Last class:

Main results:

(a) division with remainder:

a, b integers, $b > 0$

$\Rightarrow \exists$ unique q and r, $0 \leq r < b$ s.t.

$$a = qb + r$$

(b) a, b integers $\Rightarrow \exists$ integers s and t s.t.

$$\gcd(a,b) = as + bt$$

Def. (a) An integer a is called <u>prime</u> if its only divisors are ± 1 and $\pm a$

(b) Two integers a and b are <u>relatively prime</u> if $\gcd(a,b) = 1$

Euclid's Lemma

a, b integers, p prime

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

Proof. assume $p \nmid a$

$\Rightarrow \gcd(p, a) = 1$

by previous result: $1 = sa + tp$ for some integers s and t

$$b = b \cdot 1 = b(sa + tp) = abs + btp$$

obv. $p \mid btp$

by ass. $p \mid abs$

$\Big\}$ $p \mid (abs + btp) = b$ ✓

application:

Theorem (Uniqueness of Prime Decomposition)

Any integer n can be written as a product of primes uniquely up to the order of the primes

(e.g. $30 = 2 \cdot 3 \cdot 5 = 5 \cdot 3 \cdot 2 \ldots$)

(proof later as needed)

proof of uniqueness statement depends on Euclid's Lemma

Modular Arithmetic

Question: Is $1173 \cdot 2357$ odd or even?

answer: both numbers are odd

we know odd · odd = odd

make this mathematically precise

Def. Let a, n be integers, $n > 0$

We write $a \bmod n = r$

if $a = qn + r$ with $0 \leq r < n$

Examples:

$1173 \bmod 2 = 1$

$2357 \bmod 2 = 1$

$27 \bmod 12 = 3$

Lemma Let a, b, n be integers, $n > 0$

$$a \bmod n = b \bmod n \iff n \mid (a-b)$$

proof Let $a = q_1 n + r_1$ $\quad 0 \le r_1, r_2 < n$

$b = q_2 n + r_2$

"$\Rightarrow$" by assumption $r_1 = r_2$

(r_1: $a \bmod n$, r_2: $b \bmod n$)

$$\Rightarrow \quad a - b = q_1 n + r_1 - (q_2 n + r_2)$$

$$= (q_1 - q_2) n + \underbrace{r_1 - r_2}_{=0} \quad \text{by ass.}$$

$$\Rightarrow n \mid (a-b)$$

$\Leftarrow$ (exercise

(can reverse steps from "$\Rightarrow$")

Theorem a, b, n integers, $n > 0$

$a \bmod n = r_1$

$b \bmod n = r_2$

$\Rightarrow$

(a) $a+b \bmod n = r_1 + r_2 \bmod n$

(b) $ab \bmod n = r_1 r_2 \bmod n$

Proof. (a) enough to show: $n \mid a+b-(r_1+r_2)$

by lemma

$$a+b-r_1-r_2 = \underbrace{(q_1 n + r_1)}_{=a} + \underbrace{(q_2 n + r_2)}_{=b} - r_1 - r_2$$

$$= q_1 n + q_2 n$$

$$= n(q_1 + q_2)$$

i.e. $n \mid a+b-r_1-r_2$ ✓

(b) same strategy $a = q_1 n + r_1$, $b = q_2 n + r_2$

$$ab - r_1 r_2 = (q_1 n + r_1)(q_2 n + r_2) - r_1 r_2$$

$$= q_1 q_2 n^2 + q_1 n r_2 + r_1 q_2 n + r_1 r_2 - r_1 r_2$$

$$= n(q_1 q_2 n + q_1 r_2 + r_1 q_2)$$

$$\Rightarrow n \mid ab - r_1 r_2$$

Examples: (1) n odd $\Leftrightarrow$ $n \bmod 2 = 1$

$1173 \bmod 2 = 1$

$2357 \bmod 2 = 1$

$\Rightarrow 1173 \cdot 2357 \bmod 2 = 1 \cdot 1 \bmod 2 = 1$

$\Rightarrow$ product is also odd

(2) Calculate $19^5 \bmod 17$

Sol. $19 \bmod 17 = 2$

$\Rightarrow 19^5 \bmod 17 = 2^5 \bmod 17$

$= 32 \bmod 17$

$= 15$

(3) Calculate the last digit of 3^{403}

Sol. need to calculate $3^{403} \bmod 10$

$3^2 \bmod 10 = 9 \bmod 10 = 9$

$3^3 \bmod 10 = 27 \bmod 10 = 7$

$3^4 \bmod 10 = 81 \bmod 10 = 1$

$$3^{403} = 3^{4 \cdot 100 + 3}$$

$$= (3^4)^{100} \cdot 3^3$$

$$\Rightarrow 3^{403} \bmod 10 = (3^4)^{100} \cdot 3^3 \bmod 10$$

$$= 1^{100} \cdot 7 \bmod 10$$

theorem ↗

$$= 7$$

Remark: Calculating $a^k \bmod n$ for high powers k is simplified by

- determine smallest number h s.t. $a^h = 1 \bmod n$ (if possible)
- write $k = qh + r$ $\Rightarrow a^k = a^{hq+r}$

$$a^k \bmod n = a^{hq+r} \bmod n \qquad a^h \bmod n = 1 !$$

$$= a^r \bmod n$$

(4) Prove that $x^2 - y^2 = 1002$ can not have any integer solutions.

Solution. Consider this equation mod 4

r.h.s. : $1002 \bmod 4 = 2$

$x \bmod 4$	$x^2 \bmod 4$
0	0
1	1
2	0
3	1

$4 \bmod 4 = 0$

$9 \bmod 4 = 1$

$x^2 \bmod 4$ is either 0 or 1

same for $y^2 \bmod 4$

Consider all possible cases

$x^2 \bmod 4$	$y^2 \bmod 4$	$x^2 - y^2 \bmod 4$
0	0	0
1	0	1
0	1	$-1 \bmod 4 = 3$
1	1	0

Recall: $x^2 - y^2 \bmod 4 \neq 2$

for any choice of integers x and y

$\Rightarrow$ $x^2 - y^2 = 1002$ does not have an integer solution.