1. Equivalence mod m
2. Modular Arithmetic
3. Using mod "tricks" to simplify calculations

10/12/23

L14: Modular Arithmetic -- ANSWERS

Definitions of mod

①

Remainder mod: a mod m

- a **mod** m is the integer in {0, …, m-1} which is the remainder when a is divided by m

②

Modular Equivalence: $a \equiv b \pmod m$

$a \equiv b \pmod m$ means

- a and b have the same remainder when divided by m
- $a - b$ is a multiple of m
- There is an integer k such that $a = b + km$

③

Relating the two mods

$a \equiv b \pmod m$ means $a \bmod m = b \bmod m$

Warm Up Exercises

$((3 \times 7) + 4) \bmod 7 = 4$

1. (a) 8 mod 5 = 3 (b) $(25 \bmod 7)^2 = (4)^2 = 16$

2. T / F $27 \equiv 32 \pmod 5$ — $5 \times 5 + 2$, $5 \times 6 + 2$

   T / F $27 \equiv 2 \pmod 5$ — $5 \times 5 + 2$, $5 \times 0 + 2$

   T / F $27 \equiv -3 \pmod 5$ — $5 \times 5 + 2$, $5 \times (-1) + 2$

   T / F $28 \equiv 1 \pmod 9$ — $9 \times 3 + 1$, $9 \times 0 + 1$

   negative ints should also be included!

3. Find 3 numbers, including at least one negative number, that are equivalent to 30 (mod 9):

   21≡ 3 ≡ -6 ≡ -24 ≡ 129 ≡ 30 (mod 9), for example

Summary: Algebra vs. Modular Arithmetic

	Algebra	Modular Arithmetic
Domain	real numbers	integers
We care about	Equality ex: x = y	Equivalence with respect to a modulus m ex: x ≡ y (mod m)
How many unique numbers?	Infinitely many ex: -153.21, 76, $\sqrt{2}$	The are only unique numbers in mod m are: $0, 1, \ldots, m-1$
Valid arithmetic operations	+ : addition – : subtraction × : multiplication ÷ : division	+ : addition – : subtraction × : multiplication **NO DIVISION**

③ Suppose
$a \equiv b \pmod m$
$c \equiv d \pmod m$
$\Rightarrow$
$a+c \equiv b+d \pmod m$
$a-c \equiv b-d \pmod m$
$ac \equiv bd \pmod m$

apply

Mod "tricks" Exercises

1. Find the value of $(592)^4(1033)^2 \ mod\ 5$

   In mod 5,

   $$(592)^4(1033)^2 \equiv (2)^4(3)^2 \pmod 5$$
   $$\equiv 16 \cdot 9 \pmod 5$$
   $$\equiv 1 \cdot 4 \pmod 5$$
   $$\equiv 4 \pmod 5$$

   Using the "same remainder" definition of modular equivalence, the above equivalence gives us $(592)^4(1033)^2 \ mod\ 5 = 4 \ mod\ 5 = 4$.

2. Find the last digit of 3^{100}

   The last digit of any integer is the same as its value mod 10.

   In mod 10,

   $$3^{100} \equiv (3^2)^{50} \pmod{10}$$
   $$\equiv 9^{50} \pmod{10}$$
   $$\equiv (-1)^{50} \pmod{10}$$
   $$\equiv 1 \pmod{10}$$

   So $3^{100} \ mod\ 10 = 1 \ mod\ 10 = 1$. Thus the last digit of 3^{100} is 1.

12

Proof: $a = b + mk_1$, $c = d + mk_2$

$a + c = b + d + m(k_1 + k_2)$

Proof: $a = b + mk_1$, $c = d + mk_2$

$ac = bd + m(dk_1 + bk_2 + m k_1 k_2)$

Exercise 3: Modular Exponentiation

Find the value of 5^{20} mod 27

Solution:

In mod 27,

- We can find $5^{20} \equiv (5^{10})^2$
- Similarly, $5^{10} \equiv (5^5)^2$
- And $5^5 \equiv (5^2)^2 \cdot 5 \equiv (25)^2 \cdot 5$
  $\equiv (-2)^2 \cdot 5 \equiv 4 \cdot 5 \equiv 20$
- This gives $5^{10} \equiv (5^5)^2 \equiv 20^2$
  $\equiv (-7)^2 \equiv 49 \equiv 22$
- Finally, $5^{20} \equiv (5^{10})^2 \equiv 22^2$
  $\equiv (-5)^2 \equiv 25$ (mod 27)

So, $5^{20} \bmod 27 = 25$.

14

Exercise 4: Divisible by 7

Prove that $2^n + 6 \cdot 9^n$ is divisible by 7 for any n

Solution

Translating into the language of mod,

"x is divisible by 7" means $x \equiv 0 \pmod 7$.

In mod 7,

$$\begin{aligned} 2^n + 6 \cdot 9^n &\equiv 2^n + (-1) \cdot 2^n \quad &(mod\ 7) \\ &\equiv 2^n - 2^n &(mod\ 7) \\ &\equiv 0 &(mod\ 7) \end{aligned}$$

Thus, $2^n + 6 \cdot 9^n$ is divisible by 7.

16

Exercise 5: Last Digit

Find the last digit of $(38475393)^{324334}$

Solution:

Use mod 10 to find the last digit.

In mod 10,

$$\begin{aligned} (38475393)^{324334} &\equiv (3)^{324334} \quad &(mod\ 10) \\ &\equiv (3^2)^{324334/2} &(mod\ 10) \\ &\equiv (9)^{324334/2} &(mod\ 10) \\ &\equiv (-1)^{324334/2} &(mod\ 10) \\ &\equiv (-1)^{some\_even\_power} &(mod\ 10) \\ &\equiv 1 &(mod\ 10) \end{aligned}$$

Thus the last digit of $(38475393)^{324334}$ is 1.

Exercise 6: Divisible by 11

A number is called a *palindrome* if it is the same when written backwards.
E.g. 37173, 854458, 2222 are all palindromes.

Show that any 6-digit palindrome is divisible by 11.

Solution: A 6-digit palindrome N has the form $abccba$, where a, b, c are digits.
We want to show that $N \equiv 0 \pmod{11}$.

We can write N as:

$$\begin{aligned} N &= a10^5 + b10^4 + c10^3 + c10^2 + b10^1 + a \\ &= a(10^5 + 1) + b(10^4 + 10) + c(10^3 + 10^2) \\ &= a(10^5 + 1) + 10b(10^3 + 1) + 100c(10 + 1) \end{aligned}$$

In mod 11, $10^x \equiv -1$ whenever x is odd. So in mod 11,

$$\begin{aligned} N &\equiv a(10^5 + 1) + 10b(10^3 + 1) + 100c(10 + 1) \quad &(mod\ 11) \\ &\equiv a\left((-1)^5 + 1\right) + 10b\left((-1)^3 + 1\right) + 100c(-1 + 1) &(mod\ 11) \\ &\equiv a \cdot 0 + b \cdot 0 + c \cdot 0 &(mod\ 11) \\ &\equiv 0 &(mod\ 11) \end{aligned}$$

Thus, any 6-digit palindrome is divisible by 11.

Attempts: Modular Exponentiation

- Compute 5^8 mod 27
  - Method 1: $5^8 = 390625$
    - Now who wants to reduce 390625 mod 27?
  - Method 2: $5^{i+1} \equiv 5^i \cdot 5$
    - $5^2 \equiv 25$ $\quad 5^3 \equiv 5^2 \cdot 5 \equiv 25 \cdot 5 \equiv -2 \cdot 5 \equiv -10 \equiv 17$
      $5^4 \equiv 5^3 \cdot 5 \equiv -10 \cdot 5 \equiv -50 \equiv 4$ $\quad \dots \dots \dots$
    - $5^8 \equiv 16$ (mod 27)
  - Method 3: $5^{2i} \equiv \left(5^i\right)^2$

    Winner! Fewest calcs
    - $5^2 \equiv 25$
    - $5^4 \equiv (5^2)^2 \equiv 25^2 \equiv (-2)^2 \equiv 4$
    - $5^8 \equiv (5^4)^2 \equiv 4^2 \equiv 16$ $\quad$ (mod 27)

Fast Modular Exponentiation Algorithm

- Computing x^n mod m has 2 cases:
  - Case 1: $\boldsymbol{n}$ **is even**, $n = 2k$
    - $x^n \equiv \left(x^k\right)^2$ (mod m)
  - Case 2: $\boldsymbol{n}$ **is odd**, $n = 2k + 1$
    - $x^n \equiv \left(x^k\right)^2 \cdot x$ (mod m)

- Keep breaking down exponent as above, until the exponent is 1

(One) Reason why doing mod n is good

How large is m^a where a is 300 digit number (so $a \approx 10^{300}$) ?
Suppose m > 10. Then m^a has more than 10^{300} digits

Claim: number of atoms in known universe is at most 10^{82}
So cannot even write this number down even if we can store 1 bit per atom!!

Why? Number of atoms in 1 Kilo of matter about 10^{28}.
A typical star (like our Sun) weights about 10^{30} Kilos
A typical Galaxy has about 100 billion (10^{11}) stars
(Known) Universe has about 2 trillion ($<10^{13}$) galaxies

Computation time of naïve exponentiation

Computing m^a naively will need $\approx 10^{300}$ multiplications
($m \times m \times m$ …. a times)

Let us try to estimate the time.

- Fastest current supercomputer: Frontier (Oak ridge National labs)
- Peak speed: 10^3 petaflops (10^{18} floating pt operations per sec).
- Suppose (optimistically) each multiplication takes 1 flop.
- 1 year has about 31.5 million seconds (say $<10^8$ seconds)
- Age of universe 15 billion years (say $<10^{11}$ years)

Hence, can do only 10^{37} multiplications even on fastest supercomputer in 100 billion yrs.

Fast exponentiation needs at most 1024 multiplications (number of bits of a)
Can do in a microsecond even on your cellphone! Smart algorithms are good!