

Jan 16th

Theorem (Fundamental Theorem of Arithmetic)

Every natural number  $> 1$  can be written as a product of

$$n = \underbrace{p_1 \cdots p_k}_{\text{prime}}$$

$$12 = 2 \cdot 3 \cdot 3$$

Proof: Suppose there exist numbers with non unique factorizations into primes

Let  $N$  be the smallest such number

$\underbrace{2, 3, 4, 5, \dots, N-1, N}_{\text{have unique factorizations}}$  has at least two factorizations

$$N = \underbrace{p_1 \cdots p_k}_{\text{primes}} = \underbrace{q_1 \cdots q_h}_{\text{primes}} \quad \text{different factorizations}$$

Claim:  $p_i \neq q_j$  for any  $i, j$

Why can't we have  $p_i = q_1$  ?  
if  $p_i = q_1 \Rightarrow \frac{N}{p_i} = p_2 \cdots p_k = \frac{N}{q_1} = q_2 \cdots q_h < N$

$\frac{N}{p_i}$  natural number  $< N$   
with two distinct factorizations. Contradiction since  $N$  is the smallest such number.

So  $p_i \neq q_j$ , for any  $i, j$  in particular  $p_1 \neq q_1$

$\Rightarrow$  two possibilities  $p_1 > q_1$  or  $p_1 < q_1$ .

Cases 1:  $p_1 > q_1$       Case 2:  $p_1 < q_1$ .

Look at  $N - q_1 p_2 \cdots p_k = M$

$M > N > 0$  natural number  $N = p_1 p_2 \cdots p_k$

$$M = p_1 p_2 \cdots p_k - q_1 p_2 \cdots p_k = (p_1 - q_1) p_2 \cdots p_k$$

$$M = (p_1 - q_1) p_2 \cdots p_k < N$$

$(p_1 - q_1) < N \Rightarrow$  has a unique prime factorization

$$p_1 - q_1 = \underbrace{a_1 \cdots a_n}_{\text{primes}}$$

$$M = \underbrace{(a_1 \cdots a_n)}_{p_1 - q_1} p_2 \cdots p_k$$

$$p_1 - q_1$$

$$M = N - q_1 p_2 \cdots p_k = \underbrace{q_1 q_2 \cdots q_h}_{N} - q_1 p_2 \cdots p_k = q_1 (\underbrace{q_2 \cdots q_h - p_2 \cdots p_k}_{b_1 \cdots b_s \text{ prime factorizations}}) = q_1 b_1 \cdots b_s$$

$$M = \underbrace{a_1 \cdots a_n}_{\substack{\text{two factorizations} \\ \text{of } M \text{ and } M < N}} p_2 \cdots p_k = q_1 b_1 \cdots b_s$$

$\Rightarrow$  these two factorizations are the same up to reordering, should appear in the 1st factorization somewhere  $q_i \neq p_j$  for any  $j \Rightarrow q_i = a_i$  for some  $i$ .

$$p_1 \cdot g_1 = a_1 \cdots a_i \cdots a_n = g_i \quad \text{C-natural numbers}$$

... Check 4.1 for detailed proof.

---

**Corollary:** If  $p$  is prime and  $p \mid ab$  then  $p \mid a$  or  $p \mid b$

Note:  $a \mid b$  means  $a$  divides  $b$

$$\text{Ex: } 3 \mid 6 \cdot 2 \Rightarrow 3 \mid 6 \text{ or } 3 \mid 2$$

Is this true if  $p$  is not prime?

$$12 \mid 3 \cdot 8 = 24 \quad 12 \mid 3, 12 \mid 8$$

$$12 \mid 3 \cdot 4 \text{ but } 12 \nmid 3, 12 \nmid 4$$

**Proof:** Let  $\underset{\text{prime}}{p} \mid a \cdot b \Rightarrow a \cdot b = p \underset{\text{primes}}{g_1 \cdots g_s}$

$$a = \underset{\text{primes}}{m_1 \cdots m_m}$$

$$ab = m_1 \cdots m_m t_1 \cdots t_n$$

$$b = \underset{\text{primes}}{t_1 \cdots t_n}$$

$\Rightarrow p$  is one of  $m_i$ 's or  $p$  is one of  $t_j$ 's  
 $\Rightarrow p \mid a$  or  $p \mid b$

**Corollary:** if  $n > 1$  is a natural number as  $n = \underset{\text{distinct primes}}{p_1^{k_1} \cdots p_i^{k_i}}$

and this factorization is unique.

$$60 = 4 \cdot 15 = 4 \cdot 3 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3^1 \cdot 5^1$$

If  $p_1 \neq p_2$  are primes and  $p_1 \mid a$  and  $p_2 \mid a \Rightarrow p_1 p_2 \mid a$   
ex:  $2 \mid 24, 3 \mid 24 \Rightarrow 2 \cdot 3 = 6 \mid 24$

IS this true if  $p_1, p_2$  not prime?

Example:  $4 \mid 12, 6 \mid 12$ , but  $4 \times 6 = 24 \nmid 12$

---

## Modular Arithmetic

Def'n:  $a, b, m$  integers

We say  $a \equiv b \pmod{m}$

$a$  is equivalent to  $b$  modulo  $m$  if  $m | a-b$

Ex:  $12 \equiv 2 \pmod{5}$

$$5 | 12-2=10$$

$$12 \not\equiv 4 \pmod{5}$$

$$9 \equiv -1 \pmod{5}$$

$$5 | 12-4=8$$

$$9-(-1)=10 \text{ divided by } 5$$

is

$$-3 \quad 2 \quad -10 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13$$

which numbers are equivalent to 3 mod 5

$$3+5k, k=0, \pm 1, \pm 2, \pm 3 \dots$$

Properties:  $a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$

then

$$a+c \equiv b+d \pmod{m}$$

$$a-c \equiv b-d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

Ex:  $12 \equiv 2 \pmod{5}$

$$3 \equiv -2 \pmod{5}$$

$$12+3 \equiv 0 \pmod{5}$$

$$12-3 \equiv 4 \pmod{5}$$

$$12 \cdot 3 \equiv 2 \cdot (-2) \pmod{5}$$

Proof:  $a \equiv b \pmod{m}$  means  $a-b=mk$

$$a=b+mk$$

$c \equiv d \pmod{m}$  means  $c-d=m \cdot l$

$$c=d+ml$$

$$a+c=b+d+m(k+l)$$

$$(a+c)-(b+d)=m(k+l)$$

$$a+c \equiv b+d \pmod{m}$$

$$ac=(b+mk)(d+ml)=bd+mkd+bml+m^2kl$$

$$ac-bd=m(kd+bl+mkl)$$

$$\Rightarrow ac \equiv bd \pmod{m}$$

Does this work mod m?

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

*NO*

*ex:*  $m=4$   $c=2 \not\equiv 0 \pmod{4}$   
 $a=2$   $b=0$

$$ac = 4 \equiv bc = 0 \pmod{4}$$

but  $a \not\equiv b \pmod{4}$   
 $2 \not\equiv 0 \pmod{4}$

Corollary: If  $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$  for any  $n$

Proof. We use mathematical induction. The case  $n = 1$  is the hypothesis. Assume that the result is true for  $n = k$ ; that is,  $ak \equiv bk \pmod{m}$ . Since  $a \equiv b \pmod{m}$ , using part (ii) of Theorem 3.1.5 gives  $a \cdot ak = b \cdot bk \pmod{m}$ , or  $ak+1 \equiv bk+1 \pmod{m}$ .

### APPLICATION

$$2^{100} \pmod{7} = ?$$

$$2^1 \equiv 2 \pmod{7}$$

$$2^2 \equiv 4 \pmod{7}$$

$$2^3 \equiv 1 \pmod{7}$$

$$(2^3)^k \equiv 1^k \pmod{7}$$

$2^{100}$  What is the last digit?

$$2^{100} \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

$$2^7 \equiv 8 \pmod{10}$$

$$2^8 \equiv 6 \pmod{10}$$

$$2^9 \equiv 4 \pmod{10}$$

$$2^{10} \equiv 8 \pmod{10}$$

$$2^{11} \equiv 6 \pmod{10}$$

$$2^{12} \equiv 4 \pmod{10}$$

$$2^{13} \equiv 8 \pmod{10}$$

$$2^{14} \equiv 6 \pmod{10}$$

$$2^{15} \equiv 4 \pmod{10}$$

$$2^{16} \equiv 8 \pmod{10}$$

$$2^{17} \equiv 6 \pmod{10}$$

$$2^{18} \equiv 4 \pmod{10}$$

$$2^{19} \equiv 8 \pmod{10}$$

$$2^{20} \equiv 6 \pmod{10}$$

$$2^{21} \equiv 4 \pmod{10}$$

$$2^{22} \equiv 8 \pmod{10}$$

$$2^{23} \equiv 6 \pmod{10}$$

$$2^{24} \equiv 4 \pmod{10}$$

$$2^{25} \equiv 8 \pmod{10}$$

$$2^{26} \equiv 6 \pmod{10}$$

$$2^{27} \equiv 4 \pmod{10}$$

$$2^{28} \equiv 8 \pmod{10}$$

$$2^{29} \equiv 6 \pmod{10}$$

$$2^{30} \equiv 4 \pmod{10}$$

$$2^{31} \equiv 8 \pmod{10}$$

$$2^{32} \equiv 6 \pmod{10}$$

$$2^{33} \equiv 4 \pmod{10}$$

$$2^{34} \equiv 8 \pmod{10}$$

$$2^{35} \equiv 6 \pmod{10}$$

$$2^{36} \equiv 4 \pmod{10}$$

$$2^{37} \equiv 8 \pmod{10}$$

$$2^{38} \equiv 6 \pmod{10}$$

$$2^{39} \equiv 4 \pmod{10}$$

$$2^{40} \equiv 8 \pmod{10}$$

$$2^{41} \equiv 6 \pmod{10}$$

$$2^{42} \equiv 4 \pmod{10}$$

$$2^{43} \equiv 8 \pmod{10}$$

$$2^{44} \equiv 6 \pmod{10}$$

$$2^{45} \equiv 4 \pmod{10}$$

$$2^{46} \equiv 8 \pmod{10}$$

$$2^{47} \equiv 6 \pmod{10}$$

$$2^{48} \equiv 4 \pmod{10}$$

$$2^{49} \equiv 8 \pmod{10}$$

$$2^{50} \equiv 6 \pmod{10}$$

$$2^{51} \equiv 4 \pmod{10}$$

$$2^{52} \equiv 8 \pmod{10}$$

$$2^{53} \equiv 6 \pmod{10}$$

$$2^{54} \equiv 4 \pmod{10}$$

$$2^{55} \equiv 8 \pmod{10}$$

$$2^{56} \equiv 6 \pmod{10}$$

$$2^{57} \equiv 4 \pmod{10}$$

$$2^{58} \equiv 8 \pmod{10}$$

$$2^{59} \equiv 6 \pmod{10}$$

$$2^{60} \equiv 4 \pmod{10}$$

$$2^{61} \equiv 8 \pmod{10}$$

$$2^{62} \equiv 6 \pmod{10}$$

$$2^{63} \equiv 4 \pmod{10}$$

$$2^{64} \equiv 8 \pmod{10}$$

$$2^{65} \equiv 6 \pmod{10}$$

$$2^{66} \equiv 4 \pmod{10}$$

$$2^{67} \equiv 8 \pmod{10}$$

$$2^{68} \equiv 6 \pmod{10}$$

$$2^{69} \equiv 4 \pmod{10}$$

$$2^{70} \equiv 8 \pmod{10}$$

$$2^{71} \equiv 6 \pmod{10}$$

$$2^{72} \equiv 4 \pmod{10}$$

$$2^{73} \equiv 8 \pmod{10}$$

$$2^{74} \equiv 6 \pmod{10}$$

$$2^{75} \equiv 4 \pmod{10}$$

$$2^{76} \equiv 8 \pmod{10}$$

$$2^{77} \equiv 6 \pmod{10}$$

$$2^{78} \equiv 4 \pmod{10}$$

$$2^{79} \equiv 8 \pmod{10}$$

$$2^{80} \equiv 6 \pmod{10}$$

$$2^{81} \equiv 4 \pmod{10}$$

$$2^{82} \equiv 8 \pmod{10}$$

$$2^{83} \equiv 6 \pmod{10}$$

$$2^{84} \equiv 4 \pmod{10}$$

$$2^{85} \equiv 8 \pmod{10}$$

$$2^{86} \equiv 6 \pmod{10}$$

$$2^{87} \equiv 4 \pmod{10}$$

$$2^{88} \equiv 8 \pmod{10}$$

$$2^{89} \equiv 6 \pmod{10}$$

$$2^{90} \equiv 4 \pmod{10}$$

$$2^{91} \equiv 8 \pmod{10}$$

$$2^{92} \equiv 6 \pmod{10}$$

$$2^{93} \equiv 4 \pmod{10}$$

$$2^{94} \equiv 8 \pmod{10}$$

$$2^{95} \equiv 6 \pmod{10}$$

$$2^{96} \equiv 4 \pmod{10}$$

$$2^{97} \equiv 8 \pmod{10}$$

$$2^{98} \equiv 6 \pmod{10}$$

$$2^{99} \equiv 4 \pmod{10}$$

$$2^{100} \equiv 8 \pmod{10}$$

$$2^{101} \equiv 6 \pmod{10}$$

$$2^{102} \equiv 4 \pmod{10}$$

$$2^{103} \equiv 8 \pmod{10}$$

$$2^{104} \equiv 6 \pmod{10}$$

$$2^{105} \equiv 4 \pmod{10}$$

$$2^{106} \equiv 8 \pmod{10}$$

$$2^{107} \equiv 6 \pmod{10}$$

$$2^{108} \equiv 4 \pmod{10}$$

$$2^{109} \equiv 8 \pmod{10}$$

$$2^{110} \equiv 6 \pmod{10}$$

$$2^{111} \equiv 4 \pmod{10}$$

$$2^{112} \equiv 8 \pmod{10}$$

$$2^{113} \equiv 6 \pmod{10}$$

$$2^{114} \equiv 4 \pmod{10}$$

$$2^{115} \equiv 8 \pmod{10}$$

$$2^{116} \equiv 6 \pmod{10}$$

$$2^{117} \equiv 4 \pmod{10}$$

$$2^{118} \equiv 8 \pmod{10}$$

$$2^{119} \equiv 6 \pmod{10}$$

$$2^{120} \equiv 4 \pmod{10}$$

$$2^{121} \equiv 8 \pmod{10}$$

$$2^{122} \equiv 6 \pmod{10}$$

$$2^{123} \equiv 4 \pmod{10}$$

$$2^{124} \equiv 8 \pmod{10}$$

$$2^{125} \equiv 6 \pmod{10}$$

$$2^{126} \equiv 4 \pmod{10}$$

$$2^{127} \equiv 8 \pmod{10}$$

$$2^{128} \equiv 6 \pmod{10}$$

$$2^{129} \equiv 4 \pmod{10}$$

$$2^{130} \equiv 8 \pmod{10}$$

$$2^{131} \equiv 6 \pmod{10}$$

$$2^{132} \equiv 4 \pmod{10}$$

$$2^{133} \equiv 8 \pmod{10}$$

$$2^{134} \equiv 6 \pmod{10}$$

$$2^{135} \equiv 4 \pmod{10}$$

$$2^{136} \equiv 8 \pmod{10}$$

$$2^{137} \equiv 6 \pmod{10}$$

$$2^{138} \equiv 4 \pmod{10}$$

$$2^{139} \equiv 8 \pmod{10}$$

$$2^{140} \equiv 6 \pmod{10}$$

$$2^{141} \equiv 4 \pmod{10}$$

$$2^{142} \equiv 8 \pmod{10}$$

$$2^{143} \equiv 6 \pmod{10}$$

$$2^{144} \equiv 4 \pmod{10}$$

$$2^{145} \equiv 8 \pmod{10}$$

$$2^{146} \equiv 6 \pmod{10}$$

$$2^{147} \equiv 4 \pmod{10}$$

$$2^{148} \equiv 8 \pmod{10}$$

$$2^{149} \equiv 6 \pmod{10}$$

$$2^{150} \equiv 4 \pmod{10}$$

$$2^{151} \equiv 8 \pmod{10}$$

$$2^{152} \equiv 6 \pmod{10}$$

$$2^{153} \equiv 4 \pmod{10}$$

$$2^{154} \equiv 8 \pmod{10}$$

$$2^{155} \equiv 6 \pmod{10}$$

$$2^{156} \equiv 4 \pmod{10}$$

$$2^{157} \equiv 8 \pmod{10}$$

$$2^{158} \equiv 6 \pmod{10}$$

$$2^{159} \equiv 4 \pmod{10}$$

$$2^{160} \equiv 8 \pmod{10}$$

$$2^{161} \equiv 6 \pmod{10}$$

$$2^{162} \equiv 4 \pmod{10}$$

$$2^{163} \equiv 8 \pmod{10}$$

$$2^{164} \equiv 6 \pmod{10}$$

$$2^{165} \equiv 4 \pmod{10}$$

$$2^{166} \equiv 8 \pmod{10}$$

$$2^{167} \equiv 6 \pmod{10}$$

$$2^{168} \equiv 4 \pmod{10}$$

$$2^{169} \equiv 8 \pmod{10}$$

$$2^{170} \equiv 6 \pmod{10}$$

$$2^{171} \equiv 4 \pmod{10}$$

$$2^{172} \equiv 8 \pmod{10}$$

$$2^{173} \equiv 6 \pmod{10}$$

$$2^{174} \equiv 4 \pmod{10}$$

$$2^{175} \equiv 8 \pmod{10}$$

$$2^{176} \equiv 6 \pmod{10}$$

$$2^{177} \equiv 4 \pmod{10}$$

$$2^{178} \equiv 8 \pmod{10}$$

$$2^{179} \equiv 6 \pmod{10}$$

$$2^{180} \equiv 4 \pmod{1$$

$$2^{3^{101}} \pmod{5} \equiv ?$$

$$\hookrightarrow \text{means } 2^{(3^{101})} \quad \begin{aligned} 2^1 &\equiv 2 \pmod{5} \\ 2^2 &\equiv 4 \pmod{5} \\ 2^3 &\equiv 3 \pmod{5} \\ 2^4 &\equiv 1 \pmod{5} \end{aligned} \quad \begin{aligned} 2^{\frac{4k+1}{4k+2}} &\equiv 2 \pmod{5} \\ 2^{\frac{4k+2}{4k+3}} &\equiv 4 \pmod{5} \\ 2^{\frac{4k+3}{4k+4}} &\equiv 3 \pmod{5} \\ 2^{\frac{4k+4}{4k+5}} &\equiv 1 \pmod{5} \end{aligned}$$

We need to figure out what is  $\boxed{3^{101} \pmod{4}}$

$$\begin{aligned} 3^1 &\equiv -1 \pmod{4} \\ 3^2 &\equiv 1 \pmod{4} \\ 3^3 &\equiv -1 \pmod{4} \\ 3^4 &\equiv 1 \pmod{4} \end{aligned} \quad 3^k \equiv (-1)^k \quad \begin{cases} +1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd} \end{cases}$$

$$3^{101} \equiv -1 \pmod{4} \quad \text{b/c } 101 \text{ is odd}$$

$$\Rightarrow 3^{101} \equiv 3 \pmod{4}$$

$$3^{101} = 4k + 3 \text{ for some } k$$

$$\Rightarrow 2^{3^{101}} = 2^{\frac{4k+3}{4k+4}} \equiv 3 \pmod{5}$$

Theorem: A natural number  $n$  is divisible by 9 iff the sum of its digits is divisible by 9.

$$27 = 2 + 7 = 9$$

$$35 - \text{not divisible} \quad 3+5=8 \quad \times$$

$$3456 \quad 3+4+5+6=18=9 \cdot 2 \\ \text{divisible by 9.}$$

$$n = \overline{a_k a_{k-1} \dots a_0} = a_0 \cdot 1 + a_1 \cdot 10 + \dots + a_k \cdot 10^k \quad 0 \leq a_i \leq 9$$

$$\begin{aligned} 237 &= 7 + 3 \cdot 10 + 2 \cdot 10^2 \\ 3456 &= 6 + 5 \cdot 10 + 4 \cdot 10^2 + 3 \cdot 10^3 \end{aligned}$$

**Proof** see next page.

$$\text{then: } a_0 \cdot 10^0 + a_1 \cdot 10^1 + \dots + a_k \cdot 10^k \equiv a_0 + \dots + a_k \pmod{9}$$

$$10 \equiv 1 \pmod{9}$$

$$100 \equiv 1 \pmod{9}$$

... ...

$$\Rightarrow 10^k \equiv 1 \pmod{9}$$

$$10^k \cdot a^k \equiv a^k \pmod{9} \text{ for any } k \text{ and any } a$$

$$+ a_0 \cdot 10^0 \equiv a_0 \pmod{9}$$

$$+ a_1 \cdot 10^1 \equiv a_1 \pmod{9}$$

$$+ a_2 \cdot 10^2 \equiv a_2 \pmod{9}$$

... ...

$$a_0 \cdot 10^0 + a_1 \cdot 10^1 + \dots + a_k \cdot 10^k \equiv a_0 + a_1 + \dots + a_k \pmod{9}$$