INTEGERS

PLAN FOR TODAY

- Quotient, remainder, mod function
- Divisors, multiples
- Greatest common divisor (GCD)
- Euclid's algorithm
- Least common multiple (LCM)
- Primes and prime factorization
- Base-b expansion
- Mathematical induction

HEADS-UP FOR NEXT WEEK

Logic and proofs

Lots of basic definitions — not so fun to hear a lecture about

Please make sure to read Chapter 2 in advance, so that the lecture makes sense even if we move fast

Secs 2.1–2.4	Important; will also be covered in class
Sec 2.5	Also essential, but left for you to read
Sec 2.6	Useful and interesting, but not compulsory reading

QUOTIENT and REMAINDER

Let $d \in \mathbb{Z}^+$

For any m there exist $q \in \mathbb{Z}$ and $0 \le r < d$ s.t.

$$m = q \cdot d + r$$

$m = 12$	$d = 5$	$12 = (2) \cdot 5 + 2$
$m = 5$	$d = 12$	$5 = (0) \cdot 12 + 5$
$m = -12$	$d = 5$	$-12 = (-3) \cdot 5 + 3$
$m = -5$	$d = 12$	$-5 = (-1) \cdot 12 + 7$

Usually focus on $m \in \mathbb{Z}^+$

mod-d function: returns remainder r ($m \bmod d$)

In C, Python, F# $m \,\%\, d$

Definitions for negative numbers might vary — best to avoid in practice

$m \in \mathbb{Z}$, $d \in \mathbb{Z}^+$

$$m = q \cdot d + r \qquad 0 \le r < d$$

If $r = 0$ then
- d divides m $\quad d \mid m$
- m multiple of d

If $r \neq 0$
- d does not divide m, $\quad d \nmid m$

d divides m if $\exists\, q \in \mathbb{Z}$ s.t. $m = q \cdot d$

Ex $\quad 3 \mid 12 \qquad 5 \nmid 16$

PROPERTIES OF DIVISORS

$m, n \in \mathbb{Z}$, $d \in \mathbb{Z}^+$

(1) $m \mid m$, $1 \mid m$, $d \mid 0$

(2) If $d \mid m$ or $d \mid n$ then $d \mid mn$

(3) If $d \mid m$ and $d \mid n$, then $d \mid (sm + tn)$ $\forall s, t \in \mathbb{Z}$

(4) If $d \mid m$ and $m \mid n$, then $d \mid n$ [transitivity]

QUESTION: If $d \mid mn$, is it true that $d \mid m$ or $d \mid n$?

Proof: Just use the definition

E.g., for (3)

$m = q_1 \cdot d$ $\quad n = q_2 \cdot d$

$sm + tn = (sq_1 + tq_2)\, d$

so $d \mid (sm + tn)$ as claimed

Let $a, b, d \in \mathbb{Z}^+$

d **common divisor** of a & b if $d \mid a$ and $d \mid b$

What are the common divisors of 30 and 36

$30 = 2 \cdot 3 \cdot 5$ $\quad 36 = 2 \cdot 2 \cdot 3 \cdot 3$

Common divisors 2, 3, 6

d is **GREATEST COMMON DIVISOR** of a & b if $d \mid a$, $d \mid b$ and d is largest of all common divisors

$GCD(30, 36) = 6$

KBR THEOREM 4

If $d = GCD(a,b)$, then $a, b, d \in \mathbb{Z}^+$

(a) $d = sa + tb$ for some $s, t \in \mathbb{Z}$

(b) For any other common divisor c of a and b it holds that $c \mid d$.

Game plan:

1. Let d^* be minimal element in set $\{ m \mid m > 0,\ m = sa + tb,\ s,t \in \mathbb{Z} \}$. (†)
2. Show that if $c \mid a$ and $c \mid b$, then $c \mid d^*$.
3. Observe that if $c \mid d^* > 0$, then $c \leq d^*$ so if d^* is a common divisor, then it is the largest one.
4. So all we need to prove is $d^* \mid a$ and $d^* \mid b$ – then $d^* = GCD(a,b)$ and the theorem follows.

Proof

Define d^* as in (†)

[BTW, how do we know that this infinitely large set has a minimal element?

Not true for $\{ r \mid r > 0,\ r = \frac{sa}{tb},\ s,t \in \mathbb{Z} \}$, for instance.

But (†) is a set of POSITIVE INTEGERS, and the LEAST NUMBER PRINCIPLE says that such a set has a smallest member. This is equivalent to the PRINCIPLE OF MATHEMATICAL INDUCTION, which we will talk more about soon.]

Suppose $c|a$ and $c|b$. Then by Property (3) it holds that

$$c| \; sa + tb = d^*$$

That is, there is a $q \in \mathbb{Z}^+$ such that

$$d^* = q \cdot c$$

which means that

$$d^* \geq c$$

so d^* is at least as large as any common divisor of a and b.

It remains to prove that $d^*|a$ and $d^*|b$. Let us prove the first claim. Write

$$a = q \cdot d^* + r \qquad 0 \leq r < d^*$$

If $r = 0$ we have $d^*|a$, which is what we want.

Suppose $r \neq 0$, i.e., $d^* \nmid a$. Then

$$\begin{aligned} r &= a - q \cdot d^* \\ &= a - q \cdot (sa + tb) \\ &= (1 - qs) \cdot a + (-qt) \cdot b \end{aligned}$$

But then $r > 0$ is in the set $(\dagger)$ and $r < d^*$. This contradicts that d^* is the smallest number in $(\dagger)$.
Hence $r = 0$ and $d^*|a$.

In exactly the same way one can show that $d^*|b$. The theorem follows ☒

Theorem 4 is true, but not very constructive

To find GCD, use **EUCLIDEAN ALGORITHM**

Key ideas:

- $GCD(r, 0) = r$
- $GCD(a, b) = GCD(a \bmod b, b)$
- And $(a \bmod b) < b$

Recall $a \bmod b = r$ for

$a = qb + r \qquad 0 \le r < b \qquad (*)$

$r = a - qb \qquad (**)$

By (*) and Property (3), any common divisor of b and r divides a

By (**) and Property (3), any common divisor of a and b divides r.

So, in particular, $GCD(a,b) = GCD(b,r)$

EUCLID (a, b) $\qquad a, b \in \mathbb{N}$

```
if (b > a)
    return EUCLID(b, a)
else if (b = 0)
    return a
else
    return EUCLID(b, a mod b)
```

Or writing it out as calculation

$$a = q_1 \cdot b + r_1 \qquad 0 \le r_1 < b$$
$$b = q_2 \cdot r_1 + r_2 \qquad 0 \le r_2 < r_1$$
$$r_1 = q_3 \cdot r_2 + r_3 \qquad 0 \le r_3 < r_2$$

$GCD(a,b) = GCD(b, r_1) = GCD(r_1, r_2) = \dots$

When $r_k = 0$, we have $GCD(a,b) = r_{k-1}$

Ex 1 $\boxed{GCD(36, 30) \ ?}$

$$36 = 1 \cdot 30 + 6$$
$$30 = 5 \cdot 6 + 0$$

So $GCD(36, 30) = 6$

Ex 2 $\boxed{GCD(90, 28) \ ?}$

$$90 = 3 \cdot 28 + 6$$
$$28 = 4 \cdot 6 + 4$$
$$6 = 1 \cdot 4 + 2$$
$$4 = 2 \cdot 2 + 0$$

$GCD(90, 28) = 2$

How can we find $s, t \in \mathbb{Z}$ such that $GCD(90, 28) = 2 = 5 \cdot 90 + t \cdot 28$?

Run Euclidean algorithm backwards!

$$2 = 6 - 1 \cdot 4$$
$$= 6 - 1 \cdot (28 - 4 \cdot 6) =$$
$$= (-1) \cdot 28 + 5 \cdot 6$$
$$= (-1) \cdot 28 + 5 \cdot (90 - 3 \cdot 28)$$
$$= 5 \cdot 90 + (-16) \cdot 28$$

You should be able to do calculations like these...

Let $a, b, m \in \mathbb{Z}^+$

m is a **COMMON MULTIPLE** of a and b if $a|m$ and $b|m$

m is the **LEAST COMMON MULTIPLE** $LCM(a,b)$ of a and b if m is the smallest of all common multiples of a & b

PROPOSITION $\boxed{LCM(a,b) = \frac{a \cdot b}{GCD(a,b)}}$

Ex $LCM(8,10) = 40 = \frac{8 \cdot 10}{2}$

Positive integer $p > 1$ is **PRIME** if only (positive) divisors are 1 and p

Ex 2, 3, 5, 7, 11, 13, 17

NOT: 0, 1, -2, 4, 12

$a, b \in \mathbb{Z}^+$ are **RELATIVELY PRIME** if $GCD(a,b) = 1$

Ex 12 and 25 are relatively prime

12 and 15 are not

(Run Euclidean algorithm to verify!)

FUNDAMENTAL THEOREM OF ARITHMETIC

Any positive integer $m > 1$ has a **UNIQUE PRIME FACTORIZATION**

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}$$

where $p_1 < p_2 < p_3 < \cdots$ primes

and $a_i \in \mathbb{Z}^+$

Suppose $m = \prod_{i=1}^{k} p_i^{a_i}$

d divides m if $d = \prod_{i=1}^{k} p_i^{b_i}$
for $0 \leq b_i \leq a_i$ for all i

Suppose $n = \prod_{i=1}^{k} p_i^{b_i}$

Then

$$GCD(m,n) = \prod_{i=1}^{k} p_i^{\min(a_i, b_i)}$$

$$LCM(m,n) = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)}$$

BASE-b EXPANSION

Let $b > 1$ be a positive integer

Any $m \in \mathbb{Z}^+$ can be written (for large enough k) as

$$m = d_k \cdot b^k + d_{k-1} \cdot b^{k-1} + \cdots + d_2 \cdot b^2 + d_1 b + d_0$$

for $d_k \neq 0$ and $0 \leq d_i < b$ for all i

NOTATION:

$$(d_k\, d_{k-1} \cdots d_2\, d_1\, d_0)_b$$

base-b expansion of m

Ex $b = 10$

$$935 = 9 \cdot 10^2 + 3 \cdot 10^1 + 5$$
$$= (935)_{10}$$

Except we usually omit parentheses and suffix when we use base 10...

COMMON BASES

DECIMAL $b = 10$

BINARY $b = 2$

OCTAL $b = 8$

HEXADECIMAL $b = 16$ digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Ex Convert to decimal basis

$$(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1$$
$$= 16 + 8 + 2 + 1$$
$$= 27$$

To find expansion in base b, compute remainders

$$m = q_0 \cdot b + r_0 \qquad 0 \le r_0 < b$$
$$q_0 = q_1 \cdot b + r_1 \qquad 0 \le r_1 < b$$
$$q_1 = q_2 \cdot b + r_2 \qquad 0 \le r_2 < b$$

r_0: least significant digit

et cetera

Ex Write 99 in octal basis

$$99 = 12 \cdot 8 + 3$$
$$12 = 1 \cdot 8 + 4$$
$$1 = 0 \cdot 8 + 1$$

$$(99)_{10} = (143)_8$$

You should be able to do conversions like these...

MATHEMATICAL INDUCTION

(1) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

Check for $n = 1, 2, 3, 4$ — TRUE

(2) For p a prime number

$2^p - 1$ is prime (MERSENNE PRIME NUMBER)

True for $p = 2, 3, 5, 7$.

(3) All swans are white

True for all swans we've seen so far.

(3) Is an example of empirical induction — not good enough for math

(2) fails for $p = 11$ (but works again for $p = 13, 17, 19$)

(1) Is true because you've seen it in lecture notes

But how to prove it?

"Falling Dominoes principle"

INDUCTION PRINCIPLE

If $P(n)$ is a statement for integers such that

(a) $P(n_0)$ is true — BASE CASE

(b) If for $n \geq n_0$ it holds that $P(n)$ true, then $P(n+1)$ is also true — INDUCTION STEP

Then $P(n)$ is true for all $n \geq n_0$

How to prove the induction principle?
We can't — we accept it as obviously true
An AXIOM
Follows from the LEAST NUMBER PRINCIPLE
and implies it — so they are equivalent

Prove (1) by induction

Base case ($n = 1$)

$$1^2 = \frac{1 \cdot 2 \cdot 3}{6} \quad \text{OK}$$

Induction step
Suppose

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2$$

$$= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \quad \left[\text{induction hypothesis}\right]$$

$$= \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)(n+1)}{6}$$

$$= \frac{(n+1)\left(n(2n+1) + 6(n+1)\right)}{6}$$

$$= \frac{(n+1)(2n^2 + 7n + 6)}{6}$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}$$

The equality follows by the induction principle