mid (n_1-n_2)$

First, let us prove that if n_1 and n_2 correspond to the same pair (r_a, r_b) , then $n_1 \equiv n_2 \mod ab$:

- $n_1 \equiv r_a \equiv n_2 \pmod{a}$
- $n_1 \equiv n_2 \pmod{a} \Rightarrow a \mid (n_1 n_2)$
- Similarly, $b \mid (n_1 n_2)$
- a and b are coprime and both divide (n_1-n_2) , so $ab \mid (n_1-n_2)$
- $ab \mid (n_1 n_2) \Rightarrow n_1 \equiv n_2 \pmod{ab}$

Corollary

- Different r lead to different pairs (r_a, r_b)
- This already proves the first part of the theorem
- The number of remainders r modulo ab is ab, and the number of pairs of remainders (r_a,r_b) is also $a\cdot b=ab$
- Each r corresponds to unique (r_a, r_b) , so each pair (r_a, r_b) corresponds to unique r
- We will also show a constructive proof

• GCD(a, b) = 1, so 1 = ax + by for some integer x, y

- GCD(a, b) = 1, so 1 = ax + by for some integer x, y
- $ax \equiv 1 \pmod{b}$, $by \equiv 1 \pmod{a}$

- GCD(a, b) = 1, so 1 = ax + by for some integer x, y
- $ax \equiv 1 \pmod{b}$, $by \equiv 1 \pmod{a}$
- Thus ax corresponds to pair of remainders (0,1), and by corresponds to (1,0)

- GCD(a, b) = 1, so 1 = ax + by for some integer x, y
- $ax \equiv 1 \pmod{b}$, $by \equiv 1 \pmod{a}$
- Thus ax corresponds to pair of remainders (0,1), and by corresponds to (1,0)
- Combine: $(r_a, r_b) = r_a \cdot (1, 0) + r_b \cdot (0, 1)$

- $\operatorname{GCD}(a,b)=1$, so 1=ax+by for some integer x,y
- $ax \equiv 1 \pmod{b}$, $by \equiv 1 \pmod{a}$
- Thus ax corresponds to pair of remainders (0,1), and by corresponds to (1,0)
- Combine: $(r_a,r_b)=r_a\cdot (1,0)+r_b\cdot (0,1)$
- Consider $n = r_a by + r_b ax$

- GCD(a, b) = 1, so 1 = ax + by for some integer x, y
- $ax \equiv 1 \pmod{b}$, $by \equiv 1 \pmod{a}$
- Thus ax corresponds to pair of remainders (0,1), and by corresponds to (1,0)
- Combine: $(r_a, r_b) = r_a \cdot (1, 0) + r_b \cdot (0, 1)$
- Consider $n = r_a by + r_b ax$
- $n = r_a by + r_b ax \equiv r_a by \equiv r_a \pmod{a}$

- $\operatorname{GCD}(a,b)=1$, so 1=ax+by for some integer x,y
- $ax \equiv 1 \pmod{b}$, $by \equiv 1 \pmod{a}$
- Thus ax corresponds to pair of remainders (0,1), and by corresponds to (1,0)
- Combine: $(r_a, r_b) = r_a \cdot (1, 0) + r_b \cdot (0, 1)$
- Consider $n = r_a by + r_b ax$
- $n = r_a by + r_b ax \equiv r_a by \equiv r_a \pmod{a}$
- $n = r_a b y + r_b a x \equiv r_b a x \equiv r_b \pmod{b}$

Algorithm

The proof gives us this simple algorithm to find such n:

- Use extended Euclid's algorithm to find such x,y that ax+by=1
- Take $n = r_a \cdot by + r_b \cdot ax$

More Modules

What about the case of 3 modules a, b and c?

More Modules

What about the case of 3 modules a, b and c?

Turns out, if all pairs (a,b), (a,c) and (b,c) are coprime, then remainders modulo a,b and c uniquely determine remainder modulo abc.

More Modules

What about the case of 3 modules a, b and c?

Turns out, if all pairs (a,b), (a,c) and (b,c) are coprime, then remainders modulo a,b and c uniquely determine remainder modulo abc.

To prove, first go from remainders modulo a and b to remainder modulo ab, then go from remainders modulo ab and c to remainder modulo abc.

Computations with Large Integers

Instead of large integers, we can work with their remainders modulo several big prime numbers: if $0 \le n_1, n_2 < p_1 p_2 \dots p_k$, and $n_1 \equiv n_2 \bmod p_i$ for all i, then $n_1 = n_2$.

In this form, it would be fast to sum and multiply large integers, but hard to compare. This is actually used to speed up computations.

Conclusion

- Remainder modulo n uniquely determines remainder modulo any divisor of n
- Remainders modulo a and b are independent if and only if GCD(a,b)=1
- Remainders modulo coprime a and b uniquely determine remainder modulo ab
- Algorithm for constructing remainder modulo ab given remainders modulo coprime a and b
- Extends to more modules if every pair is coprime