CSE 301 Concrete Mathematics Lecture Note Scribes

Tahmid Hasan

CSE, BUET

Lect - 1 (Section A)
CSE 301 M.A. for C.S.
Part A: Tahmid Hasan

Textbook: Concrete Mathematics (Graham, Knuth, Patashnik)

Syllabus: 1) Recurrence (Ch 1)
2) Sums (Ch 2)
3) Number Theory (Ch 4)
4) Special Numbers (Ch 6)
5) Generating Functions (Ch 7)

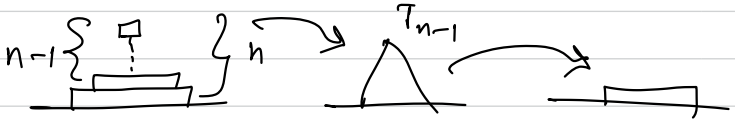
Recurrence

$f_n = f_{n-1} + f_{n-2}$

Tower of Hanoi

$T_0 = 0$
$T_1 = 1$
$T_2 = 3$
$T_3 = 7$
$T_4 = 15$
$T_5 = 31$
$T_6 = 63$

$T_n \leq T_{n-1} + 1 + T_{n-1} = 2T_{n-1} + 1$



$T_n \geq 1 + T_{n-1} + T_{n-1}$

$T_0 = 0$
$T_n = 2T_{n-1} + 1$

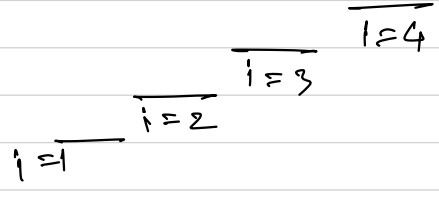
$T_n = 2^n - 1$

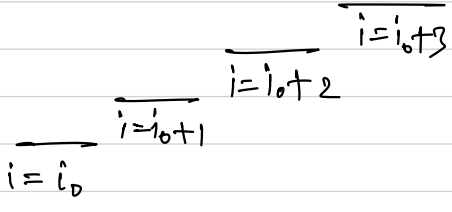
Mathematical Induction: P(K) (Sipser p. 29)

induction hypothesis

1) Basis: P(1)

2) Induction step: for any $i \geq 1$, if $P(i)$ is true, then $P(i+1)$ true





1) Basis: $P(i_0)$

2) Induction step: for any $i \geq i_0$ if $P(i_0), P(i_0+1), \ldots, P(i)$ is true, then $P(i+1)$ is true.

$$\left.\begin{array}{l} T_0 = 0 \\ T_n = 2T_{n-1} + 1 \end{array}\right\} \quad T_n = 2^n - 1$$

1) Basis: $T_0 = 2^0 - 1 = 0$

Hypo: given $P(i_0), P(i_0+1), \ldots, P(i)$ true

$$T_{i+1} = 2T_i + 1 = 2(2^i - 1) + 1$$
$$= 2^{i+1} - 2 + 1 = 2^{i+1} - 1$$

CS E 301: M.A. for C.S. Lect-1: Section B

Part A: Tahmid Hasan

Textbook: Concrete Mathematics (Graham, Knuth, Patashnik)

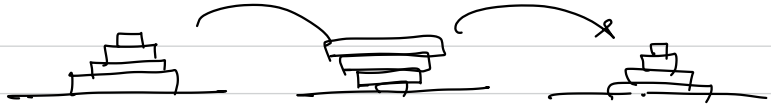
Syllabus: 1) Recurrence (Ch 1)
2) Sums (Ch 2)
3) Number Theory (Ch 4)
4) Special Numbers (Ch 6)
5) Generating functions (Ch 7)

Recurrence

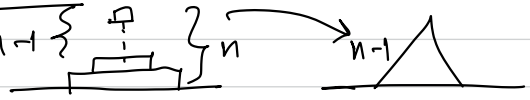
$S_n = n + S_{n-1}$

$f_n = f_{n-1} + f_{n-2}$

Tower of Hanoi:



$T_n \leq T_{n-1} + 1 + T_{n-1}$



$T_n \geq 1 + T_{n-1} + T_{n-1}$

$T_n = 2T_{n-1} + 1$

$T_n = 2^n - 1$

$T_1 = 1$ $T_0 = 0$

$T_2 = 3$

$T_3 = 7$

$T_4 = 15$

$T_5 = 31$

$T_6 = 63$

$T_7 = 127$

Mathematical Induction: $P(K)$, $K \in \mathbb{N}$ (Sipser P.23)

Basis: $P(1)$ is true.
Induction: for any $i \geq 1$, if $P(i)$ is true, then $P(i+1)$ is true (Induction hypothesis)

$K=1$, $K=2$, $K=3$, $K=4$, $K=i_0$, $K=i_0+1$, $K=i_0+2$, $K=i_0+3$

Basis: $P(i_0)$ is true.
Induction: for any $i \geq i_0$, if $P(i_0), P(i_0+1), \ldots, P(i)$ is true, then $P(i+1)$ is true.

$T_n = 2^n - 1$

$T_0 = 0$
$T_n = 2T_{n-1} + 1$

Basis: $i=0$, $T_0 = 2^0 - 1 = 0$
Induction: for any $i \geq 0$, if $T(i)$ is true, then we need to prove $T(i+1)$ is true

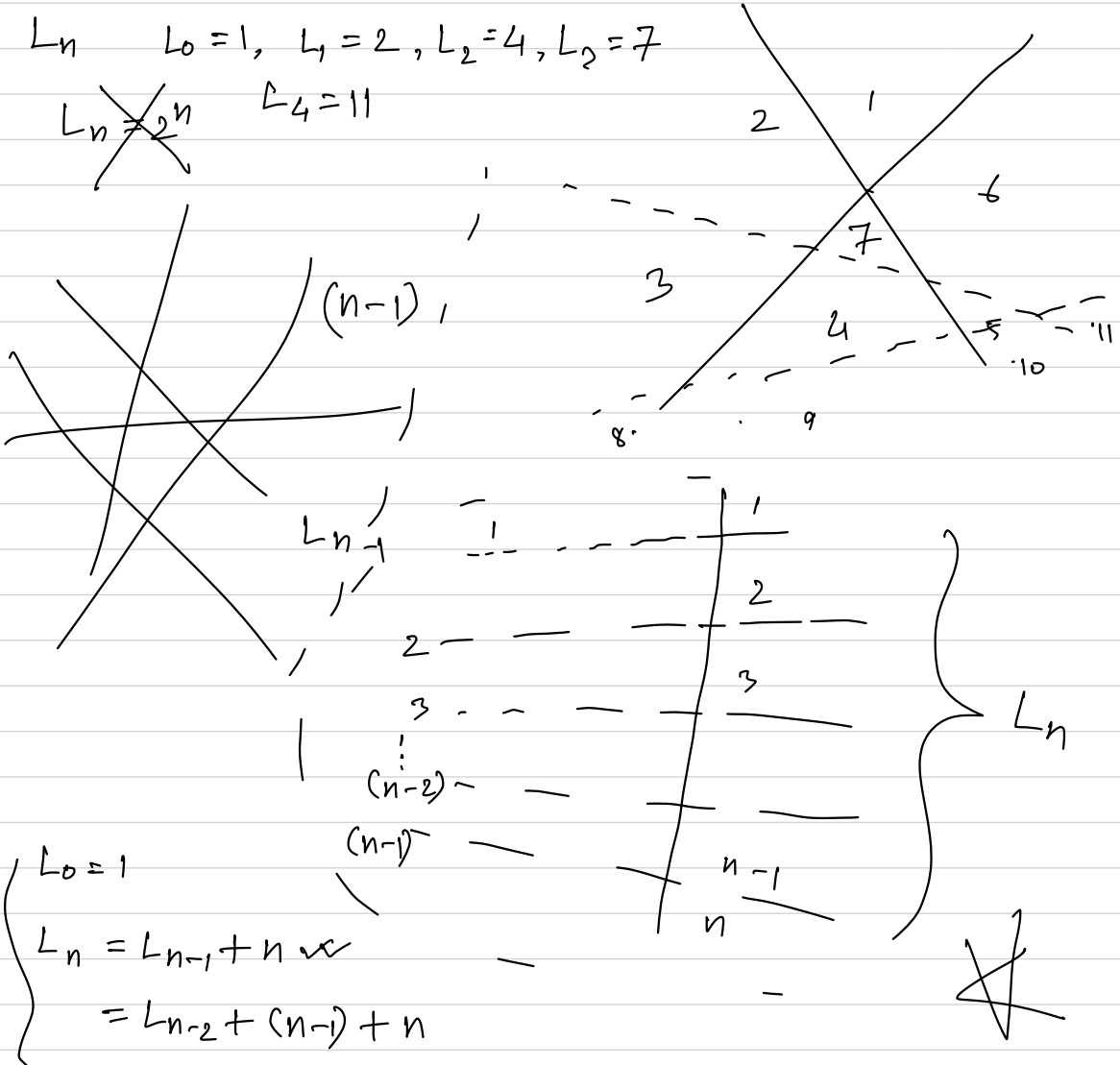
$T_{i+1} = 2T_i + 1 = 2 \times (2^i - 1) + 1$
$= 2^{i+1} - 2 + 1 = 2^{i+1} - 1$

Lect-2: Lines on a plane

Section: B

L_n $L_0 = 1,\ L_1 = 2,\ L_2 = 4,\ L_3 = 7$

$L_n \neq 2^n$ $L_4 = 11$



$L_0 = 1$

$L_n = L_{n-1} + n$

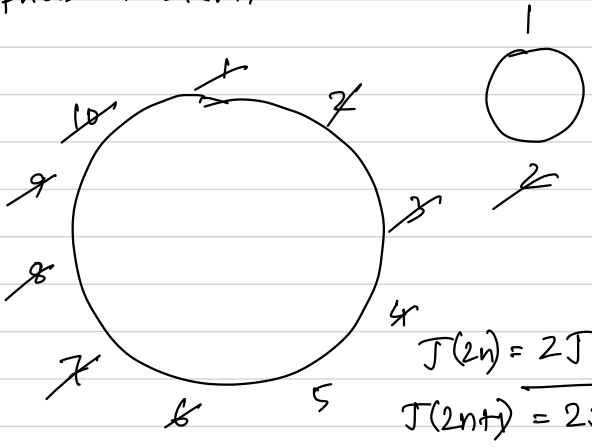
$= L_{n-2} + (n-1) + n$

$= L_{n-3} + (n-2) + (n-1) + n$

$\vdots$

$= L_0 + \underbrace{1 + 2 + 3 \cdots + n}_{} = 1 + \frac{n(n+1)}{2}$

Josephus Problem:

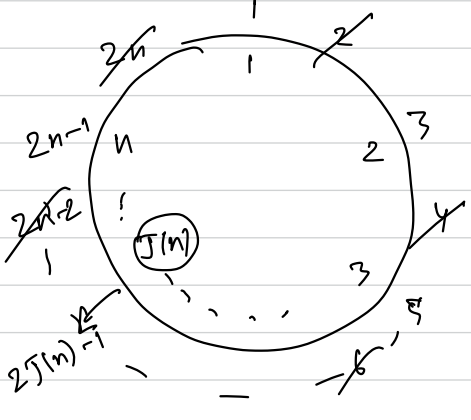


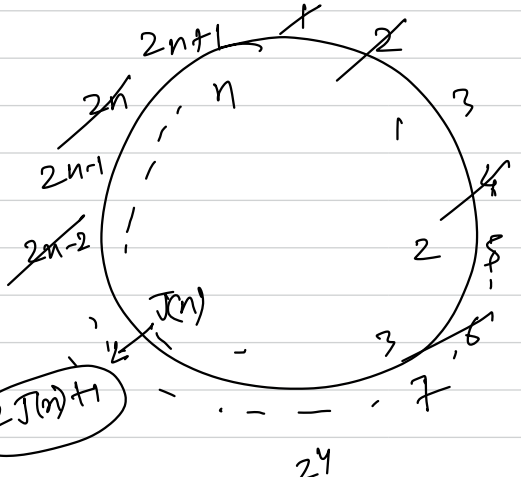
n	1	2	3	4	5	6
J(n)	1	1	3	1	3	5

$J(2n) = 2J(n) - 1$ $\quad J(1) = 1$

$J(2n+1) = 2J(n) + 1$ $\quad \Big\} O(\lg n)$

$J(2n)$





n	2^0 1	2^1 2	3	2^2 4	5	6	7	2^3 8	9	10	11	12	13	14	15	2^4 16
J(n)	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1
	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7								

$n = 2^m + \ell$ $\quad J(n) = 2\ell + 1 \Rightarrow J(2^m + \ell) = 2\ell + 1 \quad m \geq 0$

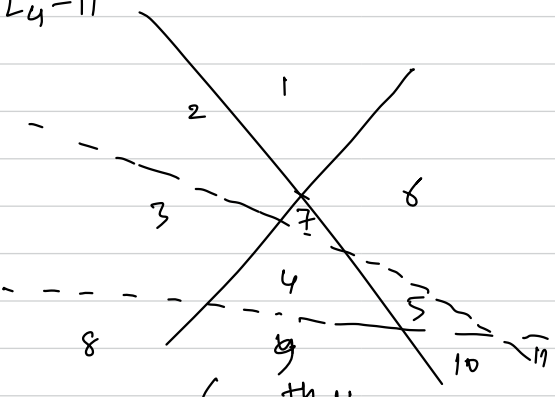
$n < 2^{m+1} \Rightarrow 2^m + \ell < 2^{m+1} \Rightarrow \ell < 2^{m+1} - 2^m = 2^m \Rightarrow 0 \leq \ell < 2^m$

Induction on m:

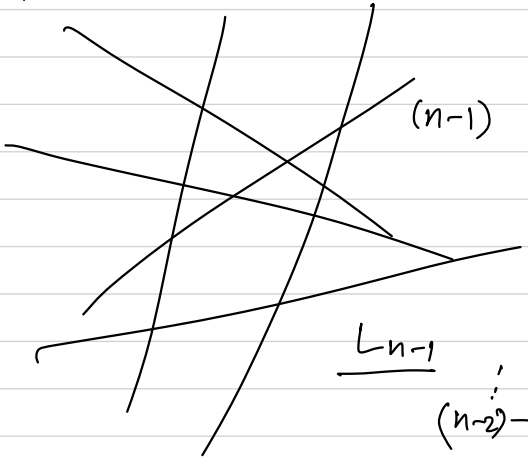
Lect 2: Lines on a plane Sec. A

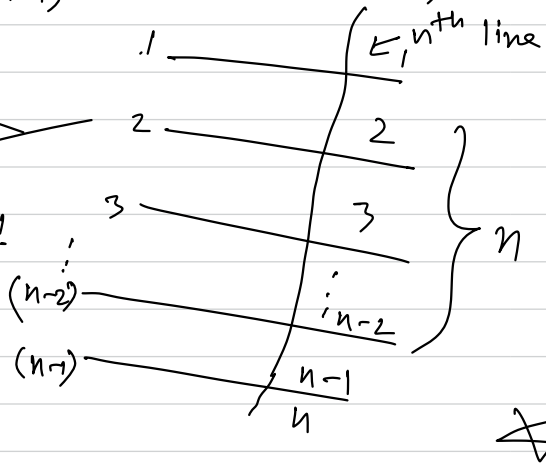
L_n $L_0=1$, $L_1=2$, $L_2=4$, $L_3=7$, $L_4=11$

$L_n = 2^n$



L_{n-1}





L_n

$L_0 = 1$

$L_n = L_{n-1} + n$

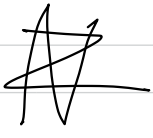
$= L_{n-2} + (n-1) + n$

$= L_{n-3} + (n-2) + (n-1) + n$

$\vdots$

$= L_0 + 1 + 2 + 3 + \cdots + (n-2) + (n-1) + n$

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

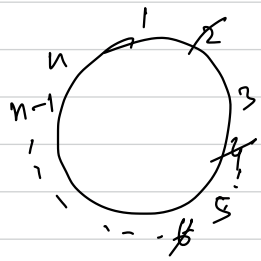


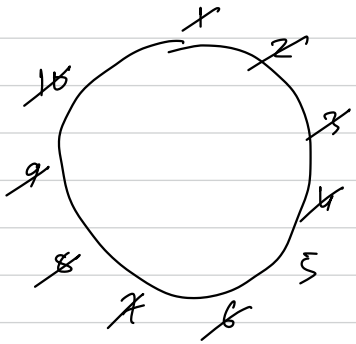
Josephus Problem:

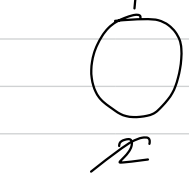
$J(n)$

$J(10) = 5$

$J(2) = 1$







$J(n) = n/2$

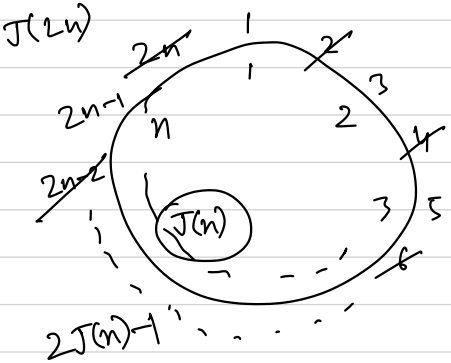
n	1	2	3	4	5	6
$J(n)$	1	1	3	1	3	5

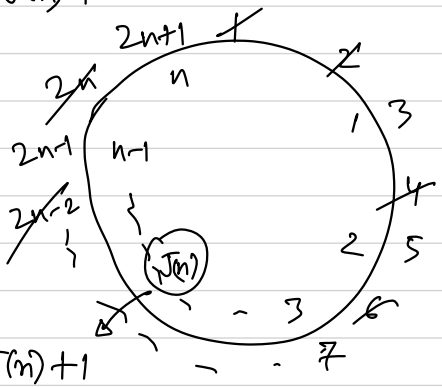
$J(1) = 1$

$J(2n) = 2J(n) - 1$

$O(\lg n)$

$J(2n)$





$J(2n+1) = 2J(n) + 1$

	2^0	2^1		2^2				2^3							2^4
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1
	0	1	2	3	4	5	6	7								

$15 = 2^3 + 7$

$25 = 2^4 + 9$

$n = 2^m + l$ $\quad J(n) = 2l + 1$

$n < 2^{m+1} \Rightarrow 2^m + l < 2^{m+1} \Rightarrow l < 2^{m+1} - 2^m = 2^m$

$0 \le l < 2^m$

$J(1) = 1$

$J(2n) = 2J(n) - 1$

$J(2n+1) = 2J(n) + 1$

$J(2^m + l) = 2l + 1 \quad ; \quad m \ge 0, \ 0 \le l < 2^m$

Induction on m

Lect-3: Josephus contd. sec. A

$J(1)=1$
$J(2n)=2J(n)-1$
$J(2n+1)=2J(n)+1$

$n=2^m+l \; ; \; m\geq 0, \; 0\leq l<2^m$

$J(2^m+l)=2l+1$

$0\leq l<2^0 \Rightarrow 0\leq l<1$

Basis: $m=0 \quad J(2^m+l)=J(2^0+0)=2\cdot 0+1=2l+1$

$\Rightarrow J(1)=1$

Induction:

Assume true for $0,\ldots,m-1$

$J(\underbrace{2^m+l}_{e \;\; \text{to} \;\; e}) = 2J(2^{m-1}+l/2)-1 = 2(2\cdot l/2+1)-1 = 2l+1$

$J(\underbrace{2^m+l}_{e \;\; \text{to} \;\; 0}) = J(\underbrace{2^m+l-1}_{2n}+1) = 2J(2^{m-1}+\frac{l-1}{2})+1$

$= 2(2\cdot\frac{l-1}{2}+1)+1 = 2l+1$

$n=(b_m b_{m-1} b_{m-2} \ldots b_1 b_0)_2$

$n=b_m 2^m + b_{m-1}2^{m-1}+\ldots+b_1 x 2+b_0$

$n=(1\, b_{m-1} b_{m-2} \ldots b_1 b_0)_2$

$2^m=(1\;0\;0\;\ldots 0\;0)_2$

$l=(0\, b_{m-1} b_{m-2} \ldots b_1 b_0)_2$

$2l=(b_{m-1} b_{m-2} \ldots b_1 b_0 0)_2$

$2l+1=(b_{m-1} b_{m-2} \ldots b_1 b_0 1)_2$

$\hookrightarrow b_m$

$n=2^m+l \Rightarrow l=n-2^m$

$J((b_m b_{m-1} \ldots b_1 b_0)_2)=(b_{m-1} b_{m-2} \ldots b_1 b_0 b_m)_2$

$J((1101)_2) = (101)_2 \to (11)_2 \to (1)_2$

fixed point $f(n) = n$

$J(n) = n/2$

$\Rightarrow 2l+1 = (2^m+l)/2$

$\Rightarrow 4l+2 = 2^m+l \Rightarrow l = \frac{1}{3}(2^m-2)$

$m=0 \to l \times$

$m=1 \to l=0$

$m=2 \to l \times$

$m=3 \to l=2$

m	l	$n = 2^m+l$	$J(n) = 2l+1 = n/2$	n (binary)
1	0	2	1	10
3	2	10	5	1010
5	10	42	21	101010
7	42	170	85	10101010

$J(1) = 1$

$J(2n) = 2J(n) - 1$

$J(2n+1) = 2J(n) + 1$

$f(1) = \alpha$

$f(2n) = 2f(n) + \beta$

$f(2n+1) = 2f(n) + \gamma$

n	$f(n)$
1.	α
2.	$2\alpha + \beta$
3.	$2\alpha + \gamma$
4.	$4\alpha + 3\beta$
5.	$4\alpha + 2\beta + \gamma$
6.	$4\alpha + \beta + 2\gamma$
7.	$4\alpha + 3\gamma$
8.	$8\alpha + 7\beta$
9.	$8\alpha + 6\beta + \gamma$

$f(n) = A(n)\alpha + B(n)\beta + C(n)\gamma$

$n = 2^m + l$

$A(n) = 2^m$

$B(n) = 2^m - l - 1$

$C(n) = l$

$B(n) + C(n) = 2^m - 1$

$\frac{3x+2}{(x-1)(x-2)} \equiv \frac{A}{(x-1)} + \frac{B}{(x-2)}$

Lect-3: Josephus cont. Sec. B

$J(1)=1$
$J(2n)=2J(n)-1$
$J(2n+1)=2J(n)+1$

$n=2^m+l$; $m\geq 0$ & $0\leq l<2^m$

$J(n)=2l+1$ ---- (1)

$0\leq l<2^0 \Rightarrow 0\leq l<1$
$\hookrightarrow l=0$

Basis: $m=0$; $J(2^m+l)=2l+1$
$\Leftrightarrow J(2^0+0)=2\cdot 0+1$
$\Leftrightarrow J(1)=1$

Induction: Assume (1) is true for $0, 1, \ldots, m-1$

$J(\overbrace{2^m+l}^{2n}) = 2J(2^{m-1}+l/2)-1 = 2(2\cdot l/2+1)-1 = 2l+1$
(e e; 0)

$J(\overbrace{2^m+l}^{o}) = J(\overbrace{2^m+l-1}^{e}+1) = 2J\left(2^{m-1}+\frac{l-1}{2}\right)+1$
(e o)
$= 2\left(2\cdot\frac{l-1}{2}+1\right)+1 = 2l+1$

$n=(b_m b_{m-1}\ldots b_1 b_0)_2$ ($b_m=1$)

$n=b_m 2^m+b_{m-1}2^{m-1}+\ldots+2b_1+b_0$

$n=(1\, b_{m-1}\ldots b_1 b_0)_2$
$2^m=(1\,0\ldots 0\,0)_2$

$l=(0\, b_{m-1}\ldots b_1 b_0)_2$
$2l=(b_{m-1}b_{m-2}\ldots b_0 0)_2$
$2l+1=(b_{m-1}b_{m-2}\ldots b_0 1)_2$

$n=2^m+l \Rightarrow l=n-2^m$

$J((b_m b_{m-1}\ldots b_1 b_0)_2)=(b_{m-1}b_{m-2}\ldots b_1 b_0 b_m)_2$

$(1011)_2 \to (0111)_2 \to (111)_2 \to (111)_2$

$(10110010101110\,1)$
$111, 111, 111$

$J(n)=n$ → fixed point
$f(n)=n$

$J(n) = n/2$ $\quad n = 2^m + l, \Rightarrow J(n) = 2l+1$

$\Rightarrow 2l+1 = (2^m+l)/2 \Rightarrow 4l+2 = 2^m + l \Rightarrow \underline{l = \tfrac{1}{3}(2^m - 2)}$

m	l	$n = 2^m + l$	$J(n) = n/2 = 2l+1$	n (binary)
1	0	2	1	10
3	2	10	5	1010
5	10	42	21	101010
7	42	170	85	10101010

$J(1) = 1$
$J(2n) = 2J(n) - 1$
$J(2n+1) = 2J(n) + 1$

$f(1) = \alpha$
$f(2n) = 2f(n) + \beta$
$f(2n+1) = 2f(n) + \gamma$

$f(n) = A(n)\alpha + B(n)\beta + C(n)\gamma$

n	f(n)
1.	α
2.	$2\alpha + \beta$
3.	$2\alpha + \gamma$
4.	$4\alpha + 3\beta$
5.	$4\alpha + 2\beta + \gamma$
6.	$4\alpha + \beta + 2\gamma$
7.	$4\alpha + 3\gamma$
8.	$8\alpha + 7\beta$
9.	$8\alpha + 6\beta + \gamma$

$n = 2^m + l$

$A(n) = \underline{2^m}$

$C(n) = \underline{l}$

$B(n) + C(n) = 2^m - 1$

$\Rightarrow B(n) + l = 2^m - 1$

$\Rightarrow B(n) = \underline{2^m - l - 1}$

$$f(n) = A(n)\alpha + B(n)\beta + C(n)\gamma \quad \ldots(1)$$

$f(1) = \alpha$
$f(2n) = 2f(n) + \beta$
$f(2n+1) = 2f(n) + \gamma$

$A(n) = 2^m$
$B(n) = 2^m - l - 1$
$C(n) = l$

$n = 2^m + l$

$$\frac{3x+2}{(x-1)(x-2)} \equiv \frac{A}{x-1} + \frac{B}{x-2}$$

$(\alpha, \beta, \gamma) \equiv (1, 0, 0)$

$A(1) = 1$
$A(2n) = 2A(n)$
$A(2n+1) = 2A(n)$

n	1	2	3	4	5	6	7	8	9
A(n)	1	2	2	4	4	4	4	8	8

$f(n) = A(n)$

$\boxed{A(n) = 2^m}$ ✓

$f(n) = 1 \Rightarrow$
$1 = \alpha$
$1 = 2 \cdot 1 + \beta$
$1 = 2 \cdot 1 + \gamma$
$\Rightarrow (\alpha, \beta, \gamma) = (1, -1, -1)$

$\boxed{A(n) - B(n) - C(n) = 1} \Rightarrow B(n) = A(n) - C(n) - 1 = \underline{2^m - l - 1}$ ✓

$f(n) = n \Rightarrow$
$1 = \alpha$
$2n = 2 \cdot n + \beta$
$2n+1 = 2 \cdot n + \gamma$
$\Rightarrow (\alpha, \beta, \gamma) = (\underline{1}, \underline{0}, \underline{1})$

$\boxed{A(n) + C(n) = n}$

$C(n) = n - 2^m = \underline{l}$ ✓

Repertoire method: ex. 16 & 20

$J((b_m b_{m-1} \cdots b_1 b_0)_2) = (b_{m-1} \cdots b_1 b_0 b_m)_2 ; \quad b_m = 1$

$f(1) = \alpha$
$f(2n+j) = 2f(n) + \beta_j ; \quad j \in \{0, 1\}, \quad \beta_0 = \beta, \ \beta_1 = \gamma$

$d \mid a$, $a = dq + r$

$$\begin{array}{r|l} 2 & 2n+j \\ \hline & 2n \\ \hline & j \end{array} \quad n$$

$$f((b_m b_{m-1} \cdots b_1 b_0)_2) = 2f((b_m b_{m-1} \cdots b_1)_2) + \beta_{b_0}$$
$$= 2(2f(b_m b_{m-1} \cdots b_2)_2 + \beta_{b_1}) + \beta_{b_0}$$
$$= 4f((b_m b_{m-1} \cdots b_2)_2) + 2\beta_{b_1} + \beta_{b_0}$$
$$= 8f((b_m b_{m-1} \cdots b_3)_2) + 4\beta_{b_2} + 2\beta_1 + \beta_{b_0}$$
$$\vdots$$
$$= 2^m f((b_m)_2) + 2^{m-1}\beta_{b_{m-1}} + 2^{m-2}\beta_{b_{m-2}} + \cdots + 2\beta_{b_1} + \beta_{b_0}$$
$$= 2^m \alpha + 2^{m-1}\beta_{b_{m-1}} + 2^{m-2}\beta_{b_{m-2}} + \cdots + 2\beta_{b_1} + \beta_{b_0}$$
$$= (\alpha \beta_{b_{m-1}} \beta_{b_{m-2}} \cdots \beta_{b_1} \beta_{b_0})_2 \text{ — notation abuse!}$$

$f(100) = f(2^6 + 36) = 2 \cdot 36 + 1 = 73$

$\alpha = 1$

$\beta = -1 = \beta_0$

$\gamma = 1 = \beta_1$

$100 \to (1100100)_2$

$2^6 \times 1 + 2^5 \times 1 + 2^4 \times (-1) + 2^3 \times (-1) + 2^2 \times 1 + 2^1 \times (-1) + 2^0 \times (-1)$

$= \underline{\underline{73}}$

$f(j) = \alpha_j$ for $1 \le j < d$

$f(dn + j) = cf(n) + \beta_j$ for $0 \le j < d$; $n \ge 1$

$f((b_m b_{m-1} \cdots b_1 b_0)_d) = (\alpha_{b_m} \beta_{b_{m-1}} \beta_{b_{m-2}} \cdots \beta_{b_1} \beta_{b_0})_c$

Lect. 4': Generalised Josephus Sec. B

$f(1)=\alpha$
$f(2n)=2f(n)+\beta$
$f(2n+1)=2f(n)+\gamma$

$f(n)=A(n)\alpha+B(n)\beta+C(n)\gamma \cdots (1)$
$A(n)=2^m,\ B(n)=2^m-l-1,\ C(n)=l$

$\frac{3n+2}{(n-1)(n-2)} \equiv \frac{A}{n-1}+\frac{B}{n-2}$

$(\alpha,\beta,\gamma)\equiv(1,0,0)$ $A(1)=1$
$f(n)=A(n)$ $A(2n)=2A(n)$
$A(2n+1)=2A(n)$

n	1	2	3	4	5	6	7	8	9
$A(n)$	1	2	2	4	4	4	4	8	8

$n=2^m+l \Rightarrow \boxed{A(n)=2^m}$ ✓

$f(n)=1 \Rightarrow 1=\alpha,\ 1=2\cdot1+\beta,\ 1=2\cdot1+\gamma \Rightarrow (\alpha,\beta,\gamma)\equiv(1,-1,-1)$
$\boxed{A(n)-B(n)-C(n)=1}$

$f(n)=n \Rightarrow 1=\alpha,\ 2n=2\cdot n+\beta,\ 2n+1=2\cdot n+\gamma \Rightarrow (\alpha,\beta,\gamma)\equiv(1,0,1)$
$\boxed{A(n)+C(n)=n} \Rightarrow C(n)=n-2^m=l$ ✓

$A(n)-B(n)-C(n)=1 \Rightarrow B(n)=A(n)-C(n)-1=2^m-l-1$ ✓

Repertoire method: Ex. 16 & 20.

$J((b_m b_{m-1}\cdots b_1 b_0)_2)=(b_{m-1}\cdots b_1 b_0 b_m)_2$ $b_m=1$

$d \mid a \mid q$
dq
r

$a=dq+r;\ 0\le r<d$

$f(1)=\alpha$
$f(2n+j)=2f(n)+\beta_j;\ j\in\{0,1\},\ \beta_0=\beta,\ \beta_1=\gamma$

$2 \mid 2n+j \mid n$
$2n$
j

$$f((b_m b_{m-1} \cdots b_1 b_0)_2) = 2f((b_m b_{m-1} \cdots b_1)_2) + \beta_{b_0}$$

$$= 2(2f(b_m b_{m-1} \cdots b_2)_2 + \beta_{b_1}) + \beta_{b_0}$$

$$= 4f((b_m b_{m-1} \sim b_2)_2) + 2\beta_{b_1} + \beta_{b_0}$$

$$= 8f((b_m b_{m-1} \cdots b_3)_2) + 4\beta_{b_2} + 2\beta_{b_1} + \beta_{b_0}$$

$$\vdots$$

$$= 2^m f((b_m)_2) + 2^{m-1}\beta_{m-1} + \cdots + 4\beta_{b_2} + 2\beta_{b_1} + \beta_{b_0}$$

$$= 2^m \alpha + 2^{m-1}\beta_{m-1} + \cdots + 4\beta_{b_2} + 2\beta_{b_1} + \beta_{b_0}$$

$$= (\alpha \beta_{b_{m-1}} \cdots \beta_{b_2} \beta_{b_1} \beta_{b_0})_2 \rightarrow \text{notation abuse!}$$

$J(100) = J(2^6 + 36) = 36 \cdot 2 + 1 = 73$

$(\overset{b_m}{1}\ \overset{b_{m-1}}{1}\ \overset{b_{m-2}}{0}\ \cdots\ \overset{b_1}{0}\ \overset{b_0}{1}\ 0\ 0)_2$

$J(1) = 1 \qquad \alpha = 1$

$J(2n) = 2J(n) - 1 \qquad \beta = -1 = \beta_0$

$J(2n+1) = 2J(n) + 1 \qquad \gamma = 1 = \beta_1$

$2^6 \times 1 + 2^5 \times 1 + 2^4 \times (-1) + 2^3 \times (-1) + 2^2 \times 1 + 2^1 \times (-1) + 2^0 \times (-1)$

$= 64 + 32 - 16 - 8 + 4 - 2 - 1 = 73$

$f(j) = \alpha_j \qquad 1 \le j < d$

$f(dn + j) = cf(n) + \beta_j \qquad 0 \le j < d \ ; \ n \ge 1$

$f((b_m b_{m-1} \cdots b_1 b_0)_d) = (\alpha_{b_m} \beta_{b_{m-1}} \beta_{b_{m-2}} \cdots \beta_{b_1} \beta_{b_0})_c$

$f(1) = 1$

$f(2) = 2$

$f(3n) = 4f(n) + 1$

$f(3n+1) = 4f(n) + 2$

$f(3n+2) = 4f(n) + 3$

Lect 5 : Sums Sec. B

Sum of first n integers: $1+2+3+\cdots+(n-1)+n$

$1+2+\cdots+n$ ↳ term

$1+\_\_+n$

$a_1+a_2+\cdots+a_n \rightarrow$ general term: a_k

$1+2+\cdots+2^{n-1} \rightarrow a_k = 2^{k-1} \quad | \quad 2^0+2^1+\cdots+2^{n-1}$

Sigma notation: $\sum_{k=1}^{n} a_k \rightarrow$ delimited form

Generalized sigma notation: $\sum_{1\le k\le n} a_k \longrightarrow \sum_{P(k)} a_k$: sum of all terms satisfying $P(k)$

$\sum_{\substack{1\le k\le 100 \\ k \text{ odd}}} k^2 \equiv \sum_{k=0}^{49} (2k+1)^2 \quad | \quad \sum_{\substack{1\le p\le N \\ p \text{ prime}}} \frac{1}{p} = \sum_{k=1}^{\pi(N)} \frac{1}{p_k}$

$\downarrow \sum_{k} a_k [P(k)]$

$\sum_{1\le k\le n} a_k = \sum_{1\le k+1\le n} a_{k+1}$;

$P(k) \equiv 1\le k\le n$

$\sum_{k=2}^{n-1} k(k-1)(n-k) = \sum_{k=0}^{n} k(k-1)(n-k)$

$\sum_{p} \frac{1}{p} [p \text{ prime}] [p\le N]$

$[\text{statement}] = \begin{cases} 1; & \text{if statement is true} \\ 0; & \text{if statement is false} \end{cases}$

↳ Iverson notation

Sum → Recurrence : $S_n = \sum_{k=0}^{n} a_k \rightarrow S_0 = a_0$; $S_n = \sum_{k=0}^{n-1} a_k + a_n$

$\Rightarrow S_n = S_{n-1} + a_n$

$a_k = \beta + \gamma k$ $\boxed{R_0 = \alpha, R_n = R_{n-1} + \beta + \gamma n}$

$R_1 = \alpha+\beta+\gamma$, $R_2 = \alpha+2\beta+3\gamma \rightarrow R_n = A(n)\alpha + B(n)\beta + C(n)\gamma$

$R_n = 1$; $1 = \alpha$; $1 = 1+\beta+\gamma n \Rightarrow \beta+\gamma n = 0+0\cdot n$ $(\alpha,\beta,\gamma) = (1,0,0)$

$\boxed{A(n) = 1}$

$R_n = n$; $0 = \alpha$, $n = n-1+\beta+\gamma n \Rightarrow \beta+\gamma n = 1+0\cdot n$ $(\alpha,\beta,\gamma) = (0,1,0)$

$\boxed{B(n) = n}$

$R_n = n^2$; $0 = \alpha$, $n^2 = (n-1)^2 + \beta + \gamma n \Rightarrow \beta + \gamma n = 2n - 1$; $(\alpha, \beta, \gamma) = (0, -1, 2)$

$2C(n) - B(n) = n^2 \Rightarrow \boxed{C(n) = (n^2+n)/2}$

$R_n = \alpha + \beta n + \gamma(n^2+n)/2$; $a_k = \beta + \gamma k$; $a_0 = \alpha$

$$\sum_{k=0}^{n} (a + bk)$$

Recurrence → Sum

$T_0 = 0$, $T_n = 2T_{n-1} + 1 \rightarrow$ $T_n/2^n = T_{n-1}/2^{n-1} + 1/2^n$; $S_n = T_n/2^n$

↳ $T_0/2^0 = 0/2^0$;

$S_n = 1 - 1/2^n$

$\Rightarrow T_n/2^n = 1 - 1/2^n$

$\Rightarrow T_n = 2^n - 1$

↳ $S_n = S_{n-1} + 1/2^n$

$= S_{n-2} + 1/2^{n-1} + 1/2^n$

$= \vdots$

$= S_0 + \frac{1}{2} + \frac{1}{2^2} + \cdots + 1/2^n$

$= 0 + \frac{\frac{1}{2}(1 - 1/2^n)}{1 - 1/2} = 1 - \frac{1}{2^n}$

Lect. 5 : Sums Sec. A

Sum of first n integers: $1+2+3+\cdots+(n-1)+n$

$1+2+\cdots+n$ ↳term

$1+\cdots+n$

$a_1+a_2+\cdots+a_n$. Generalterm: a_k

$1+2+\cdots+2^{n-1}$; $a_k=2^{k-1}$

$\sum_{k=1}^{n} a_k$ (sigma notation) $\sum_{1\le k\le n} a_k$ (generalized sigma notation)

$\sum_{\substack{1\le k\le 100\\ k \text{ odd}}} k^2$ $\sum_{k=0}^{49}(2k+1)^2$ | $\sum_{\substack{p\le N\\ p \text{ prime}}} \frac{1}{p}$ $\sum_{k=1}^{\pi(N)} \frac{1}{p_k}$

$\sum_{1\le k\le n} a_k = \sum_{1\le k+1\le n} a_{k+1}$; $\sum_{k=1}^{n} a_k = \sum_{k=0}^{n-1} a_{k+1}$

$\sum a_k$ sum over all k satisfying property $P(k)$

$\sum_{k=2}^{n-1}{}^{P(k)} k(k-1)(n-k) = \sum_{k=0}^{n} k(k-1)(n-k)$

$[\text{statement}] = \begin{cases} 1, & \text{if statement is true} \\ 0, & \text{if statement is false} \end{cases}$ Iverson notation

$\sum_{k} a_k [P(k)]$ $\sum_{p} \frac{1}{p}[p\le N][p \text{ prime}]$

Sums → Recurrence $S_n = \sum_{k=0}^{n} a_k$, $S_0 = a_0$; $S_n = \sum_{k=0}^{n-1} a_k + a_n$

$S_n = S_{n-1} + a_n$

$a_n = \beta + \gamma n$; $R_0 = \alpha$, $R_n = R_{n-1} + \beta + \gamma n$

$R_1 = \alpha+\beta+\gamma$, $R_2 = \alpha+2\beta+3\gamma$ $R_n = A(n)\alpha + B(n)\beta + C(n)\gamma$

$R_n = 1$; $1 = \alpha$, $1 = 1 + \beta + \gamma n \Rightarrow \beta + \gamma n = 0 + 0 \cdot n$ $(\alpha, \beta, \gamma) = (1, 0, 0)$

$\boxed{A(n) = 1}$

$R_n = n$; $0 = \alpha$, $n = n - 1 + \beta + \gamma n \Rightarrow \beta + \gamma n = 1 + 0 \cdot n$ $(\alpha, \beta, \gamma) = (0, 1, 0)$

$\boxed{B(n) = n}$

$R_n = n^2$; $0 = \alpha$, $n^2 = (n-1)^2 + \beta + \gamma n \Rightarrow \beta + \gamma n = -1 + 2n$ $(\alpha, \beta, \gamma) = (0, -1, 2)$

$-B(n) + 2C(n) = n^2 \Rightarrow C(n) = (n^2 + n)/2$

$\sum_{K=0}^{n} (a + bk)$ $\quad a = \alpha$, $a = \beta$, $b = \gamma$ $\quad R_0 = a\ (\alpha)$, $R_n = \beta + \gamma k$ ($\beta \to a$, $\gamma \to b$)

Recurrence → Sum

$T_0 = 0$, $T_n = 2T_{n-1} + 1 \Rightarrow T_n/2^n = T_{n-1}/2^{n-1} + 1/2^n$; $S_n = T_n/2^n$, $S_{n-1} = T_{n-1}/2^{n-1}$

↳ $T_0/2^0 = 0/2^0$

$\Rightarrow S_n = S_{n-1} + 1/2^n$

$= S_{n-2} + 1/2^{n-1} + 1/2^n$

$\vdots$

$= S_0 + 1/2 + 1/2^2 + \cdots + 1/2^n$

$T_n/2^n = \frac{\frac{1}{2}\left(1 - \frac{1}{2^n}\right)}{1 - 1/2} = 1 - 1/2^n$

$\Rightarrow T_n = 2^n - 1$

$T_0 = 0,\ T_n = 2T_{n-1} + 1$

$a_n T_n = b_n T_{n-1} + c_n \Rightarrow s_n a_n T_n = s_n b_n T_{n-1} + s_n c_n$

$[s_n b_n = s_{n-1} a_{n-1}] \Rightarrow s_n a_n T_n = s_{n-1} a_{n-1} T_{n-1} + s_n c_n$

$[s_n a_n T_n = \sigma_n] \Rightarrow \sigma_n = \sigma_{n-1} + s_n c_n$

$= \sigma_{n-2} + s_{n-1} c_{n-1} + s_n c_n$

$\vdots$

$\Rightarrow s_n a_n T_n = \sigma_0 + \sum_{k=1}^{n} s_k c_k = s_0 a_0 T_0 + \sum_{k=1}^{n} s_k c_k = s_1 b_1 T_0 + \sum_{k=1}^{n} s_k c_k$

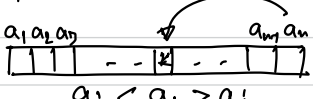
$\Rightarrow T_n = \frac{1}{s_n a_n}\left(s_1 b_1 T_0 + \sum_{k=1}^{n} s_k c_k\right)$

$s_n b_n = s_{n-1} a_{n-1} \Rightarrow s_n = \frac{a_{n-1}}{b_n} s_{n-1} = \frac{a_{n-1}}{b_n} \times \frac{a_{n-2}}{b_{n-1}} \times s_{n-2} = \cdots = \frac{a_{n-1} \cdots a_1}{b_n \cdots b_2} s_1$

ToH: $a_n = 1, b_n = 2, c_n = 1$; $s_n = \underbrace{\frac{1}{2} \times \frac{1}{2} \times \cdots \times \frac{1}{2}}_{(n-1)} \times \frac{1}{2} = 1/2^n$

$T_n = 2^n \times 1 \times \sum_{k=1}^{n} \frac{1}{2^k} \times 1 = 2^n - 1$

Quicksort:



$C_0 = 0$

$C_n = (n+1) + C_0 + C_{n-1}$

$C_n = (n+1) + C_1 + C_{n-2}$

$C_n = (n+1) + C_2 + C_{n-3}$

$\vdots$

$C_n = (n+1) + C_{n-1} + C_0$

$nC_n = n(n+1) + 2\sum_{k=0}^{n-1} C_k \Rightarrow (n-1)C_{n-1} = n(n-1) + 2\sum_{k=0}^{n-2} C_k$

$\Rightarrow C_n = n + 1 + \frac{2}{n}\sum_{k=0}^{n-1} C_k$

$\Rightarrow nC_n - (n-1)C_{n-1} = 2n + 2C_{n-1}$

$\Rightarrow nC_n = (n+1)C_{n-1} + 2n$

$a_n T_n = b_n T_{n-1} + c_n$

$$\delta_n = \frac{a_{n-1}a_{n-2}\cdots a_1}{b_n b_{n-1}\cdots b_2} = \frac{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n+1)\,n\,(n-1)\cdots 3} = \frac{2}{n(n+1)}$$

$$C_n = n(n+1)/2 \times \frac{1}{n}\sum_{k=1}^{n}\frac{2}{k(k+1)}\times 2k = 2(n+1)\sum_{k=1}^{n}\frac{1}{k+1}$$

$$H_n = 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} = \sum_{k=1}^{n}\frac{1}{k}\quad[\text{Harmonic number}]$$

$$\sum_{k=1}^{n}\frac{1}{k+1} = \sum_{1\le k\le n}\frac{1}{k+1} = \sum_{1\le k-1\le n}\frac{1}{k} = \sum_{2\le k\le n+1}\frac{1}{k} = \sum_{2\le k\le n}\frac{1}{k} + \frac{1}{n+1}$$

$$= \sum_{1\le k\le n}\frac{1}{k} + \frac{1}{n+1} - 1$$

$$= H_n - \frac{n}{n+1}$$

$$C_n = 2(n+1)\left(H_n - \frac{n}{n+1}\right)$$

$$= 2(n+1)H_n - 2n$$

$$= O(n\lg n)$$

$$\lim_{n\to\infty} H_n = \ln n + \gamma \quad [0.577\ldots, \text{a constant}]$$

Manipulation of sums: (K is a finite set of integers)

1) $\sum_{k\in K} ca_k = c\sum_{k\in K} a_k$ (distributive law)

2) $\sum_{k\in K}(a_k+b_k) = \sum_{k\in K} a_k + \sum_{k\in K} b_k$ (associative law)

3) $\sum_{k\in K} a_k = \sum_{p(k)\in K} a_{p(k)}$ (commutative law) $P(k)$ is a permutation over $\mathbb{Z}$

$K=\{-1,0,1\}$, $P(k)=-k$ $\quad -1\to 1,\ 0\to 0,\ 1\to -1$

$a_{-1}+a_0+a_1 = a_1+a_0+a_{-1}$

$P(k) = n-k$ $\quad 0\to n,\ 1\to n-1,\ \ldots,\ n\to 0$

$$0\le n-k\le n \to \begin{matrix} k\le n \\ 0\le k \\ \to 0\le k\le n\end{matrix}$$

$$S = \sum_{0\le k\le n}(a+bk)$$

$$= \sum_{0\le n-k\le n}(a+b(n-k)) = \sum_{0\le k\le n}(a+b(n-k))$$

$$2S = \sum_{0\le k\le n}(a+bk+a+b(n-k))$$

$$= \sum_{0\le k\le n}(2a+bn)$$

$$= (2a+bn)\sum_{0\le k\le n} 1 = (2a+bn)(n+1) \Rightarrow S = (a+\tfrac{1}{2}bn)(n+1)$$

Lect. 6: Summation factors and manipulation of sums Sec. 3

$T_0 = 0,\ T_n = 2T_{n-1} + 1$

$a_n T_n = b_n T_{n-1} + c_n \Rightarrow s_n a_n T_n = s_n b_n T_{n-1} + s_n c_n$

$[s_n b_n = s_{n-1} a_{n-1}] \Rightarrow s_n a_n T_n = s_{n-1} a_{n-1} T_{n-1} + s_n c_n$

$[s_n a_n T_n = S_n] \Rightarrow S_n = S_{n-1} + s_n c_n$

$= S_{n-2} + s_{n-1} c_{n-1} + s_n c_n$

$\vdots$

$= S_0 + s_1 c_1 + s_1 c_2 + \cdots + s_n c_n = S_0 + \sum_{k=1}^{n} s_k c_k$

$s_n a_n T_n = s_0 a_0 T_0 + \sum_{k=1}^{n} s_k c_k = s_1 b_1 T_0 + \sum_{k=1}^{n} s_k c_k$

$\Rightarrow T_n = \frac{1}{s_n a_n}\left(s_1 b_1 T_0 + \sum_{k=1}^{n} s_k c_k\right)$

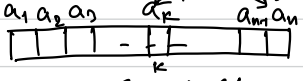
$s_n b_n = s_{n-1} a_{n-1} \Rightarrow s_n = \frac{a_{n-1}}{b_n} \times s_{n-1} = \frac{a_{n-1}}{b_n} \times \frac{a_{n-2}}{b_{n-1}} \times s_{n-2} = \cdots = \frac{a_{n-1} \cdots a_1}{b_n \cdots b_2} s_1$

ToH: $T_n = 2T_{n-1} + 1$ $\quad a_n = 1$ $\quad s_n = \frac{1 \times 1 \cdots \times 1}{2 \times 2 \cdots \times 2} s_1 = \frac{1}{2^{n-1}} \times \frac{1}{2} = \frac{1}{2^n}$

$a_n T_n = b_n T_{n-1} + c_n$ $\quad b_n = 2$

$c_n = 1$

Quicksort:



$a_i < a_k > a_j$

$C_0 = 0$

$C_n = (n+1) + C_0 + C_{n-1}$

$C_n = (n+1) + C_1 + C_{n-2}$

$\vdots$

$C_n = (n+1) + C_{n-1} + C_0$

$nC_n = n(n+1) + 2\sum_{k=0}^{n-1} C_k \longrightarrow (n-1)C_{n-1} = n(n-1) + 2\sum_{k=0}^{n-2} C_k$

$\Rightarrow C_n = (n+1) + \frac{2}{n}\sum_{k=0}^{n-1} C_k \Rightarrow nC_n - (n-1)C_{n-1} = 2n + 2C_{n-1}$

$\Rightarrow nC_n = (n+1)C_{n-1} + 2n$

$a_n T_n = b_n T_{n-1} + c_n$

$$s_n = \frac{a_{n+1}a_{n-2}\cdots a_1}{b_n b_{n-1}\cdots b_2} = \frac{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n+1)n(n-1)\cdots 3} = \frac{2}{n(n+1)}$$

$$C_n = n(n+1)/2 \times \frac{1}{n}\sum_{k=1}^{n}\frac{2}{k(k+1)} \times 2k = 2(n+1)\sum_{k=1}^{n}\frac{1}{k+1}$$

$$H_n = 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} = \sum_{k=1}^{n}\frac{1}{k} \quad \text{[Harmonic number]}$$

$$\sum_{k=1}^{n}\frac{1}{k+1} = \sum_{1\le k\le n}\frac{1}{k+1} = \sum_{1\le k-1\le n}\frac{1}{k-1+1} = \sum_{2\le k\le n+1}\frac{1}{k} = \sum_{2\le k\le n}\frac{1}{k}+\frac{1}{n+1}$$

$$= \sum_{1\le k\le n}\frac{1}{k}+\frac{1}{n+1}-1 = H_n - \frac{n}{n+1} \qquad \lim_{n\to\infty}(H_n - \ln n) = \gamma \ [0.577\ldots \text{ a const.}]$$

$$C_n = 2(n+1)\left(H_n - \frac{n}{n+1}\right) = 2(n+1)H_n - 2n = O(n\lg n)$$

Manipulation of sums: K is a finite set of integers

1) $\sum_{k\in K} ca_k = c\sum_{k\in K} a_k$ (distributive law)

2) $\sum_{k\in K}(a_k+b_k) = \sum_{k\in K} a_k + \sum_{k\in K} b_k$ (associative law)

3) $\sum_{k\in K} a_k = \sum_{p(k)\in K} a_{p(k)}$ (commutative law) $p(k)$ is a permutation over $\mathbb{Z}$

$K=\{-1,0,1\}$ $p(k)=-k$ $\begin{matrix}-1\to 1\\ 0\to 0\\ 1\to -1\end{matrix}$ $a_{-1}+a_0+a_1 = a_1+a_0+a_{-1}$

$S = \sum_{0\le k\le n}(a+bk)$ $p(k)=n-k$ $\begin{matrix}0\to n\\ 1\to n-1\\ \vdots\\ n\to 0\end{matrix}$ $S = \sum_{0\le n-k\le n}(a+b(n-k)) = \sum_{0\le k\le n}(a+b(n-k))$

$2S = \sum_{0\le k\le n}(a+bk)+\sum_{0\le k\le n}(a+b(n-k))$ $\frac{0\le n-k}{\Rightarrow k\le n}$ $\frac{n-k\le n}{0\le k}$ $\Rightarrow 0\le k\le n$

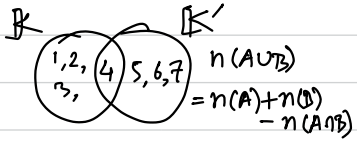
$= \sum_{0\le k\le n}(a+bk+a+bn-bk) = \sum_{0\le k\le n}(2a+bn) = (2a+bn)\sum_{0\le k\le n}1$

$= (2a+bn)(n+1)$

$\Rightarrow S = (a+\frac{1}{2}bn)(n+1)$

Lecd. 7: Manipulation of Sums (contd.) & Multiple Sums

$$\sum_{k\in K} a_k + \sum_{k\in K'} a_k = \sum_{k\in K\cap K'} a_k + \sum_{k\in K\cup K'} a_k$$



$$a_1+a_2+a_3+a_4 = a_4+a_1+a_2+a_3$$
$$+a_4+a_5+a_6+a_7 \quad +a_4+a_5+a_6+a_7$$

$$\sum_{k=1}^{m} a_k + \sum_{k=m}^{n} a_k = \sum_{k=1}^{n} a_k + a_m$$

$$S_n = \sum_{0\le k\le n} a_k \rightarrow S_{n+1} = \sum_{0\le k\le n+1} a_k = \sum_{0\le k\le n} a_k + a_{n+1} = S_n + a_{n+1}$$

$$S_{n+1} = a_0 + \sum_{1\le k\le n+1} a_k = a_0 + \sum_{1\le k+1\le n+1} a_{k+1} = a_0 + \sum_{0\le k\le n} a_{k+1}$$

$$S_n + a_{n+1} = a_0 + \sum_{0\le k\le n} a_{k+1} \quad \text{[Perturbation method]}$$

$$S_n = \sum_{0\le k\le n} ax^k \Rightarrow \underline{S_n + ax^{n+1}} = a + \sum_{0\le k\le n} ax^{k+1} = \underline{a + xS_n}$$

$$\Rightarrow S_n(1-x) = a(1-x^{n+1}) \Rightarrow S_n = \frac{a(1-x^{n+1})}{1-x}$$

$$=$$

$$S_n = \sum_{0\le k\le n} k2^k \Rightarrow S_n + (n+1)2^{n+1} = \sum_{0\le k\le n} (k+1)2^{k+1} = \sum_{0\le k\le n} k2^{k+1} + \sum_{0\le k\le n} 2^{k+1}$$

$$= 2S_n + \frac{2\cdot(1-2^{n+1})}{1-2} = 2S_n + 2^{n+2} - 2$$

$$\Rightarrow S_n + (n+1)2^{n+1} = 2S_n + 2^{n+2} - 2 \Rightarrow S_n = (n+1)2^{n+1} - 2\cdot 2^{n+1} + 2$$
$$= (n-1)2^{n+1} + 2$$

$$\sum_{k=0}^{n} kx^k = \frac{x-(n+1)x^{n+1}+nx^{n+2}}{(1-x)^2} \quad [x\neq 1]$$

Multiple sums: $\sum_{1\le j,k\le 3} a_j b_k = a_1b_1 + a_1b_2 + a_1b_3 \quad (a_1')$

$+ a_2b_1 + a_2b_2 + a_2b_3 \quad (a_2') \rightarrow (a_1+a_2+a_3)$

$+ a_3b_1 + a_3b_2 + a_3b_3 \quad (a_3') \qquad (b_1+b_2+b_3)$

$b_1' \qquad b_2' \qquad b_3' \qquad s$

$\sum_{P(j,k)} a_{j,k} = \sum_{j,k} a_{j,k}[P(j,k)]$ ✓

$\sum_j \left(\sum_k a_{j,k}[P(j,k)] \right) = \sum_k \left(\sum_j a_{j,k} P[j,k] \right)$ [Interchanging order of summation]

$$\sum_{1\le j,k\le 3} a_j b_k = \sum_{j,k} a_j b_k [1\le j,k\le 3] = \sum_{j,k} a_j b_k [1\le j\le 3][1\le k\le 3]$$

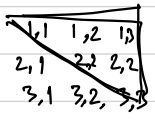
$$= \sum_j \left(\sum_k a_j b_k [1\le j\le 3][1\le k\le 3] \right)$$

$$= \sum_j \left(a_j [1\le j\le 3] \sum_k b_k [1\le k\le 3] \right)$$

$$= \sum_j a_j [1\le j\le 3] \left(\sum_{k=1}^{3} b_k \right) = \sum_{k=1}^{3} b_k \left(\sum_j a_j [1\le j\le 3] \right)$$

$$= \sum_{k=1}^{3} b_k \times \sum_{j=1}^{3} a_j = \left(\sum_{j=1}^{3} a_j \right)\left(\sum_{k=1}^{3} b_k \right)$$

$$\sum_{\substack{j\in\mathbb{J} \\ k\in\mathbb{K}}} = \left(\sum_{j\in\mathbb{J}} a_j \right)\left(\sum_{k\in\mathbb{K}} b_k \right)$$



$$\sum_{j\in\mathbb{J}} \sum_{k\in\mathbb{K}} a_{j,k} = \sum_{\substack{j\in\mathbb{J} \\ k\in\mathbb{K}}} a_{j,k} = \sum_{k\in\mathbb{K}} \sum_{j\in\mathbb{J}} a_{j,k}$$

$$\sum_{j\in\mathbb{J}} \sum_{k\in\mathbb{K}(j)} a_{j,k} = \sum_{k\in\mathbb{K}'} \sum_{j\in\mathbb{J}'(k)} a_{j,k}$$

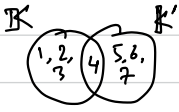
$$\Rightarrow \sum_j \sum_k a_{j,k} [j\in\mathbb{J}][k\in\mathbb{K}(j)] = \sum_k \sum_j a_{j,k} [k\in\mathbb{K}'][j\in\mathbb{J}'(k)]$$

$$\Rightarrow [j\in\mathbb{J}][k\in\mathbb{K}(j)] = [k\in\mathbb{K}'][j\in\mathbb{J}'(k)]$$

Lect. 7: Manipulation of Sums (contd.) & Multiple Sums

Sec. B

$$\sum_{K\in\mathbb{K}} a_K + \sum_{K\in\mathbb{K}'} a_K = \sum_{K\in\mathbb{K}\cap\mathbb{K}'} a_K + \sum_{K\in\mathbb{K}\cup\mathbb{K}'} a_K$$



$(a_1+a_2+a_3+a_4)+(a_4+a_5+a_6+a_7) = a_4+a_1+a_2+a_3+\cdots+a_7$ $\quad n(A\cup B)=n(A)+n(B)-n(A\cap B)$

$\Rightarrow n(A)+n(B)=n(A\cap B)+n(A\cup B)$

$$\sum_{K=1}^{m} a_K + \sum_{K=m}^{n} a_K = \sum_{K=1}^{n} a_K + a_m$$

$$\sum_{0\le K\le n} = a_0 + \sum_{1\le K\le n} a_K = \sum_{0\le K\le n-1} a_K + a_n$$

$$S_n = \sum_{0\le K\le n} a_K \Rightarrow S_{n+1} = \sum_{0\le K\le n+1} a_K = \sum_{0\le K\le n} a_K + a_{n+1} = \underline{S_n + a_{n+1}}$$

$$= a_0 + \sum_{1\le K\le n+1} a_K = a_0 + \sum_{1\le K+1\le n+1} a_{K+1} = a_0 + \sum_{0\le K\le n} a_{K+1}$$

$$S_n = \sum_{0\le K\le n} ax^K$$

[Perturbation method]

$$\Rightarrow S_n + ax^{n+1} = a + \sum_{0\le K\le n} ax^{K+1} = a + x\sum_{0\le K\le n} ax^K = a + xS_n$$

$$\Rightarrow S_n(1-x) = a(1-x^{n+1}) \Rightarrow S_n = \frac{a(1-x^{n+1})}{(1-x)}$$

$$=$$

$$S_n = \sum_{0\le K\le n} K2^K \Rightarrow \underline{S_n + (n+1)2^{n+1}} = \sum_{0\le K\le n} (K+1)2^{K+1} = \sum_{0\le K\le n} K2^{K+1} + \sum_{0\le K\le n} 2^{K+1}$$

$$= 2\sum_{0\le K\le n} K2^K + \frac{2(1-2^{n+1})}{1-2} = \underline{2S_n + 2^{n+2} - 2}$$

$$\Rightarrow S_n = (n+1)2^{n+1} - 2\cdot 2^{n+1} + 2 = (n-1)2^{n+1} + 2$$

$$\sum_{K=0}^{n} Kx^K = \frac{x-(n+1)x^{n+1}+nx^{n+2}}{(1-x)^2}\ ;\ x\neq 1$$

Multiple Sums: $\sum_{1\le j,k\le 3} a_j b_k = a_1b_1 + a_1b_2 + a_1b_3 \quad (a_1')$

$+ a_2b_1 + a_2b_2 + a_2b_3 \quad (a_2') = (a_1+a_2+a_3)(b_1+b_2+b_3)$

$+ a_3b_1 + a_3b_2 + a_3b_3 \quad (a_3')$

$\qquad\qquad (b_1') \quad (b_2') \quad (b_3') \qquad s$

$$\sum_{P(j,k)} a_{j,k} = \sum_{j,k} a_{j,k}[P(j,k)]$$

$$\sum_j \sum_k a_{j,k}[P(j,k)] = \sum_j \left(\sum_k a_{j,k}[P(j,k)]\right) = \sum_k \left(\sum_j a_{j,k}[P(j,k)]\right)$$

$$\sum_{1\le j,k\le 3} a_j b_k = \sum_{j,k} a_j b_k [1\le j,k\le 3] = \sum_{j,k} a_j b_k [1\le j\le 3][1\le k\le 3]$$

$$= \sum_j \left(\sum_k a_j b_k [1\le j\le 3][1\le k\le 3]\right)$$

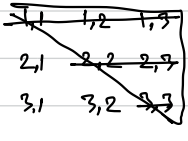
$$= \sum_j a_j [1\le j\le 3]\left(\sum_k b_k [1\le k\le 3]\right) = \sum_j a_j [1\le j\le 3]\left(\sum_{k=1}^{3} b_k\right)$$

$$= \left(\sum_{k=1}^{3} b_k\right)\left(\sum_j a_j [1\le j\le 3]\right) = \left(\sum_{k=1}^{3} b_k\right)\left(\sum_{j=1}^{3} a_j\right) = \left(\sum_{j=1}^{3} a_j\right)\left(\sum_{k=1}^{3} b_k\right)$$

$$\sum_{\substack{j\in\mathbb{J}\\ k\in\mathbb{K}}} a_j b_k = \left(\sum_{j\in\mathbb{J}} a_j\right)\left(\sum_{k\in\mathbb{K}} b_k\right)$$

$$\sum_{j\in\mathbb{J}}\sum_{k\in\mathbb{K}} a_{j,k} = \sum_{\substack{j\in\mathbb{J}\\ k\in\mathbb{K}}} a_{j,k} = \sum_{k\in\mathbb{K}}\sum_{j\in\mathbb{J}} a_{j,k}$$

$$\sum_{j\in\mathbb{J}}\sum_{k\in\mathbb{K}(j)} = \sum_{k\in\mathbb{K}'}\sum_{j\in\mathbb{J}'(k)} a_{j,k}$$



$$\Leftrightarrow \sum_j \sum_k a_{j,k}[j\in\mathbb{J}][k\in\mathbb{K}(j)] = \sum_k \sum_j a_{j,k}[k\in\mathbb{K}'][j\in\mathbb{J}'(k)]$$

$$\Leftrightarrow [j\in\mathbb{J}][k\in\mathbb{K}(j)] = [k\in\mathbb{K}'][j\in\mathbb{J}'(k)]$$

$$[1\le j\le n][j\le k\le n]=[1\le j\le k\le n]=[1\le k\le n][1\le j\le k]$$

$$\begin{bmatrix} a_1a_1 & a_1a_2 & \cdots & a_1a_n \\ a_2a_1 & a_2a_2 & \cdots & a_2a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_na_1 & a_na_2 & \cdots & a_na_n \end{bmatrix}$$

$0<x<y<1$

$$\int_0^1\int_0^y f(x,y)\,dx\,dy$$

$$\int_0^1\int_x^1 f(x,y)\,dy\,dx$$

$$S_\triangle=\sum_{1\le j\le k\le n} a_ja_k=\sum_{1\le k\le j\le n} a_ka_j=\sum_{1\le k\le j\le n} a_ja_k=S_\triangleright$$

$$[1\le j\le k\le n]+[1\le k\le j\le n]=[1\le j,k\le n]+[1\le j=k\le n]$$

$a_ia_j=a_ja_i$ ↳ $[i,j]$ $[j,i]$

$$2S_\triangle=S_\triangle+S_\triangleright=\sum_{1\le j,k\le n} a_ja_k+\sum_{1\le j=k\le n} a_ja_k$$

$$=\left(\sum_{j=1}^n a_j\right)\left(\sum_{k=1}^n a_k\right)+\sum_{1\le j\le n} a_j^2$$

$$=\left(\sum_{j=1}^n a_j\right)^2+\sum_{j=1}^n a_j^2$$

$=$

$$S=\sum_{1\le j<k\le n}(a_k-a_j)(b_k-b_j)=\sum_{1\le k<j\le n}(a_j-a_k)(b_j-b_k)=\sum_{1\le k<j\le n}(a_k-a_j)(b_k-b_j)$$

$$[1\le j<k\le n]+[1\le k<j\le n]=[1\le j,k\le n]-[1\le j=k\le n]$$

$$2S=\sum_{1\le j,k\le n}(a_k-a_j)(b_k-b_j)-\sum_{1\le j=k\le n}(a_k-a_j)(b_k-b_j)$$

$$=\sum_{1\le j,k\le n} a_kb_k-\sum_{1\le j,k\le n} a_jb_k-\sum_{1\le j,k\le n} a_kb_j+\sum_{1\le j,k\le n} a_jb_j$$

$$=2\sum_{1\le j,k\le n} a_kb_k-2\sum_{1\le j,k\le n} a_jb_k$$

$$\sum_{1\le j,k\le n} a_k b_k = \sum_{1\le k\le n}\sum_{1\le j\le n} a_k b_k = \sum_{1\le k\le n} a_k b_k \sum_{1\le j\le n} 1 = \sum_{1\le k\le n} a_k b_k n = n\sum_{1\le k\le n} a_k b_k$$

$$2S = 2n\sum_{1\le k\le n} a_k b_k - 2\left(\sum_{k=1}^n a_k\right)\left(\sum_{k=1}^n b_k\right)$$

$$\left(\sum_{k=1}^n a_k\right)\left(\sum_{k=1}^n b_k\right) = n\sum_{k=1}^n a_k b_k - \sum_{1\le j<k\le n} (a_k - a_j)(b_k - b_j)$$

x y z $\Rightarrow y - x = z \ge 0 \Rightarrow x \le y$

$$\left(\sum_{k=1}^n a_k\right)\left(\sum_{k=1}^n b_k\right) \le n\sum_{k=1}^n a_k b_k \text{ ; if } a_1 \le \cdots \le a_n \text{ ; } b_1 \le \cdots \le b_n$$

$$\left(\sum_{k=1}^n a_k\right)\left(\sum_{k=1}^n b_k\right) \ge n\sum_{k=1}^n a_k b_k \text{ ; if } a_1 \le \cdots \le a_n \text{ ; } b_1 \ge \cdots \ge b_n$$

↳ Chebyshev's monotonic inequalities.

↳ $y - x = z \le 0 \Rightarrow x \ge y$

$$S_n = \sum_{1\le j<k\le n} \frac{1}{k-j} \quad [S_1 = 0,\ S_2 = 1,\ S_3 = S_2]$$

$$= \sum_{1\le k\le n}\sum_{1\le j<k} \frac{1}{k-j} = \sum_{1\le j\le n}\sum_{j<k\le n} \frac{1}{k-j}$$

$$= \sum_{1\le k\le n}\sum_{1\le k-j<k} \frac{1}{j} \quad [j \leftarrow k-j] = \sum_{1\le j\le n}\sum_{j<k+j\le n} \frac{1}{k} \quad [k \leftarrow k+j]$$

$1 \le k-j \Rightarrow j \le k-1$; $k-j<k \Rightarrow 0<j$

$$= \sum_{1\le k\le n}\sum_{0<j\le k-1} \frac{1}{j} = \sum_{1\le j\le n}\sum_{0<k\le n-j} \frac{1}{k}$$

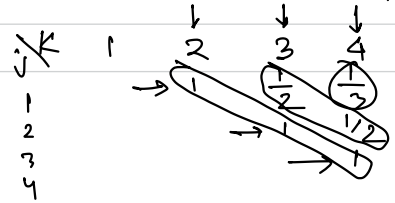
$$= \sum_{1\le k\le n} H_{k-1} = \sum_{1\le j\le n} H_{n-j}$$

$$= \sum_{0\le k<n} H_k \quad [k \leftarrow k+1] = \sum_{1\le n-j\le n} H_j = \sum_{0\le j<n} H_j$$

$$S_n = \sum_{1\le j<k\le n} \frac{1}{k-j} = \sum_{1\le j<k+j\le n} \frac{1}{k} \quad [k \leftarrow k+j]$$

$$= \sum_{1\le k\le n}\sum_{1\le j\le n-k} \frac{1}{k} = \sum_{1\le k\le n} \frac{n-k}{k} = \sum_{1\le k\le n} \frac{n}{k} - \sum_{1\le k\le n} 1 = nH_n - n = \sum_{0\le k<n} H_k$$

↳ $\frac{4-1}{1} + \frac{4-2}{2} + \frac{4-3}{3}$



Lect. 8 ; Multiple Sums contd. Sec. A

$$[1\le j\le n][j\le K\le n]=[1\le j\le K\le n]=[1\le K\le n][1\le j\le K]$$

$$\begin{bmatrix} a_1a_1 & a_1a_2 & \cdots & a_1a_n \\ a_2a_1 & a_2a_2 & \cdots & a_2a_n \\ \vdots & & \ddots & \vdots \\ a_na_1 & a_na_2 & \cdots & a_na_n \end{bmatrix}$$

$$\sum_{j=1}^{n}\sum_{K=j}^{n} a_{j,K}=\sum_{1\le j\le K\le n} a_{j,K}=\sum_{K=1}^{n}\sum_{j=1}^{K} a_{j,K}$$

$0<x<y<1$

$$\int_0^1\int_0^y f(x,y)\,dx\,dy$$

$$\int_0^1\int_x^1 f(x,y)\,dy\,dx$$

$$S_\nabla=\sum_{1\le j\le K\le n} a_ja_K=\sum_{1\le K\le j\le n} a_Ka_j=\sum_{1\le K\le j\le n} a_ja_K=S_\triangle$$

$$2S_\nabla=S_\nabla+S_\triangle=\sum_{1\le j,K\le n} a_ja_K+\sum_{1\le j=K\le n} a_ja_K$$

$$\sum_{1\le j,K\le n} a_ja_K=\left(\sum_{j=1}^{n}a_j\right)\left(\sum_{K=1}^{n}a_K\right)=\left(\sum_{j=1}^{n}a_j\right)^2;\quad \sum_{1\le j=K\le n} a_ja_K=\sum_{1\le j\le n} a_j^2=\sum_{j=1}^{n}a_j^2$$

$$S_\nabla=\frac{1}{2}\left(\left(\sum_{j=1}^{n}a_j\right)^2+\sum_{j=1}^{n}a_j^2\right)$$

$$S=\sum_{1\le j<K\le n}(a_K-a_j)(b_K-b_j)=\sum_{1\le K<j\le n}(a_j-a_K)(b_j-b_K)=\sum_{1\le K<j\le n}(a_K-a_j)(b_K-b_j)$$

$$2S=\sum_{1\le j,K\le n}(a_K-a_j)(b_K-b_j)-\sum_{1\le j=K\le n}(a_K-a_j)(b_K-b_j)$$

$$=\sum_{1\le j,K\le n}a_Kb_K-\sum_{1\le j,K\le n}a_jb_K-\sum_{1\le j,K\le n}a_Kb_j+\sum_{1\le j,K\le n}a_jb_j$$

$$=2\sum_{1\le j,K\le n}a_Kb_K-2\sum_{1\le j,K\le n}a_jb_K$$

$$\sum_{1\le j,K\le n}a_Kb_K=\sum_{1\le K\le n}\sum_{1\le j\le n}a_Kb_K=\sum_{1\le K\le n}a_Kb_K\sum_{1\le j\le n}1=\sum_{1\le K\le n}a_Kb_K\,n=n\sum_{1\le K\le n}a_Kb_K$$

$$\Rightarrow S=n\sum_{K=1}^{n}a_Kb_K-\left(\sum_{j=1}^{n}a_j\right)\left(\sum_{K=1}^{n}b_K\right)$$

$$\Rightarrow \underbrace{\left(\sum_{K=1}^{n}a_K\right)}_{x}\left(\sum_{K=1}^{n}b_K\right)=n\underbrace{\sum_{K=1}^{n}a_Kb_K}_{y}-\underbrace{\sum_{1\le j<K\le n}(a_K-a_j)(b_K-b_j)}_{z}$$

$x = y - z \Rightarrow y - x = z \geq 0 \Rightarrow y - x \geq 0 \Rightarrow x \leq y$ (a_i, b_i monotonically increasing)

$(\sum_{k=1}^{n} a_k)(\sum_{k=1}^{n} b_k) \leq n \sum_{k=1}^{n} a_k b_k$; $a_1 \leq \cdots \leq a_n$, $b_1 \leq \cdots \leq b_n$

$(\sum_{k=1}^{n} a_k)(\sum_{k=1}^{n} b_k) \geq n \sum_{k=1}^{n} a_k b_k$; $a_1 \leq \cdots \leq a_n$, $b_1 \geq \cdots \geq b_n$

↳ Chebyshev's monotonic inequalities

$S_n = \sum_{1 \leq j < k \leq n} \frac{1}{k-j}$ $[S_1 = 0, S_2 = 1, S_3 = 5/2]$

$= \sum_{1 \leq k \leq n} \sum_{1 \leq j < k} \frac{1}{k-j}$

$= \sum_{1 \leq k \leq n} \sum_{1 \leq k-j < k} \frac{1}{j}$ $[j \leftarrow k-j]$

$[1 \leq k-j \Rightarrow j \leq k-1$
$k-j < k \Rightarrow 0 < j]$

$= \sum_{1 \leq k \leq n} \sum_{0 < j \leq k-1} \frac{1}{j}$

$= \sum_{1 \leq k \leq n} H_{k-1}$

$= \sum_{0 \leq k < n} H_k$

$= \sum_{1 \leq j \leq n} \sum_{j < k \leq n} \frac{1}{k-j}$

$= \sum_{1 \leq j \leq n} \sum_{j < k+j \leq n} \frac{1}{k}$ $[k \leftarrow k+j]$

$j < k+j \Rightarrow 0 < k$
$k+j \leq n \Rightarrow k \leq n-j$

$= \sum_{1 \leq j \leq n} \sum_{0 < k \leq n-j} \frac{1}{k}$

$= \sum_{1 \leq j \leq n} H_{n-j}$

$= \sum_{1 \leq n-j \leq n} H_j$ $[j \leftarrow n-j] = \sum_{0 \leq j < n} H_j$

$S_n = \sum_{1 \leq j < k \leq n} \frac{1}{k-j}$

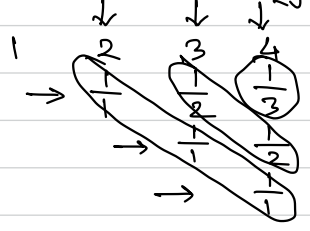
$= \sum_{1 \leq j < k+j \leq n} \frac{1}{k}$ $[K \leftarrow k+j]$

$= \sum_{1 \leq k \leq n} \sum_{1 \leq j \leq n-k} \frac{1}{k}$

$= \sum_{1 \leq k \leq n} \frac{1}{k} \sum_{1 \leq j \leq n-k} 1 = \sum_{1 \leq k \leq n} \frac{n-k}{k} = \sum_{1 \leq k \leq n} \frac{n}{k} - \sum_{1 \leq k \leq n} 1$

$= n \sum_{1 \leq k \leq n} \frac{1}{k} - n = nH_n - n = \sum_{0 \leq k < n} H_k$

$\frac{1}{k-j}$	j/k
$j<k$	1
	2
	3
	4



$\frac{4-1}{1} = \frac{3}{1} = 3 \times \frac{1}{1}$, $\frac{4-2}{2} = 2 \times \frac{1}{2}$, $\frac{4-3}{3} = \frac{1}{3}$

Lect. 9: General methods for sums

n | 0 | 1 | 2 | 3 | 4 | ....

$S_n = \sum_{0 \le k \le n} k^2$; S_n | 0 | 1 | 5 | 14 | 30 | ....

Method 0: Look it up : $S_n = n(n+1)(2n+1)/6 \rightarrow$

Method 1: Guess the answer; prove by induction

$S_n = an^3 + bn^2 + cn + d$; $0 = d$, $1 = a+b+c$

$5 = 8a+4b+2c$ $\quad (a,b,c) = (\frac{1}{3}, \frac{1}{2}, \frac{1}{6})$

$14 = 27a+9b+3c$

$S_n = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$

$= n/6\,(2n^2+3n+1) = \frac{n}{6}(n+1)(2n+1) \rightarrow$ prove by induction

Method 2: Perturbation

$\underset{a_{n+1}}{S_n} + (n+1)^2 = \underset{a_0}{0} + \sum_{0 \le k \le n} (k+1)^2 = \sum_{0 \le k \le n} (k^2+2k+1) = \underset{a_{k+1}}{\sum_{0 \le k \le n} k^2} + 2\sum_{0 \le k \le n} k + \sum_{0 \le k \le n} 1$

$\Rightarrow 2\sum_{0 \le k \le n} k = (n+1)^2 - (n+1)$ $\qquad = S_n + 2\sum_{0 \le k \le n} k + (n+1)$

$C_n = \sum_{0 \le k \le n} k^3$; $C_n + (n+1)^3 = 0 + \sum_{0 \le k \le n} (k+1)^3 = \sum_{0 \le k \le n} (k^3+3k^2+3k+1)$

$= \sum_{0 \le k \le n} k^3 + 3\sum_{0 \le k \le n} k^2 + 3\sum_{0 \le k \le n} k + \sum_{0 \le k \le n} 1$

$= C_n + 3S_n + 3 \cdot \frac{n(n+1)}{2} + (n+1)$

Method 3: Repertoire Method

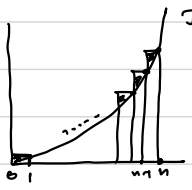
$R_0 = \alpha$

$R_n = R_{n-1} + \beta + \gamma n + \delta n^2$ $\quad R(n) = A(n)\alpha + B(n)\beta + C(n)\gamma + D(n)\delta$

$R_n = 1, n, n^2, n^3$

Method 4: Replace sums by integrals

$S_n = \sum_{0\le K\le n} K^2 = 1^2+2^2+3^2+\cdots = 1\cdot 1 + 1\cdot 4 + 1\cdot 9 + \cdots + 1\cdot n^2$



Area under the curve $= \int_0^n x^2\,dx = \frac{1}{3}n^3$

$E_n = S_n - \frac{1}{3}n^3 = S_{n-1} + n^2 - \frac{1}{3}n^3 = E_{n-1} + \frac{1}{3}(n-1)^3 + n^2 - \frac{1}{3}n^3$

$[S_n = E_n + \frac{1}{3}n^3]$

$= E_{n-1} + \frac{1}{3}n^3 - n^2 + n - \frac{1}{3} + n^2 - \frac{1}{3}n^3$

$= E_{n-1} + (n - \frac{1}{3})$

$S_n - \int_0^n x^2\,dx = \sum_{K=1}^n K^2 - \sum_{K=1}^n \left(\int_{K-1}^K x^2\,dx\right)$

$= \sum_{K=1}^n \left(K^2 - \int_{K-1}^K x^2\,dx\right) = \sum_{K=1}^n \left(K^2 - \frac{K^3-(K-1)^3}{3}\right)$

$= \sum_{K=1}^n (K - \frac{1}{3})$

Method 5: Expand and contract

$[1\le j\le n][j\le K\le n] = [1\le j\le K\le n] = [1\le K\le n][1\le j\le K]$

$S_n = \sum_{1\le K\le n} K^2 = \sum_{1\le K\le n} K\cdot K = \sum_{1\le K\le n} K\cdot \sum_{1\le j\le K} 1$

$= \sum_{1\le K\le n}\ \sum_{1\le j\le K} K = \sum_{1\le j\le K\le n} K = \sum_{1\le j\le n}\ \sum_{j\le K\le n} K$

$= \sum_{1\le j\le n} \left(\sum_{K=1}^n K - \sum_{K=1}^{j-1} K\right)$

$j + (j+1) + (j+2) + \cdots + n$

$= 1+2+\cdots+(j-1) + j + \cdots + n - (1+2+\cdots+(j-1))$

$= \sum_{1\le j\le n} \left(\frac{n(n+1)}{2} - \frac{j(j-1)}{2}\right)$

$= \frac{1}{2}n^2(n+1) - \frac{1}{2}\sum_{1\le j\le n}(j^2 - j) = \frac{1}{2}n^2(n+1) - \frac{1}{2}\sum_{1\le j\le n} j^2 + \frac{1}{2}\sum_{1\le j\le n} j$

$= \frac{1}{2}n^2(n+1) - \frac{1}{2}S_n + \frac{1}{2}\times\frac{1}{2}(n+1)n$

$\Rightarrow \frac{3}{2}S_n = \frac{1}{2}n^2(n+1) + \frac{1}{4}n(n+1) \Rightarrow S_n = n(n+1)(2n+1)/6$

Lect. 9: General methods for Sums Sec. 5

$S_n = \sum_{0\le k\le n} k^2$ 1st Strategy:

n	0	1	2	3	4
S_n	0	1	5	14	30

Method 0: Look it up

Method 1: Guess the answer; prove by induction

$S_n = an^3+bn^2+cn+d$; $0=d$; $a+b+c=1$ $\quad (a,b,c)=(\frac{1}{3},\frac{1}{2},\frac{1}{6})$

$8a+4b+2c=5$

$27a+9b+3c=14$

$S_n = \frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$

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

Method 2: Perturbation

$S_n + (n+1)^2 = \overset{a_0}{0} + \sum_{0\le k\le n} \overset{a_{k+1}}{(k+1)^2} = \sum_{0\le k\le n}(k^2+2k+1) = \sum_{0\le k\le n} k^2 + 2\sum_{0\le k\le n} k + \sum_{0\le k\le n} 1$

$= S_n + 2\sum_{0\le k\le n} k + (n+1)$

$\Rightarrow 2\sum_{0\le k\le n} k = (n+1)^2-(n+1)$

$C_n = \sum_{0\le k\le n} k^3$; $C_n + \overset{a_{n+1}}{(n+1)^3} = \overset{C_0}{0} + \sum_{0\le k\le n} \overset{a_{k+1}}{(k+1)^3} = \sum_{0\le k\le n} k^3 + 3\sum_{0\le k\le n} k^2 + 3\sum_{0\le k\le n} k + \sum_{0\le k\le n} 1$

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

$\Rightarrow S_n = n(n+1)(2n+1)/6$

Method 3: Repertoire

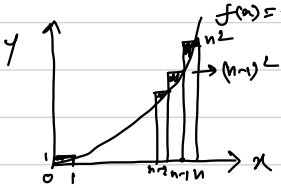
$R_0 = \alpha$

$R_n = R_{n-1} + \overbrace{\beta+\gamma n+\delta n^2}^{a_n}$ $\quad R_n = A(n)\alpha + B(n)\beta + C(n)\gamma + D(n)\delta$

$R_n = 1, n, n^2, n^3$

Method 4: Replace sums by integrals

$S_n = \sum_{1\le K\le n} K^2 = 1^2+2^2+\cdots+n^2 = 1\cdot 1 + 1\cdot 4 + 1\cdot 9 + \cdots + 1\cdot(n-1)^2 + 1\cdot n^2$



Area under curve $= \int_0^n x^2\,dx = \frac{1}{3}n^3$

$E_n = S_n - \frac{1}{3}n^3 = S_{n-1} + n^2 - \frac{1}{3}n^3$

$\hookrightarrow S_n = E_n + \frac{1}{3}n^3$ | $= E_{n-1} + \frac{1}{3}(n-1)^3 + n^2 - \frac{1}{3}n^3$

$= E_{n-1} + \cancel{\frac{1}{3}n^3} - \cancel{n^2} + n - \frac{1}{3} \cancel{+n^2} - \cancel{\frac{1}{3}n^3}$

$= E_{n-1} + (n - \frac{1}{3})$

$\vdots$

$E_n = S_n - \int_0^n x^2\,dx$

$= \sum_{K=1}^n K^2 - \int_0^n x^2\,dx$

$= \sum_{K=1}^n K^2 - \sum_{K=1}^n \left(\int_{K-1}^K x^2\,dx\right) = \sum_{K=1}^n \left(K^2 - \int_{K-1}^K x^2\,dx\right)$

$= \sum_{K=1}^n \left(K^2 - \frac{K^3-(K-1)^3}{3}\right)$

$= \sum_{K=1}^n (K - \frac{1}{3})$

Method 5: Expand and contract

$S_n = \sum_{1\le K\le n} K^2 = \sum_{1\le K\le n} K\cdot K = \sum_{1\le K\le n} K \cdot \sum_{1\le j\le K} 1 = \sum_{1\le K\le n} \sum_{1\le j\le K} K$

$\hookrightarrow [1\le j\le K\le n] = [1\le K\le n][1\le j\le K]$ | $= \sum_{1\le j\le K\le n} K$

$\hookrightarrow [1\le j\le n][j\le K\le n]$

$= \sum_{1\le j\le n} \sum_{j\le K\le n} K$ | $j+(j+1)+\cdots+n$
$=1+2+\cdots+(j-1)+j+\cdots+n$
$-(1+2+\cdots+(j-1))$

$= \sum_{1\le j\le n} \left(\sum_{K=1}^n K - \sum_{K=1}^{j-1} K\right)$ =

$= \sum_{1\le j\le n} \left(\frac{n(n+1)}{2} - \frac{j(j-1)}{2}\right) = \frac{n^2(n+1)}{2} - \frac{1}{2}\sum_{1\le j\le n}(j^2-j)$

$= \frac{n^2(n+1)}{2} - \frac{1}{2}\sum_{1\le j\le n} j^2 + \frac{1}{2}\sum_{1\le j\le n} j = \frac{n^2(n+1)}{2} - \frac{1}{2}S_n + \frac{1}{2}\cdot\frac{n(n+1)}{2}$

$\Rightarrow \frac{3}{2}S_n = \frac{n^2(n+1)}{2} - \frac{n(n+1)}{4} \Rightarrow S_n = \frac{n(n+1)(2n+1)}{6}$

m divides n (or n is divisible by m) [2 divides 6; 6 is divisible by 2]
if $m > 0$ and n/m is an integer.
$m \mid n \iff m > 0$ & $n = mk$ for some integer k.

gcd (greatest common divisor): gcd of m, n is the largest integer that divides both m and n.

$$\gcd(m,n) = \max\{k \mid k \mid m \ \&\ k \mid n\}$$

$m = 0, n > 0 \Rightarrow \gcd(m,n) = \gcd(0,n) = n$

$12/18 = 2/3 \quad \frac{0}{n} = 0$

$7/12 + 1/18 = 21/36 + 2/36 = \frac{23}{36}$

lcm (least common multiple): $\operatorname{lcm}(m,n) = \min\{k \mid k > 0,\ m \mid k \ \&\ n \mid k\}$

Euclid's algorithm: $\gcd(m,n)$, for $0 \le m < n$

$\gcd(0,n) = n$

$\gcd(m,n) = \gcd(n \bmod m, m)$ $[0 \le n \bmod m < m]$

divisor d | dividend a = dq + r ← remainder $[0 \le r < d]$; quotient q

$a = dq + r \rightarrow a \bmod d$

$12 \mid 18 \mid 1$ (12); $6 \mid 12 \mid 2$ (12); 0

$n = m\lfloor n/m \rfloor + n \bmod m$

$\Rightarrow n \bmod m = n - m\lfloor n/m \rfloor$

$m \mid n \mid \lfloor n/m \rfloor = q$

$n \bmod m$

$18 \mid 12 \mid 0$ (12); $12 \mid 18$

Diophantine eq^n: $ax + by = c \quad x \in \mathbb{Z}, y \in \mathbb{Z}$ (coeff, var, coeff, var)

$2x + 3y = 5$

→ has solutions (x,y) iff $\gcd(a,b) \mid c$

$5/2 = 2.5$

$\lfloor x \rfloor$ = integer part of x

$\lfloor n/m \rfloor$

Necessity: solution exists $\Rightarrow \gcd(a,b) \mid c$

L.H.S. $= ax + by = a'kx + b'ky$

$= k(a'x + b'y) \Rightarrow k \mid \text{LHS} \Rightarrow k \mid \text{RHS} \Rightarrow k \mid c$

$\Rightarrow \gcd(a,b) \mid c$

$\gcd(a,b) = k \ [k \mid a, k \mid b]$

$a = a'k, \ b = b'k$

Sufficiency (using book's notation):

Given m, n ; we need to compute m', n' such that

$m'm + n'n = \gcd(m,n)$

var coeff var coeff

$\gcd(0,n) = n$

$\gcd(m,n) = \gcd(\underbrace{n \bmod m}_{r}, m)$

If $m=0$, RHS $= \gcd(0,n) = n$

L.H.S. $= \underbrace{m'}_{0}\underbrace{m}_{0} + \underbrace{n'}_{1}n = n$ If $m=0$, we pick $(m', n') = (0,1)$

$r = n \bmod m$, for r and m, we compute $\bar{r}$ and $\bar{m}$ such that

$\bar{r}r + \bar{m}m = \gcd(r,m)$ [$\gcd(r,m) = \gcd(n \bmod m) = \gcd(m,n)$]

$r = n - m\lfloor n/m \rfloor$

$\bar{r}(n - m\lfloor n/m \rfloor) + \bar{m}m = \gcd(m,n)$

$\Rightarrow \bar{r}n - \bar{r}m\lfloor n/m \rfloor + \bar{m}m = \gcd(m,n)$

$\Rightarrow \underbrace{(\bar{m} - \bar{r}\lfloor n/m \rfloor)}_{m'} m + \underbrace{\bar{r}}_{n'} n = \gcd(m,n)$

$m' = \bar{m} - \lfloor n/m \rfloor \bar{r}$, $n' = \bar{r}$

18 | 30 | 1
18
12 | 18 | 1
12
6 | 12 | 2
12
0

$m=18, n=12$, $m' \times 18 + n' \times 12 = \gcd(12,18) = 6$

$6 = 0 \times 0 + 1 \times 6 = \overset{(1-2\cdot0)}{1} \times 6 + \overset{(0-1\times1)}{0} \times 12 = (-1) \times 12 + 1 \times 18 = 18 - 30$

$\bar{r}$ r $\bar{m}$ m m' m n' n

$ax + by = c$

Linear combination of x & y. [Self-certifying solution]

$k \mid m$ & $k \mid n \iff k \mid \gcd(m,n)$ [self-study]

Lect. 11: Primes Sec. A+B

A positive integer is prime iff it has only two divisors, 1 & p.

2, 3, 5, 7, 11, ---- [otherwise, composite]

Any positive number can be expressed uniquely as a product of primes.

$n = p_1 p_2 \cdots p_m = \prod_{k=1}^{m} p_k$, $p_1 \le p_2 \le \cdots \le p_m$; [$12 = 2\times2\times3$, $18 = 2\times3\times3$]

(maybe empty)

Fundamental th^m of arithmetic.

Proof: Base case. $n = 1$ [empty set of product]

Prove for any $n > 1$ assuming true for all numbers $< n$.

Assume otherwise: $n = p_1 \cdots p_m = q_1 \cdots q_k$, $p_1 \le \cdots \le p_m$, $q_1 \le \cdots \le q_k$

We will prove $p_1 = q_1$. If not, say $p_1 < q_1 \Rightarrow p_1 \neq q_1 \Rightarrow \gcd(p_1, q_1) = 1$

$\exists\, a, b$ s.t. $ap_1 + bq_1 = 1 \Rightarrow ap_1q_2\cdots q_k + bq_1q_2\cdots q_k = q_2\cdots q_k$

$\Rightarrow ap_1q_2\cdots q_k + bn = q_2\cdots q_k \Rightarrow p_1 \mid q_2\cdots q_k$

$p_1 < q_1 \le q_2 \le \cdots \le q_k$, a contradiction.

$p_2 \cdots p_m = q_2 \cdots q_k = n/p_1 < n$

↳ $p_2 \cdots p_m$ is eq. to $q_2 \cdots q_k$

$\Rightarrow p_1 p_2 \cdots p_m$ is eq. to $q_1 q_2 \cdots q_k$ [Proven by induction + contradiction]

$12 = 2^2 \times 3$, $18 = 2 \times 3^2$; $n = \prod_p p^{n_p}$, $n_p \ge 0$ [Prime power factorization]

$12 = 2^2 \times 3^0 \times 5^0 \times 7^0 \times \cdots$

$k = mn \iff k_p = m_p + n_p \ \forall p$ → $6 \mid 12$

$m \mid n \iff m_p \le n_p$

$k = \gcd(m,n) \iff k_p = \min(m_p, n_p)\ \forall p$

$k = \mathrm{lcm}(m,n) \iff k_p = \max(m_p, n_p)\ \forall p$

$\gcd(12,18) = \gcd(2^2\times 3^1, 2\times 3^2) = 2^{\min(2,1)}\times 3^{\min(1,2)} = 2\times 3 = 6$

$\text{lcm}(12,18) = \text{lcm}(2^2\times 3, 2\times 3^2) = 2^{\max(2,1)}\times 3^{\max(1,2)} = 2^2\times 3^2 = 36$

Primes are infinite. Proof by contradiction. (not divisibly by any of $P_1, P_2, \dots, P_K$)

Assume finite: $P_1, P_2, \dots, P_K$. $\mathbb{P} = P_1P_2\cdots P_K + 1$, ↑ contradiction

Euclid number: $e_1 = 1$, $e_n = e_1\cdots e_{n-1} + 1$. $e_5 = 1807 = 13\cdot 139$

$\gcd(e_m, e_n) = 1$; $m \neq n$ [self-study]

↳ $\gcd(1, e_m) = \gcd(0, 1) = 1$

Mersenne numbers: $2^p - 1$ is prime only if p is prime.

Proof by contradiction: $p = mk$. $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$

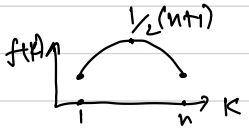
$2^{mk} - 1 = (2^m)^k - (1)^k = (2^m - 1)(2^{m(k-1)} + 2^{m(k-2)} + \cdots + 1) \Rightarrow$ composite

$2^{11} - 1 = 2047 = 23\cdot 89$

Composite number: $n! = 1\cdot 2\cdot 3\cdots n = \prod_{K=1}^{n} K$

$(n!)^2 = (1\cdot 2\cdots n)(n\cdots 2\cdot 1) = \prod_{K=1}^{n} K(n+1-K)$

$f(K) = K(n+1-K)$



$n \leq K(n+1-K) \leq \frac{1}{4}(n+1)^2$

↳ $n^n \leq \prod_{K=1}^{n} K(n+1-K) \leq \frac{1}{4^n}(n+1)^{2n}$

$\Rightarrow n^n \leq (n!)^2 \leq \frac{1}{4^n}(n+1)^{2n} \Rightarrow n^{n/2} \leq n! \leq \frac{1}{2^n}(n+1)^n$

$n! \sim \sqrt{2\pi n}\,(n/e)^n$ [Stirling's approximation]

What is the highest power of (2) p is (10) $n!$ $\quad 5! = 120 = 2^{(3)} \times 15$

	1	2	3	4	5	6	7	8	9	10	power of 2
divisible by 2		X		X		X		X		X	$\lfloor 10/2 \rfloor = 5$
divisible by 4		period 2		X				X			$\lfloor 10/4 \rfloor = 2$
divisible by 8		period 4						X			$\lfloor 10/8 \rfloor = 1$
				period 8							8

$$\in_2(n!) = \lfloor n/2 \rfloor + \lfloor n/4 \rfloor + \cdots = \sum_{K \geq 1} \lfloor n/2^K \rfloor$$

$$\in_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97 \qquad \lfloor n/2^{K+1} \rfloor = \lfloor \lfloor n/2^K \rfloor / 2 \rfloor$$

$100 = (1100100)_2$

$\lfloor 100/2 \rfloor = (110010)_2$

$\lfloor 100/4 \rfloor = (11001)_2$

$$\in_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots = \sum_{K \geq 1} \lfloor n/p^K \rfloor$$

$\lfloor x \rfloor$ = largest integer not exceeding x

↳ $\lfloor x \rfloor \leq x$

$$\in_p(n!) \leq n/p + n/p^2 + n/p^3 + \cdots$$

$$= n/p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = n/p \times \frac{1}{1 - \frac{1}{p}} = \frac{n}{p} \times \frac{p}{p-1} = \frac{n}{p-1}$$

$97 \leq 100$

HW: Calculate the number of trailing zeroes in 100!

Lect. 12: Relative primality and Stern-Brocot tree Sec. A

Two integers m, n are relatively prime (co-prime) when $\gcd(m,n) = 1$ [$m \perp n$]

$12/18 = 2/3$. A fraction m/n is in its lowest term iff $m \perp n$ [irreducible fraction]

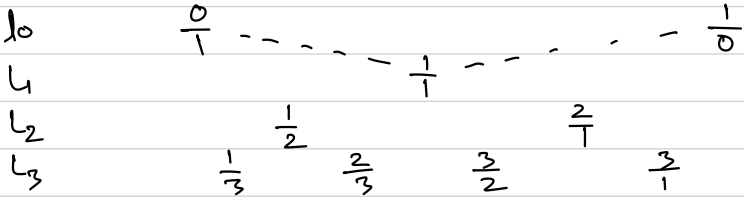
12, 18: $\gcd(12,18) = 6$, $\frac{12}{6} = 2$, $\frac{18}{6} = 3$. $\frac{m}{\gcd(m,n)} \perp \frac{n}{\gcd(m,n)}$

$m = 2^2 \times 3^0 \times 5^0 \times 7^1 = 28$; $n = 2^0 \times 3^1 \times 5^1 \times 7^0 = 15$; $\gcd(m,n) = 1$

$m \perp n \iff \min(m_p, n_p) = 0 \iff m_p n_p = 0$

$k \perp m$ & $k \perp n \iff k \perp mn$; $2 \perp 3$ & $2 \perp 5 \iff 2 \perp 3 \times 5 = 15$

Stern-Brocot Tree: Insert $\frac{m+m'}{n+n'}$ between two adjacent nodes $\frac{m}{n}$ & $\frac{m'}{n'}$



If $\frac{m}{n}$ & $\frac{m'}{n'}$ are consecutive fractions at any stage of the construction of the Stern-Brocot tree, then $m'n - mn' = 1$

Proof: By induction (on the level). Base case: $\frac{m}{n} = \frac{0}{1} \Rightarrow m = 0, n = 1$

$\frac{m'}{n'} = \frac{1}{0} \Rightarrow m' = 1, n' = 0$

$\Rightarrow m'n - mn' = 1 \cdot 1 - 0 \cdot 0 = 1$

Hypothesis: True upto level k. $\rightarrow$ consecutive fraction $\frac{m}{n}$ & $\frac{m'}{n'}$ [$m'n - mn' = 1$]

Induction step: Level $(k+1) \rightarrow \frac{m}{n} \rightarrow \frac{m+m'}{n+n'} \rightarrow \frac{m'}{n'}$

$(m+m')n - m(n+n') = \cancel{mn} + m'n - \cancel{mn} - mn' = m'n - mn' = 1$

$m'(n+n') - (m+m')n' = m'n + \cancel{m'n'} - mn' - \cancel{m'n'} = m'n - mn' = 1$

$\gcd(m+m', n+n') = 1$;

Let $\gcd(m+m', n+n') = d$. So, $d \mid m+m'$, $d \mid n+n'$

$\Rightarrow d \mid (m+m')n$, $d \mid (n+n')m$

$\Rightarrow d \mid (m+m')n - (n+n')m$

$\Rightarrow d \mid \cancel{mn} + m'n - \cancel{mn} - mn'$

$\Rightarrow d \mid m'n - mn' = 1 \Rightarrow d \mid 1 \Rightarrow d = 1$ [Proved]

$m/n < \frac{m+m'}{n+n'} < m'/n'$. Proof: $\frac{m}{n} < \frac{m+m'}{n+n'} \Leftrightarrow \cancel{mn} + mn' < \cancel{mn} + m'n$

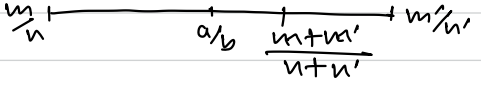
$\Leftrightarrow 0 < m'n - mn' = 1$

↳ The construction preserves order; so no fraction occurs twice.

Claim: All non-negative fractions are present in the tree.

Proof (By contradiction): Assume a/b doesn't exist in this tree.

$m/n = 0/1 < (a/b) < 1/0 = m'/n'$



if $a/b < \frac{m+m'}{n+n'}$; then $m'/n' \leftarrow \frac{m+m'}{n+n'}$

if $a/b > \frac{m+m'}{n+n'}$; then $m/n \leftarrow m+m'/n+n'$

if $a/b = m+m'/n+n'$, we are done.

$\frac{a}{b} - \frac{m}{n} > 0$ & $\frac{m'}{n'} - \frac{a}{b} > 0$

$\Rightarrow an - bm > 0$ & $bm' - an' > 0$

$\Rightarrow an - bm \geq 1$ & $bm' - an' \geq 1$

$\Rightarrow (m'+n')(an - bm) \geq m'+n'$ & $(m+n)(bm' - an') \geq m+n$

$\Rightarrow (m'+n')(an - bm) + (m+n)(bm' - an') \geq m'+n'+m+n$

$\Rightarrow am'n + \cancel{ann'} - \cancel{bmn'} - bmn' + \cancel{bmn'} + bm'n - amn' - \cancel{ann'} \geq m'+n'+m+n$

$\Rightarrow a(m'n - mn') + b(m'n - mn') \geq m'+n'+m+n$

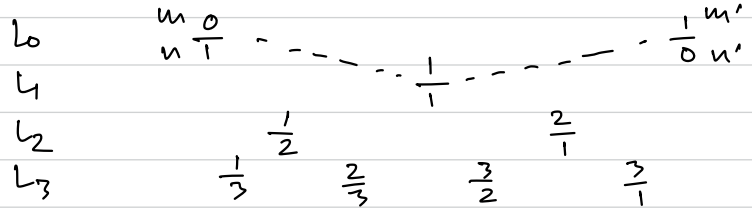
$\Rightarrow \underbrace{a+b}_{\text{fixed}} \geq \underbrace{m'+n'+m+n}_{\text{increase with every itr.}}$ [contradiction]

Two integers m, n are relative prime (co-prime) when $\gcd(m,n) = 1$
$12/18 = 2/3$. A fraction m/n is in lowest terms iff $m \perp n$ [relatively prime]

$12/6 = 2, 18/6 = 3$; $m/\gcd(m,n) \perp n/\gcd(m,n)$

$m = 2^2 \times 3^0 \times 5^0 \times 7^1 = 28$, $n = 2^0 \times 3^1 \times 5^1 \times 7^0 = 15$; $\gcd(m,n) = 1$
$m \perp n \Leftrightarrow \min(m_p, n_p) = 0 \; \forall p$. $m \perp n \Leftrightarrow m_p n_p = 0 \; \forall p$
$k \perp m$ & $k \perp n \Leftrightarrow k \perp mn$. $2 \perp 3$ & $2 \perp 5 \Leftrightarrow 2 \perp 15$

Stern-Brocot tree: Insert $\frac{m+m'}{n+n'}$ between two adjacent fractions $\frac{m}{n}$ & $\frac{m'}{n'}$



If m/n & m'/n' are two consecutive fractions at any stage of the construction of the Stern-Brocot tree, then $m'n - mn' = 1$ [Invariant]

Proof: By induction on the level k.
Base case, L_0: $m'n - mn' = 1 \cdot 1 - 0 \cdot 0 = 1$
Hypo.: True up to L_k. $\Rightarrow m/n$ & m'/n' at $L_k \Rightarrow m'n - mn' = 1$
At $L_{k+1} \Rightarrow m/n \leftrightarrow \frac{m+m'}{n+n'} \leftrightarrow m'/n'$

Now, $(m+m')n - m(n+n') = \cancel{mn} + m'n - \cancel{mn} - mn' = m'n - mn' = 1$
Again, $m'(n+n') - (m+m')n' = m'n + \cancel{m'n'} - mn' - \cancel{m'n'} = m'n - mn' = 1$

$\gcd(m+m', n+n') = 1$;

Proof: Let $\gcd(m+m', n+n') = d$. So, $d \mid m+m'$, $d \mid n+n'$

$\Rightarrow d \mid n(m+m')$, $d \mid m(n+n')$

$\Rightarrow d \mid n(m+m') - m(n+n')$

$\Rightarrow d \mid mn + m'n - mn - mn'$

$\Rightarrow d \mid m'n - mn' = 1 \Rightarrow d \mid 1 \Rightarrow d = 1$

$m/n < \frac{m+m'}{n+n'} < m'/n'$. Proof: $m/n < \frac{m+m'}{n+n'} \Leftrightarrow m(n+n') < n(m+m')$

$\Leftrightarrow mn + mn' < mn + m'n$

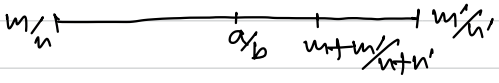
$\Leftrightarrow 0 < m'n - mn' = 1 \Leftrightarrow 0 < 1$

↳ The construction preserves order, so no fraction occurs twice.

Claim: All non-negative fractions are present in the tree.

Proof (By contradiction): Assume a/b is absent from the tree.

$$m/n = 0/1 < a/b < 1/0 = m'/n'$$



if $a/b = \frac{m+m'}{n+n'}$, we are done.

if $a/b < \frac{m+m'}{n+n'}$, $m'/n' \leftarrow \frac{m+m'}{n+n'}$

if $a/b > \frac{m+m'}{n+n'}$, $m/n \rightarrow \frac{m+m'}{n+n'}$

$a/b - m/n > 0$ & $m'/n' - a/b > 0$

$\Rightarrow an - bm > 0$ & $bm' - an' > 0$

$\Rightarrow an - bm \geq 1$ & $bm' - an' \geq 1$

$\Rightarrow (m'+n')(an - bm) \geq m'+n'$ & $(m+n)(bm' - an') \geq m+n$

$\Rightarrow (m'+n')(an - bm) + (m+n)(bm' - an') \geq m'+n'+m+n$

$\Rightarrow am'n + an'n - bmn' - bm'n + bmn' + bm'n - amn' - an'n \geq m'+n'+m+n$

$\Rightarrow a(m'n - mn') + b(m'n - mn') \geq m'+n'+m+n$

$\Rightarrow a+b \geq m'+n'+m+n$ [contradiction]

$a+b$: fixed; $m'+n'+m+n$: increase with every itr.

$a = mq + r;\ 0 \le r < m \Rightarrow a = m\lfloor a/m \rfloor + a \bmod m$ (%)

Def^n: $a \equiv b \pmod m \Leftrightarrow a \bmod m = b \bmod m$

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

1st part: $a = \lfloor a/m \rfloor m + a \bmod m$ (L → R)

$b = \lfloor b/m \rfloor m + b \bmod m$

$a - b = (\lfloor a/m \rfloor - \lfloor b/m \rfloor)m + a \bmod m - b \bmod m \Rightarrow m \mid a-b$

2nd part: $m \mid a-b;\ a = \lfloor a/m \rfloor m + r_1$ & $b = \lfloor b/m \rfloor m + r_2$ (R → L)

$\Rightarrow a - b = (\lfloor a/m \rfloor - \lfloor b/m \rfloor)m + r_1 - r_2\ [0 \le r_1 < m,\ 0 \le r_2 < m]$

$\Rightarrow m \mid r_1 - r_2;\ \max(r_1 - r_2) = m-1;\ \min(r_1 - r_2) = -(m-1)$

Multiples of m: $\ldots -3m, -2m, -m, 0, m, 2m, 3m, \ldots$

$r_1 - r_2 = 0 \Rightarrow r_1 = r_2 \Rightarrow a \bmod m = b \bmod m \Rightarrow a \equiv b \pmod m$

- $a \equiv a \pmod m$ [Reflexive law] LHS = RHS $\Rightarrow$ LHS $\equiv$ RHS (mod m)
- $a \equiv b \Rightarrow b \equiv a \pmod m$ [Symmetric law]
- $a \equiv b$ & $b \equiv c \Rightarrow a \equiv c \pmod m$ [Transitive Law]

\# $a \equiv b$ & $c \equiv d \Rightarrow a + c \equiv b + d \pmod m$

$a - b = mk,\ c - d = ml \Rightarrow a - b + c - d = m(k+l) \Rightarrow (a+c) - (b+d) = m(k+l)$

$\Rightarrow m \mid (a+c) - (b+d) \Rightarrow a + c \equiv b + d \pmod m$

\# $a \equiv b$ & $c \equiv d \Rightarrow a - c \equiv b - d \pmod m$

\# $a \equiv b$ & $c \equiv d \Rightarrow ac \equiv bd \pmod m$

$a - b = mk,\ c - d = ml$. Now, $ac \equiv bd \pmod m \Leftrightarrow m \mid ac - bd$

$\Leftrightarrow m \mid c(a-b) + b(c-d) \Leftrightarrow m \mid cmk + bml$, which is true

[$ac - bc + bc - bd$]

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

$10 \equiv 6 \pmod 4 \qquad 14 \equiv 8 \pmod 3$

$\Rightarrow 5 \cdot 2 \equiv 3 \cdot 2 \pmod 4 \Rightarrow 7 \cdot 2 \equiv 4 \cdot 2 \pmod 3$

$\Rightarrow 5 \equiv 3 \pmod 4$ ✗ $\Rightarrow 7 \equiv 4 \pmod 3$ ✓

$\Rightarrow \frac{5 \cdot 2 - 3 \cdot 2}{4} = 2\left(\frac{5-3}{4}\right) \qquad \frac{7 \cdot 2 - 4 \cdot 2}{3} = 2\left(\frac{7-4}{3}\right)$

$\Rightarrow 2 \equiv -1 \pmod 3$

$\Rightarrow 2^n \equiv (-1)^n \pmod 3$

if n even $3 \mid 2^n - 1$

n odd, $3 \mid 2^n + 1$

$\Rightarrow 3 \mid 2^n + 1 - 3 = 2^n - 2$

#$ad \equiv bd \pmod m \Leftrightarrow a \equiv b \pmod m$, $d \perp m$

$\exists\, d', m'$ s.t. $dd' + mm' = \gcd(d, m) = 1$

$\Rightarrow dd' + mm' \equiv 1 \pmod m \Rightarrow dd' \equiv 1 \pmod m$

Now, $ad \equiv bd \pmod m \Rightarrow add' \equiv bdd' \pmod m \Rightarrow a \equiv b \pmod m$

$d' \to 1/d$, multiplicative inverse of d modulo m.

#$ad \equiv bd \pmod{md} \Leftrightarrow a \equiv b \pmod m$ $[d \neq 0]$

$md \mid ad - bd \Rightarrow ad - bd = mdk \Rightarrow d(a-b) = mdk \Rightarrow a - b = mk$

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

#$ad \equiv bd \pmod m \Leftrightarrow a \equiv b \left(\mod \frac{m}{\gcd(d,m)}\right)$ $\left[\frac{ad-bd}{m} = \frac{d(a-b)}{m}\right]$

$\exists\, d', m'$, s.t. $dd' + mm' = \gcd(d, m)$

$\Rightarrow dd' \equiv \gcd(d, m) \pmod m$

Now, $ad \equiv bd \pmod m \Rightarrow add' \equiv bdd' \pmod m$

$\Rightarrow a\cancel{\gcd(d,m)} \equiv b\cancel{\gcd(d,m)} \left(\mod \frac{m}{\gcd(d,m)} * \cancel{\gcd(d,m)}\right)$

$\Rightarrow a \equiv b \left(\mod \frac{m}{\gcd(d,m)}\right)$

#$a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod m$

#$a \equiv b \pmod m$ & $a \equiv b \pmod n \Leftrightarrow a \equiv b \pmod{\text{lcm}(m,n)}$

$d \mid m$, $d \mid n \Rightarrow d \mid \gcd(m,n)$

$m \mid d$, $n \mid d \Rightarrow \text{lcm}(m,n) \mid d$ $[mn = \gcd(m,n) * \text{lcm}(m,n)]$

if $m \perp n$, $a \equiv b \pmod m$ & $a \equiv b \pmod n \Leftrightarrow a \equiv b \pmod{mn}$

Chinese Remainder Theorem (Ex. 30)

Lect. 13: Congruence (Modular Arithmetic) Sec. A

$a = mq + r, 0 \le r < m \Rightarrow a = m\lfloor a/m \rfloor + a \bmod m$

Def^n: $a \equiv b \pmod m \iff a \bmod m = b \bmod m$

$a \equiv b \pmod m \iff m \mid (a-b)$

1st part: $a = \lfloor a/m \rfloor m + a \bmod m$, $b = \lfloor b/m \rfloor m + b \bmod m$

$\Rightarrow a - b = (\lfloor a/m \rfloor - \lfloor b/m \rfloor)m + a \bmod m - b \bmod m \Rightarrow m \mid (a-b)$

2nd part: $m \mid (a-b)$

$a = \lfloor a/m \rfloor m + r_1$, $b = \lfloor b/m \rfloor m + r_2$; $0 \le r_1, r_2 < m$

$a - b = (\lfloor a/m \rfloor - \lfloor b/m \rfloor)m + r_1 - r_2 \Rightarrow m \mid (r_1 - r_2)$

$\max(r_1 - r_2) = m - 1$, $\min(r_1 - r_2) = -(m-1)$

Multiples of m: $\ldots -3m, -2m, -m, 0, m, 2m, 3m, \ldots$

$r_1 - r_2 = 0 \Rightarrow r_1 = r_2 \Rightarrow a \bmod m = b \bmod \Rightarrow a \equiv b \pmod m$

- $a \equiv a \pmod m$ [reflexive law] LHS = RHS $\Rightarrow$ LHS $\equiv$ RHS (mod m)
- $a \equiv b \iff b \equiv a \pmod m$ [symmetric law]
- $a \equiv b$ & $b \equiv c \Rightarrow a \equiv c \pmod m$ [transitive law]

$a \equiv b$ & $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$

$m \mid (a-b)$, $m \mid c-d \Rightarrow m \mid (a-b) + (c-d) \Rightarrow m \mid (a+c) - (b+d)$

$\Rightarrow (a+c) \equiv (b+d) \pmod m$

$a \equiv b$ & $c \equiv d \pmod m \Rightarrow a - c \equiv b - d \pmod m$

$a \equiv b$ & $c \equiv d \Rightarrow ac \equiv bd \pmod m$ [$ac - bd = ac - bc + bc - bd$]

$m \mid a-b$, $m \mid c-d$; $m \mid ac - bd \iff m \mid c(a-b) + b(c-d)$

$\iff m \mid cmk + bml$, which is true

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

$3 \mid 2^n - 2$

$10 \equiv 6 \pmod 4$ $\quad 14 \equiv 8 \pmod 3$

$\Rightarrow 5 \cdot 2 \equiv 3 \cdot 2 \pmod 4$ $\quad \Rightarrow 7 \cdot 2 \equiv 4 \cdot 2 \pmod 3$

$\Rightarrow 5 \equiv 3 \pmod 4$ ✗ $\quad \Rightarrow 7 \equiv 4 \pmod 3$ ✓

$\frac{10-6}{4} = \frac{2(5-3)}{4}$ $\quad \frac{14-8}{3} = \frac{2(7-4)}{3}$

$2 \equiv -1 \pmod 3$

$\Rightarrow 2^n \equiv (-1)^n \pmod 3$

n even $3 \mid 2^n - 1$

n odd $3 \mid 2^n + 1 \Rightarrow 3 \mid 2^n + 1 - 3$

$\Rightarrow 3 \mid 2^n - 2$

$ad \equiv bd \Leftrightarrow a \equiv b \pmod m$ when $d \perp m$

$\gcd(d, m) = 1$; $\exists\, d', m'$, s.t. $dd' + mm' = 1$

$\Rightarrow dd' \equiv 1 \pmod m$

Now, $ad \equiv bd \Rightarrow add' \equiv bdd' \Rightarrow a \equiv b \pmod m$

d' → multiplicative inverse of d modulo m

Cyclic group of order m. $(\mathbb{Z}/m\mathbb{Z})^\times$

$ad \equiv bd \pmod{md} \Leftrightarrow a \equiv b \pmod m$; $d \neq 0$

$ad \equiv bd \pmod m \Leftrightarrow a \equiv b \pmod{m/\gcd(d,m)}$

$\exists\, d', m'$, s.t. $dd' + mm' = \gcd(d, m)$

$\Rightarrow dd' \equiv \gcd(d,m) \pmod m$

$ad \equiv bd \pmod m \Leftrightarrow add' \equiv bdd' \pmod m$

$\Leftrightarrow a \gcd(d,m) \equiv b \gcd(d,m) \pmod{m/\gcd(d,m) * \gcd(d,m)}$

$\Leftrightarrow a \equiv b \pmod{m/\gcd(d,m)}$

$a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod m$

$a \equiv b \pmod m$ & $a \equiv b \pmod n$

$\Leftrightarrow a \equiv b \pmod{\text{lcm}(m,n)}$

$40 \equiv 4 \pmod{12}$

$40 \equiv 4 \pmod{18}$

$40 \equiv 4 \pmod{216}$ ✗

$40 \equiv 4 \pmod{36}$ ✓

$d \mid m$ & $d \mid n \Rightarrow d \mid \gcd(m,n)$

$m \mid d$ & $n \mid d \Rightarrow \text{lcm}(m,n) \mid d$

$mn = \gcd(m,n) * \text{lcm}(m,n)$

$m \perp n$; $a \equiv b \pmod m$ & $a \equiv b \pmod n \Leftrightarrow a \equiv b \pmod{mn}$

↳ Ex.30 (Chinese Remainder Theorem)

$a \equiv b \pmod m \Leftrightarrow a \equiv b \pmod{p^{m_p}}\ \forall p$

Chinese Remainder Th^m: Let $m_1, \ldots, m_r$ be integers greater than 1 with $m_j \perp m_k$ for $1 \le j < k \le r$.

Let $M = m_1 \cdots m_r$.

If $a_1, \ldots, a_r$ are any integers then

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo M.

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \\ x &\equiv ? \pmod{105} \\ &\hookrightarrow 23 \end{aligned}$$

Uniqueness: Let x, y be two solutions to the system s.t. $x \not\equiv y \pmod M$.

$$\begin{aligned} x \equiv a_1 \pmod{m_1} \ \&\ y \equiv a_1 \pmod{m_1} &\Rightarrow x \equiv y \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \ \&\ y \equiv a_2 \pmod{m_2} &\Rightarrow x \equiv y \pmod{m_2} \\ \vdots \qquad\qquad\quad \vdots &\quad\ \vdots \\ x \equiv a_r \pmod{m_r} \ \&\ y \equiv a_r \pmod{m_r} &\Rightarrow x \equiv y \pmod{m_r} \end{aligned}$$

$\Rightarrow x \equiv y \pmod M$, a contradiction.

Existence (implicit construction):

Proof by induction r. Base case: $r = 2$.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

$m_1 \perp m_2$. $\exists\, m_1', m_2'$, s.t. $m_1 m_1' + m_2 m_2' = 1$

We claim $x = a_1 m_2 m_2' + a_2 m_1 m_1'$

Indeed, $x = a_1(1 - m_1 m_1') + a_2 m_1 m_1' = a_1 + (a_2 - a_1) m_1 m_1'$

$x \equiv a_1 \pmod{m_1}$

Analogously, $x \equiv a_2 \pmod{m_2}$

Hypo.: True upto $(r-1)$. Let $\hat{M} = m_1 \cdots m_{r-1}$. By induction hypo. $\exists\, x \equiv \hat{A} \pmod{\hat{M}}$

Induction step: $\gcd(\hat{M}, m_r) = 1$. Using the same argument of the base case, we can show that $\exists\, \hat{M}', m_r'$ s.t. $\hat{M}\hat{M}' + m_r m_r' = 1$

and $x = \hat{A} m_r m_r' + a_r \hat{M}\hat{M}'$ is a solution. [Proved]

$x \bmod 15$	$x \bmod 3$	$x \bmod 5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

$7 * 13 \pmod{15}$

$7 * 13 \equiv 1 \cdot 1 \pmod 3$

$7 * 13 \equiv 2 \cdot 3 \equiv 1 \pmod 5$

Self-study: $x^2 \equiv 1 \pmod m$

$Res(x) = (x \bmod m_1, x \bmod m_2, \dots x \bmod m_r),\ m_j \perp m_k$

$\gcd(8,12) = 4$

$0\times 8 \bmod 12,\ 1\times 8 \bmod 12,\ 2\times 8 \bmod 12,\ \dots\dots,\ 11 * 8 \bmod 12$

$0 \qquad 8 \qquad 4 \qquad 0,8,4, \quad 0,8,4, \quad 0,8,4$

$0\times n \bmod m,\ 1\times n \bmod m,\ 2\times n \bmod m,\ \dots\dots,\ (m-1)n \bmod m$ [# m numbers]

Let $\gcd(m,n) = d$

There are $\underbrace{(0, d, 2d, 3d, \dots\dots, m-d)}_{m/d \qquad (m/d-1)\,d}$ in d copies $[m/(m/d) = d]$

$Kn \equiv sd \pmod m$ Let $m = m'd,\ n = n'd$ where $\gcd(m', n') = 1$

$\Leftrightarrow Kn'd \equiv sd \pmod{m'd}$

$\Leftrightarrow Kn' \equiv s \pmod{m'}$ $\qquad [l = -t]$

$\Leftrightarrow m' \mid Kn' - s \Leftrightarrow Kn' - s = tm' \Leftrightarrow Kn' - tm' = s \Leftrightarrow Kn' + lm' = s$

$\gcd(m', n') = 1;\ \exists\ K', l'$ s.t. $K'n' + l'm' = 1 \Rightarrow \underbrace{K's}_{K}\, n' + \underbrace{l's}_{l}\, m' = s$

$jn \equiv (j + m/d)n \pmod m$

$\Leftrightarrow jn \equiv jn + m/d * n \pmod m$

$\Leftrightarrow n/d * m \equiv 0 \pmod m$, which is true.

What if period $< m/d$?

Let $\exists\ 0 \le j, k < m/d$ s.t. $jn = Kn$. Now,

$jn \equiv Kn \pmod m$

$\Leftrightarrow jn'd \equiv Kn'd \pmod{m'd}$

$\Leftrightarrow jn' \equiv Kn' \pmod{m'}$

$\Leftrightarrow j \equiv K \pmod{m/d} \Leftrightarrow j = K$, a contradiction.

Chinese Remainder Th^m: Let $m_1, \dots, m_r$ be integers greater than 1 with $m_j \perp m_k$ for $1 \le j < k \le r$.
Let $M = m_1 \cdots m_r$. If $a_1, \dots, a_r$ are any integers, then

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo M.

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \\ x &\equiv ? \pmod{105} \end{aligned}$$

↳ 23

Uniqueness: $\exists x, y$ s.t. $x \not\equiv y \pmod M$ but both satisfy the systems

$$\begin{aligned} x \equiv a_1 \pmod{m_1} \ \&\ y \equiv a_1 \pmod{m_1} &\Rightarrow x \equiv y \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \ \&\ y \equiv a_2 \pmod{m_2} &\Rightarrow x \equiv y \pmod{m_2} \\ \vdots \qquad\qquad \vdots \qquad\qquad &\vdots \\ x \equiv a_r \pmod{m_r} \ \&\ y \equiv a_r \pmod{m_r} &\Rightarrow x \equiv y \pmod{m_r} \end{aligned}$$

$\Big\}$ $x \equiv y \pmod M$, a contradiction

Existence (implicit construction):
Proof by induction on r. Base case: $r = 2$

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

$m_1 \perp m_2$. $\exists\, m_1', m_2'$ s.t. $m_1 m_1' + m_2 m_2' = 1$
We claim, $x = a_1 m_2 m_2' + a_2 m_1 m_1'$ is a solution
Indeed, $x = a_1(1 - m_1 m_1') + a_2 m_1 m_1' = a_1 + (a_2 - a_1) m_1 m_1' \Rightarrow x \equiv a_1 \pmod{m_1}$
Analogously, $x = a_1 m_2 m_2' + a_2(1 - m_2 m_2') = (a_1 - a_2) m_2 m_2' + a_2 \Rightarrow x \equiv a_2 \pmod{m_2}$
Hypothesis: True upto $(r-1)$. Let $\hat{M} = m_1 \cdots m_{r-1}$. By induction hypothesis,
$\exists\, \hat{A}$ s.t. $x \equiv \hat{A} \pmod{\hat{M}}$
Induction step: $\gcd(\hat{M}, m_r) = 1$. Using the same argument as the base case,
we can show that, $\exists\, \hat{M}', m_r'$ s.t. $\hat{M}\hat{M}' + m_r m_r' = 1$
and $x = \hat{A} m_r m_r' + a_r \hat{M}\hat{M}'$ is a solution. [Proved]

$Res(x) = (x \bmod m_1, x \bmod m_2, \cdots, x \bmod m_r)$; $m_j \perp m_k$; $1 \le j < k \le r$.

$x \bmod 15$	$x \bmod 3$	$x \bmod 5$
0	0	0
1	$\equiv 1$	$\equiv 1$
2	2	2
3	0	3
4	$\equiv 1$	4
5	2	0
6	0	$\equiv 1$
7	$\equiv 1$	2
8	2	3
9	0	4
10	$\equiv 1$	0
11	2	$\equiv 1$
12	0	2
13	$\equiv 1$	3
14	2	4

$7 * 13 \bmod 15$

$7 * 13 \equiv 1 \cdot 1 \pmod 3$

$7 * 13 \equiv 2 \cdot 3 \equiv 6 \equiv 1 \pmod 5$

Self-study: $x^2 \equiv 1 \pmod m$

$0\times 8 \bmod 12,\ 1\times 8 \bmod 12,\ 2\times 8 \bmod 12,\ \ldots\ldots,\ 11*8 \bmod 12$ $\quad \gcd(12,8)=4$

$0 \qquad 8 \qquad 4 \qquad 0,8,4,\ 0,8,4,\ 0,8,4$

$0\times n \bmod m,\ 1\times n \bmod m,\ 2\times n \bmod m,\ \ldots\ldots,\ (m-1)\times n \bmod m \quad [\gcd(m,n)=d]$

$\underbrace{0, d, 2d, 3d, \ldots\ldots, m-d}_{m/d \text{ numbers}}$ $\quad (m/d-i)d$ $\quad$ # copies: $m/(m/d)=d$ (total numbers)

$\#\ kn \equiv sd \pmod m \quad [m=m'd,\ n=n'd,\ \gcd(m',n')=1]$

$\Leftrightarrow kn'd \equiv sd \pmod{m'd}$

$\Leftrightarrow kn' \equiv s \pmod{m'}$

$\Leftrightarrow m' \mid kn'-s \Leftrightarrow kn'-s=tm' \Leftrightarrow kn'-tm'=s \Leftrightarrow kn'+lm'=s \quad [l=-t]$

$\exists\ k', l',\ s.t.\ k'n'+l'm'=1 \Rightarrow \underbrace{k's}_{k}n'+\underbrace{l's}_{l}m'=s$

$\#\ jn \equiv (j+m/d)n \pmod m$

$\Leftrightarrow jn \equiv jn + m/d * n \pmod m$

$\Leftrightarrow m/d * m \equiv 0 \pmod m$, which is true

What if period $< m/d$?

Let $\exists\ 0 \le j,k < m/d$ & $jn = kn$. Now,

$jn \equiv kn \pmod m$

$\Leftrightarrow jn'd \equiv kn'd \pmod{m'd}$

$\Leftrightarrow jn' \equiv kn' \pmod{m'}$

$\Leftrightarrow j \equiv k \pmod{m/d} \Leftrightarrow j=k$, a contradiction.

Lect.15: Fermat's th^m, Wilson's th^m, Euler's th^m Sec. B

$x^2 \equiv 1 \pmod m \Rightarrow x^2 \equiv 1 \pmod p$; $p > 2$

$p \mid x^2 - 1 \Rightarrow p \mid (x+1)(x-1)$. If $p \mid x+1$ & $p \mid x-1$, $p \mid (x+1)-(x-1) \Rightarrow p \mid 2 \Rightarrow p = 2$ ✗

$p \mid x+1$ or $p \mid x-1$

$\Rightarrow x \equiv -1 \pmod p$ or $x \equiv +1 \pmod p \Rightarrow x \equiv \pm 1 \pmod p$

The m numbers $0 \bmod m, n \bmod m, 2n \bmod m, \ldots, (m-1)n \bmod m$ consist of precisely d copies of the m/d numbers $0, d, 2d, \ldots, m-d$ in some order. where $d = \gcd(m, n)$

If $m \perp n$, then there is exactly 1 copy of the m numbers $0, d, 2d, \ldots, (m-1)d \equiv 0, 1, 2, \ldots, m-1$. (complete residue class)

If m is a prime p, then

$n \cdot 2n \cdot 3n \cdot \ldots \cdot (p-1)n \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod p$

$\Rightarrow n^{p-1} (p-1)! \equiv (p-1)! \pmod p$

$\Rightarrow n^{p-1} \equiv 1 \pmod p$, $n \perp p$ [Fermat's little th^m]

Wilson's th^m: $(n-1)! \equiv -1 \pmod n \Leftrightarrow n$ is prime; if $n > 1$.

Proof: Sufficiency: If $n > 1$ is not a prime, it has a prime divisor $p < n$

$p \mid (n-1)!$, a contradiction. Because if $(n-1)! \equiv -1 \pmod n$

$\Rightarrow (n-1)! \equiv -1 \pmod p$, but $p \mid (n-1)! \Rightarrow (n-1)! \equiv 0 \pmod p$.

Necessity: $(p-1)! \equiv -1 \pmod p$ for any prime p.

Case 1: $p = 2$. LHS $= (2-1)! = 1! = 1 \equiv -1 \pmod 2$, which is true.

Case 2: $p > 2$. $\forall\, n < p$, and $n \perp p \Rightarrow \exists\, n'$; s.t. $n'n \equiv 1 \pmod p$

$1 \cdot \underbrace{2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2)}_{1 \cdot 1 \cdot \ldots \cdot 1} (p-1) \equiv 1 \cdot (-1) \equiv -1 \pmod p$

$p = 5$

$1' = 1, 2' = 3, 3' = 2, 4' = 4$

$n' \equiv n \Rightarrow n^2 \equiv 1 \pmod p$

$\Rightarrow n \equiv \pm 1 \pmod p$

$\Rightarrow n \equiv \{1, p-1\}$

Euler's th^m:

How many integers $< m$ i.e.; $\{0, 1, 2, \cdots, m-1\}$ are relatively prime to m?

$\varphi(m) \Rightarrow$ Euler's totient function.

$\varphi(1) = 1$, $\varphi(p) = p-1$

Euler's th^m: $n^{\varphi(m)} \equiv 1 \pmod m$, $n \perp m$.

If $m = p^k$; $n \perp m \Rightarrow n \perp p^k \Rightarrow n \perp p. \Rightarrow p \nmid n$

The multiples of p in $\underbrace{\{0, 1, \cdots, p^k - 1\}}_{p^k}$ are $\underbrace{\{0, p, 2p, \cdots, (p^{k-1}-1)p\}}_{p^{k-1}}$

$\varphi(p^k) = p^k - p^{k-1}$

$m > 1$ and not a prime power, $m = m_1 m_2$, $m_1 > 1$, $m_2 > 1$, $m_1 \perp m_2$

$\underbrace{n \perp m}_{\varphi(m)} \Leftrightarrow n \perp m_1 \;\&\; n \perp m_2 \Leftrightarrow \gcd(n, m_1) = 1 \;\&\; \gcd(n, m_2) = 1$

$\Leftrightarrow \gcd(n \bmod m_1, m_1) = 1 \;\&\; \gcd(n \bmod m_2, m_2) = 1$

$\Leftrightarrow \underbrace{n \bmod m_1 \perp m_1}_{\varphi(m_1)} \;\&\; \underbrace{n \bmod m_2 \perp m_2}_{\varphi(m_2)}$

$\varphi(m) = \varphi(m_1)\varphi(m_2)$, $m_1 \perp m_2$ [Multiplicative function]

$$\varphi(m) = \varphi\Big(\prod_{p \mid m} p^{m_p}\Big) = \prod_{p \mid m} \varphi(p^{m_p}) = \prod_{p \mid m} p^{m_p} - p^{m_p - 1} = \prod_{p \mid m} p^{m_p}(1 - 1/p)$$

$$= p_1^{m_1}(1 - 1/p_1)\, p_2^{m_2}(1 - 1/p_2) \cdots p_k^{m_k}(1 - 1/p_k)$$

$$= m \prod_{p \mid m} (1 - 1/p)$$

The m numbers $0 \bmod m, n \bmod m, 2n \bmod m, \ldots, (m-1)n \bmod m$ consist of precisely d copies of the m/d numbers $0, d, 2d, \ldots, m-d$ in some order, where $d = \gcd(m,n)$.

If $m \perp n$, there is exactly 1 copy of the m numbers $0, d, 2d, \ldots m-d \equiv 0, 1, 2, \ldots, m-1$ (complete residue class)

If m is a prime p, then

$$n \cdot 2n \cdot 3n \cdot \cdots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod p$$

$$\Rightarrow n^{p-1} (p-1)! \equiv (p-1)! \pmod p \Rightarrow n^{p-1} \equiv 1 \pmod p$$ [Fermat's little th^m]

$x^2 \equiv 1 \pmod p, p > 2. \Rightarrow p \mid x^2 - 1 \Rightarrow p \mid (x+1)(x-1)$

If $p \mid x+1$ & $p \mid x-1 \Rightarrow p \mid (x+1) - (x-1) \Rightarrow p \mid 2 \Rightarrow p = 2$, a contradiction.

So, $p \mid x+1$ or, $p \mid x-1 \Rightarrow x \equiv -1 \pmod p$ or, $x \equiv +1 \pmod p \Rightarrow x \equiv \pm 1 \pmod p$.

$\Rightarrow x \equiv 1, p-1 \pmod p$

Wilson's th^m: $(n-1)! \equiv -1 \pmod n \Leftrightarrow n$ is prime, if $n > 1$

Proof: Sufficiency: Given $(n-1)! \equiv -1 \pmod n$, we need to prove n is prime.

Assume $n > 1$ is not a prime. If has a prime divisor $p < n$.

$p \mid (n-1)!$, this is in violation of our assumption. Because;

$(n-1)! \equiv -1 \pmod n \Rightarrow (n-1)! \equiv -1 \pmod p$. But $p \mid (n-1)! \Rightarrow (n-1)! \equiv 0 \pmod p$.

Necessity: $(p-1)! \equiv -1 \pmod p$, p is prime.

Case 1 ($p = 2$): If $p = 2$, $(2-1)! = 1 \equiv -1 \pmod 2$

Case 2 ($p > 2$): $\forall n < p$, $n \perp p$. And $n \perp p$ implies $\exists n'$, s.t. $n'n \equiv 1 \pmod p$

$1, 2, 3, \ldots, (p-2), (p-1) \pmod p$

$\equiv 1 \quad \underbrace{1 \cdot 1 \cdot 1 \cdots 1}_{} \quad (-1) \pmod p$

$\equiv -1 \pmod p$

$p = 5$

$1' = 1, \ 2' = 3, \ 3' = 2, \ 4' = 4$

$n' \equiv n \Rightarrow n^2 \equiv 1 \pmod p$

$\Rightarrow n \equiv \pm 1 \pmod p$

$\equiv 1, (p-1) \pmod p$

Euler's th^m:

How many integers $\{0,1,\ldots,m-1\}$ are relatively prime to m?

$\varphi(m) \to$ Euler's totient function.

$\varphi(1)=1$, $\varphi(p)=p-1$. Euler's th^m: $n^{\varphi(m)} \equiv 1 \pmod m$, if $n \perp m$.

If $m=p^k$, $n \perp m \Rightarrow n \perp p^k \Rightarrow n \perp p \Rightarrow p \times n$

The multiples of p in $\underbrace{\{0,1,2,\ldots,p^k-1\}}_{p^k}$ are $\underbrace{\{0, p, 2p, \ldots, p^k-p\}}_{0\cdot p,\ 1\cdot p,\ 2\cdot p,\ \ldots,\ (p^{k-1}-1)p}$ p^{k-1}

$\varphi(p^k) = p^k - p^{k-1}$

$m>1$ is not a prime. Then, $m = m_1 m_2$; $m_1>1$, $m_2>1$ & $m_1 \perp m_2$

$\underbrace{n \perp m}_{\varphi(m)} \Leftrightarrow n \perp m_1$ & $n \perp m_2 \Leftrightarrow \gcd(n, m_1)=1$ & $\gcd(n, m_2)=1$

$\Leftrightarrow \gcd(n \bmod m_1, m_1)=1$ & $\gcd(n \bmod m_2, m_2)=1$

$\Leftrightarrow \underbrace{n \bmod m_1 \perp m_1}_{\varphi(m_1)}$ & $\underbrace{n \bmod m_2 \perp m_2}_{\varphi(m_2)}$

$\varphi(m) = \varphi(m_1)\varphi(m_2)$, $m_1 \perp m_2$ [Multiplicative function]

$m = p_1^{m_1} p_2^{m_2} \cdots p_K^{m_K}$

$$\varphi(m) = \varphi\Big(\prod_{p \mid m} p^{m_p}\Big) = \prod_{p \mid m} \varphi(p^{m_p}) = \prod_{p \mid m} (p^{m_p} - p^{m_p-1}) = \prod_{p \mid m} p^{m_p}\left(1-\tfrac{1}{p}\right)$$

$$= p_1^{m_1}\left(1-\tfrac{1}{p_1}\right) p_2^{m_2}\left(1-\tfrac{1}{p_2}\right) \cdots p_K^{m_K}\left(1-\tfrac{1}{p_K}\right)$$

$$= m \prod_{p \mid m} \left(1-\tfrac{1}{p}\right)$$

Lect. 16: Generating functions (and Euler's th^{m} contd.) Sec. A

"There's a time in your life before you understand generating functions and a time after, and I can't think of anything that connects them other than a leap of faith." - Grant Sanderson (3Blue1Brown)

Find the number of subsets of $\{1, \ldots, 2000\}$ where the sum of the elements is divisible by 5. sum$\{3,1,4\} = 8 \times$ sum$\{2,3,5\} = 10 \checkmark$

Total subset: 2^{2000} Guess: $\frac{1}{5} \cdot 2^{2000}$

Simpler example: $\{1,2,3,4,5\}$

$\{\} \to 0$	$\{1\} \to 1$	$\{2\} \to 2$	$\{3\} \to 3$	$\{4\} \to 4$
			$\{1,2\} \to 3$	$\{1,3\} \to 4$
$\{5\} \to 5$	$\{1,5\} \to 6$	$\{2,5\} \to 7$	$\{3,5\} \to 8$	$\{4,5\} \to 9$
$\{1,4\} \to 5$	$\{2,4\} \to 6$	$\{3,4\} \to 7$	$\{1,2,5\} \to 8$	$\{1,3,5\} \to 9$
$\{2,3\} \to 5$	$\{1,2,3\} \to 6$	$\{1,2,4\} \to 7$	$\{1,3,4\} \to 8$	$\{2,3,4\} \to 9$
$\{1,4,5\} \to 10$	$\{2,4,5\} \to 11$	$\{3,4,5\} \to 12$	$\{1,3,4,5\} \to 13$	$\{2,3,4,5\} \to 14$
$\{2,3,5\} \to 10$	$\{1,2,3,5\} \to 11$	$\{1,2,4,5\} \to 12$		
$\{1,2,3,4\} \to 10$				

Ans: $8 > \frac{1}{5} \cdot 32$

$\{1,2,3,4,5\} \to 15$

Trivial ex. of expansion: $(a+b)^2$

$= (a+b)(a+b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b$

$= a^2 + 2ab + b^2$

$P(x) = (1+x)(1+x^2)(1+x^3)(1+x^4)(1+x^5)$ $x = ? \to$ just a symbol

expansion: 5 binary choices (which term from each parenthesis to choose from)

$1 + x + x^2 + x^3 + x^3 + x^4 + x^4 + x^5 + x^5 + x^5 + \cdots$

$\equiv 1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + \cdots$

↳ $P(x)$: generating function.

Fibonacci numbers: $f_n = f_{n-1} + f_{n-2}$

$F(x) = 0 + 1x^1 + 1x^2 + 2x^3 + 3x^4 + 5x^5 + \cdots$

$F(x) = xF(x) + x^2F(x) + x \Rightarrow F(x) = \frac{x}{1-x-x^2}$

Art: Deduce the co-efficients without doing the expansion. (Next class)

Reduced residue class: a subset X of the integers is called a "reduced residue class" $(\text{mod } m)$ if:

1. $\gcd(x, m) = 1 \quad \forall x \in X$.
2. X contains $\varphi(m)$ elements.
3. No two elements of X are congruent $(\text{mod } m)$. i.e., $x_i \not\equiv x_j \pmod m \; \forall 1 \le i < j \le \varphi(m)$

Now, let $X = \{x_1, x_2, \ldots, x_{\varphi(m)}\}$ be a reduced residue class $(\text{mod } m)$.

Claim: $X_a = \{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ $(a \perp m)$ is also a reduced residue class $(\text{mod } m)$.

1. $\gcd(ax_i, m) = 1 \quad \forall x_i \in X_a$.

pf: $\gcd(a, m) = 1$, $\gcd(x_i, m) = 1$; $a \perp m$ & $x_i \perp m \Rightarrow ax_i \perp m \Rightarrow \gcd(ax_i, m) = 1$

2. X_a contains $\varphi(m)$ elements. ✓

3. $ax_i \not\equiv ax_j \pmod m$ where $1 \le i < j \le \varphi(m)$.

pf: Assume, $\exists\, i, j$, s.t. $1 \le i < j \le \varphi(m)$ and $ax_i \equiv ax_j \pmod m$

$\Rightarrow x_i \equiv x_j \pmod m$, but this violates the third property of X being a reduced residue class. so a contradiction.

Hence, X_a is a permutation of X. $\Rightarrow$ They will yield the same product $(\text{mod } m)$

$$\Rightarrow \cancel{\prod_{i=1}^{\varphi(m)} x_i} \equiv \prod_{i=1}^{\varphi(m)} ax_i \equiv ax_1 ax_2 \cdots ax_{\varphi(m)} \equiv a^{\varphi(m)} \cancel{\prod_{i=1}^{\varphi(m)} x_i} \pmod m$$

$\Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$, $a \perp m$. [Proved]

Self-study: $\sum_{d \mid m} \varphi(d) = m$

Lect. 16: Generating functions (and Euler's th^{m} contd.) Sec. B

"There's a time in your life before you understand generating functions and a time after, and I can't think of anything that connects them other than a leap of faith." - Grant Sanderson (3Blue1Brown)

Find the number of subsets of $\{1, 2, \ldots, 2000\}$ where the sum of those subsets is divisible by 5. sum$\{3,1,4\} = 8$ ✗ sum$\{2,3,5\} = 10$ ✓

Total subsets: 2^{2000} Guess: $\frac{1}{5} \cdot 2^{2000}$ not an integer

Simpler example: $\{1,2,3,4,5\}$

$\{\} \to 0$	$\{1\} \to 1$	$\{2\} \to 2$	$\{3\} \to 3$	$\{4\} \to 4$
			$\{1,2\} \to 3$	$\{1,3\} \to 4$
$\{5\} \to 5$	$\{1,5\} \to 6$	$\{2,5\} \to 7$	$\{3,5\} \to 8$	$\{4,5\} \to 9$
$\{1,4\} \to 5$	$\{2,4\} \to 6$	$\{3,4\} \to 7$	$\{1,2,5\} \to 8$	$\{1,3,5\} \to 9$
$\{2,3\} \to 5$	$\{1,2,3\} \to 6$	$\{1,2,4\} \to 7$	$\{1,3,4\} \to 8$	$\{2,3,4\} \to 9$
$\{1,4,5\} \to 10$	$\{2,4,5\} \to 11$	$\{3,4,5\} \to 12$	$\{1,3,4,5\} \to 13$	$\{2,3,4,5\} \to 14$
$\{2,3,5\} \to 10$	$\{1,2,3,5\} \to 11$	$\{1,2,4,5\} \to 12$		
$\{1,2,3,4\} \to 10$				
$\{1,2,3,4,5\} \to 15$				

Ans: $8 > \frac{1}{5} \cdot 32$

$P(x) = (1+x)(1+x^2)\cdots(1+x^{2000})$

Trivial ex. of expansion: $(a+b)^2$

$= (a+b)(a+b) = a\cdot a + a\cdot b + b\cdot a + b\cdot b$

$= a^2 + 2ab + b^2$

$P(x) = (1+x)(1+x^2)(1+x^3)(1+x^4)(1+x^5)$ $x = ?$ ⇒ just a symbol

expansion - 5 binary choices (which term for each parenthesis to choose)

$P(x) = 1 + x + x^2 + x^3 + x^3 + x^4 + x^4 + x^5 + x^5 + x^5 + \cdots$

$= 1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + \cdots$

↳ generating function. ↳ encodes the number of subsets with a particular sum, namely, the corresponding exponent.

Fibonacci number: $F(x) = 0 + 1x^1 + 1x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 \cdots$ $f(n) = f(n-1) + f(n-2)$

$F(x) = x\,F(x) + x^2 F(x) + x \Rightarrow F(x) = \frac{x}{1 - x - x^2}$

Art: Deduce the co-efficients without doing the expansion.

Reduced residue system: a subset X of the integers is called a "reduced residue class" $(\bmod m)$ if:

1. $\gcd(x_i, m) = 1 \ \forall x_i \in X$.
2. X contains $\varphi(m)$ elements.
3. No two elements of X are congruent $(\bmod m)$. i.e., $x_i \not\equiv x_j \pmod m$ $\forall \ 1 \le i \ne j \le \varphi(m)$

Now, let $X = \{x_1, x_2, \cdots, x_{\varphi(m)}\}$ be a reduced residue class $(\bmod m)$.

Claim: $X_a = \{ax_1, ax_2, \cdots, ax_{\varphi(m)}\}$ $(a \perp m)$ is also a reduced residue class $(\bmod m)$.

1. $\gcd(ax_i, m) = 1 \ \forall ax_i \in X_a$.

pf: $\gcd(x_i, m) = 1 \Rightarrow x_i \perp m$, $a \perp m \Rightarrow ax_i \perp m \Rightarrow \gcd(ax_i, m) = 1 \ \forall ax_i \in X_a$.

2. X_a contains $\varphi(m)$ elements. ✓

3. Assume $\exists \ i, j$, $1 \le i \ne j \le \varphi(m)$ s.t. $ax_i \equiv ax_j \pmod m$ $[1 \le i \ne j \le \varphi(m)]$

$\Rightarrow x_i \equiv x_j \pmod m$, but this violates the third property of X being a reduced residue class, so a contradiction.

Hence X_a is a permutation of $X \Rightarrow$ they will yield the same product $(\bmod m)$

$$\Rightarrow \cancel{\prod_{i=1}^{\varphi(m)} x_i} \equiv \prod_{i=1}^{\varphi(m)} ax_i \equiv ax_1 \cdot ax_2 \cdots ax_{\varphi(m)} \equiv a^{\varphi(m)} \cancel{\prod_{i=1}^{\varphi(m)} x_i} \pmod m$$

$$\Rightarrow a^{\varphi(m)} \equiv 1 \pmod m \ (a \perp m) \ [\text{Proved}]$$

Self-study: $\sum_{d \mid m} \varphi(d) = m$

Lect. 17: Generating functions (contd.) Sec. A

$G(z) = g_0 + g_1 z + g_2 z^2 + g_3 z^3 + \cdots = \sum_{n\geq 0} g_n z^n$; $g_n = [z^n] G(z)$

$a_{n+1} = 2a_n + 1$ $(n \geq 0, a_0 = 0)$ [Generatingfunctionology]

Generating function: $A(x) = \sum_{n\geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$

Multiply both sides by x^n and sum over all values of $n \geq 0$

LHS: $\sum_{n\geq 0} a_{n+1} x^n = a_1 + a_2 x + a_3 x^2 + \cdots = \frac{(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots) - a_0}{x} = A(x)/x$

RHS: $\sum_{n\geq 0} (2a_n + 1) x^n = 2\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} x^n = 2A(x) + \frac{1}{1-x}$; $|x| < 1$

$A(x)/x = 2A(x) + \frac{1}{1-x} \Rightarrow A(x) = \frac{x}{(1-x)(1-2x)} = x\left(\frac{2}{1-2x} - \frac{1}{1-x}\right)$

$\Rightarrow A(x) = 2x(1 + 2x + 2^2x^2 + \cdots) - x(1 + x + x^2 + \cdots)$

$= (2x + 2^2x^2 + 2^3x^3 + \cdots) - (x + x^2 + x^3 + \cdots)$

$= (2-1)x + (2^2-1)x^2 + (2^3-1)x^3 + \cdots + (2^n - 1)x^n + \cdots$

$a_{n+1} = 2a_n + n$ $(n \geq 0; a_0 = 1)$ Generating function: $A(x) = \sum_{n\geq 0} a_n x^n$

LHS: $\sum_{n\geq 0} a_{n+1} x^n = a_1 + a_2 x + a_3 x^2 + \cdots = \frac{(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots) - a_0}{x} = \frac{A(x) - 1}{x}$

RHS: $\sum_{n\geq 0} (2a_n + 1) x^n = 2\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} n x^n = 2A(x) + \frac{x}{(1-x)^2}$; $|x| < 1$

$\sum_{n\geq 0} n x^n = \frac{x}{(1-x)^2}$

$\sum_{n\geq 0} n x^{n-1} = \frac{1}{(1-x)^2}$ $|x| < 1$

$\frac{A(x) - 1}{x} = 2A(x) + \frac{x}{(1-x)^2} \Rightarrow A(x) = \frac{1 - 2x + 2x^2}{(1-x)^2(1-2x)} = \frac{A}{(1-x)^2} + \frac{B}{1-x} + \frac{C}{1-2x}$ (−1, 2)

$\Rightarrow A(x) = \frac{-1}{(1-x)^2} + \frac{2}{1-2x}$

$[x^n] \frac{-1}{(1-x)^2} = -(n+1)$; $[x^n] \frac{2}{1-2x} = [x^n] 2(1 + 2x + 2^2x^2 + \cdots + 2^n x^n + \cdots)$

$= [x^n] (2 + 2^2 x + 2^3 x^2 + \cdots + 2^{n+1} x^n + \cdots$

$[x^n] A(x) = 2^{n+1} - (n+1)$

$f_{n+1} = f_n + f_{n-1}$ $(n \geq 1; f_0 = 0, f_1 = 1)$ Generating function: $F(x) = \sum_{n \geq 0} f_n x^n$

Multiply both sides by x^n and sum over all values of $n \geq 1$

$$LHS = f_2 x + f_3 x^2 + f_4 x^3 + \cdots = \frac{(f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + \ldots) - f_1 x - f_0}{x} = \frac{F(x) - x}{x}$$

$$RHS = (f_0 + f_1 x + f_2 x^2 + \cdots) + (f_0 x + f_1 x^2 + f_2 x^3 + \ldots) = F(x) + x F(x)$$

$$\frac{F(x) - x}{x} = F(x) + x F(x) \Rightarrow F(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - x r_+)(1 - x r_-)}$$

$$= \frac{1}{(r_+ - r_-)} \left(\frac{1}{1 - x r_+} - \frac{1}{1 - x r_-} \right) \quad [r_\pm = (1 \pm \sqrt{5})/2]$$

$$= 1/\sqrt{5} \left(\sum_{n \geq 0} r_+^n x^n - \sum_{n \geq 0} r_-^n x^n \right)$$

$$\Rightarrow x^n [F(x)] = f(n) = \frac{1}{\sqrt{5}} (r_+^n - r_-^n) = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right\}$$

$G(z) = g_0 + g_1 z + g_2 z^2 + g_3 z^3 + \cdots = \sum_{n\geq 0} g_n z^n$; $[z^n]G(z) = g_n$

$a_{n+1} = 2a_n + 1 \quad (n \geq 0; a_0 = 0)$ [Generatingfunctionology]

Generating function: $A(x) = \sum_{n\geq 0} a_n x^n$

Multiply both sides of the recurrence by x^n and sum over $\forall n \geq 0$.

LHS: $\sum_{n\geq 0} a_{n+1} x^n = a_1 + a_2 x + a_3 x^2 + \cdots = \frac{a_1 x + a_2 x^2 + a_3 x^3 + \cdots}{x}$

$= \frac{(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots) - a_0}{x} = A(x)/x$

RHS $= \sum_{n\geq 0} 2a_n x^n = 2A(x) + \underbrace{\sum_{n\geq 0} x^n}_{1 + x + x^2 + x^3 + \cdots} = 2A(x) + \frac{1}{1-x}$; $|x| < 1$

$A(x)/x = 2A(x) + \frac{1}{1-x} \Rightarrow A(x) = \frac{x}{(1-2x)(1-x)} = x\left\{\frac{2}{1-2x} - \frac{1}{1-x}\right\}$

$= 2x(1 + 2x + 2^2x^2 + 2^3x^3 + \cdots) - x(1 + x + x^2 + \cdots)$

$= (2x + 2^2x^2 + 2^3x^3 + \cdots) - (x + x^2 + x^3 + \cdots)$

$= (2-1)x + (2^2-1)x^2 + (2^3-1)x^3 + \cdots + (2^n-1)x^n + \cdots$

$a_{n+1} = 2a_n + n \quad (n \geq 0, a_0 = 1)$

LHS $= A(x) - 1/x$

RHS $= 2A(x) + \sum_{n\geq 0} n x^n$

$= 2A(x) + \frac{x}{(1-x)^2}$

$\sum_{n\geq 0} n x^n = x + 2x^2 + 3x^3 + \cdots$

$= \frac{x}{(1-x)^2}$; $|x| < 1$

$\Rightarrow \sum_{n\geq 0} n x^{n-1} = \frac{1}{(1-x)^2}$

$\Rightarrow A(x) - 1/x = 2A(x) + \frac{x}{(1-x)^2} \Rightarrow A(x) = \frac{1 - 2x + 2x^2}{(1-x)^2(1-2x)} = \frac{A}{(1-x)^2} + \frac{B}{1-x} + \frac{C}{1-2x}$ (−1, 0, 2)

$\Rightarrow A(x) = \frac{-1}{(1-x)^2} + \frac{2}{1-2x}$

$$[x^n]\frac{-1}{(1-x)^2} = -(n+1)$$

$$\frac{2}{1-2x} = 2(1+2x+2^2x^2+2^3x^3+\cdots) = 2+2^2x+2^3x^2+\cdots+2^{n+1}x^n+\cdots$$

$$[x^n]\,A(x) = 2^{n+1}-(n+1)$$

$$f_{n+1} = f_n + f_{n-1}\ (n\geq 1,\ f_0=0,\ f_1=1)$$

$$F(x) = \sum_{n\geq 0} f_n x^n = f_0+f_1x+f_2x^2+\cdots$$

Multiply both sides by x^n and sum over $\forall n \geq 1$

LHS: $f_2x+f_3x^2+f_4x^3+\cdots = \dfrac{f_2x^2+f_3x^3+f_4x^4+\cdots}{x}$

$$= \frac{(f_0+f_1x+f_2x^2+f_3x^3+\cdots)-f_1x-f_0}{x} = \frac{F(x)-x}{x}$$

RHS $= F(x)+(f_0x+f_1x^2+f_2x^3+\cdots)$

$= F(x)+x(f_0+f_1x+f_2x^2+\cdots)$

$= F(x)+xF(x)$

$$\frac{F(x)-x}{x} = F(x)+xF(x) \Rightarrow F(x) = \frac{x}{1-x-x^2}$$

$$1-x-x^2 = (1-xr_+)(1-xr_-)\ ;\ [r_\pm = (1\pm\sqrt{5})/2]$$

$$F(x) = \frac{x}{1-x-x^2} = \frac{1}{r_+-r_-}\left(\frac{1}{1-xr_+}-\frac{1}{1-xr_-}\right)$$

$$= \frac{1}{\sqrt{5}}\left\{\sum_{n\geq 0} r_+^n x^n - \sum_{n\geq 0} r_-^n x^n\right)$$

$$F_n = \frac{1}{\sqrt{5}}(r_+^n - r_-^n) = \frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right\}$$

Lect 18: Binomial coefficients and dominoes Sec. B

GFs with two variables:

$f(n,k) = f(n-1,k) + f(n-1,k-1)$ $(f(n,0)=1;\ k \le n)$

For each $n = 0, 1, 2, \ldots$ let $B_n(x) = \sum_{k \ge 0} f(n,k)x^k = f(n,0) + f(n,1)x + f(n,2)x^2 + \cdots$

$B_{n-1}(x) = f(n-1,0) + f(n-1,1)x + f(n-1,2)x^2 + \cdots$

Multiply the recurrence by x^k and sum over all $k \ge 1$

LHS: $\sum_{k \ge 1} f(n,k)x^k = (f(n,0) + f(n,1)x + f(n,2)x^2 + \cdots) - f(n,0) = B_n(x) - 1$

RHS: $\sum_{k \ge 1} f(n-1,k)x^k + \sum_{k \ge 1} f(n-1,k-1)x^k$

$= \{f(n-1,0) + f(n-1,1)x + f(n-1,2)x^2 + \cdots\} - f(n-1,0)$

$+ f(n-1,0)x + f(n-1,1)x^2 + \cdots$

$= B_{n-1}(x) - 1 + x B_{n-1}(x)$

$\Rightarrow B_n(x) - 1 = B_{n-1}(x) - 1 + x B_{n-1}(x) \Rightarrow B_n(x) = (1+x) B_{n-1}(x)$

$\Rightarrow B_n(x) = (1+x)^n B_0(x)$ $[B_0(x) = \sum_{k \ge 0} f(0,k)x^k = f(0,0) = 1]$

$\Rightarrow B_n(x) = (1+x)^n$ [Binomial function]

$[x^k] B_n(x) = \binom{n}{k} = \frac{n!}{(n-k)!\,k!}$; $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

How many ways T_n to cover a $2\times n$ rectangle with 2×1 dominoes?

$n=0$ $T_0=1$; $n=1$ $T_1=1$; $n=2$ $T_2=2$; $n=3$ $T_3=3$

$T_n = f_{n+1}$

$T_n = T_{n-1} + T_{n-2}$

Generating function: "sum" of all possible $2\times n$ tilings

$T = 1 + \square + \square\square + \square\square + \square\square\square + \square\square\square + \square\square\square + \cdots$

↳ $1\times\square = \square = \square\times 1$ → multiplicative identity ↳ combinatorial objects

$= 1 + \square(1 + \square + \square\square + \square\square + \cdots) + \square(1 + \square + \cdots)$

$= 1 + \square T + \square T \Rightarrow T = 1 + \square T + \square T \Rightarrow T - \square T - \square T = 1$

$\Rightarrow T(1 - \square - \square) = 1 \Rightarrow T = \dfrac{1}{1-\square-\square} = 1 + (\square + \square) + (\square + \square)^2 + \cdots$

$= 1 + (\square + \square) + (\square\square + \square\square + \square\square + \square\square) + \cdots$

Compress: $\square\square$, $\square\square$

$T = 1 + \square + \square^2 + \square^2 + \square^3 + 2\square\square^2 + \square^4 + 3\square^2\square^2 + \square^4 + \cdots$

$$T = \frac{1}{1-(\square+\square^2)} = 1 + (\square+\square^2) + (\square+\square^2)^2 + \cdots$$
$$= \sum_{k\geq 0} (\square+\square^2)^k$$
$$= \sum_{k\geq j\geq 0} \binom{k}{j} \square^j \square^{2k-2j} \quad [m = k-j \Rightarrow k = j+m]$$
$$= \sum_{j,m\geq 0} \binom{j+m}{j} \square^j \square^{2m}$$

Hence, $\binom{j+m}{j}$ is the number of ways to tile a $2\times(j+2m)$ rectangle with j vertical & $2m$ horizontal dominoes.

$n = j+2m \Rightarrow j+m = n-m$; Now $\binom{j+m}{m} = \binom{n-m}{m}$, which is the number of tilings with exactly m pairs of horizontal dominoes.

$$T_n = \sum_{0\leq m\leq \lfloor n/2 \rfloor} \binom{n-m}{m}$$

$0 \leq 2m \leq n$

$\Rightarrow 0 \leq m \leq \lfloor n/2 \rfloor$

Self-study: $3\times n$ rectangle.

Lect. 18: Binomial coefficients and dominoes Sec. A

GFs with two variables: $f(n,k) = f(n-1,k) + f(n-1,k-1)$ $[f(n,0)=1;\ k \le n]$

For each $n = 0, 1, 2, \ldots$, let $B_n(x) = \sum_{k \ge 0} f(n,k)x^k = f(n,0) + f(n,1)x + f(n,2)x^2 + \cdots$

$B_{n-1}(x) = f(n-1,0) + f(n-1,1)x + f(n-1,2)x^2 + \cdots$

Multiply the recurrence by x^k & sum over all $k \ge 1$

LHS: $\sum_{k \ge 1} f(n,k)x^k = \{f(n,0) + f(n,1)x + f(n,2)x^2 + \cdots\} - f(n,0) = B_n(x) - 1$

RHS: $\sum_{k \ge 1} f(n-1,k)x^k + \sum_{k \ge 1} f(n-1,k-1)x^k$

$= \{f(n-1,0) + f(n-1,1)x + f(n-1,2)x^2 + \cdots\} - f(n-1,0)$

$+ f(n-1,0)x + f(n-1,1)x^2 + \cdots$

$= B_{n-1}(x) - 1 + xB_{n-1}(x)$

$\Rightarrow B_n(x) - 1 = B_{n-1}(x) - 1 + xB_{n-1}(x) \Rightarrow B_n(x) = (1+x)B_{n-1}(x)$

$\Rightarrow B_n(x) = (1+x)^n B_0(x)$ $[B_0(x) = \sum_{k \ge 0} f(0,k)x^k = f(0,0) = 1]$

$= (1+x)(1+x)B_{n-2}(x)$

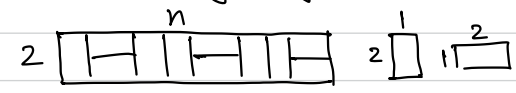
$\vdots$

$= (1+x)^n B_0(x)$

$= (1+x)^n$ [Binomial function]

$[x^k]B_n(x) = \binom{n}{k} = \frac{n!}{(n-k)!\,k!}$; $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

How many ways T_n to cover a $2\times n$ rectangle with 2×1 dominoes?



$n=0$; $n=1$; $n=2$; $n=3$ $T_n = T_{n-1} + T_{n-2}$

$T_0=1$ $T_1=1$ $T_2=2$ $T_3=3$ $T_n = f_{n+1}$

Generating function: "sum" of all possible $2\times n$ tilings.

$(1\times \square = \square = \square\times 1)$ → multiplicative identity ↗ combinatorial object

$T = 1 + \square + \square\square + \square\square + \square\square\square + \square\square + \square\square + \cdots$

$= 1 + \square(1 + \square + \square\square + \square\square + \cdots) + \square\square(1 + \square + \cdots) = 1 + \square\square T + \square\square T$

$\Rightarrow T - \square\square T - \square\square T = 1 \Rightarrow T(1 - \square\square - \square\square) = 1 \Rightarrow T = \frac{1}{1-\square\square-\square\square}$

$\Rightarrow T = 1 + (\square + \square\square) + (\square + \square\square)^2 + \cdots = 1 + (\square + \square\square) + (\square\square + \square\square + \square\square + \square\square) + \cdots$

Compress:

$T = 1 + \square + \square^2 + \square\square^2 + \square^3 + 2\square\square^2 + \square^4 + 3\square^2\square^2 + \square^4 + \cdots$

$$T = \frac{1}{1-(\square + \square\square)} = 1 + (\square + \square\square) + (\square + \square\square)^2 + (\square + \square\square)^3 + \cdots$$

$$= \sum_{K\geq 0} (\square + \square\square)^K \qquad K - j = m \Rightarrow K = j + m$$

$$= \sum_{K \geq j \geq 0} \binom{K}{j} \square^j \square^{2K-2j}$$

$$= \sum_{j,m\geq 0} \binom{j+m}{j} \square^j \square^{2m} \qquad n = j + 2m$$

Hence, $\binom{j+m}{j}$ is the number of ways to tile a $2\times(j+2m)$ rectangle with j vertical dominoes and $2m$ horizontal dominoes.

$n = j + 2m \Rightarrow j + m = n - m$; Now, $\binom{j+m}{j} = \binom{j+m}{m} = \binom{n-m}{m}$, which is the number of tilings with exactly m pair of horizontal dominoes.

$$T_n = \sum_{0\leq m\leq \lfloor n/2 \rfloor} \binom{n-m}{m}$$

$0 \leq 2m \leq n$

$\Rightarrow 0 \leq m \leq \lfloor n/2 \rfloor$

Self-study: $3\times n$ rectangle

Lect 19: Coin change and integer partitioning — Sec. A

How many ways are there to pay 50 cents?

① pennies, ⑤ nickels, ⑩ dimes, ㉕ quarters, ㊿ half.

Only pennies: $P = 1 + ① + ①① + ①①① + \cdots = 1 + ① + ①^2 + ①^3 + \cdots$.

+ Nickels: $N = P + ⑤P + ⑤⑤P + \cdots = (1 + ⑤ + ⑤^2 + \cdots)P$

+ Dimes: $D = (1 + ⑩ + ⑩^2 + \cdots)N$

+ Quarters: $Q = (1 + ㉕ + ㉕^2 + \cdots)D$

+ Half: $H = (1 + ㊿ + ㊿^2 + \cdots)Q$

$P = 1 + z + z^2 + z^3 + \cdots \Rightarrow P = \frac{1}{1-z} \Rightarrow P(1-z) = 1$ $\quad P_0 + P_1 z^2 + P_2 z^3 + \cdots + P_{n-1} z^{n} + P_n z^{n+1}$

$N = (1 + z^5 + z^{10} + z^{15} + \cdots)P \Rightarrow N = \frac{P}{1-z^5} \Rightarrow N(1-z^5) = P$

$D = (1 + z^{10} + z^{20} + z^{30} + \cdots)N \Rightarrow D = \frac{N}{1-z^{10}} \Rightarrow D(1-z^{10}) = N$

$Q = (1 + z^{25} + z^{50} + z^{75} + \cdots)D \Rightarrow Q = \frac{D}{1-z^{25}} \Rightarrow Q(1-z^{25}) = D$

$H = (1 + z^{50} + z^{100} + z^{150} + \cdots)Q \Rightarrow H = \frac{Q}{1-z^{50}} \Rightarrow H(1-z^{50}) = Q$

Let P_n, N_n, D_n, Q_n, H_n be the number of ways to pay n cents when max coin allowed are 1, 5, 10, 25, 50, respectively. [Coefficients of z^n in the series above]

$P_n - P_{n-1} = [n=0] \Rightarrow P_n = P_{n-1} + [n=0]$

$N_n - N_{n-5} = P_n \Rightarrow N_n = N_{n-5} + P_n$

$D_n - D_{n-10} = N_n \Rightarrow D_n = D_{n-10} + N_n$

$Q_n - Q_{n-25} = D_n \Rightarrow Q_n = Q_{n-25} + D_n$

$H_n - H_{n-50} = Q_n \Rightarrow H_n = H_{n-50} + Q_n$

$H = \frac{Q}{1-z^{50}} = \frac{D}{1-z^{25}} \cdot \frac{1}{1-z^{50}} = \frac{N}{1-z^{10}} \cdot \frac{1}{1-z^{25}} \cdot \frac{1}{1-z^{50}} = \frac{P}{1-z^5} \cdot \frac{1}{1-z^{10}} \cdot \frac{1}{1-z^{25}} \cdot \frac{1}{1-z^{50}}$

$= \frac{1}{1-z} \cdot \frac{1}{1-z^5} \cdot \frac{1}{1-z^{10}} \cdot \frac{1}{1-z^{25}} \cdot \frac{1}{1-z^{50}}$

A partition of a positive integer n is a way of writing n as a sum of positive integers (each integer in the sum is called a part). For example, 4 can be partitioned into five distinct ways: $4, 3+1, 2+2, 2+1+1, 1+1+1+1$.

Show that for each positive integer n, the number of partitions of n into unequal parts is equal to the number of partitions of n into odd parts. For instance, if $n=6$, there are 4 partitions into unequal parts: $6, 5+1, 4+2, 3+2+1$. And there are four partitions into odd parts: $5+1, 3+3, 3+1+1+1, 1+1+1+1+1+1$.

GF for partitioning into odd parts: $\frac{1}{1-x} \cdot \frac{1}{1-x^3} \cdot \frac{1}{1-x^5} \cdot \frac{1}{1-x^7} \cdots\cdots$

GF for partitioning into unequal parts: $(1+x)(1+x^2)(1+x^3)\cdots$

$= \frac{1-x^2}{1-x} \cdot \frac{1-x^4}{1-x^2} \cdot \frac{1-x^6}{1-x^3} \cdot \frac{1-x^8}{1-x^4} \cdot \frac{1-x^{10}}{1-x^5} \cdots\cdots$

$a_n = \begin{cases} 1, & \text{if } n=0 \\ 4/11, & \text{if } n=1 \\ \frac{a_{n-1}a_{n-2}}{2a_{n-2}-a_{n-1}} & [n-2, n-3, n-4] \end{cases}$ $\quad a_n = \frac{4}{7n+4}$ Top-down, bottom-up both work!

$\sum_{k=1}^{n} (-1)^n (2k-1)$

→ Calculate first few terms, generalize, prove by induction

→ Convert to recurrence, solve using repertoire

→ perturbation

→ Convert to multiple sums

Lect. 19: Coin change and integer partitioning Sec. B

How many ways are there to pay 50 cents? (denominations)
① pennies, ⑤ nickels ⑩ dimes, ㉕ quarters ㊿ half.

Only pennies: $P = 1 + ① + ①① + ①①① + \cdots = 1 + ① + ①^2 + ①^3 + \cdots$.
+ Nickels: $N = P + ⑤P + ⑤⑤P + \cdots = (1 + ⑤ + ⑤^2 + \cdots)P$
+ Dimes: $D = (1 + ⑩ + ⑩^2 + \cdots)N$
+ Quarter: $Q = (1 + ㉕ + ㉕^2 + \cdots)D$
+ Half: $H = (1 + ㊿ + ㊿^2 + \cdots)Q$

$P = P_0 + P_1 z + P_2 z^2 + P_3 z^3 + \cdots \Rightarrow P_z = P_0 z + P_1 z^2 + \cdots + P_n z^{n+1} + \cdots$

$P = 1 + z + z^2 + z^3 + \cdots \Rightarrow P = \frac{1}{1-z} \Rightarrow P(1-z) = 1$
$N = (1 + z^5 + z^{10} + \cdots)P \Rightarrow N = \frac{P}{1-z^5} \Rightarrow N(1-z^5) = P$
$D = (1 + z^{10} + z^{20} + \cdots)N \Rightarrow D = \frac{N}{1-z^{10}} \Rightarrow D(1-z^{10}) = N$
$Q = (1 + z^{25} + z^{50} + \cdots)D \Rightarrow Q = \frac{D}{1-z^{25}} \Rightarrow Q(1-z^{25}) = D$
$H = (1 + z^{50} + z^{100} + \cdots)Q \Rightarrow H = \frac{Q}{1-z^{50}} \Rightarrow H(1-z^{50}) = Q$

Let P_n, N_n, D_n, Q_n, H_n be the number of ways to pay n cents when max coin allowed are 1, 5, 10, 25, 50, respectively. (by def^n, coefficients of z^n in the series above)
Equating the coefficients of z^n in both sides:
$P_n - P_{n-1} = [n=0] \Rightarrow P_n = P_{n-1} + [n=0]$
$N_n - N_{n-5} = P_n \Rightarrow N_n = N_{n-5} + P_n$
$D_n - D_{n-10} = N_n \Rightarrow D_n = D_{n-10} + N_n$
$Q_n - Q_{n-25} = D_n \Rightarrow Q_n = Q_{n-25} + D_n$
$H_n - H_{n-50} = Q_n \Rightarrow H_n = H_{n-50} + Q_n$

$H = \frac{Q}{1-z^{50}} = \frac{D}{1-z^{25}} \cdot \frac{1}{1-z^{50}} = \frac{N}{1-z^{10}} \cdot \frac{1}{1-z^{25}} \cdot \frac{1}{1-z^{50}} = \frac{P}{1-z^5} \cdot \frac{1}{1-z^{10}} \cdot \frac{1}{1-z^{25}} \cdot \frac{1}{1-z^{50}}$
$= \frac{1}{1-z} \cdot \frac{1}{1-z^5} \cdot \frac{1}{1-z^{10}} \cdot \frac{1}{1-z^{25}} \cdot \frac{1}{1-z^{50}}$

A partition of a positive integer n is a way of writing n as a sum of positive integers (each integer in the sum is called a part). For example, 4 can be partitioned into five distinct ways: $4, 3+1, 2+2, 2+1+1, 1+1+1+1$.

Show that for each positive integer n, the number of partitions of n into unequal parts is equal to the number of partitions of n into odd parts. For instance, if $n=6$, there are 4 partitions into unequal parts: $6, 5+1, 4+2, 3+2+1$. And there are four partitions into odd parts: $5+1, 3+3, 3+1+1+1, 1+1+1+1+1+1$.

GF for partitioning into odd parts: $\frac{1}{1-z} \cdot \frac{1}{1-z^3} \cdot \frac{1}{1-z^5} \cdot \frac{1}{1-z^7} \cdot \cdots$

GF for partitioning into unequal parts: $(1+z)(1+z^2)(1+z^3)\cdots$

$= \frac{1-z^2}{1-z} \cdot \frac{1-z^4}{1-z^2} \cdot \frac{1-z^6}{1-z^3} \cdot \frac{1-z^8}{1-z^4} \cdot \frac{1-z^{10}}{1-z^5} \cdots = \frac{1}{1-z} \cdot \frac{1}{1-z^3} \cdot \frac{1}{1-z^5} \cdot \cdots$

$a_n = \begin{cases} 1, & \text{if } n=0 \\ 4/11, & \text{if } n=1 \\ \frac{a_{n-1}a_{n-2}}{2a_{n-2}-a_{n-1}} & [n-2, n-3, n-4] \end{cases}$ $\quad a_n = \frac{4}{7n+4}$ Top-down, bottom-up both work!

$\sum_{k=1}^{n} (-1)^{k+1}(2k-1)$
- → Calculate first few terms, generalize, prove by induction
- → Convert to recurrence, solve using repertoire
- → perturbation
- → Convert to multiple sum