Math 103A Fall 2022

Chapter 0

Well Ordering Principle:

Every nonempty set of positive integers contains a smallest element.

Def: • For $s,t \in \mathbb{Z}$ we say t divides s or t is a divisor of s (and write $t \mid s$) if $\frac{s}{t} \in \mathbb{Z}$. When $\frac{s}{t} \notin \mathbb{Z}$ we write $t \nmid s$
or s is a multiple of t

• A prime is an integer greater than 1 whose only positive divisors are 1 and itself.

Thm 0.1 (The Division Algorithm):

If $a,b \in \mathbb{Z}$ with $b>0$ then there exist unique integers q,r such that $0 \leq r < b$ and

$$a = bq + r$$

Pf: (Existence) Set

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}$$

Notice $S \neq \emptyset$ since:

- when $a \geq 0$, $a - b \cdot 0 \in S$
- when $a < 0$, $a - b \cdot (2a) = a(1-2b)$ is positive and thus belongs to S

By W.O.P. S contains a least element r.
Since all elements of S are non-negative, $r \geq 0$.
Since $r \in S$, there is $q \in \mathbb{Z}$ with $r = a - bq$, meaning $a = bq + r$.

Finally, we must have $r<b$ as otherwise $r-b = a-b(q+1)$ would belong to S but be smaller than r (contradicting that r is smallest element of S).

(Uniqueness) Suppose $a = bq+r = bq'+r'$ with $q,q',r,r' \in \mathbb{Z}$, $0 \le r,r' < b$.

Notice that $bq+r = bq'+r'$ implies $b(q-q') = r'-r$.

Also note $-b < r'-r < b$. If $q \neq q'$ then

$|r'-r| = |b(q-q')| = |b| \cdot |q-q'| \ge |b| > |r'-r|$,

a contradiction. So $q=q'$ and thus $r=r'$ since $r'-r = b(q-q') = 0$. $\square$

Ex: $a=32,\ b=5 \longrightarrow 32 = 5\cdot 6+2$

$a=-24,\ b=7 \longrightarrow -24 = 7\cdot(-4)+4$

Def: • The greatest common divisor (~~gcd~~ written $\gcd(a,b)$) of $a,b \in \mathbb{Z}\setminus\{0\}$ is the largest integer that divides both a and b

• $a,b \in \mathbb{Z}\setminus\{0\}$ are relatively prime if $\gcd(a,b)=1$

Thm 0.2: For any $a,b \in \mathbb{Z}\setminus\{0\}$ there are $s,t \in \mathbb{Z}$ with $\gcd(a,b) = as+bt$. Moreover $\gcd(a,b)$ is the least ~~positive~~ member of $S = \{am+bn : m,n \in \mathbb{Z},\ am+bn > 0\}$

(use $n=0$, $m=\pm 1$)

Pf: Easy to check $S \neq \emptyset$. By W.O.P. S has a least element $d = as+bt$.

Claim: d is a common divisor of a and b.

By division alg. $a = dq + r$, $0 \leq r < d$.

Notice $r = a - dq = a - (as + bt)q = a(1 - sq) + b(-qt)$.

So r cannot be positive, otherwise it would be an element of ~~S~~ S smaller than d.

Thus $r = 0$ and $d \mid a$.

By symmetry, $d \mid b$ as well.

Claim: d is the greatest common divisor of a and b

If d' is any common divisor of a, b then there are $h, k \in \mathbb{Z}$ with $a = d'h$, $b = d'k$. Then

$$d = as + bt = d'hs + d'kt = d'(hs + kt)$$

so $d' \mid d$ and thus $d = |d| \geq |d'| \geq d'$ $\square$

Ex: $\gcd(8, 11) = 1 = 8 \cdot (-4) + 11 \cdot 3$

$\gcd(21, 15) = 3 = 21 \cdot (-2) + 15 \cdot 3$

$\gcd(6, 12) = 6 = 6 \cdot 1 + 12 \cdot 0$

Euclid's lem: If p prime and $p \mid ab$ then $p \mid a$ or $p \mid b$

Pf: Assume $p \mid ab$. If $p \mid a$ we're done.

If $p \nmid a$ then $\gcd(p, a) = 1$ so $\exists s, t \in \mathbb{Z}$ $1 = ps + at$. Then $b = psb + atb$ and p divides $psb + atb$ so $p \mid b$. $\square$

Thm 0.3 (Fundamental Theorem of Arithmetic):
Every integer $n>1$ can be written as a product of primes, and the prime factors are unique up to permuting their order

Defn: The least common multiple of $a,b\in\mathbb{Z}\setminus\{0\}$, denoted $\mathrm{lcm}(a,b)$, is the smallest positive integer that is a multiple of both a and b.

Defn: Let $a,b\in\mathbb{Z}$ with $b>0$. We write
$a \bmod b = r$ if $0\le r<b$ and there is $q\in\mathbb{Z}$ with $a=bq+r$.
In other words, $\frac{a}{b}=\frac{bq+r}{b}=q+\frac{r}{b}$ is an integer plus the non-negative remainder $\frac{r}{b}$

Ex: $4 \bmod 3 = 1$
$-4 \bmod 3 = 2$
$38 \bmod 11 = 5$
$20897 \bmod 2 = 1$
$10 \bmod 5 = 0$

Lem: Let $a_1, a_2, n\in\mathbb{Z}$ with $n>0$.
Then $a_1 \bmod n = a_2 \bmod n$ iff $n \mid (a_1-a_2)$

Pf: Pick $q_1,q_2,r_1,r_2\in\mathbb{Z}$ with $a_1=n\cdot q_1+r_1$, $a_2=n\cdot q_2+r_2$, and $0\le r_1,r_2<n$.

Then $a_1 - a_2 = n(q_1 - q_2) + r_1 - r_2$ is divisible by n iff $r_1 - r_2$ is divisible by n. Since $0 \le r_1 < n$ and $-n < -r_2 \le 0$, we have $-n < r_1 - r_2 < n$, so n divides $r_1 - r_2$ iff $r_1 - r_2 = 0$. (i.e. $r_1 = r_2$). This completes the proof since $a_1 \bmod n = r_1$ and $a_2 \bmod n = r_2$. $\square$

Lem: Let $a_1, a_2, b_1, b_2, n \in \mathbb{Z}$ with $n > 0$.
If $a_1 \bmod n = a_2 \bmod n$ and $b_1 \bmod n = b_2 \bmod n$
then ① $a_1 + b_1 \bmod n = a_2 + b_2 \bmod n$
and ② $a_1 \cdot b_1 \bmod n = a_2 \cdot b_2 \bmod n$

Proof: From previous lemma, we know $n \mid (a_1 - a_2)$ and $n \mid (b_1 - b_2)$. Therefore n divides

$$(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$$

so ① holds by previous lemma. Similarly,

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 \\ &= a_1 \underbrace{(b_1 - b_2)}_{\text{divisible by } n} + \underbrace{(a_1 - a_2)}_{\text{divisible by } n} b_2 \end{aligned}$$

is divisible by n, so ② holds. $\square$

Ex: • $38 \cdot 51 \bmod 11 = 5 \cdot 7 \bmod 11 = 35 \bmod 11 = 2$
• $19^5 \bmod 17 = 2^5 \bmod 17 = 32 \bmod 17 = 15$

Ex: Calculate last digit of 3^{403}

Fact: If $n>0$, the last digit of n is $n \bmod 10$

$3^2 \bmod 10 = 9 \bmod 10 = 9$
$3^3 \bmod 10 = 27 \bmod 10 = 7$
$3^4 \bmod 10 = 81 \bmod 10 = 1$!

$3^{403} = (3^4)^{100} \cdot 3^3$ so

$$\begin{aligned} 3^{403} \bmod 10 &= (3^4)^{100} \cdot 3^3 \bmod 10 \\ &= 1^{100} \cdot 3^3 \bmod 10 \\ &= 3^3 \bmod 10 = 7 \end{aligned}$$

Fact: If $a^h \bmod n = 1$ and $k = hq + r$ with $h, k, q, r \geq 0$ then $a^k \bmod n = a^r \bmod n$.

Ex: Prove that $x^2 - y^2 = 1002$ has no solutions with $x, y \in \mathbb{Z}$

Consider the equation mod 4.
$1002 \bmod 4 = 2$

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

$x^2 \bmod 4$ and $y^2 \bmod 4$ are each either 0 or 1

Consider all possible cases

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

So for all $x, y \in \mathbb{Z}$, $x^2 - y^2 \bmod 4 \neq 2 = 1002 \bmod 4$
and thus $x^2 - y^2 \neq 1002$

Equivalence relations generalize the concept of equality

Defn: An equivalence relation R on a set S is
a set of ordered pairs of elements of S such that:
① (Reflexive) $\forall a \in S$ $(a,a) \in R$
② (Symmetric) $\forall a, b \in S$ $(a,b) \in R \Leftrightarrow (b,a) \in R$
③ (Transitive) $\forall a, b, c \in S$ $[(a,b) \in R \text{ and } (b,c) \in R] \Rightarrow (a,c) \in R$
In this setting, we typically write "aRb" to mean "$(a,b) \in R$"
Often we use symbols such as $\sim$, $\approx$, or $\equiv$
to denote the equivalence relation R.
When R is an equivalence relation on S and $a \in S$
we define
$$[a] = [a]_R = \{ b \in S : aRb \}$$

Ex: The following are equivalence relations
- $S = P(\mathbb{N})$, $R = \{ (A,B) : A, B \in P(\mathbb{N}) \ |A| = |B| \}$
- $S = P(\mathbb{N}) \setminus \{\emptyset\}$, $R = \{ (A,B) : A, B \in S \ \min A = \min B \}$
- $S = \mathbb{Z}$, $R = \{ (n,m) \in \mathbb{Z}^2 : nm > 0 \text{ or } n = m = 0 \}$

- $S = \mathbb{R}$, $R = \{(a,b) \in \mathbb{R}^2 : \exists q \in \mathbb{Z} \;\; a = b + 2\pi q\}$
- Fix $n \in \mathbb{Z}$, $n > 0$. $S = \mathbb{Z}$, $R = \{(a,b) \in \mathbb{Z}^2 : a \bmod n = b \bmod n\}$

Defn: A partition of a set S is a collection of nonempty subsets of S that are pairwise disjoint and that have union S.

Ex: $\{\{2,3,5,6\}, \{1,7\}, \{4\}\}$ is a partition of $S = \{1,2,3,4,5,6,7\}$

Thm 0.7: ① If R is an equivalence relation on S, then $P = \{[a]_R : a \in S\}$ is a partition of S.
② If P is a partition of S, then $R = \{(a,b) \in S \times S : \exists D \in P \;\; a,b \in D\}$ is an equivalence relation on S.

Pf: ① (Pairwise disjoint) Suppose $[a]_R \neq [b]_R$. We claim $[a]_R \cap [b]_R = \emptyset$. Suppose not, say $c \in [a]_R \cap [b]_R$ (meaning $(a,c), (b,c) \in R$). For any $x \in [a]_R$ we have $(a,x) \in R$ hence $(x,a) \in R$ (symmetry). Since $(x,a), (a,c) \in R$, we have $(x,c) \in R$ (transitivity) hence $(c,x) \in R$ (symmetry). Finally, since $(c,x), (b,c) \in R$ we have $(b,x) \in R$ (transitivity) meaning $x \in [b]_R$. Therefore $[a]_R \subseteq [b]_R$ and by symmetry $[b]_R \subseteq [a]_R$. So $[a]_R = [b]_R$, contradiction. We conclude $[a]_R \cap [b]_R = \emptyset$.
(Union is S) Clearly $\bigcup P \subseteq S$. Conversely, for every $a \in S$ $a \in [a]_R$ so $\{a\} \subseteq [a]_R$ and $\bigcup P = \bigcup_{a \in S} [a]_R \supseteq \bigcup_{a \in S} \{a\} = S$

(2) Clearly $\forall a \in S$ $(a,a) \in R$ and $\forall a,b \in S$ $(a,b) \in R \Leftrightarrow (b,a) \in R$. Now let $a,b,c \in S$ and assume $(a,b),(b,c) \in R$. Pick $D, D' \in P$ with $a,b \in D$, $b,c \in D'$. Since P is a partition, either $D = D'$ or $D \cap D' = \emptyset$. But $b \in D \cap D'$, so we must have $D = D'$. Therefore $a,c \in D$ and $(a,c) \in R$. $\square$