4-7 Number-Theoretic Algorithms.

- Card. Magic
- CRT & Generalized CRT.
- Co-prime ~~testing~~
  (CLRS 31.2-9)
- Analysis of Euclidean Alg.
  Euclid
  (CLRS 31.2-5).

"Happy May Day"

CRT & Cards – Numberphile

x	
1 →	2
2 →	3
3	4
4	5
5	1
5	4
4	3
3	2
2	1
1	5

hearts

1, 2, 3, 4

$(1\ 2\ 3\ \cdots\ m-2, m-1, m)$ (# of cards)

m 1 → 2 → 3

$m-1$

$m-2$

$\cdots$

ℓ shuffles

spades

$(1\ 2\ 3\ 4\ 5)$

4, 3, 2, 1

$(5\ 4\ 3\ 2\ 1)$

$(m, m-1, m-2, \cdots, 3, 2, 1)$

m → $m-1$ → $m-2$ $\cdots$

1

2

3

$\cdots$

r shuffles

Q: Relation?

(The Magic Number) ~~x~~ (# of shuffles)

$$\ell + r = 11$$

After ℓ shuffles:

$1 \to \boxed{\ell+1}$ on ~~the~~ top

After r shuffles:

$\boxed{m-r}$.

$$\ell + 1 = m - r$$

$$\ell + r = m - 1$$

$$\Rightarrow m = 12\ ???$$

It is: $\ell + 1 \equiv m - r \pmod{m}$

$$\cancel{\Rightarrow} \Leftrightarrow \boxed{\ell + r \equiv -1 \pmod{m}}$$

CRT.
$$\begin{cases} 11 \equiv -1 \pmod{4} \\ 11 \equiv -1 \pmod{3} \\ 11 \equiv -1 \pmod{2}. \end{cases}$$

(Key Number)

CRT (corollary 31.29)

$x \equiv a \pmod{n_i}$ — $n_1, \ldots n_k$ are pairwise ~~relatively prime~~ coprime

$\boxed{\Leftrightarrow}\ x \equiv a \pmod{n}$. — a is any integer.

CRT (corollary 31.29 generalized to non-coprime moduli)

$n_1, \ldots n_k$ may be non-coprime.

$x \equiv a \pmod{n_i}$

$\boxed{\Leftrightarrow}\ x \equiv a \pmod{[n_1, n_2, \ldots n_i]}$.

CRT (Thm 31.27)

$cx+b$?

$$\begin{cases} \cancel{x} \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

(1) The n_i's are pairwise coprime.

$N = n_1 \ldots n_k = \prod_{i=1}^{k} n_i$.

(2) a_i's are ~~integers~~ any.

Then. there is a unique solution $\pmod N$.

Pf: Existence + uniqueness $\pmod N$

$x_1 \equiv x_2 \pmod N$

Existence

Pf method 1.

Non-constructive proof. ⟸ ~~Group~~ theory? — Direct product. → Ring (三环)

$R: \mathbb{Z}_N \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$.

$R: x \mapsto (x \bmod n_1, \ldots x \bmod n_k)$.

(We want to show bijection.)

It is injective. (uniqueness!) $\underline{R}$: ring isomorphism.

⟹ It is surjective ($|\mathbb{Z}_N| = |\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_k}|$)

~~⟹ Bijection..~~

~~R is a~~

2

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \cdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

$n_1, n_2, \ldots n_k$ pairwise coprime.

Pf method 2 (constructive proof)

$$x \equiv a_1 \cdot \begin{cases} x_1 \equiv 1 \pmod{n_1} \\ x_1 \equiv 0 \pmod{n_2} \\ \vdots \\ x_1 \equiv 0 \pmod{n_k} \end{cases} + a_2 \cdot \begin{cases} x_2 \equiv 0 \pmod{n_1} \\ x_2 \equiv 1 \pmod{n_2} \\ \vdots \\ x_2 \equiv 0 \pmod{n_k} \end{cases}$$

$$+ \boxed{a_i \cdot \begin{cases} x_i \equiv 0 \pmod{n_1} \\ \vdots \\ x_i \equiv 1 \pmod{n_i} \\ \vdots \\ x_i \equiv 0 \pmod{n_k} \end{cases}} + a_k \cdot \begin{cases} x_k \equiv 0 \pmod{n_1} \\ \vdots \\ x_k \equiv 1 \pmod{n_k} \end{cases}$$

$$\Downarrow \quad \boxed{x_i = y_i \cdot M_i \quad \left(\boxed{M_i \triangleq N/n_i}\right)}$$

$$\equiv \prod_{i=1}^{k} a_i \cdot \underset{(N/n_i)}{\underset{\triangleq}{M_i}} \cdot \underbrace{\left(M_i^{-1} \bmod n_i\right)}_{\boxed{y_i}} \pmod{n}$$

$$\boxed{\begin{aligned} y_i \cdot M_i &\equiv 1 \pmod{n_i} \\ y_i &\equiv M_i^{-1} \pmod{n_i} \\ M_i &\perp n_i \ \boxed{\text{coprime}} \end{aligned}}$$

3

CRT Example. 《射雕英雄传》第二十九回.

$$\begin{cases} X \equiv 2 \pmod 3 \\ X \equiv 3 \pmod 5 \\ X \equiv 2 \pmod 7 \end{cases}$$

$X \equiv 23 \pmod{105}$.

$$\begin{cases} X \equiv 3 \pmod 8 \\ X \equiv 11 \pmod{20} \\ X \equiv 1 \pmod{15} \end{cases}$$

$$\begin{cases} X \equiv 3 \pmod 8 \\ \begin{cases} X \equiv 11 \pmod 4 \\ X \equiv 11 \pmod 5 \end{cases} \\ \begin{cases} X \equiv 1 \pmod 3 \\ X \equiv 1 \pmod 5 \end{cases} \end{cases}$$

$\Rightarrow X \equiv 3 \pmod 4$

$\Rightarrow X \equiv 1 \pmod 5$

$$\begin{cases} X \equiv 3 \pmod 8 \\ X \equiv 1 \pmod 5 \\ X \equiv 1 \pmod 3 \end{cases} \Rightarrow X \equiv -29 \pmod{120}$$

$X \equiv 91 \pmod{120}$

$= [8, 20, 15]$.

CRT (Generalized CRT Theorem)

$$\begin{cases} X \equiv a_1 \pmod{n_1} \\ \vdots \qquad\qquad \vdots \\ X \equiv a_k \pmod{n_k} \end{cases}$$

$n_1, \dots n_k$ may be non-coprime

If $\boxed{a_i \equiv a_j \pmod{(n_i, n_k)}}$

Then there is a unique solution mod $[n_1, n_2, \dots n_k]$.

4

CRT. (Example) ~~Exercise~~.

$$19x \equiv 556 \pmod{1155}$$

$$1155 = 3 \cdot 5 \cdot 7 \cdot 11$$

CRT Exercise.

$2^{400} \bmod 319$. $(319 = 11 \cdot 29)$.

CLRS 31.2-9 (Co-prime).

Prove that n_1, n_2, n_3, n_4 are pairwise co-prime iff

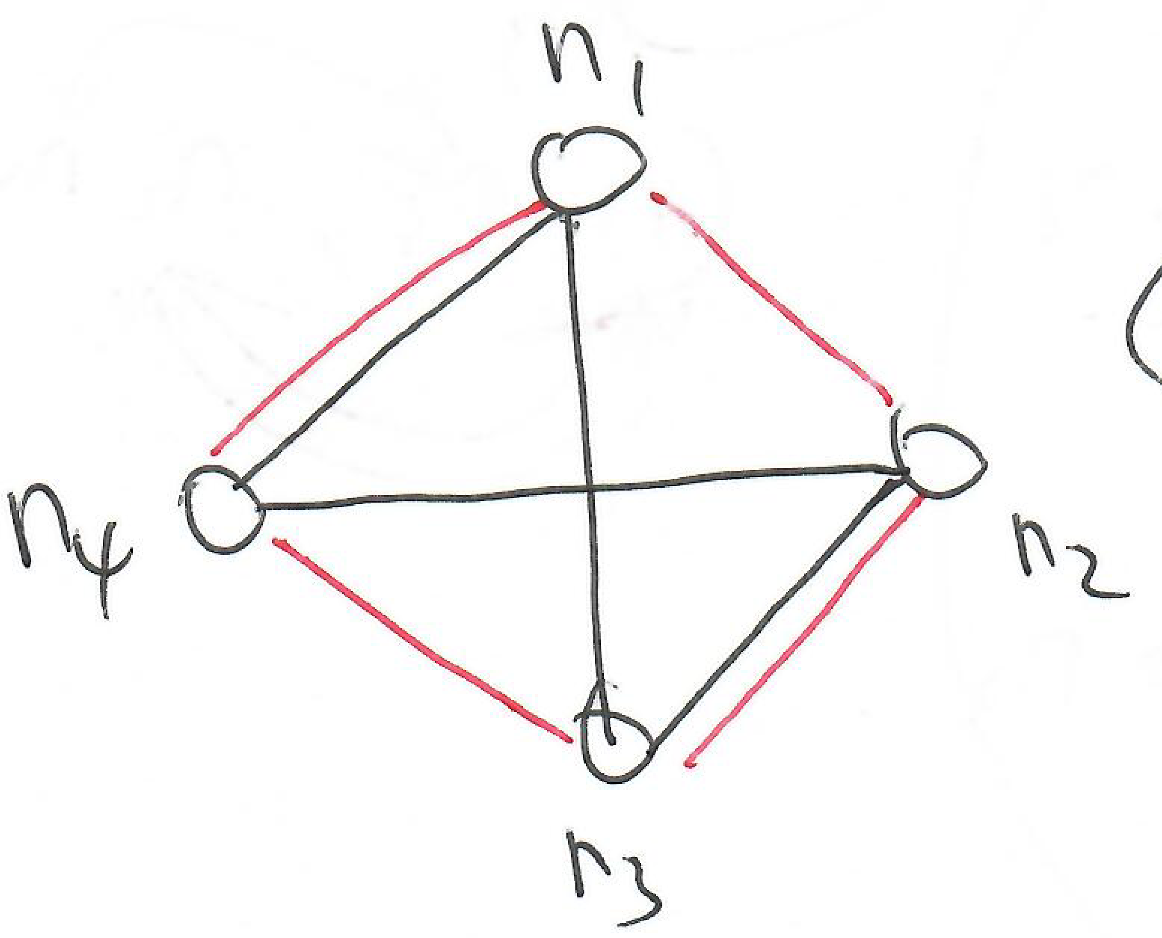
$$(n_1 n_2, n_3 n_4) = (n_1 n_3, n_2 n_4) = 1.$$

pair

More generally, show that $n_1, \dots n_k$ are pairwise coprime iff a set of $\lceil \lg k \rceil$ pairs of numbers derived from the n_i are relatively prime.

$$\underbrace{(\square, \square) = (\square, \square) = \cdots = (\square, \square)}_{\#\text{ of pairs} = \lceil \lg k \rceil} = 1$$

$k=4$: $(n_1 n_2, n_3 n_4) = (n_1 n_3, n_2 n_4) = 1$

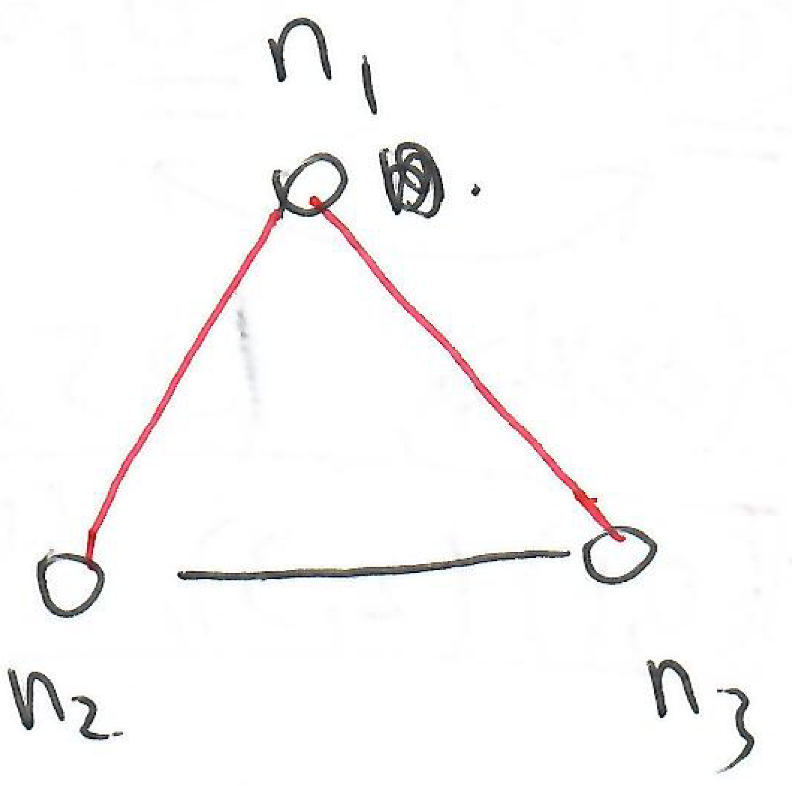


(complete graph).

Covering a complete graph using complete bipartite subgraphs!

$k=2$: $(n_1, n_2) = 1$

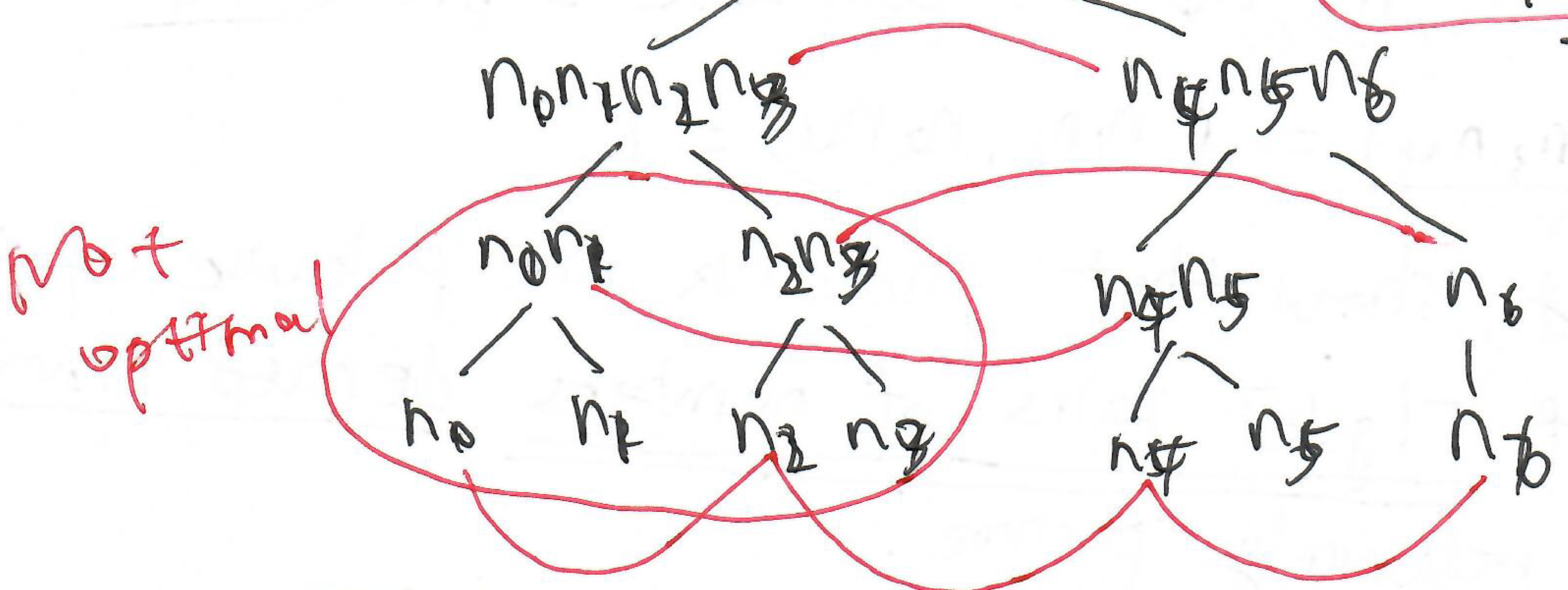
$k=3$.



$(n_1, n_2 n_3) = (n_2, n_3) = 1$

$k=7$

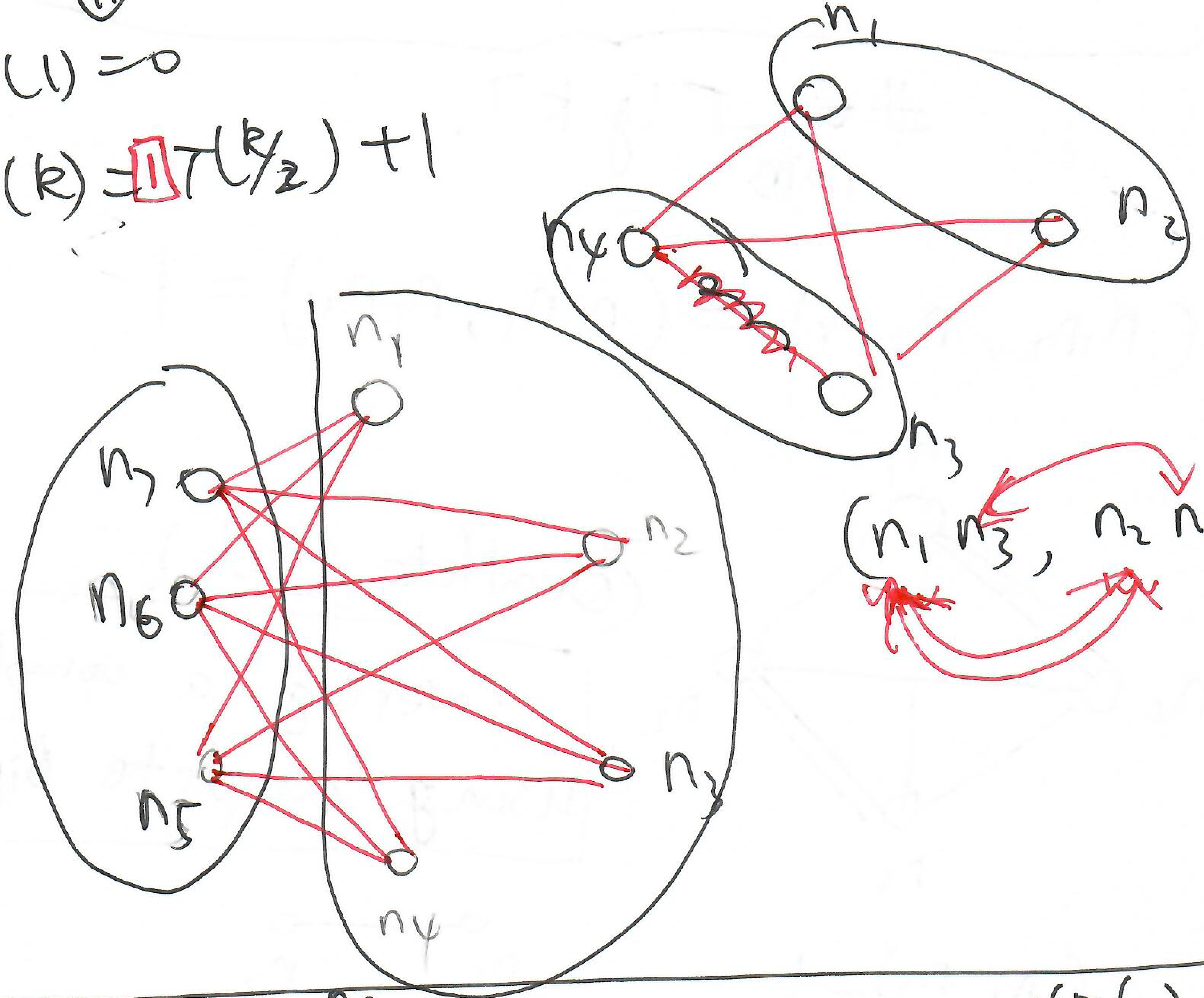
☆ (换成 $n_0, n_1, \cdots n_6$) in class.



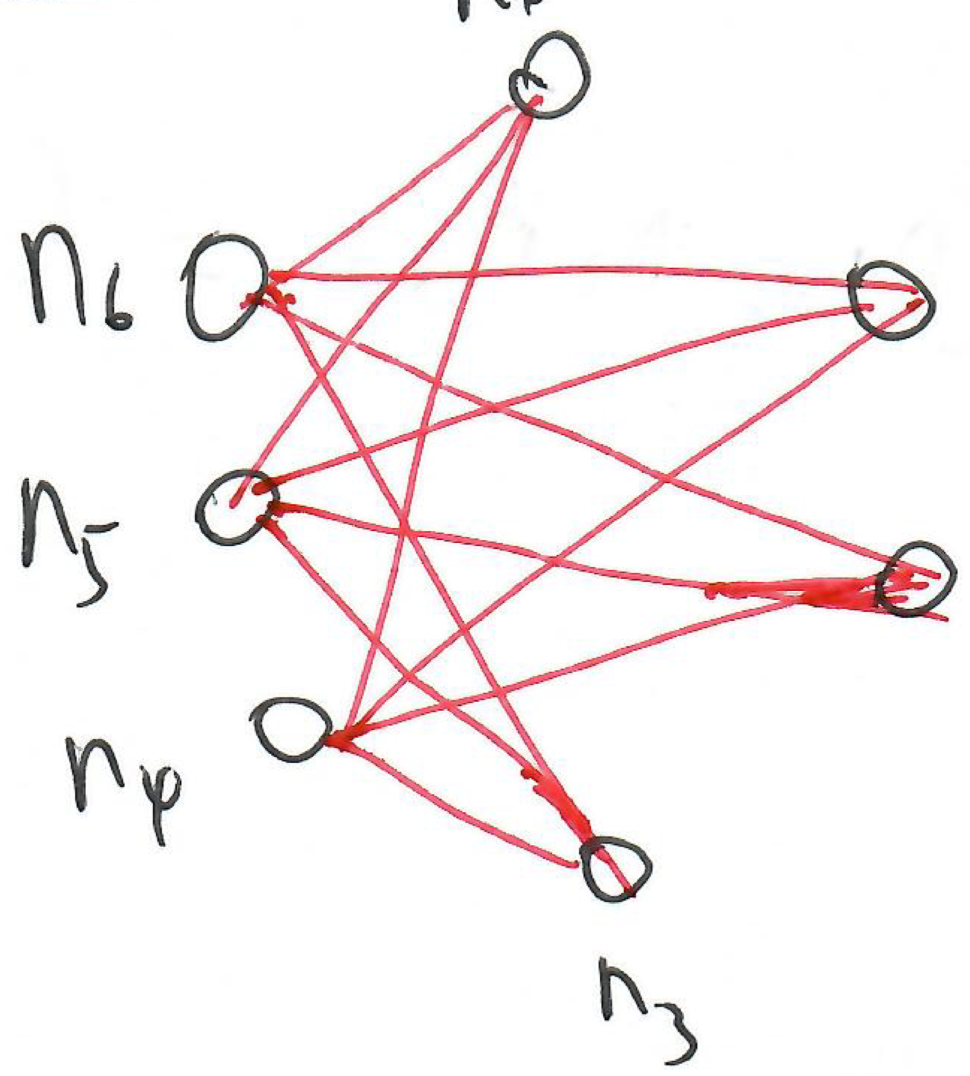
$$\begin{cases} T(1) = 0 \\ T(k) = 2T(k/2) + 1 \end{cases} \Rightarrow T(k) = k-1.$$

$\Downarrow$

Not Easy.
$$\begin{cases} T(1) = 0 \\ T(k) = \boxed{1}\, T(k/2) + 1 \end{cases}$$



$(n_1 n_3,\ n_2 n_4)$



$(0123,\ 456)$

$(\underline{01}, 23)$ $(\underline{45}, 6)$

$(0246,\ 135)$

$(0,1)\ (2,3),\ (4,5),\ (6)$

Lower bound? $T(k) \geq \lceil \lg k \rceil$?

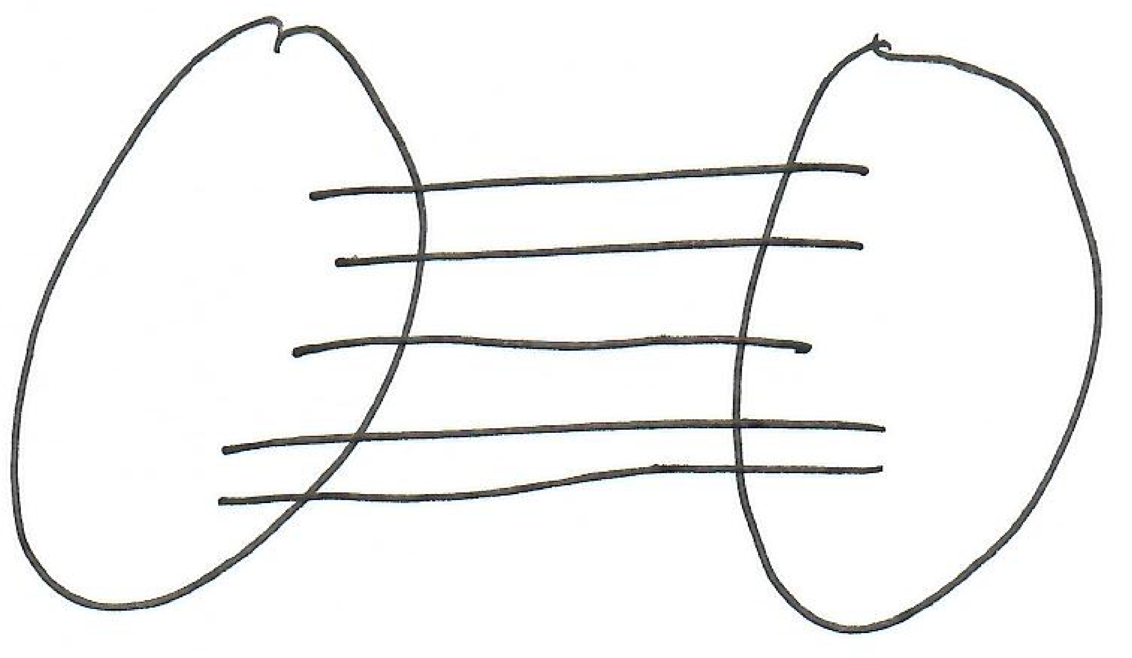
pf. By strong mathmatical induction on n.

To cover K_n, the first bipartite subgraph is $K_{p,q}$.

$p+q=n$.

$\cancel{p \geq \frac{n}{2}}$

at least one of p, q: $\geq \lceil \frac{n}{2} \rceil$.



K_p K_q.

$$T(k) \geq 1 + T(\lceil \tfrac{k}{2} \rceil)$$
$$\geq 1 + \lceil \lg \lceil \tfrac{k}{2} \rceil \rceil$$
$$= \lceil \lg k \rceil.$$

$\boxtimes$.

Edge-disjoint bipartite subgraph covering/partition.

$T(k) = k-1$.