Cauchy Thm: A sequence (a_n) converges if and only if (a_n) is Cauchy.

Lecture 24:

Motivation:

Q1) How to find a formula for $\sum_{i=1}^{n} i^k$?

Q2) Equal 100-coin jars in NYC?

Q3) Sorting Exams: $\{1, \ldots, 19\}$ how many swaps are needed to sort it?

Q4) $p(x) \in \mathbb{Q}(x)$ polynomial w/ rational coefficients. when $p(n) \in \mathbb{Z}$, $\forall n \in \mathbb{Z}$?

I Binomial Theorem:

Q: What is $(x+y)^n$?

Defn: For S a finite set a permutation of S is a bijection $f: S \to S$.

For $|S| = n$, how many are there? $n!$

What properties do they have? f_1, f_2
$f_1 \circ f_2$, id_S and $f \mapsto f^{-1}$.

Defn: A k-selection from S, is a subset $P \subseteq S$ s.t. $|P| = k$ $(k \leq n)$

Recall: let $[n] = \{1, \dots, n\}$ ~~be the set~~ and
$$S_n = \{ f : [n] \to [n] \mid f \text{ is bijective} \}.$$

$e \in S_n$ is the identity permutation $e(i) = i \quad \forall\, 1 \le i \le n$

a transposition is a permutation that only changes two elts.

Ex: $t_{12}(1) = 2 \qquad t_{12}(2) = 1, \quad t_{12}(i) = i \quad \forall\, 3 \le i \le n$
for $i \neq j$ in $[n]$, t_{ij} is the transposition of i and j.

~~Notation: word form $t_{12} = (12)$, $e =$~~

Q: Drummer Problem, n married couples dancing, two drummers alternating, after each dance 2 women swap partners, at the end all ~~couples~~ couples are spouses. Determine which drummer is playing at the end from the initial dancing configuration.

Consider $f(\underline{x}) = \prod_{i<j=1}^{n} (x_i - x_j)$.

For each $\sigma \in S_n$ one has

$$\sigma f(\underline{x}) \equiv \prod_{i<j=1}^{n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Claim: 1) $\sigma f(\underline{x}) = (-1)^{n_\sigma} \cdot f(\underline{x}) \quad \forall\, \sigma \in S_n.$

2) If σ_0 is the initial dance configuration, then the last drummer = first drummer

$\Updownarrow$

$(-1)^{n_{\sigma_0}}$

Interesting fact, any $\sigma \in S_n$ can be written as

$$\sigma = t_{i_1 j_1} \cdots t_{i_k j_k}$$

for a collection of transpositions.

Check for S_3.

enough to write (123) and (132) as transpositions

Another interesting fact. For any $\sigma \in S_n$, $\exists k \in \mathbb{N}$, s.t.

$$\sigma^k = e, \quad \text{and} \quad k \leq n.$$

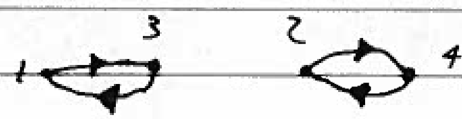
Check for S_3.

<u>Different representations:</u>

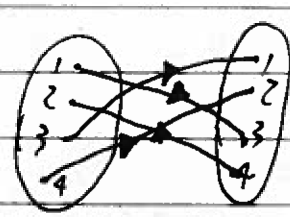
1) <u>Word form</u> $(3\,4\,1\,2)$.

2) <u>2-line form</u> $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.

3) <u>Functional digraph</u>



4) <u>Schematic representation:</u>

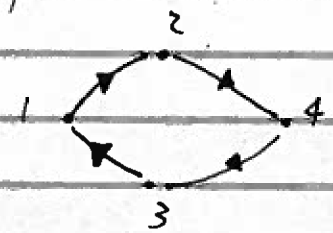


5) <u>Cycle representation:</u> $(13)(24)$

⋮

Effect of a transposition on a digraph.

Ex. Transpose 2 and 3.



$\Rightarrow$ # cycles $\longmapsto$ # cycles -1.

Claim: The # of transpositions needed to sort the word form of a permutation of $[n]$ is $n-k$, where k is the number of cycles in its cycle description.

Lecture 8: Prime Factorization.

Motivation: ~~[illegible]~~ study prime factorizations.

Claim: every integer $n \geq 1$ has an unique (up to factorization in terms of prime numbers.

Pf: Existence: n is either prime or the product of primes. (we proved this before.)

Uniqueness: $n = p_1 \cdot \ldots \cdot p_k$, suppose $n = q_1 \cdot \ldots \cdot q_\ell$ for some other primes.

Notice p_1 divides n.

Lemma: If a prime number p divides $a_1 \cdot \ldots \cdot a_k$ where $a_i \in \mathbb{N}$, then p divides a_j for some j.

$\Rightarrow$ p_1 divides q_j for some j. $\Rightarrow$ $p_1 = q_j$.

By induction we obtain $k = \ell$ and $\{p_1, \ldots, p_k\}$ is equal to $\{q_1, \ldots, q_\ell\}$.

Exercise: Fill the details, prove Lemma and fill the blank.

Given $a, b \in \mathbb{N}$, they are said to be relatively prime if $\gcd(a,b) = 1$.

Corollary: If $\gcd(a,b) = 1$, $a \mid n$ and $b \mid n$, then $ab \mid n$.

For $a, b \in \mathbb{Z}$.

<u>Important Lemma:</u> If $\gcd(a,b) = 1$, then there exists $m, n \in \mathbb{Z}$ s.t.

$$ma + n \cdot b = 1.$$

$$\gcd(a,b) = \gcd(|a|, |b|).$$

Induction on $|a| + |b|$. , if $a = 0 \Rightarrow b = \pm 1$ in which case $(m,n) = (0, \pm 1)$ does it.

[Without loss of generality we assume $|b| > |a|$. and $a > 0$.
Hence if the result is true. for $a + b \geq 2$.]

~~[Consider $a + (b+1) \geq 2$, since $(b+1) > (b+1) - a \geq 0$,~~
~~The result is true for $(b+1) - a$ and $(b+1)$~~
~~$\exists$ (m', n') s.t.~~

~~$$m'((b+1) - a) + n' \cdot (b+1)$$~~

Suppose the result is true $\forall$ (a', b') | $a' + b' \leq k$.

let $a + b = k + 1$, and $a > b$. (otherwise take $b > a$)

then $(a - b) > 0$, $b > 0$ and the result holds for $((a-b), b)$ since $(a - b) + b = a \leq k$.

$\boxed{\text{since } b \geq 1,}$

$\Rightarrow \exists\, (m', n')$ s.t.

$$m'(a-b) + n'b = 1 \Rightarrow m'a + (n'-m')b = 1.$$

$\Rightarrow (m', (n'-m'))$ is a solution for (a,b). ∎

Odd $\rightarrow$ Distinct.

$$n = a_1 \cdot 1 + a_3 \cdot 3 + a_5 \cdot 5 + \dots$$

$$= (2^{b_{11}} + 2^{b_{12}} + \dots + 2^{b_{1n_1}}) \cdot 1 + $$
$$+ (2^{b_{31}} + 2^{b_{32}} + \dots + 2^{b_{3n_3}}) \cdot 3 + \dots$$

$$= 1 \cdot 2^{b_{11}} + 1 \cdot 2^{b_{12}} + \dots + 1 \cdot 2^{b_{1n_1}} +$$
$$3 \cdot 2^{b_{31}} + 3 \cdot 2^{b_{32}} + \dots + 3 \cdot 2^{b_{3n_3}} +$$
$$\dots$$

$a_i = 2^{k_i} \cdot m_i$ $\begin{pmatrix} m_i \text{ odd.} \\ k_i \geq 0. \end{pmatrix}$

each is distinct.

Distinct $\rightarrow$ Odd.

let $\{\overline{m_1}, \overline{m_2}, \dots, \overline{m_r}\}$ be a list of distinct (odd #s)

let $I_{\overline{m_1}} = \{ i \in [k] \mid m_i = \overline{m_1} \}$.

$$n = l_1 + \dots + l_k.$$
$$= 2^{n_1} \cdot m_1 + \dots + 2^{n_k} \cdot m_k.$$

$$= \overline{m_1} \cdot \sum_{i \in I_{\overline{m_1}}} 2^{n_i} +$$
$$\overline{m_2} \cdot \sum_{i \in I_{\overline{m_2}}} 2^{n_i} + \dots$$

$[k_1]$.

$I_{\overline{m_2}} = \{ i \in [k] \mid m_i = \overline{m_2} \}$,

$\vdots$

Claim the composite is a bijection.

Lemma: $\forall a, b, k \in \mathbb{Z} \quad \gcd(a,b) = \gcd(a-kb, b)$.

Pf: let $d \mid a$ and $d \mid b \Rightarrow d \mid (a-kb)$.

$\Rightarrow \quad \gcd(a-kb, b) \geq \gcd(a,b)$.

Analogously, if $d \mid (a-kb)$ and $d \mid b$ then.

$$d \mid (a - kb + kb) = a$$

$\Rightarrow \quad \gcd(a,b) \geq \gcd(a-kb, d)$. $\blacksquare$

Idea, use the above to provide an algorithm to find $\gcd(a,b)$.

Step 1: Consider (a_1, b_1) s.t. $a_1 \geq b_1$.

Step 2: find the largest k s.t. $a_1 = k \cdot b_1 + r_1$, w/ $0 \leq r_1 < b_1$.

Step 3: Consider (b_1, r_1), ~~since $\gcd(b_1, r_1)$~~

Since $\gcd(b_1, r_1) = \gcd(r_1, b_1) = \gcd(r_1 + kb_1, b_1) = \gcd(a_1, b_1)$

Repeat Step 2 & 3 until $r_n = 0$.

Example: $(154, 35) \rightarrow 154 = 4 \cdot 35 + 14$.

$(35, 14) \rightarrow 35 = 2 \cdot 14 + 7$

Suppose $\underbrace{a \mid n \quad \text{and} \quad b \mid n}$ and $\gcd(a,b) = 1$.

$$\Downarrow$$

$$\operatorname{lcm}(a,b) \mid n.$$

By HW $\quad \operatorname{lcm}(a,b) \cdot \gcd(a,b) = a \cdot b. \Rightarrow \operatorname{lcm}(a,b) = ab.$

$$\Rightarrow ab \mid n.$$

Let ~~$A = \{p_1, \dots, p_{ka}\}$ be the primes that~~

$a = p_1 \cdot \dots \cdot p_{ka}$.

$b = q_1 \cdot \dots \cdot q_{kb}$. $\qquad \gcd(a,b) = 1. \qquad$ no $p_i = q_j$.

$n = r_1 \cdot \dots \cdot r_{kn}$. $\qquad$ and $\forall p_i \ \exists r_j$ s.t. $r_j = p_i$.

$\Rightarrow n = p_1 \cdot \dots \cdot p_{ka} \cdot q_1 \cdot \dots \cdot q_{kb} \cdot \prod_{j \in J} r_j. \quad \mid n.$

$$\Rightarrow a \cdot b \mid n.$$

Nov. 26. Problem: n divided by 3 has remainder 1,
n divided by 5 has remainder 2, and
n divided by 7 has remainder 4.

Q: What is the minimum n?

Defn: A relation on a set S is a subset $R \subset S \times$ ~~We say that~~ For $x, y \in S$, we say x is in relation to y (or x is related to y) if $(x,y) \in R$.

Examples: (i) $S =$ (student) people at UI, $(x,y) \in R$ if x is in a (dogs with) student of y.

(ii) $S = \mathbb{Z}$, $(x,y) \in R$ if $x-y$ is divisible by

(iii) $f: A \to A$ a function, $\Gamma(f) \subset A \times A$ is a relation.

Defn: Equivalence relation if
(i) (reflexive) if $\forall x \in S$, $(x,x) \in R$;
(ii) (symmetric) if $\forall x, y \in S$ $(x,y) \in R \Rightarrow (y,x) \in R$,
(iii) (transitive) if $\forall x, y, z \in S$ $(x,y) \in R$ and $(y,z) \in R$
$\Rightarrow (x,z) \in R$;

Ex: (ii) $(x,x) \in R$, $(x,y) \in R \Rightarrow (y,x) \in R$ and
$((x,y) \in R \wedge (y,z) \in R) \Rightarrow (x,z) \in R$.

More generally, $R = \{(x,y) \in \mathbb{Z} \mid (x-y)$ is divisible by $n\}$.

(iv) Let $f: S \to T$ be a function.

Define $R \subset S \times S$.
$$R = \{(x,y) \mid f(x) = f(y)\}$$

R is an equivalence relation.

<u>Non-examples:</u> a) S = students at UI. (not transitive)

b) $S = \mathcal{P}(A)$, $(x,y) \in R$ if $x \subset y$.

(antisymmetric), if $(x,y) \in R$ and $(y,x) \in R \Rightarrow x = y$.

<u>Rk:</u> A reflexive, anti-symmetric and transitive relation is called an <u>order relation</u>.

<u>Defn:</u> Let R be an equivalence relation on S, for $x \in S$ $[x] = \{y \in S \mid (x,y) \in R\}$ is the <u>equivalence class</u> of x

<u>Example:</u> (ii) let $1 \in \mathbb{Z}$, $[1] = \{\ldots, -3, -1, 1, 3, \ldots\}$
$[0] = \{\ldots, -2, 0, 2, \ldots\}$.

$[0] \cup [1] = \mathbb{Z}$ <u>(partition)</u>

(iv) For $x \in S$, $[x]$ is $\{y \in S \mid f(y) = f(x)\} = f^{-1}(f(x))$

$\bigcup_{t \in T} f^{-1}(t)$ is a partition of S.

<u>Exercise:</u> How example (ii) is a particular case of example (iv).

Proposition: Let $a, b \in \mathbb{Z}$ $b \neq 0$. Then there exists unique $k, r \in \mathbb{Z}$ s.t.

$$a = kb + r \quad \text{and} \quad 0 \leq r \leq |b| - 1.$$

Pf: 1) Consider $A = \{ a - nb \mid n \in \mathbb{Z} \text{ and } a - nb \geq 0 \}$

Claim: $A \neq \emptyset$. , by Arithmetic property there always exist N s.t. $N(-b) \geq -a$.
~~a ≥ 0, take n = 0~~ $\forall\ b, a \in \mathbb{Z}$.

2) Let $r = \min A$, i.e. $r = \inf A$ and $r \in A$.

3) $0 \leq r < |b|$.
Indeed, if $r \geq |b|$, then $\exists\ m \in \mathbb{Z}$ s.t.
$r = a - mb$, and $a - (m+1)b \geq 0$.
$\Rightarrow$ $a - (m+1)b < r$ and $a - (m+1)b \in A$.

4) Let $r = \min A$, i.e. $r = a - mb$ for some $m \in \mathbb{Z}$ $\Rightarrow$ $a = r + mb$, take $k = m$.

5) Suppose $\exists\ k', r'$ s.t. $r' = a - k' \cdot b = \min A = r = a - kb$.

6) Consider $r' - r = (a - k'b) - (a - kb) = (k - k') \cdot b$.

$\Rightarrow$ $b \mid (r' - r)$. and

Now, $0 \leq r' < |b|$ and $0 \leq r < |b|$ $\qquad r' - r \geq 0 - r > -|b|$

$\Rightarrow$ $r' - r < |b| - r \leq |b|$

So $\quad -|b| < r - r' < |b|.$

7) Contradiction.

$r - r' = l \cdot b$ for some integer and

$-|b| < l b < |b| \Rightarrow \boxed{l = 0}$

Jacob & Ismael. +1. Bryan.

Nov. 30.

For every $n \in \mathbb{N}$, $R_n \subseteq \mathbb{Z} \times \mathbb{Z}$, $(x,y) \in R_n$ if $n \mid (x-y)$ is an equivalence relation.

Q: What are the equivalence classes of R_n?
A: $[0], [1], \ldots, [n-1]$.

Defn: $\mathbb{Z}/n\mathbb{Z} \equiv$ set of equivalence classes of R_n.

FACT 1: $\mathbb{Z}/n\mathbb{Z}$ has an addition operation.

$$[a]+[b] \underset{\text{defn.}}{\equiv} [a+b].$$

$$[a] = [a+n] = [a+2n] = \ldots$$

If $[a]=[a']$ and $[b]=[b']$, want to check that.

$$[a]+[b] = [a']+[b'].$$
$$[a+b] = [a'+b'] \quad ?$$

$a = k \cdot n + a'$
$b = l \cdot n + b'$

$$\Rightarrow [a+b] = [a'+b'+(k+l)\cdot n].$$
$$= [a'+b'].$$ ∎

FACT 2: $\mathbb{Z}/n\mathbb{Z}$ has a multiplication operation.
for $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ let
$$[a]\cdot[b] \equiv [a \cdot b].$$

Notation: $a \equiv b \mod n$ if $[a]_n = [b]_n$ w.r.t. R_n.

Prop: Suppose a and b are relatively prime, and $x \in \mathbb{Z}$. Then $\{x, x+b, x+2b, \ldots, x+(a-1)\cdot b\}$ all have distinct remainder upon division by a.

Pf: Suppose $x + ib \equiv x + jb \mod a$ for $i \neq j$, $0 \leq i, j \leq (a-1)$.

$\Rightarrow (i-j)b \equiv 0 \mod a.$

$\Rightarrow$ a divides. $(i-j)\cdot b \overset{\gcd(a,b)=1}{\Rightarrow} a \mid (i-j).$

$\Rightarrow$ Contradiction since $0 < i-j < a-1$ or $-(a-1) < i-j < 0.$ $\lightning$

Cor: ~~Let $a \cdot x \equiv$ mod n~~ For a and n fixed the equation
$$a x \equiv 1 \mod n \text{ has}$$
a solution if $\gcd(a,n) = 1$. ~~And $[a]$~~ And $[x] = [x']$ for any two solutions.

Pf: Consider $[a] : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
$$[b] \mapsto [a \cdot b]$$
If $\gcd(a,n) = 1$
$\{[a]\cdot[0], [a]\cdot[1], \ldots, [a]\cdot[n-1]\}$ are all distinct numbers.

Since, $\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$,

$\Rightarrow [a]\cdot$ is injective.

Since, $\mathbb{Z}/n\mathbb{Z}$ is finite $\Rightarrow$ $[a]\cdot$ is bijective.

Cor: For p a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

For any $a \in \mathbb{Z}/p\mathbb{Z}$, $\exists\, x \in \mathbb{Z}/p\mathbb{Z}$ s.t.

$$ax \equiv 1 \mod p.$$

$(i.e. \quad x = a^{-1})_a.$

+ check other axioms.

Thm: p prime and $a \not\equiv 0 \mod p$, then

$$a^{p-1} \equiv 1 \mod p.$$

Pf: Consider $[a] \in \mathbb{Z}_p - \{0\}$.

Claim 1) $\exists\, k \geq 1$ s.t. $[a]^k = [1]$.

Otherwise: $\{[a], [a^2], [a^3], \dots\}$ is a list of ∞-many distinct elements.

2) $k \mid (p-1)$.

Lemma: $\forall\, a \not\equiv 0 \mod p$ and $\forall\, x \neq 0$ in $\mathbb{Z}$ the list

$S_x = \{[x], [ax], [a^2x], \dots\}$ has exactly k distinct elements.

Pf: Finite by above. Let k be the size of S_x and l the size of S_y, $[a^k x] = [x]$ and $[a^l y] = [y]$.

$\cancel{\Rightarrow \quad x - a^k x \equiv 0 \mod p \quad \text{and}}$

$\cancel{y - a^l y \equiv 0 \mod p.}$

$\cancel{x(1 - a^k) \equiv 0 \quad \Rightarrow \quad 1 \equiv a^k \quad \Rightarrow \quad k = l.}$

$\cancel{y(1 - a^l) \equiv 0 \qquad 1 \equiv a^l}$

$\Rightarrow \quad x - a^k x \equiv 0 \quad \Rightarrow \quad x(1 - a^k) \equiv 0 \quad \Rightarrow \quad (1 - a^k) \equiv 0.$

$\Rightarrow \quad y - a^l y \equiv 0 \quad \Rightarrow \quad y(1 - a^l) \equiv 0 \quad \Rightarrow \quad (1 - a^l) \equiv 0.$

$\Rightarrow \quad a^k = 1$ and $a^l = 1 \quad \Rightarrow \quad a^k = a^l$ since k and l were minimal $\Rightarrow \boxed{k = l.}$

So, $\mathbb{Z}_p \setminus \{0\} = \bigcup_{i \in I} A_i$. with $|A_i| = k$.

Indeed, if $a^i x = a^j y$ $\Rightarrow$ ~~[illegible]~~

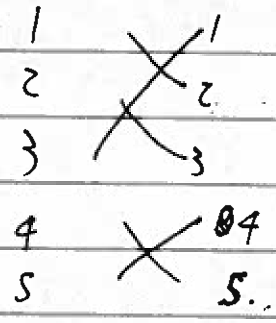
$\Rightarrow \quad x = a^{k+j-i} y$;

Since $(p-1) = m \cdot k \quad \Rightarrow \quad a^{p-1} \equiv (a^k)^m \equiv 1^m \equiv 1.$

mod p

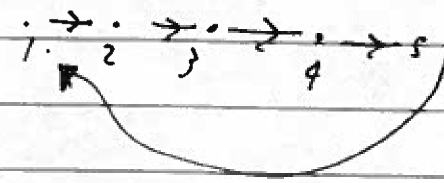
Chapter 5.

I.

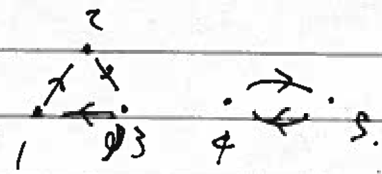


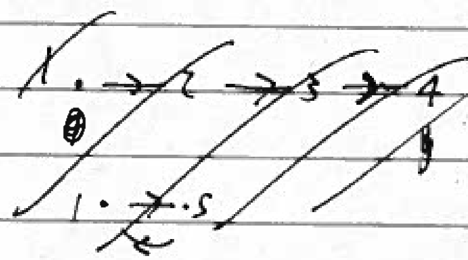
(23154).

(t_{14})

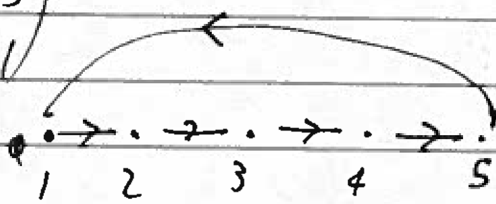


$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ $\quad t_{14} \quad$ $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

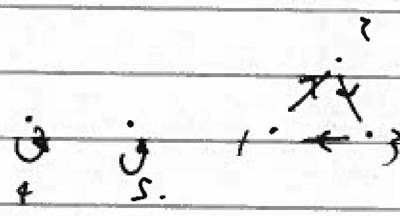




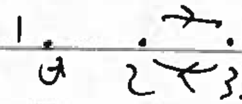
t_{14} $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$



t_{45}

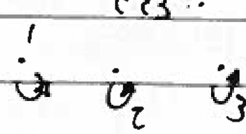


t_{12}



$(5-2=3)$

t_{23}..



Chapter 5.

II.
$$\binom{n}{k} = \frac{n(n-1)\cdot \ldots \cdot (n-k+1)}{k!}$$

$$\frac{n^k}{k!} + \left(\sum_{j=1}^{k-1}(-j)\right)\cdot\frac{1}{k!} = \frac{-1}{k!}\binom{k}{2}n^{k-1} + \frac{n^k}{k!} + \cdots$$

$$n^k = k!\binom{n}{k} + \binom{k}{2}n^{k-1} + O(n^{k-2}).$$

$$\sum_{n=1}^{m} n^k = k!\sum_{n=1}^{N}\binom{n}{k} + \binom{k}{2}\sum_{n=1}^{N} n^{k-1} + O(n^{k-1})$$

$$= k!\binom{N+1}{k+1} + \binom{k}{2}\cdot p(N) + O(N^{k-1}).$$

$$= \frac{(N+1)\cdot N \cdots (N-k+1)}{(k+1)} + \binom{k}{2}\cdot p(N).$$

$$= \frac{N^{k+1}}{k+1} + \underbrace{q(N)}_{\deg \le N.}$$

Chapter 6.

I. let $\deg(a) = n$, $\deg(b) = m$.

Strong Induction on n. If $n < m$ then $r = a$. ∎

If $n \geq m$ let

$$a = a_n \cdot x^n + O(x^{n-1})$$
$$b = b_m \cdot x^m + O(x^{m-1})$$

$$h(x) = \frac{a_n}{b_m} \cdot x^{n-m}$$

$$\Rightarrow \quad h(x) \cdot b = a_n \cdot x^n + O(x^{n-1})$$

$$= a_n \cdot x^n + s(x) \text{ w/}$$

~~$\deg q(x) < n$~~

~~$\Rightarrow q(x) = b \cdot q'(x) + r'(x)$~~

$$a_n x^n = h \cdot b - s(x)$$

$\Rightarrow$

$$\Rightarrow \quad a - a_n \cdot x^n = t(x) \text{ w/ } \deg t < n.$$

$$\Rightarrow \quad t(x) = b \cdot q' + r'.$$

$$\Rightarrow \quad a = t + hb - s$$
$$= hb + \underbrace{t - s}_{\deg < n}$$

$\Rightarrow$ result by induction

II. $I \subset \mathbb{R}[x]$ if

(i) $\forall\ p,q \in I,\ p+q \in I$;
(ii) $\forall p \in I,\ \forall r \in \mathbb{R}[x]$; $r \cdot p \in I$.

A <u>principal ideal</u> if $\exists\ g \in \mathbb{R}[x]$ s.t.

$$I = \{p \cdot g \mid p \in \mathbb{R}[x]\}.$$

<u>Example:</u> (i) $\{p \in \mathbb{R}[x] \mid p(0) = 0\} \subseteq \mathbb{R}[x]$.
$\Rightarrow p = x \cdot q$ w/ $q \in \mathbb{R}[x]$.

<u>Non-example:</u> $\mathbb{R}[x,y]$, $I = \{x \cdot f + y \cdot g \mid f, g \in \mathbb{R}[x,y]\}$.

Let $b \in I$, $b \neq 0$ of least deg.

$\forall\ a \in I$, $a = q \cdot b + r$

$\deg(r) < 0$.

$a - q \cdot b \in I$.

$\Rightarrow r \in I$. $\Rightarrow \boxed{0 = r.}$

Chapter 7.

II. Main claim: p prime, then $a^2 \equiv 1 \mod p$

$\Leftrightarrow$ $a \equiv 1 \mod p$ or $a \equiv p-1 \mod p$.

$p \mid (a^2-1) \Rightarrow p \mid (a-1)(a+1) \Rightarrow p \mid a-1$ or $p \mid a+1$.

$\Rightarrow a \equiv p+1 \mod p$

$a \equiv p-1$

$\Rightarrow a \equiv 1 \mod p$,

Assume $2 \leq i \leq p-2$, then $\exists!\ i'$ s.t.

$$i \cdot i' \equiv 1 \mod p.$$

$$\Rightarrow \prod_{i=2}^{p-2} i \equiv 1 \mod p$$

$$\Rightarrow \prod_{i=1}^{p-1} i \equiv (p-1) \mod p.$$

$$\boxed{(p-1)! \equiv -1 \mod p.}$$