CSC3001: Discrete Mathematics

Assignment 2

Instructions:

1. Print out this question paper (**two-sided**) and write down your full working on the blank area.
2. You can have discussions with your classmates. However, make sure all the solutions you submit are your own work. Any plagirism will be given **ZERO** mark.
3. Submission of this assignment should **NOT** be later than **5pm on 8th of November**.
4. Before your submission, please **make a softcopy** of your work for further discussion in a tutorial.
5. After making your softcopy, submit your assignment to the dropbox located on the 4th floor in Chengdao Building.

Student Number: 118010350

Name: 解惠仔

1. (*20 points*) Let p be an odd prime. Prove that there are exactly $\frac{p-1}{2}$ integers $a \in \{1, \ldots, p-1\}$ such that $x^2 \equiv a \pmod{p}$ for some x.

Proof. W.L.O.G. we only consider $x \in \{1, 2, \cdots p-1\}$.

Since any set like $\{kp+1, kp+2, \cdots kp+p-1\}$.

we have $kp+1 \equiv 1 \pmod{p} \cdots \; kp+p-1 \equiv p-1 \pmod{p}$

thus $(kp+1)^2 \equiv 1^2 \pmod{p} \cdots \; (kp+p-1)^2 \equiv (p-1)^2 \pmod{p}$.

which gives the ~~same~~ same result.

Assume $x_1, x_2 \in \{1, 2, \cdots p-1\}$.

s.t. $x_1^2 \equiv a \pmod{p}$ and $x_2^2 \equiv a \pmod{p}$.

then $x_1^2 - x_2^2 \equiv 0 \pmod{p}$.

$\Leftrightarrow (x_1 + x_2)(x_1 - x_2) \equiv 0 \pmod{p}$.

Since p is an odd prime, $x_1, x_2 < p$.

then we have $x_1 + x_2 = p$ or $x_1 = x_2$.

That is x_1^2, x_2^2 are congruent to each other.

if and only if $x_1 + x_2 = p$ or $x_1 = x_2$.

Since $x \in \{1, 2, \cdots p-1\}$, then we have. $\frac{p-1}{2}$ pairs.

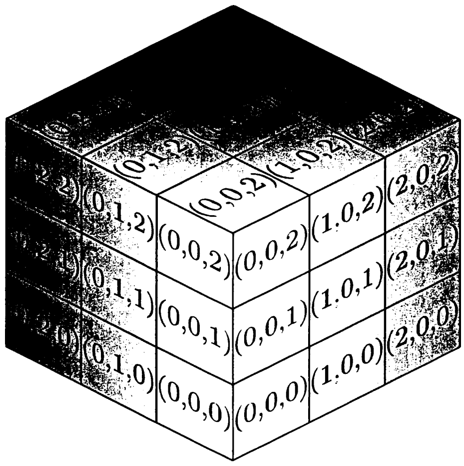
of (x_1, x_2). s.t $x_1 + x_2 = p$. that is $(1, p-1), (2, p-2)$.

$\cdots (\frac{p-1}{2}, \frac{p+1}{2})$.

Thus there are $\frac{p-1}{2}$ integers $a \in \{1, \cdots p-1\}$.

s.t $x^2 \equiv a \pmod p$ for some x.

2. (*20 points*) Suppose that n^3 unit cubes are stacked into a large $n \times n \times n$ cube. Let $x, y, z \in \mathbb{Z}_n$ and label each unit cube by (x, y, z) with respect to its location (see the picture for $n = 3$).



The unit cubes (x, y, z) and (x', y', z') are adjacent if one of the following conditions holds:

- $x' - x \equiv \pm 1 \pmod n$ and $y' = y$, $z' = z$; or
- $|y' - y| \equiv 1 \pmod n$ and $x' = x$, $z' = z$; or
- $|z' - z| \equiv 1 \pmod n$ and $x' = x$, $y' = y$.

For each $n \in \mathbb{Z}^+$, provide an ordering of all the unit cubes satisfying the following:

- every two consecutive cubes are adjacent;
- the last cube and the first cube in the list are adjacent.

(**Note:** You may draw pictures to demonstrate your idea.)

① If n is even $(n=2,4,6,\dots)$.

Suppose $n=2k$, $k \in \mathbb{N} \setminus \{0\}$. The strategy of forming cube list is as following:

Start with $(0,0,0) \longrightarrow (0,0,n-1)$

$\downarrow$

$(1,0,0) \longleftarrow (1,0,n-1)$

$\downarrow$

$(2,0,0) \longrightarrow (2,0,n-1)$

$\downarrow$

repeat steps.

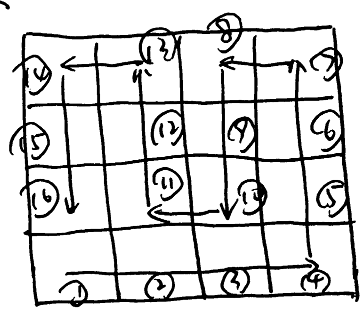
...

$\downarrow$

$(0,1,n-1) \longrightarrow (0,1,0)$.

The ordering of the list is formed by going up and down repeatedly. And we can always find a way to go through every cube column in top view.

e.g. $n=4$. top view:



①, ③, ... ⑬, ⑮: go up.

②, ④, ... ⑭, ⑯: go down.

② If n is odd, $(n=3,5,7,\cdots)$.

Suppose $n=2k+1$, $k \in \mathbb{N} \setminus \{0\}$. The strategy of forming cube list is as following:

Start with $(0,0,0) \longrightarrow (0,0,n-1)$

$\downarrow$ *(1)

$(n-1,0,n-2) \longleftarrow (n-1,0,n-1)$.

$\downarrow$ *(2)

$(n-1,1,n-2) \longrightarrow (n-1,1,n-3)$.

$\downarrow$ *(3).

$(n-1,2,n-4) \longleftarrow (n-1,2,n-3)$

$\downarrow$ repeat seps.

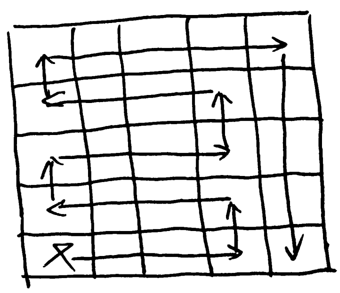
...

$\downarrow$ *(n-1).

$(n-1,0,0)$.

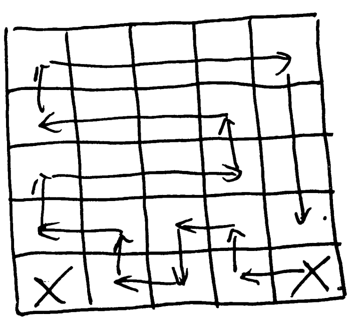
*(1) go through all cubes in level $n-1$, $(z=n-1)$

top view $(n=5)$:

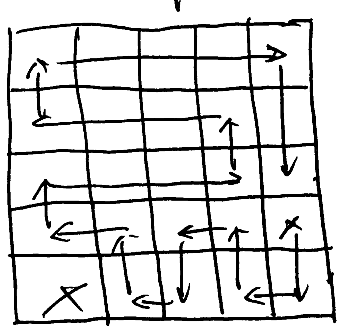


*(2) go through all cubes in level $n-2$, $(z=n-2)$. except $(0,0,n-2)$.

top view. $(n=5)$.



*(3) go through all cubes in level $n-3$, $(z=n-3)$ except $(0,0,n-3)$.



the ordering of list is formed by go through each level and go to the next lower level repeatedly. At each level, strat with $(n-1,k,l)$. end with $(n-1,k+1,l)$. At last level, we can go back to the final cube $(n-1,0,0)$.

3. (*20 points*) Let $n \in \mathbb{N}$ be with $n \geq 2$. Let $k \in \{1, 2, \ldots, n-1\}$ be a fixed number such that $\gcd(k, n) = 1$. Given the balls labeled by $1, 2, \ldots, n-1$, we try to color each ball black or white such that

(1) i and $n - i$ are of the same color;

(2) for each $i \neq k$, we have i and $|i - k|$ are of the same color.

Prove that all the balls are of the same color.

(a). when. If $n=2$, nothing to prove.

(b) when $n>2$.

Proof. ① If. $k=1$ or $k=n-1$, then $\gcd(k,n)=1$.

(1). $\Rightarrow$ ~~(1, n-1), (2, n-2)~~ ..

if. n is odd, then $(1, n-1), (2, n-2), \cdots (\frac{n-1}{2}, \frac{n+1}{2})$. have the same color.

If n is even, then $(1, n-1)$ ~~(2, n-2)~~ $\cdots (\frac{n}{2}-1, \frac{n}{2}+1)$, $\frac{n}{2}$ have the same color.

(2) $\Rightarrow$. when $k=1$, then $(2,3), (3,4) \cdots (n-2, n-1)$ have the same color, then $(2, 3, \cdots n-1)$ have the same color, with $(1, n-1)$ is same. we get $(1, 2, 3, \cdots n-1)$ have same color.

when $k=n-1$, then $(1, n-2), (2, n-3), \cdots$ have the same color. ~~then~~ with (1), then $(1, 2, 3, \cdots n-1)$ have same color.

②. If. k is ~~other~~ number $\in$ {~~1, 2, ... n-1~~} $\{2, \cdots n-2\}$ s.t $\gcd(k, n) = 1$.

Similarly. (1) $\Rightarrow$ If n is odd, $(1, n-1), \cdots (\frac{n-1}{2}, \frac{n+1}{2})$ same.

If n is even, $(1, n-1), \cdots (\frac{n}{2}-1, \frac{n}{2}+1)$, $\frac{n}{2}$ same.

Suppose for contradiction that not all balls have the same color.

By (1) & (2), that is, some $\# \in \{1, 2, \cdots n-1\}$ repeatedly appears in $\{i, n-i, |i-k|\}$ for some given i, and they can not take full values of $\{1, 2, \cdots n-1\}$.

Thus, we must have $i, n-i, |i-k|$ are under some relation of multiple.

Case 1: $i = ak$. $a \in \{1, 2, 3, 4, \cdots\}$.

Then ~~$n-ak = ak-k$~~ $n-i = |i-k| \Rightarrow n-ak = ak-k$

$\Rightarrow n = (2a-1)k$.

$\Rightarrow \gcd(n, k) \neq 1$.

Case 2: $k = bi$. $b \in \{1, 2, 3, 4, \cdots\}$.

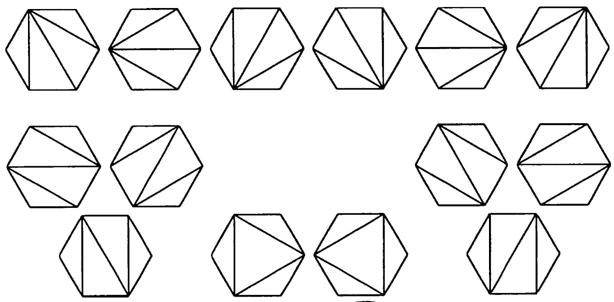
Then $n-i = c|i-k| \Rightarrow n-i = c(bi-i) = bci-ci$.

$\Rightarrow n = (bc-c+1)i$

$\Rightarrow \gcd(n, k) \neq 1$. ($\in i$).

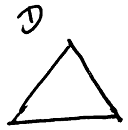
By contradiction, we get if $\gcd(n, k) = 1$, then all the balls have the same color.

4. (*20 points*) Let T_n denote the number of different ways that a convex polygon with $n+2$ sides can be cut into triangles by connecting vertices with non-crossing line segments. (For example, $T_n = 14$ for $n = 4$ as shown below)



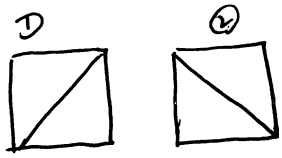
Find the recurrence relation of T_n and hence find the closed form of T_n using generating functions.

(1) when $n=1$, have $n+2=3$ sides



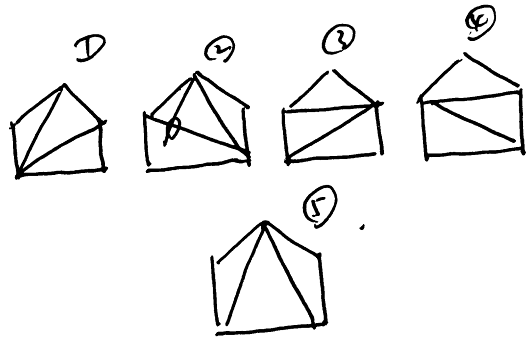
$\Rightarrow T_1 = 1$.

when $n=2$, have $n+2=4$ sides



$\Rightarrow T_2 = 2$.

when $n=3$, have $n+2=5$ sides.



$\Rightarrow T_3 = 5$.

when $n=4$, have $n+2=6$ sides

$\Rightarrow T_4 = 14$.

If we define $T_0 = 1$, then we can find that.

$T_0 = 1$, $T_1 = 1$, $T_2 = 1\times1 + 1\times1 = T_0 \cdot T_1 + T_1 \cdot T_0 = 2$.

$T_3 = 1\times2 + 1\times1 + 2\times1 = T_0 \cdot T_2 + T_1 \cdot T_1 + T_2 \cdot T_0 = 5$.

$T_4 = \cancel{5} \; 1\times5 + 1\times2 + 2\times1 + 5\times1 = T_0 \cdot T_3 + T_1 \cdot T_2 + T_2 \cdot T_1 + T_3 \cdot T_0 = 14$

$\Rightarrow T_n = T_0 \cdot T_{n-1} + T_1 \cdot T_{n-2} + \cdots + T_{n-2} \cdot T_1 + T_{n-1} \cdot T_0$

$= \sum_{i=1}^{n} T_{i-1} \cdot T_{n-i} \quad (T_0 = 1)$.

(2) Let $f(x) = \sum_{i=0}^{\infty} T_i \cdot x^i = T_0 + T_1 \cdot x + T_2 \cdot x^2 + T_3 \cdot x^3 + \cdots$

$$= T_0 + T_1 \cdot x + (T_0 \cdot T_1 + T_1 \cdot T_0) x^2 + (T_0 \cdot T_2 + T_1 \cdot T_1 + T_2 \cdot T_0) \cdot x^3 + \cdots$$

$$f^2(x) = (T_0 + T_1 x + T_2 x^2 + \cdots) \cdot (T_0 + T_1 x + T_2 x^2 + \cdots).$$

$$= T_0 + (T_0 \cdot T_1 + T_1 \cdot T_0) x + (T_0 \cdot T_2 + T_1 \cdot T_1 + T_2 \cdot T_0) x^2 + \cdots$$

$$= T_1 + T_2 \cdot x + T_3 \cdot x^2 + \cdots$$

$$= \sum_{i=0}^{\infty} T_{i+1} \cdot x^i.$$

Then we find that $f^2(x) = \dfrac{f(x) - 1}{x}$.

$$\Rightarrow x \cdot f^2(x) - f(x) + 1 = 0.$$

Solve. ~~solve~~ for $f(x)$, get $f(x) = \dfrac{1 - \sqrt{1-4x}}{2x}$.

$$f(x) = -\frac{1}{2x}\left((1-4x)^{\frac{1}{2}} - 1 \right) = -\frac{1}{2x} \cdot \left(\sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} \cdot (-4x)^n - 1 \right).$$

$$= -\frac{1}{2x}\left(\sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n+1} (-4x)^{n+1} \right).$$

$$= \sum_{n=0}^{\infty} \underbrace{\left(-\frac{1}{2}\right) \cdot (-4)^{n+1} \binom{\frac{1}{2}}{n+1}}_{(*)} \cdot x^n$$

Prove that $(*) = \dfrac{1}{n+1}\dbinom{2n}{n}$.

$$\frac{1}{n+1}\binom{2n}{n} = \frac{(-4)^n}{n+1}\binom{-\frac{1}{2}}{n} = 2 \cdot (-4)^n \cdot \binom{\frac{1}{2}}{n+1}.$$

$$= \left(-\frac{1}{2}\right) \cdot (-4)^{n+1} \cdot \binom{\frac{1}{2}}{n+1} = (*).$$

Thus, we get $T_n = \dfrac{1}{n+1}\dbinom{2n}{n}$.

5. (*20 points*) Consider the linear congruence

$$17x \equiv 9 \pmod{276}$$

(a) Show that this congruence has a unique solution.

(b) Show that the given congruence and the following system have the same solution.

$$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases}$$

(c) Solve the original congruence without assistance of calculator.

(a). Proof: Since $276 = 4 \times 3 \times 23$.., then ~~$17x \equiv 9 (276)$~~.

$17x \equiv 9 \pmod{276}$ can be treated as

① $17x \equiv 9 \pmod 4$. ② $17x \equiv 9 \pmod 3$ ③ $17x \equiv 9 \pmod{23}$

① $\Rightarrow$ $17x \equiv$ ~~$1 \pmod 4$~~ $1 \pmod 4$.

$\Rightarrow$. $x \equiv 1 \pmod 4$. ------ (1)

② $\Rightarrow$ $17x \equiv 0 \pmod 3$

$\Rightarrow$ $2x \equiv 0 \pmod 3$

$\Rightarrow$ $x \equiv 0 \pmod 3$ ---- (2)

③ $\Rightarrow$ $17x \equiv 9 \pmod{23}$. $17 \cdot 19 \equiv 1 \pmod{23}$

$x \equiv 171 \pmod{23}$

$x \equiv 10 \pmod{23}$ ---- (3).

~~By~~. Congruence (1).(2).(3). and 3, 4, 23 are mutually coprime, by Chinese Remainder Theorem.

$17x \equiv 9 \pmod{276}$ has a unique solution.

(b) By steps in (a), we have.

$$17x \equiv 9 \pmod{276} = \begin{cases} 17x \equiv 9 \pmod{3} \\ 17x \equiv 9 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases}$$

$17x \equiv 9 \pmod{3} \iff x \equiv 0 \pmod{3}$

$17x \equiv 9 \pmod{4} \iff x \equiv 1 \pmod{4}$

$17x \equiv 9 \pmod{23}$ keep.

Thus, $17x \equiv 9 \pmod{276}$ ~~have~~ has the same solution as

$$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases}$$

(c) Let $x = 4\cdot 3\cdot a + 4\cdot 23\cdot b + 3\cdot 23\cdot c$.

$\Rightarrow 12a \equiv 10 \pmod{23}$

$a \equiv 20 \pmod{23}$

$\Rightarrow 92b \equiv 0 \pmod{3}$

$2b \equiv 0 \pmod{3}$

$b \equiv 0 \pmod{3}$

$\Rightarrow 69c \equiv 1 \pmod{4}$

$c \equiv 1 \pmod{4}$

we can get $x \equiv 12\cdot 20 + 92\cdot 0 + 69\cdot 1 \pmod{276}$

$\equiv 33 \pmod{276}$.

6. (*10 points*) [**bonus question**] *"A computer is to a number theorist, like a telescope is to an astronomer. It would be a shame to teach an astronomy class without touching a telescope; likewise, it would be a shame to teach this class without telling you how to look at the integers through the lens of a computer."* - **William Stein, Number Theorist**

Consider a *perfect number*, defined as a positive integer n such that it is equal to the sum of all its positive divisors, excluding n itself. Denoting the sum of positive divisors of n by $\sigma(n)$, then a perfect number has the property that

$$\boxed{\sigma(n) - n = n}$$

Denoting the k-th perfect number by P_k, we have

$$P_1 = 6,\ P_2 = 28,\ P_3 = 496,\ P_4 = 8128$$

Based on the above patterns, there were some early conjectures regarding perfect numbers:

A. the n-th perfect number contains exactly n digits; and

B. the even perfect numbers end, alternately, in 6 and 8; and

C. there is no odd perfect number.

By means of a computer program, disprove the first two of these conjectures by finding and examining the fifth and the sixth perfect number. The third conjecture remains an open problem.

(Note: You will need to provide pseudocodes, and you may just concentrate on disproving (A) by actually running your program.)

A. B. Pseudocodes:

set perfect list as an empty list.

loops while length of list < 2.

for each # n > P4 (8128).

set initial sum = 0.

for each # k in (1, ..., n-1).

If k | n, then add k to sum.

Else, next k.

If sum = n, then append n to perfect list.

Else, next n.

After actually running the program,

we can find $p_5 = 33550336$, $p_6 = 8589869056$,

which disproves both A and B.

C. Maybe there is no odd perfect number.

An odd perfect number N must satisfy the following condition:

① $N > 10^{1500}$

② N is not divisible by 105.

③ N is of the form $N \equiv 1 \pmod{12}$ or $N \equiv 117 \pmod{468}$ or $N \equiv 81 \pmod{324}$

④ N is of the form $N = q^{\alpha} p_1^{2e_1} \cdots p_k^{2e_k}$.

where $q, p_1, \cdots p_k$ are distinct primes (Euler).

$q \equiv \alpha \equiv 1 \pmod 4$. (Euler).

① ② ③ ④ From Wiki.

And it is ~~known that~~ not known that if any odd perfect numbers exist.