Math 135: Post Midterm

Sets:

$$S = \{1, 2, \text{☺}, \text{☹}\}$$

$|S|$ = # of elements in $S \Rightarrow 4$

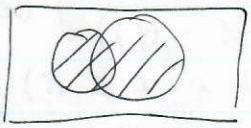
↳ $|\varnothing| = 0$, $|\{\varnothing\}| = 1$ (1 object which is a set)

Set Builder Notation

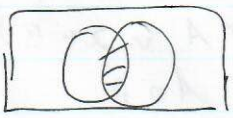
1. $\{x \in \mathcal{U} : P(x)\} \Rightarrow$ domain : statement
2. $\{f(x) : x \in \mathcal{U}\} \Rightarrow$ form of x : domain
3. $\{f(x) : x \in \mathcal{U}, P(x)\} \Rightarrow$ form of x : domain, statement (condition)

↳ $\mathbb{Q} : \left\{\frac{a}{b} : a, b \in \mathbb{R},\ b \neq 0\right\}$

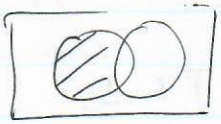
Set Operations:



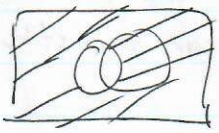
Union $\Rightarrow$ $\{x : (x \in S) \vee (x \in T)\}$
$(S \cup T)$



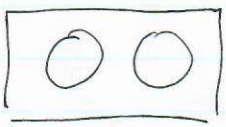
Intersection $\Rightarrow$ $\{x : (x \in S) \wedge (x \in T)\}$
$(S \cap T)$



Set Difference $\Rightarrow$ $\{x : (x \in S), \neg(x \in T)\}$
$(S - T)$



Complement $\Rightarrow$ $\{x : \neg(x \in S)\}$
$(\overline{S})$



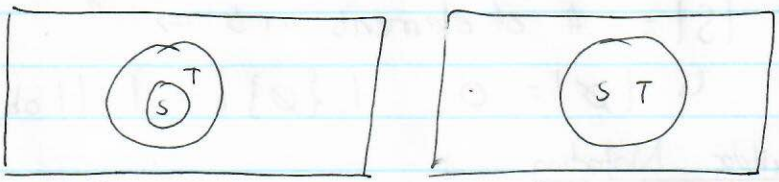
Disjoint : $S \cap T = \varnothing$

Sets $\Rightarrow$ Logical operators.
↳ Draw diagram! V. useful

Subsets:

Subset: $S \subseteq T \Rightarrow \forall x \in S$ also in T

Proper: $S \subsetneq T \Rightarrow \forall x \in S$ in T but $\neg(\forall y \in T$ are in $S)$



Proper Subset

To prove $S \subseteq T$:

1. Take arbitrary element in S
2. Arrange to make it look like it is in T
3. Proper subset: show existence of element in T NOT in S.

Be able to do this w/ logical operators:

- Ex: Prove $A - (A - B) \subseteq A \cap B$

  Assume $x \in (A - (A - B))$. Prove that $x \in (A \cap B)$

  If $x \in A - (A - B)$:

  $\Leftrightarrow x \in A \wedge x \notin (A - B)$ } Good trick!

  $\Leftrightarrow x \in A \wedge \neg(x \notin (A - B))$

  $\Leftrightarrow x \in A \wedge \neg(x \in A \wedge x \notin B)$ * Keep expanding logic *

  $\Leftrightarrow x \in A \wedge x \notin A \vee x \in B$

  Since $x \in A$ is true and $(x \notin A \vee x \in B)$ is also true,

  $x \in A \wedge x \in B \Rightarrow x \in A \cap B$

Equality

$$S = T \Leftrightarrow S \subseteq T \wedge T \subseteq S$$

Same way of proving subset except now do it x2

If proof assumes set equality, can substitute sets for one another.

Assignment Questions

1. Prove $\{3a + 5b : a, b \in \mathbb{Z}\} = \mathbb{Z}$.

   First: $\{3a + 5b : a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}$ as $3, a, 5, b \in \mathbb{Z}$, so any $x \in \{3a + 5b : a, b \in \mathbb{Z}\}$ also in $\mathbb{Z}$.

Second: To show $\mathbb{Z} \subseteq \{3a+5b : a, b \in \mathbb{Z}\}$

1. Odd + even analysis
2. Assume y is an arbitrary integer.
   We will show that y fits in $\{3a+5b : a, b \in \mathbb{Z}\}$.
   $\{3a+5b : a, b \in \mathbb{Z}\}$ and let $a = 2y$, $b = -y$

$$\therefore \quad 3a+5b = 3(2y) + 5(-y)$$
$$= 6y - 5y$$
$$= y$$

Thus $y \in \{3a+5b : a, b \in \mathbb{Z}\}$.

Key insight in problem:
Can show that some element in a set by changing set to equal element.

2. Prove that thee exists a unique T such that $S \cup T = S$.

First: prove existence.
From inspection: $S \cup \emptyset = S$

Second: prove uniqueness.
Let T' be another set where $S \cup T' = S$. We will show $T' = T$.
Nok the following set of unions.

$$T' = T' \cup T = T \cup T' = T \quad \square$$

OR

For any set $\mathbb{S}$, $T \subseteq S \cup T = S$
Consider case when $S = \emptyset$. Then $T \subseteq \emptyset \Rightarrow T = \emptyset$ which is unique.

Key insight:
① : Null set is smth. I should always account fo.
② : Chain of unions to prove uniqueness.

Greatest Common Divisor

Division Algorithm

- Bounds by Divisibility (BBD):

$$\forall a, b \in \mathbb{Z},\ b \mid a \wedge a \neq 0 \Rightarrow b \leq |a|$$

  - Proof needs following proposition:

$$\forall x \in \mathbb{R},\ |x| \geq x$$

- Division Algorithm (DA):

$$\forall a, b \in \mathbb{Z},\ b > 0,\ \exists!\ q, r,\ a = qb + r,\ 0 \leq r < b$$

  - Ex: //

    Family of $4n+k$: $a = 4k, 4k+1, 4k+2, 4k+3$

    Family of $6n+k$: $a = 6k, 6k+1, 6k+2, 6k+3, \ldots, 6k+5$

  - Esp. useful: looking at $\forall \mathbb{Z}$ + noting properties (divisibility)

Greatest Common Divisor

$$c \mid a \wedge c \mid b \Rightarrow$$ c is a common divisor

- GCD (a, b): $d = \gcd(a, b)$ if:
  1. $a \wedge b$ are not both zero:
     - $d \mid a \wedge d \mid b$ (common divisor)
     - $\forall c \in \mathbb{Z},\ c \mid a \wedge c \mid b \Rightarrow d \geq c$ (greatest of all CD)
  2. If a and b both zero: $d = 0$
  - Consider both cases!
  - Ex: // Prove $\gcd(3a+b, a) = \gcd(a, b)$

    Let $d = \gcd(3a+b)$ and $c = \gcd(a, b)$.

    Process: show $d \leq c \wedge c \leq d$ $(d = c)$ ⇐ Common trick to prove GCD

    a) Showing $d \leq c$

    Since $d = \gcd(3a+b, a) \Rightarrow d \mid (3a+b) \wedge d \mid a$

    By DIC: $d \mid (3a+b-3a) \Rightarrow d \mid b$

    Since $d \mid a \wedge d \mid b \wedge c = \gcd(a, b) \Rightarrow d \leq c$

    Show $\gcd(3a+b)$ is CD of other numbers

    b) Showing $c \leq d$

    Since $c = \gcd(a, b) \Rightarrow c \mid a \wedge c \mid b$

    By DIC: $d \mid a \wedge c \mid b \Rightarrow c \mid (3a+b)$

    Since $c \mid a \wedge c \mid 3a+b \wedge d = \gcd(3a+b, a) \Rightarrow c \leq d$

    Finally, analyzing case where both $a, 3a+b, b = 0$

    $\gcd(3a+b, a) = 0 = \gcd(a, b)$ ✓

- GCD With Remainder (GCDWR)

$\forall a, b, q, r \in \mathbb{Z}, \quad a = qb + r \Rightarrow \gcd(a,b) = \gcd(b,r)$

- Euclidean Algorithm: finding GCD:

$\gcd(39751, 13081)$

$39751 = 3(13081) + 508 \Rightarrow \gcd(39751, 13081) = \gcd(13081, 508)$

$13081 = 25(508) + 381 \Rightarrow \gcd(13081, 508) = \gcd(508, 381)$

$508 = 1(381) + 27 \Rightarrow \gcd(508, 381) = \gcd(381, 27)$

$381 = 3(127) + 0 \Rightarrow \gcd(381, 27) = \boxed{127}$

Remember: GCDWR = Euclidean Algo

- Important properties:
  1. $\gcd(a, -a) = \gcd(-a, a) = |a|$
  2. $\gcd(a, \pm 1) = 1$ (nothing else divides ± 1)
  3. $\gcd(a, 0) = |a|$

- GCDWR Proofs:
  - Ex:// Prove $\gcd(3a+b, a) = \gcd(a, b)$

    By GCDWR:

    $3a + b = 3(a) + b$

    $\therefore \gcd(3a+b, a) = \gcd(a, b)$
  - Ex:// Prove $\gcd(a, b) = \gcd(2a-3b, a-2b)$

    By GCDWR:

    $2a - 3b = 2(a-2b) + b$

    $a - 2b = -2(b) + a$

    $b = 0 \cdot a + b$ ∎ Reduced to desired gcd

    $\gcd(2a-3b, a-2b) = \gcd(a-2b, b)$

    By EA + GCDWR: $\gcd(a, b) = \gcd(2a-3b)$
  - General idea: two ways to prove $\gcd(\_\_\_) = \gcd(\_\_\_)$
    1. Use definition: show $d \le c \wedge c \le d$ by OIC + that $d|c \wedge c|d$
    2. Use GCDWR: use EA to reduce down to desired gcd

CERTIFICATE OF CORRECTNESS + BEZOUT'S LEMMA

- GCD Characterization Theorem (GCDCT)

$\forall a, b, d \in \mathbb{Z}, d \ge 0$, if:
  1. $d|a \wedge d|b$ (d is a common divisor)
  2. $\exists s, t \in \mathbb{Z} \quad as + bt = d$

then $d = \gcd(a, b)$

Very useful in proving something is gcd.

How to find certificate of correctness:

1. Back substitution
2. Extended Euclidean Algorithm

	x	y	r	q
	1	0	a	0
	0	1	b	0
$r_1 - q_1 r_2$	1	$-q_1$	$a - bq_1$	$\lfloor \frac{a}{b} \rfloor = q_1$
	⋮	⋮	⋮	$\lfloor \frac{b}{a-bq_1} \rfloor = \ldots$
			0	

) r above is gcd, whole row gives CRT

$$ax + by = r$$

- Ex: // Prove that if $\gcd(a,b) \neq 0$ and $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a,b)$, then $\gcd(x,y) = 1$

  What to prove:

  Using ~~gcd~~ GCDCT, we need to show:

  1. $\gcd(x,y) \mid 1 \;\wedge\; 1 \mid y \Rightarrow$ True
  2. $\exists m, k \in \mathbb{Z}$ s.t. $kx + my = 1$

  Assume

  $$ax + by = \gcd(a,b)$$

  Divide both sides by $\gcd(a,b)$:) Manipulate to form desired expression.

  $$kx + my = 1$$

  Therefore, by GCDCT, since $1 \mid x \wedge 1 \mid y$ and $\exists k, m \in \mathbb{Z}$ s.t. $kx + my = 1$, $\gcd(x,y) = 1$ $(1 \geq 0)$.

- Bezout's Lemma:

  $\forall a, b \in \mathbb{Z}$, $\exists s, t \in \mathbb{Z}$ such that $as + bt = d$ where $d = \gcd(a,b)$

  Reverse of GCDCT: if I have gcd, I can write a and b as linear combo to form gcd

  - Use extended Euclidean Algo to find CoC.
  - Helpful in putting relationship between a, b and $\gcd(a,b)$

- In problems:

  Show 2 conditions of GCDCT

  + Prove!

Further Properties Of GCD

- Common divisor divides GCD (CDDGCD)

  $\forall a, b, c \in \mathbb{Z},\ c \mid a \wedge c \mid b \Rightarrow c \mid \gcd(a, b)$

  - Prove $\forall a, b \in \mathbb{Z}$ and $c \in \mathbb{Z}, c \neq 0,\ \gcd(ca, cb) = c \gcd(a, b)$

    Let $d = \gcd(a, b)$ so $d \mid a \wedge d \mid b$.

    $a = kd \qquad b = md$

    Multiply both sides by c:

    $ca = kcd \qquad bc = mcd$

    $\therefore\ ca \mid cd \wedge bc \mid cd \Rightarrow$ 1st condition met.

    Also:

    $as + bt = d$

    $cas + cbt = cd$

    $(ca)s + (cb)t = cd \Rightarrow$ 2nd condition met

    → GCDCT

    By GCDCT: since $cd \geq 0$ and $d = \gcd(a, b)$,

    $cd = \gcd(ca, bc)$

- Coprimeness: $\gcd(a, b) = 1$
- Coprimeness Characterization Theorem (CCT):

  $\forall a, b \in \mathbb{Z},\ \gcd(a, b) = 1 \Leftrightarrow$ ~~$\gcd(a, b^n) \in \mathbb{Z}$~~ $at + bs = 1\ (\exists s, t)$

  - Proof:

    $\forall a, b \in \mathbb{Z},\ n \in \mathbb{N},\ \gcd(a, b) = 1 \Rightarrow \gcd(a, b^n) = 1$

    Proving via induction on n:

    Base case:

    $n = 1 \Rightarrow \gcd(a, b) = 1$ (hypothesis)

    Inductive step.

    Assume $\gcd(a, b) = 1 \Rightarrow \gcd(a, b^k) = 1 \quad k \geq 1$.

    Need to prove $\gcd(a, b^{k+1}) = 1$.

    From CCT:

    $at + sb^k = 1 \quad (\exists t, b \in \mathbb{Z})$

    Need to show:

    $ua + vb^{k+1} = 1$

    Multiply by $as + bt = 1 \Leftarrow$ Hypothesis, RHS $= 1$

    $(as + bt)(at + sb^k) = 1$

    $a(a^2s + sub^k + bt + u) + b^{k+1}(tv) = 1$

- Division by GCD (DBGCD):
  $\forall a, b \in \mathbb{Z}$ + not both zero $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ if $d = \gcd(a,b)$
- Coprimeness + Divisibility (CAD):
  $\forall a, b, c \in \mathbb{Z}$, $c \mid ab \wedge \gcd(a,c) = 1 \Rightarrow c \mid b$
  Opposite of prop 8.
  Prop. 8: $c \mid a \wedge c \mid b \Rightarrow c \mid ab$
  CAD: $c \mid ab \wedge \gcd(a,c) = 1 \Rightarrow c \mid b$

GCD

- Proving 2 GCD are equal
  1. GCDCT + BL
  2. GCDWR
- Divisibility/Multiply
  CDDGCD
  DBGCD
- Coprimeness
  1. CCT
  2. CAP

PRIMES

Euclid's Lemma:
$\forall a, b \in \mathbb{Z}$ and prime numbers p:
$p \mid ab \Rightarrow p \mid a \vee p \mid b$
↳ Similar to prop. 8 (primes)
} Generalized!

Unique Factorization Theorem / Fundamental Theorem of Arithmetic:
Every $n \in \mathbb{N}$, can be written as product of primes uniquely
↳ Can prove 2 numbers are equal if they have the same prime factorization.

Finding a Prime Factor (FPF):
For $\forall n \in \mathbb{N}$, n is prime or is thas a prime factor $\leq \sqrt{n}$
↳ Useful in figuring out if a number is prime.

PRIME FACTORIZATION + GCD

Divisors From Prime Factorization (DFPF):

Let $n \geq 2$ and $c \geq 1$ (positive integers) and let:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where $p_1 \cdots p_k$ are distinct primes and $a_1 \cdots a_k$ are ~~distinct~~ positive integers. $c \mid n$ iff.

$$c = p_1^{B_1} p_2^{B_2} \cdots p_k^{B_k} \quad (0 \leq B_k \leq A_i)$$

- Prove $a^3 \mid b^3 \Leftrightarrow a \mid b$:

"$\Leftarrow$" Assume $a \mid b$:

$$b = ka \quad (k \in \mathbb{Z})$$

Cubing both sides:

$$b^3 = k^3 a^3$$

Since $k^3 \in \mathbb{Z}$, $a^3 \mid b^3$ ✓

"$\Rightarrow$" Let $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$. be prime factorizations of a and b.

$$\therefore a^3 = p_1^{3\alpha_n} \cdots p_n^{3\alpha_n}, \quad b^3 = p_1^{3\beta_1} \cdots p_n^{3\beta_n}$$

Assume $a^3 \mid b^3$. This means that:

$$0 \leq 3\alpha_n \leq 3\beta_n$$

Dividing by 3:

$$0 \leq \alpha_i \leq \beta_i \Rightarrow \text{From DFPF, } a \mid b$$

GCD from Prime Factorization (GCDPF)

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad b = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

$$\gcd(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}$$

→ Proving gcd!

↳ Finding GCD

Proofs For Ch. 6

1. Prove $\gcd(27n-20, 4n-3) = 1$ for all $n \in \mathbb{Z}$.

We want to show that $\exists s, t \in \mathbb{Z}$, such that

$$s(27n-20) + t(4n-3) = 1$$

Consider $s = 4$, $t = -27$:

$$\begin{aligned} &4(27n-20) \text{ } \bar{+} \text{ } 27(4n-3) \\ &= 108n \text{ } \bar{+} \text{ } 80 \text{ } \bar{+} \text{ } 108n + 81 \\ &= 1 \end{aligned}$$

By CCT, since $\exists s, t$ s.t. $s(27n-20) + t(4n-3) = 1$, $\gcd(27n-20, 4n-3) = 1$.

2. Prove $\gcd(a, b) \mid \gcd(3a+b, a^3)$

Proof by CDD GCD + definition of gcd:

Since $\gcd(a, b) = d$:

$$d \mid a \wedge d \mid b$$

By DIC: $d \mid 3a+b$.

By ~~DIC~~ TD: $d \mid a \wedge a \mid a^3 : d \mid a^3$

Now, we have:

$$d \mid 3a+b \wedge d \mid a^3 \Rightarrow d \mid \gcd(3a+b, a^3) \quad (\text{CDD GCD})$$

3. Suppose $a \mid (4b+5c) \wedge a \mid (2b+2c)$. Prove that if a is odd, then $a \mid b \wedge a \mid c$.

Odd $\Rightarrow$ coprime element?

By DIC:

$$a \mid (4b+5c) \wedge a \mid (2b+2c) \Rightarrow a \mid c$$

By DIC:

$$a \mid (4b+5c) \wedge a \mid (2b+2c) \Rightarrow a \mid 2b.$$

Since a is odd, by CAD:

$$a \mid 2b \wedge \gcd(a, 2) = 1 \Rightarrow a \mid b$$

4. $\gcd(a,b,c) = \gcd(a, \gcd(b,c))$

We don't have any definition for 3 number gcd $\Rightarrow$ back to the definition:

Let $d = \gcd(a,b,c)$

$\therefore \; d|a \wedge d|b \wedge d|c.$

From CDD GCD, $\quad d|b \wedge d|c \Rightarrow d|\gcd(b,c).$

$\therefore d|a \wedge d|\gcd(b,c) \Rightarrow \underline{d \le \gcd(a, \gcd(b,c))}$

Let $e = \gcd(b,c)$:

$\therefore \; e|b \wedge e|c.$

Let $f = \gcd(a,e)$:

$\therefore \; f|a \wedge f|e$

$f|a \wedge (f|b \wedge f|c)$:

VERY COMMON PROOF TECHNIQUE

By definition:

$\underline{f \le \gcd(a,b,c)}.$

We have 2 inequalities:

① $d \le f$ ② $f \le d$ $\Big\}$ $\boxed{d = f}$

5. Find # of pos. int. n such that $n|10! \wedge \gcd(n, 2^7 \cdot 3^4 \cdot 7) = 2^7 \cdot 3 \cdot 7$

Prime factorization of $10! = 7 \cdot 5^2 \cdot 3^4 \cdot 2^8$

If $n|10!$, then by DFPF:

$n = 7^{\beta_1} \cdot 5^{\beta_2} \cdot 3^{\beta_3} \cdot 2^{\beta_4}$

$0 \le \beta_1 \le 1$

$0 \le \beta_2 \le 2$

$0 \le \beta_3 \le 4$

$0 \le \beta_4 \le 8$

By GCDPF (b/c they gave prime factorizations):

$1 = \min\{\beta_1, 1\} \Rightarrow \beta_1 = 0, 1$

$0 = \min\{\beta_2, 0\} \Rightarrow \beta_2 = 0, 1, 2$

$1 = \min\{\beta_3, 4\} \Rightarrow \beta_3 = 1$

$7 = \min\{\beta_4, 7\} \Rightarrow \beta_4 = 10\text{ish}\ 7, 8$

$\Big\}$ 6 options for n

6. Prove $\gcd(m^2, n^2) = (\gcd(m,n))^2$

$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$

$\gcd(m,n) = p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$

$(\gcd(m,n))^2 = p_1^{2\min\{\alpha_1,\beta_1\}} \cdots p_k^{2\min\{\alpha_k,\beta_k\}}$

$\gcd(m^2,n^2) = p_1^{\min\{2\alpha_1, 2\beta_1\}} \cdots p_k^{\min\{2\alpha_k, 2\beta_k\}}$

If $(\gcd(m,n))^2 = \gcd(m^2,n^2) \Rightarrow \min\{a_i \times 2, \beta_i \times 2\} = 2\min\{a_i, \beta_i\}$ for all $i = 1 \ldots k$.

Proving the minimum lemma:

① $\alpha_i < \beta_i$

$\min\{a_i \times 2, \beta_i \times 2\} = 2\alpha_i$

$2\min\{a_i, \beta_i\} = 2\alpha_i$

② $\alpha_i \geq \beta_i$

$\min\{a_i \times 2, \beta_i \times 2\} = 2\beta_i$

$2\min\{a_i, \beta_i\} = 2\beta_i$

Equal ∴ PF of GCD are equal ∴ Proven.

CH. 7: LINEAR DIOPHANTINE EQUATIONS

$ax + by = c \quad (a, b, c \in \mathbb{Z})$

1. variable: $ax = b$ (solution iff $a \mid b$)

2. variables:

#1: $ax + by = c \Leftrightarrow d \mid c \quad (d = \gcd(a,b))$

#2: If a & b are both not zero, $d = \gcd(a,b)$ and (x_0, y_0) is a particular solution, then:

$$\left\{(x,y) : x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n,\ n \in \mathbb{Z}\right\}$$

Process for solving LDE:

1. Find a certificate of correction for $\gcd(a,b)$.
2. Multiply both sides so we can get c on RHS.
3. Use values for x_0 and y_0 to construct full set.

Ch. 8: Congruences

$a \equiv b \pmod m \Leftrightarrow m \mid a-b$

Properties

Congruence is an Equivalence Relation (CER)

1. Reflexivity: $a \equiv a \pmod m$
2. Symmetry: If $a \equiv b \pmod m$ then $b \equiv a \pmod m$
3. Transistive: If $a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

Congruence Add and Multiply (CAM)

$$a_i \equiv b_i \pmod m \begin{cases} a_1 + a_2 + \dots + a_n \equiv b_1 + b_2 + \dots + b_n \pmod m \\ a_1 a_2 a_3 \dots a_n \equiv b_1 b_2 \dots b_n \pmod m \end{cases}$$

Congruence Power (CP)

$$a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$$

Is $\underline{x}$ divisible by $\underline{y}$: $\boxed{x \equiv 0 \pmod y}$

Ex: // Prove $7 \mid 5^9 + 62^{2000} - 14$

Break up one by one:

$5^9 + 62^{2000} - 14 \Rightarrow$

$5^9 = (5^2)^2 \cdot 5$

$\equiv 16 \cdot 5$

$\equiv$

5^9: Break up 5^9 into smaller powers + multiply up

① $5^2 = 25 \equiv 4 \pmod 7$

$\times 5$ ($5^3 = 5 \cdot 4 \pmod 7$

$= -1 \pmod 7$

$(5^9 \equiv (-1)^3 \pmod 7$

$\equiv -1 \pmod 7$

② 62^{2000}:

$62 \equiv -1 \pmod 7$

$62^{2000} \equiv (-1)^{2000} \pmod 7$

$\equiv 1 \pmod 7$

③ $14 \equiv 0 \pmod 7$

Combine all:

$5^9 + 62^{2000} - 14 \equiv -1 + 1 + 0 \pmod 7$

$\equiv 0 \pmod 7$

* Biggest Tip: Go to as close to 0 as possible when reducing/simplifying $(-2, -1, 0, 1, 2)$

Congruence Divide (CD)

$ac \equiv bc \pmod m \wedge \gcd(c, m) = 1 \Rightarrow a \equiv b \pmod m$

- If $\gcd(c, m) \neq 1$: CD tells nothing. (true if $\gcd(c, m) \neq 1$)

CONGRUENCE + REMAINDERS

Congruence Iff Same Remainder (CISR)

$a \equiv b \pmod m \Leftrightarrow a, b$ same remainder when divided by m

Congruent to Remainder (CTR)

$0 \leq b < m$, $a \equiv b \pmod m \Leftrightarrow a$ has remainder b when divided by m.

- Ex: //

$53 \equiv 4 \pmod 7 \Rightarrow 4$ is remainder of $53 \div 7$.

- Problem strat: take large congruence + simplify to number less than modulus.
  - Ex: // Determine remainder when $2^{22} 3^{33} 5^{55}$ is divided by 11.

$$\begin{aligned} 2^{22} 3^{33} 5^{55} &\equiv (2^5)^4 \cdot 2^2 \cdot (3^2)^{16} 3 \cdot (5^2)^{27} 5 \pmod{11} \\ &\equiv (-1)^4 \cdot 4 \cdot (-2)^{16} 3 \cdot 3^{27} \cdot 5 \pmod{11} \\ &\equiv 2^{18} 3^{28} \cdot 5 \pmod{11} \\ &\equiv (2^5)^3 \cdot 2^3 \cdot (3^2)^{14} \cdot 5 \pmod{11} \\ &\equiv (-1)^3 \cdot 8 \cdot (-2)^{14} \cdot 5 \pmod{11} \\ &\equiv -2^{17} \cdot 5 \pmod{11} \\ &\equiv -(2^5)^3 \cdot 2^2 \cdot 5 \pmod{11} \\ &\equiv -(-1)^3 \cdot 2^2 \cdot 5 \pmod{11} \\ &\equiv 20 \pmod{11} \\ &\equiv 9 \pmod{11} \end{aligned}$$

1. Find closest power of base to modulus / multiple of modulus
2. Combine with bases of similar kind (combine all 2^x)
3. Repeat

- Last decimal digit: remainder when divided by 10 ($a \equiv b \pmod{10}$)

Divisibility tests:

1. Write out decimal representation of arbitrary number: $x = d_k 10^k + d_{k-1} 10^{k-1} + \dots + d_0$
2. Look at congruence of $10 \pmod m$
3. Simplify. + put condition of $x \equiv 0 \pmod m$

Know 3 and 9 divisibility tests + $11 \mid (S_e - S_o \mid 11$

(S_e: sum of digits of even 10 powers; S_o: sum of digits of odd 10 powers)

LINEAR CONGRUENCE

$$ax \equiv c \pmod{m} \rightarrow \text{What is } x?$$

Key: Convert to LDE

$$ax \equiv c \pmod{m}$$
$$ax - c = mk$$
$$ax + mk = c \quad \in \text{Solve.}$$

1. Find 1 solution using EEA
2. Find full set of solutions using LDET 2

OR.

If m is small, look through all possible values $(0 \ldots m-1)$

Ex: // Find complete solution of $27y \equiv 36 \pmod{90}$.

1. Convert to LDE:
$$27y + 90k = 36$$
2. Find soln via inspection or EEA
$$\text{Soln: } (-3, 1)$$
$$27(-3) + 90 = 9$$
$$27(-12) + 90(4) = 36 \quad \} \times 4$$
3. Wrik complete solution via LDET 2:
$$y = -12 + 10k \quad (k \in \mathbb{Z})$$
4. Convert to congruence:
$$y \equiv 2 \pmod{10}$$

↑ Putting into mod 90.

Loop through k in mod 90 ($k = 0, 1, 2, 3, 4, 5, 6, 7, 8$) ← Desired m from $0 - \frac{m}{d} - 1$

Non linear:

1. Make table of all terms
2. Loop through all possible values from $x \equiv 0 \cdots m-1$ + add up

Linear Congruence Theorem (LCT)

1. $ax \equiv c \pmod{m}$ has a soln $\Leftrightarrow \gcd(a, m) \mid c$
2. If $x = x_0$ is a solution, then:

$$\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\tfrac{m}{d}}\} \Rightarrow 1 \text{ soln mod } \tfrac{m}{d}$$

OR

$$\{x \in \mathbb{Z} : x \equiv x_0, x_0 + \tfrac{m}{d}, x_0 + 2\left(\tfrac{m}{d}\right), \ldots, x_0 + (d-1)\tfrac{m}{d} \pmod{m}\}$$

↳ d solutions mod m

Congruence Classes + Modular Arithmetic

$$[a] \equiv \{x \in \mathbb{Z} \;:\; x \equiv a \pmod m\}$$

mod 4: $[0], [1], [2,], [3] \in \mathbb{Z}_4$

- Addition + subtraction:

$$[a] + [b] = [a+b]$$
$$[a][b] = [a \cdot b]$$

- Multiplicative: if $[b]$ is the mult. inverse of $[a]$. } Not all congruence classes have an inverse.

$$[a][b] = [1]$$

- Modular Arithmetic Theorem (MAT):

$$[a][x] = [c] \Leftrightarrow ax \equiv c \pmod m$$

By LCT so

1. Has soln: $\gcd(a, m) = 1$.
2. Solution set:

$$x = \left[x_0 + \frac{m}{d}\right], \left[x_0 + 1\,\frac{m}{d}\right], \ldots \left[x_0 + (d-1)\,\frac{m}{d}\right]$$

- Use this when trying to solve modular equations, like inverse.
- Ex:// Find multiplicative inverse of $[7]$ in $\mathbb{Z}_9$.

$$\therefore [7][x] = [1]$$

1. Convert to linear congruence.

$$7x \equiv 1 \pmod 9$$

2. Check soln: $\gcd(7, 9) \mid 1 \Rightarrow$ soln.

$$7x + 9y = 1$$

$x = 4$ is a solution

$\therefore [4] \Rightarrow$ Full solution set by MAT

$\therefore [7][9] = [1] \Rightarrow$ Solve more complicated

- Inverses:
  1. Inv in $\mathbb{Z}_m$:
     $\exists!$ inverse of a iff $\gcd(a, m) = 1$
  2. Inv in $\mathbb{Z}_p$: unique
     All non zero congruence classes in $\mathbb{Z}_p$ will have an inverse.
- To simplify equations:
  1. Convert to smaller congruences.
  2. Use multiplicative inverse to simplify.

Fermat's Little Theorem

$$a^{p-1} \equiv 1 \pmod{p} \qquad (p \nmid a)$$
$$\Downarrow$$
$$a^p \equiv a \pmod{p}$$

Multiplicative inverse: $[a]^{p-1} = 1$

$[a][a^{p-2}] = 1 \Rightarrow [a] = [a^{p-2}]$ in $\mathbb{Z}_p$.

Use when raising congruences to powers with mod p.

Ex:// Remainder when 3167^{2531} is divided by 17.

$3167 \equiv 5 \pmod{17}$

$\therefore 3167^{16} \equiv 1 \pmod{17}$ 17 prime!

Split 2531 into 16:

$$16 \overline{)2531}\ 158$$
$$16$$
$$93$$
$$80$$
$$131$$
$$128$$
$$3$$

$\therefore 3167^{2531} \equiv (3167^{16})^{158} \cdot 3167^3 \pmod{17}$ ↓ FLT

$\equiv 3167^3 \pmod{17}$

$\equiv 5^3 \pmod{17}$

$\equiv 6 \pmod{17}$

Chinese Remainder Theorem: Simultaneous Congru.

$\forall a_1, a_2 \in \mathbb{Z}$, $m_1 + m_2 \geq 0, \in \mathbb{Z}$. $\gcd(m_1, m_2) = 1$

$\Rightarrow$

$n \equiv a_1 \pmod{m_1}$

$n \equiv a_2 \pmod{m_2}$

has a unique solution in $m_1 m_2$. All solutions:

$n \equiv n_0 \pmod{m_1 m_2}$

$m_1 m_2$ is small ← → $m_1 m_2$ is large.

1. What if $m_1 m_2$ is small.
   - Ex: // Solve the simultaneous equation.
     ① $n \equiv 2 \pmod 3$
     ② $n \equiv 3 \pmod 5$
     1. Check if solution exists: $\gcd(3,5) = 1$
     2. Solution: $n \equiv n_0 \pmod{15}$
     3. Check all number from $0, \ldots, m_1 m_2 - 1$ + see if it fits the above simultaneous congruences.
        ∴ ①: 2, 5, (8), 11, 14
        ②: 3, (8), 13
     4. Find common solution:
        ∴ $n \equiv 8 \pmod{15}$

2. What if m_1, m_2 is large? Or not coprime?
   - Ex: // Solve the simultaneous congruence.
     ①: $x \equiv 2 \pmod{27}$
     ②: ~~$24x \equiv 24^{12} \pmod{63}$~~
     1. Find the simple congruence → LDE:
        ①: $x = 2 + 27k$
     2. Substitute the LDE into the other equation + make that into an LDE:
        ∴ $24^{12}(2+27k) \equiv 24^{12} \pmod{63}$
        ~~$48 + 324k = 24^{12} + 63y$~~
        $48 + 648k \equiv 12 + 63y$
        $648k \equiv 27 \pmod{63}$ ⇐ Finding values of k s.t. ② is satisfied.
     3. Find 1 solution via inspection / LDE
        ∴ $k = 5$ is a solution.
     4. Use LCT to find full set of solution
        $k \equiv 5 \pmod{9}$
        ∴ $k \equiv 5 + 7m$
     5. Plug back into ①:
        $x = 2 + 27(5 + 7m)$
        $x = 137 + 189y$
        ∴ $x \equiv 137 \pmod{189}$

3. If coefficients:
   $3x \equiv 2 \pmod 5$
   $2x \equiv 6 \pmod 7$
   } 1. Find $x \equiv \ldots$ solution.
   2. Do simultaneously.

SPLITTING THE MODULUS

If $n \equiv a \pmod{m_1 m_2}$ where $\gcd(m_1, m_2) = 1$, then it has the same solutions as

$$n \equiv a \pmod{m_1}$$
$$n \equiv a \pmod{m_2}$$

Esp. useful when dealing with large modulus + ugly non-linear eq.

Some tips:

1. Look at prime factorization of modulus.
2. Split up
3. Try to solve individual congruences.
4. Combine via CRT + simultaneous congruence strat.

- Ex: // Let $a \in \mathbb{Z}$. If $\gcd(a, 77) = 1 \Rightarrow a^{30} \equiv 1 \pmod{77}$

Let a be an arbitrary integer. Assume $\gcd(a, 77) = 1$.

By SMT: $a^{30} \equiv 1 \pmod{77}$ has the same solutions as the simultaneous congruences:

① : $a^{30} \equiv 1 \pmod{7}$

② : $a^{30} \equiv 1 \pmod{11}$

I want to use FLT, but not sure if $7 \mid a$ or $11 \mid a$.

From assumption: $\gcd(a, 77) = 1$

By BL:

$$as + 77t = 1$$
$$as + 7(11t) = 1$$
$$as + 11(7t) = 1$$

→ By CCT $\gcd(a, 7) = \gcd(a, 11) = 1$

Now, we can use FLT:

$$a^6 \equiv 1 \pmod{7}$$
$$\therefore a^{30} \equiv 1 \pmod{7} \checkmark$$
$$a^{10} \equiv 1 \pmod{11}$$
$$a^{30} \equiv 1 \pmod{11} \checkmark \quad \square$$

- Ex: // Solve $x^{14} + 3x^{13} + x^{12} + 4x + 4 \equiv 8 \pmod{12}$

By SMT: Same solutions as simultaneous congruences.

① $x^{14} + 3x^{13} + x^{12} + 4x + 4 \equiv 8 \pmod{3}$

② $x^{14} + 3x^{13} + x^{12} + 4x + 4 \equiv 8 \pmod{4}$

①: Simplify via FLT + solve for x

CHAPTER 9: RSA

PLAINTEXT $\xrightarrow{\text{Encryption}}$ CIPHERTEXT $\xrightarrow{\text{Decryption}}$ PLAINTEXT

- Private key system: user has 2 keys (public + private key)
  - $A \to B$: A uses B's public key for encryption, but only B can decrypt using private key
  - No one can use public key to find private key.

1. Setup
   1. Find distinct primes p and q. Let $n = pq$
   2. Find an integer e s.t. $\gcd(e, (p-1)(q-1)) = 1 \wedge 1 < e < (p-1)(q-1)$
   3. Solve $ed \equiv 1 \pmod{(p-1)(q-1)}$ for d.
      ↳ Use LOE.
   4. Public key: (e, n)
   5. Private key: (d, n)
2. Encryption:
   1. Take public key and $M < n$
   2. $C \equiv M^e \pmod{n}$
3. Decryption.
   1. $R = C^d \pmod{n}$

Easy way to perform calculations w/ RSA: square + multiply

1. Let us have $25^{23} \equiv \_\_ \pmod{143}$
2. Divide 25^{23} into squares.
   $$25^{23} = 25^{16} \cdot 25^4 \cdot 25^2 \cdot 25$$
3. Calculate congruence for each square + use to multiply together:
   $$25^2 \equiv 625 \equiv 53 \pmod{143}$$
   $$25^4 \equiv 53^2 \equiv x \pmod{143}$$
   $$25^{16} \equiv x^4 \equiv y \pmod{143}$$

Ch. 10: Complex Numbers

Complex Numbers Intro

If $z \in \mathbb{C}$: $z = x + yi \quad (x, y \in \mathbb{R})$

$\text{Re}(z) = x, \quad \text{Im}(z) = y.$

Same operations as real except:

- Multiplicative inverse: use this instead of division.
  - To find:
    $$z^{-1} = (x+yi)^{-1} = \frac{1}{x+yi} \Leftarrow \text{'Rationalize'}$$
  - Note: Unique to every complex numbe.
- Exponent laws: hold unless exponents are rational.
  - Use DMT
- Complex equality:

  Let $z, w \in \mathbb{C}$, If $z = w$, then.

  $$\text{Re}(z) = \text{Re}(w) \wedge \text{Im}(z) = \text{Im}(w)$$
  - When doing problems: use this properly to construct 2 eqns + solve simultaneously.
  - Ex: $6z^3 + (1+3\sqrt{2}i)z^2 - (11-2\sqrt{2}i)z - 6 = 0$
    - Split up z into $x+yi$ OR if they say that it is a real/imaginary soln, use this
    - Create 2 eqns $(\text{Re}(z) = \text{Re}(0))\ (\text{Im}(z) = \text{Im}(0))$

Conjugates

If $z = x+yi, \quad \bar{z} = x - yi$

- Properties:
  1. $(\bar{\bar{z}}) = z$
  2. $\overline{z+w} = \bar{z} + \bar{w}$
  3. $z + \bar{z} = 2\text{Re}(z)$] → Used in proofs!
  4. $z - \bar{z} = 2\,\text{Im}(z)i$]
  5. $\overline{zw} = \bar{z} \cdot \bar{w}$
  6. $(\overline{z^{-1}}) = (\bar{z})^{-1}$
- Solving conjugate problems: either split into $(x+yi)$ form or take conjugates of both sides / convert terms to each other via conj.

- Ex:// Suppose $z, w \in \mathbb{C}$ where $w \neq 0$. Prove $z \in \mathbb{R} \Leftrightarrow z = \bar{z}$

"$\Rightarrow$" Assume $z \in \mathbb{R}$. $\therefore Im(z) = 0$

$$z - \bar{z} = 2Im(z)$$
$$z - \bar{z} = 0$$
$$z = \bar{z}$$

"$\Leftarrow$" Assume $z = \bar{z}$

$$z - \bar{z} = 0$$
$$\therefore 2Im(z) = 0$$
$$\therefore Im(z) = 0.$$

Modulus

$$|z| = \sqrt{a^2 + b^2}$$

Properties:

1. $|z| = 0 \Leftrightarrow z = 0$
2. $|\bar{z}| = |z|$
3. $z\bar{z} = |z|^2$
4. $|z||w| = |zw|$
5. If $z \neq 0$, then $|z^{-1}| = |z|^{-1}$

Proof tricks:

1. Squaring!
2. Rearrange to form $(z \cdot \bar{z}) \rightarrow |z|^2$
3. Real + Im properties.

Triangle Inequality:

$$|z + w| \leq |z| + |w|$$

- Ex:// Prove:

$$\frac{z}{1+z^2} \in \mathbb{R} \Leftrightarrow z \text{ is real or } |z| = 1$$

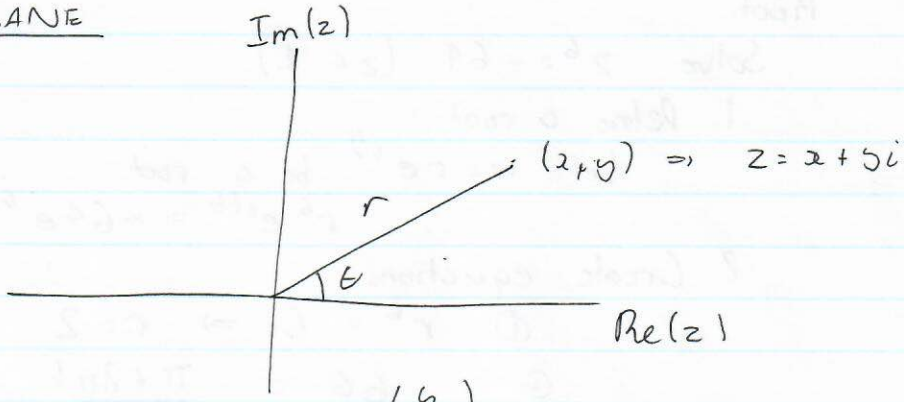
$$\frac{z}{1+z^2} \in \mathbb{R} \Leftrightarrow \frac{z}{1+z^2} = \left(\overline{\frac{z}{1+z^2}}\right)$$

$$\Leftrightarrow \frac{z}{1+z^2} = \frac{\bar{z}}{1+\bar{z}^2}$$

$$(z \cdot \bar{z})\bar{z} = \bar{z}(1+z^2)$$
$$|z|^2 \bar{z} = \bar{z}(1+z^2)$$
$$z \cdot \bar{z}^2 - \bar{z} * \bar{z}z^2 = 0$$
$$\bar{z}($$

Factor out to OR statements.

Complex Plane



$r = |z| \quad \theta = \tan^{-1}\left(\frac{y}{x}\right) \Rightarrow$ Polar form.

Be able to convert complex # $\Leftrightarrow$ polar form

$\therefore x = r\cos\theta, \; y = r\sin\theta$

Polar form rep. of complex number:

$$z = r(\cos\theta + i\sin\theta)$$

- Make sure this is the exact form + manipulate if not.

Polar Operations

Multiplication:

$$\left.\begin{aligned} z &= r_1(\cos\theta_1 + i\sin\theta_1) \\ w &= r_2(\cos\theta_2 + i\sin\theta_2) \end{aligned}\right\} \rightarrow zw = r_1 r_2 [\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)]$$

Powers (De Moivre's Theorem, DMT).

$$z = r(\cos\theta + i\sin\theta)$$
$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

Use this if trig ratios pop up.

- Ex: // Prove $\forall n \in \mathbb{Z}$, if $w \in \mathbb{C}$, $|w| = 1$ and θ is an argument w then:

$$-\frac{i}{2}(w^n - w^{-n}) = \sin n\theta.$$

Let $w = \cos\theta + i\sin\theta \Leftarrow |w| = 1$

$$\therefore -\frac{i}{2}(\cos n\theta + i\sin n\theta - \cos(-n\theta) - i\sin(-n\theta))$$

Odd + even analysis.

$$= -\frac{i}{2}(\cos n\theta + i\sin n\theta - \cos(n\theta) + i\sin n\theta)$$
$$= -i^2 \sin n\theta$$
$$= \sin(n\theta)$$

Roots:

Solve $z^6 = -64 \quad (z \in \mathbb{C})$.

1. Define a root:

Let $w = re^{i\theta}$ be a root.

$\therefore \quad r^6 e^{i6\theta} = -64e^{i(\pi + 2\pi k)}$

2. Create equations:

① $r^6 = 64 \Rightarrow r = 2$

② : $6\theta = \frac{\pi + 2\pi k}{1}$

$\theta = \frac{\pi + 2\pi k}{6}$

3. Loop from $k = 0 \ldots (n-1)$

$\therefore \theta = \pi/6, \pi/2, \frac{5\pi}{6}, \frac{7\pi}{6}, \frac{3\pi}{2}, \frac{11\pi}{6}$.

4. Create full solution set

$z = 2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}), 2(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}) \ldots$

5. Convert to standard form.

Complex N^{th} Roots Theorem (CNRT)

There are n roots of z^n. Formula given.

QUADRATIC FORMULA

$z = \frac{-b \pm w}{2a} \Rightarrow w^2 = b^2 - 4ac$

↳ Use CNRT to find w

+ plug in 1.

Solve complex polynomials either through

1) Expand to $x + yi$ (useful if conjugates involved)
2) Formula.

Ch. 11: Polynomials

Terminology

- Fields: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$
  - $\mathbb{Z}_m$ where m is not prime is a good example of a non-field.
    - ↳ Reason: $\mathbb{Z}_m$ not always have multi. inverse.
  - Really important field property.

$$ab = 0 \Rightarrow a = 0 \vee b = 0$$

Contra: $a \neq 0 \wedge b \neq 0 \Rightarrow ab \neq 0$. } → Useful in proofs.

- Polynomial in $\mathbb{F}[x]$: all coefficients $\in \mathbb{F}$.
- Polynomial equality: degree is same + coefficients of each term is same
- Arithmetic:

With mod ~~fields~~ set, reduce dom.
Also, don't use FLT.

Degree

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

Extremely useful in proofs ⇒ contradictions, factors.

Division

- Theorem: Division Algorithm for Polynomials (DAP)

$$f(x) = q(x)g(x) + r(x) \quad \text{if } g(x) \mid f(x)$$

  - $r(x)$:

$r(x) = 0 \Rightarrow g(x) \mid f(x)$. Proof technique: DP $\deg(r(x)) < \deg(g(x))$

- Long division / synthetic division.
- Modulus divisions: be careful. Reduce if possible.
- Ex: // In $\mathbb{Z}_5[x]$, $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 1$. $g(x) = 2x^2 + 3x + 4$.
  Find quotient + remainder when $f(x) \div g(x)$.

$$\begin{array}{r|l} & 3x^2 + 4x + 4 \\ \hline 2x^2 + 3x + 4 & x^4 + 2x^3 + 2x^2 + 2x + 1 \\ & \underline{x^4 + 4x^3 + 2x^2} \quad \Leftarrow \text{Multiply s.t. congruent} \\ & -3x^3 + 0 + 2x \quad \text{to same coefficient.} \\ & \underline{3x^3 + 2x^2 + x} \\ & 3x^2 + x + 1 \\ & \underline{3x^2 + 2x + 1} \\ & 4x \end{array}$$

$\therefore q(x) = 3x^2 + 4x + 4$, $r(x) = 4x$

- Ex: // $f(x) \mid g(x) \wedge g(x) \mid f(x) \Rightarrow f(x) = c\,g(x)$.

Assume $f(x) \mid g(x) \wedge g(x) \mid f(x)$. By DAP:

$g(x) = q_1(x) \cdot f(x)$. $\quad f(x) = q_2(x)\, g(x)$.

By DP:

$$\deg(g(x)) = \deg(q_1(x)) + \deg(f(x)) \quad -①$$
$$\deg(f(x)) = \deg(q_2(x)) + \deg(g(x)) \quad -②$$

→ Very clear to use DP
↳ Show factors / multiples / constants
↑ Algebra of DP

In ②:

$$\deg(f(x)) = \deg(q_2(x)) + \deg(q_1(x)) + \deg(f(x))$$
$$\therefore \deg(q_1(x)) + \deg(q_2(x)) = 0.$$

Since $\deg(q_1(x)) \geq 0 \Rightarrow \deg(q_1(x)) = \deg(q_2(x)) = 0$.

$\therefore \deg(q_2(x)) = 0 \Rightarrow q_2(x) = c$.

$\therefore f(x) = c\,g(x)$.

Do not forget case → If $f(x)$ or $g(x) = 0$. From assumption: $g(x) \mid f(x)$ so both $f(x) = g(x) = 0 \Rightarrow f(x) = c\,g(x)$.

REMAINDER THEOREM

If $f(x)$ is divided by c, then remainder is $f(c)$.

- Ex: // In $\mathbb{Z}_7[x]$, what is remainder when $f(x) = 4x^3 + 2x + 5$ is divided by $x + 6$?

By RT: $f(-6) = f(1) =$ remainder ⇒ Convert to lowest possible value!

$f(1) = 4 + 2 + 5 = 4$ in $\mathbb{Z}_7$

FACTOR THEOREM

$x - c$ is a factor of $f(x) \Leftrightarrow f(c) = 0$ (c is a root)

REDUCIBLE + IRREDUCIBLE

Reducible: $f(x) = g(x)\,h(x)$ where $\deg(g(x)) \wedge \deg(f(x)) > 0$.

Reducible in $\mathbb{F}[x]$: all polynomials in the field.

↳ Proof technique: show irreducibility.

- Ex: Prove $x^2 + 1$ is irreducible in $\mathbb{R}$

↑ FSOC: $x^2 + 1$ is irreducible in

$x^2 + 1 = f(x)\,g(x)$.

Show that factors are linear using DP

$\deg(x^2+1) = \deg(f(x)) + \deg(g(x))$

$\therefore 2 = \deg(f(x)) + \deg(g(x))$

↳ $f(x)$ + $g(x)$ have to be linear.

$x^2 + 1 = (x - c_1)(x - c_2)$ FT

$\therefore c_1$ is a root.

$c_1^2 + 1 = 0$

$c_1^2 = -1$ → $c_1 \notin \mathbb{R}$

Multiplicity: ~~the~~ max # of times a root appears.

- Ex:// Write $f(x) = x^4 + x^3 + 3x^2 + 2$ as a factor of irreducible polynomials in $\mathbb{Z}_5$.

1. Write down possible values of x in system that are as close as possible to 0.

$\therefore x = -2, -1, 0, 1, 2$ (0, 1, 2, 3, 4 → 0, 1, 2, -2, -1)

2. Use factor theorem to find 1 root:

$$f(-2) = (-2)^4 + (-2)^3 + 3(-2)^2 + 2$$
$$= 1 + 3 + 2 + 2$$
$$= 3 \times$$

$$f(2) = f(-2) = 0$$

$\therefore (x+2)(x-2)$ are factors by FT

3. Find remaining via long division.

$$x^2 - 4 \;\overline{)\; x^4 + x^3 + 3x^2 + 2 + x}$$

$x^2 + x + 2$

$x^4 \quad - 4x^2$

$x^3 + 2x^2 + 2$

$x^3 - 4x$

$2x^2 + 4x + 2$

$2x^2 \quad - 8$

$4x \quad 0$

$\therefore x^4 + x^3 + 3x^2 + 2 + x = (x+2)(x-2)(x^2 + x + 2)$.

4. To do irreducibility:

- Proof via DP
- $\mathbb{Z}_m$: Plug in possible values, show that none of them lead to $f(a) = 0$.

FUNDAMENTAL THEOREM OF ALGEBRA

$\forall f(x) \in \mathbb{C}$, if $\deg(f(x)) \geq 1$, then it has a root $\in \mathbb{C}$.

↳ Reducible to linear factors.

* Complex polynomial → reducible to linear *

Number of Roots

- Complex Polynomials of Degree N has N Roots.
  - * Repeated roots are allowed *.

Conjugate Roots

$f(x)$ s.t. real coefficients $\wedge$ $c \in \mathbb{C}$ s.t. $f(c) = 0$

then I know that $f(\bar{c}) = 0$.

Extremely useful $\Rightarrow$ double the amount of roots known.

- Ex: // Prove $\forall c_1, c_2 \in \mathbb{F}$, $c_1 \neq c_2$, if c_1 and c_2 are roots of $f(x)$, then $(x-c_1)(x-c_2) \mid f(x)$.

  Ass Let c_1, c_2 be arbitrary roots of $f(x)$. In other words: $f(c_1) = 0$, $f(c_2) = 0$.

  By FT:

  $$f(x) = q_1(x)(x-c_1) \quad -①$$
  $$f(x) = q_2(x)(x-c_2) \quad -②$$

  * Want to show: $f(x) = \underline{h(x)(x-c_1)(x-c_2)}$ $\rightarrow q(x)$!

  See how relate equations to one another!

  Substitute c_2 into ①:

  $$f(c_2) = q_1(c_2)(c_2 - c_1) = 0$$

  From $\mathbb{F}$: either $c_2 = c_1$ or $q_1(c_2) = 0$.

  $\therefore$ $q_1(x) = h(x)(x-c_2)$ by FT.

  $\therefore$ $f(x) = (x-c_2)(x-c_1)q_1(x) \Rightarrow (x-c_2)(x-c_1) \mid f(x)$

Rational Root Theorem

$$f(x) = a_0 + a_1 x_1 + a_2 x^2 + \dots + a_n x^n$$

↳ Roots: If p/q is a rational root + $\gcd(p,q) = 1$,
then $p \mid a_0$, $q \mid a_n$.
↳ Integer coefficients.

* Narrow down roots by looking at all possible p/q *

1. Find possible roots
2. Find roots s.t. $f(c_i) = 0$.
3. Division to find other factors.

Cooler application: showing numbers are irrational.

- Ex: // Prove $\sqrt{5}+\sqrt{3}$ is irrational.

1. Contradiction.

FSOC: let $\sqrt{5}+\sqrt{3} \in \mathbb{Q}$.

$$c = \sqrt{5}+\sqrt{3}$$

2. Convert to integer coefficients.

$$c^2 = 8 + 2\sqrt{15}$$
$$c^2 - 8 = 2\sqrt{15}$$
$$(c^2-8)^2 = 4 \cdot 15$$
$$c^4 - 16c^2 + 64 = 60$$
$$c^4 - 16c^2 + 4 = 0$$

} Converting to integer coefficients.

3. Convert to a function + use RT.

This means that c is a root of $f(x) = x^4 - 16x^2 + 4$.

4. Check if there are rational roots for $f(x)$:

By RRT, all rational roots should be in form p/q where $p \mid 4$ & $q \mid 1$.

$$p = \pm 1, \pm 2, \pm 4$$
$$q = \pm 1.$$

$$\therefore \frac{p}{q} = \pm 1, \pm 2, \pm 4$$ → Rational roots.

Plugging all of this in shows that none satisfy FT.

5. Conclude.

$\therefore$ Contradiction! $\sqrt{5}+\sqrt{3}$ is irrational.

Consider factoring out constants! $\Rightarrow \mathbb{Z}$ coefficients.

REAL QUADRATIC FACTOR

If $f(x) \in \mathbb{R}[x]$, ~~then~~ and if c is a root $\in \mathbb{C}$ (not real), then $f(x) = g(x)q(x) \rightarrow g(x)$ is quadratic + irreducible.

↳ RFRP (Real Factor of Real Polynomials)

$\forall f(x) \in \mathbb{R}[x]$, reduce $f(x)$ to linear + quadratic terms.