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: _____ **Name:** _____

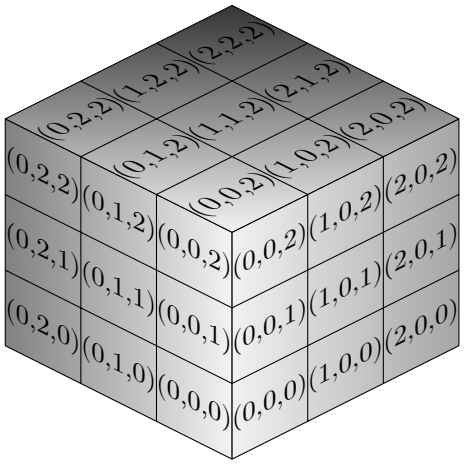
1. (*20 points*) Let p be an odd prime. Prove that there are exactly $\frac{p-1}{2}$ integers $a \in \{1, \ldots, p-1\}$ such that $x^2 \equiv a \pmod{p}$ for some x.

Proof. Let $x, y \in \{1, \ldots, p-1\}$ be distinct such that $x^2 \equiv a \equiv y^2 \pmod{p}$ for some a. Then

$$(x+y)(x-y) \equiv 0 \pmod{p} \quad \Rightarrow \quad x+y \equiv 0 \pmod{p} \quad \Rightarrow \quad y = p-x$$

If x is a solution to $x^2 \equiv a \pmod{p}$, then so is $p-x$. Thus, for each $a \in \{1, \ldots, p-1\}$, the equation $x^2 \equiv a \pmod{p}$ either has two solutions or no solutions. Hence, the result follows. □

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.)
Solution.

① If n is even, the unit cubes can be listed as follows:

$(0,0,0),\ldots,(0,0,n-1),(0,1,n-1),\ldots,(0,1,0),(0,2,0),\ldots,(0,2,n-1),\ldots,(0,n-1,0),$
$(1,n-1,0),\ldots,(1,n-1,n-1),(1,n-2,n-1),\ldots,(1,n-2,0),(1,n-3,0),\ldots,(1,0,0),$
$(2,0,0),\ldots,(3,0,0),\ldots,(n-1,0,0)$

② If n is odd, the unit cubes can be listed as follows:

$(0,0,0),\ldots,(0,0,n-2),(0,1,n-2),(0,1,n-3),\ldots,(0,1,0),(0,2,0),\ldots,(0,2,n-2),$
$(0,3,n-2),\ldots,(0,n-2,0),(0,n-1,0),\ldots,(0,n-1,n-1),\ldots,(0,0,n-1),$
$(1,0,n-1),\ldots,(1,n-2,n-1),(1,n-2,n-2),\ldots,(1,0,n-2),(1,0,n-3),\ldots,$
$(1,0,1),(1,0,0),\ldots,(1,n-1,0),\ldots,(1,n-1,n-1),$
$(2,n-1,n-1),\ldots,(2,n-1,0),(2,n-2,0),\ldots,(2,n-2,n-1),(2,n-3,n-1),\ldots,$
$(2,n-3,0),(2,n-4,0),\ldots,(2,0,0),(3,0,0),\ldots,(3,n-1,n-1),\ldots,(n-1,0,0)$

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.

Proof. For each $i \in S$ there exist $s,t \in \mathbb{Z}$ such that

$$i = sk + tn$$

We shall show that i,k are of the same color. There are three cases to consider:

$$\text{(a) } s<0,t>0 \qquad \text{(b) } s>0,t=0 \qquad \text{(c) } s>0,t<0$$

Case (a): we have i and $n-i = (-s)k + (1-t)n$ of the same color. If $t=1$, then the problem becomes (b); If $t>1$, then the problem becomes (c).
Case (b): by (2) we see that ball k has the same color as $2k$, and hence $3k,4k,\ldots,sk$.
Case (c): there are three cases between i and k.

(c1): if $i=k$, then we are done.

(c2): if $i>k$, then there exists $q \in \mathbb{Z}^+$ such that

$$i = qk + i' \qquad \text{where } i' \in \{0,1,\ldots,k-1\}$$

By (2) we have i have the same color as $i-k, i-2k,\ldots,i-qk$, so the problem reduces to (c3).

(c3): if $i < k$, then

$$k - i = (1 - s)k - tn \quad \Rightarrow \quad n - (k - i) = (s - 1)k + (t + 1)n$$

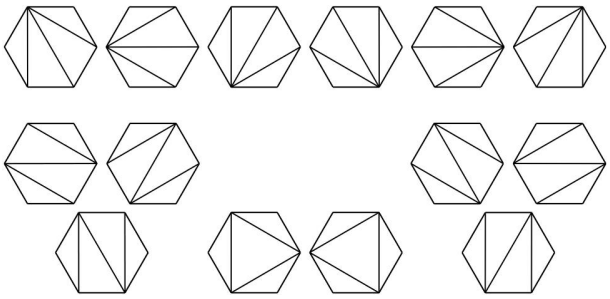
have the same color as i. Consider that

$$s > 0 \quad \Rightarrow \quad s - 1 > 0 \quad \Rightarrow \quad t + 1 \leq 0$$

If $t + 1 = 0$, then this returns to (b); if $t + 1 < 0$, then we can repeat the discussion of (c) on $n - (k - i)$ for at most $-t - 1$ times and conclude the result to (c1) or (b).

□

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.

Solution. Label the vertices of an $(n + 2)$-gon G_n clockwise by $\alpha, \beta, 1, \ldots, n$. For each cutting, α, β must connect to another vertex x so that there is a triangle (α, β, x). Set $T_0 = 1$.

① If $x = 1$, then there is an $(n + 1)$-gon needed to be cut, so the number of different cuttings is T_{n-1}.

② If $x = 2$, then G_n is bisected into a 3-gon and an n-gon, so the number of different cuttings is $T_1 T_{n-2}$.

⋮

ⓚ If $x = k$, then G_n is bisected into a $(k + 1)$-gon and an $(n - k + 2)$-gon, so the number of different cuttings is $T_{k-1} T_{n-k}$.

⋮

ⓝ If $x = n$, then there is an $(n + 1)$-gon needed to be cut, so the number of different cuttings is T_{n-1}.

Therefore, $T_n = \sum_{k=1}^{n} T_{k-1}T_{n-k}$.

Let $f(x) = T_0 + T_1x + \ldots + T_nx^n + \ldots$ be the generating function of $\{T_n\}$. Then

$$\begin{aligned}(f(x))^2 =&(T_0 + T_1x + \ldots + T_nx^n + \ldots)^2\\ =&T_0^2 + (T_0T_1 + T_1T_0)x + \ldots + \left(\sum_{k=1}^{n} T_{k-1}T_{n-k}\right)x^{n-1} + \ldots\\ =&T_1 + T_2x + \ldots + T_nx^{n-1} + \ldots\end{aligned}$$

Notice that $T_1 = 1 = T_0^2$, so

$$f(x) = T_0 + (T_1x + \ldots + T_nx^n + \ldots) = 1 + x\,(T_1 + T_2x + \ldots) = 1 + x(f(x))^2$$

Resolving $f(x)$ gives

$$f(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

Since $\lim_{x\to 0} f(x) = T_0 = 1$, we have

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

Thus,

$$T_n = \frac{1}{2(2n+1)}\binom{2n+2}{n+1} = \frac{1}{2(2n+1)}\cdot\frac{(2n+2)(2n+1)(2n)!}{(n+1)^2n!n!} = \frac{1}{n+1}\binom{2n}{n}$$

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.

Solution.

(a) Since 17 is prime, we have

$$\mathsf{gcd}(17, 276) = 1 \quad \Rightarrow \quad 17 \text{ has inverse modulo } 276$$

so the given congruence has a unique solution $x = 17^{-1} \cdot 9 \pmod{276}$.

(b) Note that $276 = 3 \cdot 4 \cdot 23$, by Chinese Remainder Theorem the given congruence is equivalent to the system

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

(c) From the first congruence, we have $x = 3k$ for some $k \in \mathbb{Z}$. Substituting into the second congruence we obtain

$$3k \equiv 1 \pmod 4$$

Multiplying both sides by 3 gives

$$k \equiv 9k \equiv 3 \pmod 4 \quad \Rightarrow \quad k = 3 + 4j$$

for some $j \in \mathbb{Z}$. Then

$$x = 3(3 + 4j) = 9 + 12j$$

Fitting this in the last congruence, we have

$$17(9 + 12j) \equiv 9 \pmod{23} \quad \Rightarrow \quad 204j \equiv -144 \pmod{23}$$

which can be reduced to

$$3j \equiv 6 \pmod{23} \quad \Rightarrow \quad j \equiv 2 \pmod{23}$$

This gives $j = 2 + 23i$ for some $i \in \mathbb{Z}$, hence

$$x = 9 + 12(2 + 23i) = 33 + 276i \quad \Rightarrow \quad x \equiv 33 \pmod{276}$$

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

$$\sigma(n) - n = n$$

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.)

Solution.

Sample Pseudocode (May be optimized in various ways)

Initialize $n = 8128$,
Initiailize $A = 0$,
Initialize $B = 1$,
Initialize $m = 2$,
while $A < m$ **do**
    $n \leftarrow n + 1$
      for k=2 to $n - 1$ **do**
        if $k \mid n$ **then**
          $B \leftarrow B + k$
      if $B = n$ **then**
        $B = 1$
        output n
        $A \leftarrow A + 1$
      else $B = 1$

Through systematic exhaustive evaluation, it can be shown that

$$P_5 = 33,550,336, \;\; P_6 = 8,589,869,056$$

Hence, there is no 5-digit perfect number (in your program, it is sufficient just to show that there is no 5-digit perfect number, since finding the fifth and sixth perfect number would take some time). In the fifth and sixth perfect numbers, while they end in 6, they do not alternate with 8.

In general, we have the following theorem by Euler:

If $2^k - 1$ is prime ($k > 1$), then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.

A prime of the form $2^k - 1$ is known as a *Mersenne prime*.

The third conjecture remains unanswered, but it has been found that any odd perfect number P must be greater 10^{1500} - trying to discover it (if it exists) will take up a lot of computing time, showing again that a computer is highly essential to a number theorist.