DISCRETE MATHEMATICS

GABRIEL MOISE

MT 2018

PROBLEM SHEET 4

Chapters 6 (Modular Arithmetic) and 7 (Asymptotic Notation)

$\boxed{4.1}$

$0^3 = 0 \equiv 0 \pmod 7$

$1^3 = 1 \equiv 1 \pmod 7$

$2^3 = 8 \equiv 1 \pmod 7$

$3^3 = 27 \equiv 6 \pmod 7$

$4^3 = 64 \equiv 1 \pmod 7$

$5^3 = 125 \equiv 6 \pmod 7$

$6^3 = 216 \equiv 6 \pmod 7$

Any other $x \in \mathbb{Z}$ can be written as $y + 7z$, where $y \in \{0,1,2,3,4,5,6\}$ and $z \in \mathbb{Z}$, where basically $z = x \text{ DIV } 7$, $y = x \text{ MOD } 7$. Therefore $x^3 \equiv (y+7z)^3 \pmod 7$

$x^3 \equiv (y^3 + 21y^2z + 147z^2 + 343z^3) \pmod 7$

$x^3 \equiv y^3 \pmod 7$

So, $\{x^3 \pmod 7 \mid x \in \mathbb{Z}\} = \{0,1,6\}$

Let's assume that there exists an $n \in \mathbb{Z}$, such that $n \equiv \pm 3 \pmod 7$ and n can be written as the sum of two integer cubes.

So, there are some $x, y \in \mathbb{Z}$ such that $n = x^3 + y^3 \Rightarrow n \equiv (x^3 + y^3) \bmod 7$, or

$n \equiv (x^3 \pmod 7) + y^3 \pmod 7)) \pmod 7$

Now, from above, we know that $x^3 \pmod 7$ and $y^3 \pmod 7 \in \{0,1,6\} \Rightarrow$

$\Rightarrow x^3 \pmod 7 + y^3 \pmod 7 \in \{0,1,6,2,7,12\} \Rightarrow (x^3 \pmod 7) + y^3 \pmod 7)) \bmod 7 \in \{0,1,2,5,6\} \Rightarrow$

$\Rightarrow n \pmod 7 \in \{0,1,2,5,6\}$

But, we stated that $n \equiv \pm 3 \pmod 7 \Rightarrow n \pmod 7 \in \{3,4\}$ $\Big| \Rightarrow$ Contradiction

Therefore, an integer n cannot be written as the sum of two integer cubes if $n \equiv \pm 3 \pmod 7$

<u>Converse</u>: If an integer n cannot be written as the sum of two integer cubes, then $n \equiv \pm 3 \pmod 7$

<u>Counterexample</u>: $n = 6$ cannot be written as a sum of two integer cubes, as all integer cubes $\in \{x^3 \mid x \in \mathbb{Z}\} = \{\ldots; -27; -8; -1; 0; 1; 8; 27; \ldots\}$ and we cannot find two which have the sum equal to 6. Moreover, $6 \equiv 1 \pmod 7$, therefore $n \not\equiv \pm 3 \pmod 7$.

$\boxed{4.2}$ We want to prove that $\gcd(m,n) = \gcd(n-km, m)$ for all $k \in \mathbb{N}$.
First, let $g = \gcd(m,n)$. Therefore, from the definition of $\gcd(m,n)$, we have:
1. $g \mid m$
2. $g \mid n$
3. if $l \mid m$ and $l \mid n \Rightarrow l \mid g$

Now, we will prove the following:
(i) $g \mid n-km$

From 1., we know that $g \mid m \Rightarrow m \equiv 0 \pmod g \Rightarrow mk \equiv 0 \pmod g$ $(\forall) k \in \mathbb{N} \Rightarrow$

$$\left.\begin{array}{l} \Rightarrow g \mid km \Rightarrow g \mid (-km) \\ \text{From 2., } g \mid n \end{array}\right| \Rightarrow g \mid n-km$$

(ii) $g \mid m$, which we know it is true from 1.
(iii) if $l \mid n-km$ and $l \mid m \Rightarrow l \mid g$

$$\left.\begin{array}{l} l \mid n-km \\ l \mid m \Rightarrow l \mid km \end{array}\right| \Rightarrow \left.\begin{array}{l} l \mid n \\ l \mid m \end{array}\right| \overset{3.}{\Rightarrow} l \mid g$$

From (i), (ii) and (iii) we conclude that $g = \gcd(n-km, m) \Rightarrow \gcd(m,n) = \gcd(n-km, m)$.

$\boxed{4.3}$ Let $n > 0$ be a fixed modulus.
We want to prove that

$m \in \mathbb{Z}_n$ has a multiplicative inverse (i.e. $(\exists) m'$ such that $mm' \equiv 1 \pmod n$) $\Leftrightarrow \gcd(m,n) = 1$

"$\Rightarrow$": We know that there is an m' such that $mm' \equiv 1 \pmod n \Rightarrow$

$\Rightarrow mm' = nk+1$, with $k \in \mathbb{Z}$ (*)

Let's say that there is a g which divides both n and m (g always exists). Then:

$$\left.\begin{array}{l} g \mid m \Rightarrow g \mid mm' \overset{(*)}{\Rightarrow} g \mid nk+1 \\ g \mid n \Longrightarrow g \mid nk \end{array}\right| \overset{(-)}{\Rightarrow} g \mid \cancel{nk}+1-\cancel{nk}$$

$$\left.\begin{array}{l} g \mid 1 \\ g \in \mathbb{N}_+ \end{array}\right| \Rightarrow g = 1 \Rightarrow \text{the only } g \text{ that divides}$$

both m and n is $1 \Rightarrow \gcd(m,n) = 1$

"$\Leftarrow$": $\gcd(m,n) = 1 \Rightarrow$ (from Euclid's Extended Algorithm) $(\exists) x, y \in \mathbb{Z}$ such that

$$mx + ny = 1 \Rightarrow mx = 1 - ny \Rightarrow mx \equiv (1-ny) \pmod n \Rightarrow$$

$\Rightarrow mx \equiv 1 \pmod n$, so we found the multiplicative inverse of m, which is x.

Let $a \in \mathbb{Z}_{12}$. From above, a has a multiplicative inverse in $\mathbb{Z}_{12}$ if and only if $\gcd(a,12) = 1$.

Therefore, $a \in \{1,5,7,11\}$ (the only values from $\mathbb{Z}_{12}$ that satisfy the property) $\Rightarrow$ 4 elements

$\boxed{4.4}$ Let $a_1, a_2, \dots, a_n$ be a sequence of n integers (not necessarily distinct).

We want to prove that there are some l, m such that $1 \leq l \leq m \leq n$ and

$$\sum_{i=l}^{m} a_i \equiv 0 \pmod n.$$

First of all, we create the sequence $S_0, S_1, S_2, \dots, S_n$ with $S_0 = 0$ and

$$S_j = \sum_{i=1}^{j} a_i \text{ , with } j \in \{1,2,3,\dots,n\}.$$

Now, $\sum_{i=l}^{m} a_i = \sum_{i=1}^{m} a_i - \sum_{i=1}^{l-1} a_i = S_m - S_{l-1}$ (if $l=1$, then $\sum_{i=1}^{l-1} a_i = S_0 = 0$).

We have $(n+1)$ terms in the sequence (S_i), $i \in \{0,1,2,\dots,n\}$ and we have n equivalence classes for $\mathbb{Z}$: $[0], [1], \dots, [n-1]$ Using <u>the Pigeonhole Principle</u>, we deduce that at least one equivalence class contains two terms of the sequence (S_i) (it can contain more, but we are only interested in two of them). Let's say S_a and S_b are in the equivalence class $[k]$, with $a, b \in \{0,1,2,\dots,n\}$ and $k \in \{0,1,2,\dots,n-1\}$, and $a > b$ (we can order them), therefore $a \geq 1$, $b < n$.

Then, $\left.\begin{array}{l} S_a \equiv k \pmod n \\ S_b \equiv k \pmod n \end{array}\right| \overset{(-)}{\Rightarrow} S_a - S_b \equiv 0 \pmod n$

But, $S_a - S_b = \sum_{i=b+1}^{a} a_i$. So, by choosing $m = a$, $l = b+1$, we found l and m with $1 \leq l \leq m \leq n$ such that $\sum_{i=l}^{m} a_i \equiv 0 \pmod n$.

$\boxed{4.5}$ (i) $n^{\log_2 3} = O(n^2)$ if $(\exists)\, c \in \mathbb{R}$ and $N \in \mathbb{N}$ with

$$|n^{\log_2 3}| \leq c|n^2| \text{ for all } n \geq N$$

As $n^{\log_2 3} \geq 0$ and $n^2 \geq 0$, we write $n^{\log_2 3} \leq cn^2$

Now, $\log_2 3 \leq \log_2 4 = 2 \Rightarrow n^{\log_2 3} \leq n^{\log_2 4} = n^2$ for all $n \geq 1$, therefore we choose $N = 1$ and $c = 1 \Rightarrow n^{\log_2 3} = O(n^2)$ is <u>TRUE</u>.

(ii) $n + 2n^2 + 3n^3 + 4n^4 = O(n^4)$

For $n \geq 1$, we have $\left.\begin{array}{l} n \leq n^4 \\ n^2 \leq n^4 \Rightarrow 2n^2 \leq 2n^4 \\ n^3 \leq n^4 \Rightarrow 3n^3 \leq 3n^4 \end{array}\right| \Rightarrow n + 2n^2 + 3n^3 + 4n^4 \leq n^4 + 2n^4 + 3n^4 + 4n^4 = 10n^4$

So, if we choose $N=1$ and $c=10 \Rightarrow n+2n^2+3n^3+4n^4 = O(n^4)$ is TRUE.

(iii) $\sqrt{n^2+n\log n} = O(n)$

We claim that

$$\sqrt{n^2+n\log n} \leq 2n, \text{ for all } n \geq 1$$

$$\sqrt{n^2+n\log n} \leq 2n \quad \Big| ()^2$$

$$n^2+n\log n \leq 4n^2 \quad \Big| -n^2$$

$$n\log n \leq 3n^2 \quad \Big| : n \neq 0$$

$\log n \leq 3n$, which is true for all $n \geq 1$, so if we choose $c=2$ and $N=1 \Rightarrow$

$\Rightarrow \sqrt{n^2+n\log n} = O(n)$ is TRUE

(iv) $n^{\log n} = O(n^2)$

Let's suppose that there exists real number c and an integer N with

$$n^{\log n} \leq cn^2 \text{ (we work with positive-valued functions) for all } n \geq N.$$

$$n^{\log n - 2} \leq c$$

However $n^{\log n - 2} \to \infty$ as $n \to \infty$, therefore $n^{\log n-2}$ cannot be bounded by a real number c, so we reach a contradiction.

Hence, the statement $n^{\log n} = O(n^2)$ is FALSE.

Now, let $b>1$ be a constant. We want to find for which values of a it is true that

$$n^a = O(b^n).$$

CASE 1: $a<0$

Then, $n^a \leq 1$ for $n \geq 1$ and as $b>1$, then $b^n > 1$ for $n \geq 1 \Rightarrow n^a \leq n^b$

By choosing $N=1$ and $c=1$ we obtained

$$n^a \leq cb^n \text{ for all } n \geq N \Rightarrow n^a = O(n^b)$$

CASE 2: $a=0$

Then $n^a = 0 \leq b^n$ for all $n \geq 1 \Rightarrow$ by choosing $N=1$ and $c=1$ we obtained

$$n^a \leq cb^n \text{ for all } n \geq N \Rightarrow n^a = O(n^b)$$

number that depends on a

CASE 3: $a > 0$

We want to prove that for all $a>0$, there exists an $N(a) \in \mathbb{Z}$ such that

$$n^a \leq b^n \ (\forall)\, n \geq N(a) \quad \text{(here we chose } c=1)$$

$n^a \leq b^n \mid \log()$

$\log(n^a) \leq \log(b^n)$

$a \log n \leq n \log b$

$\frac{\log n}{n} \leq \frac{\log b}{a}$

We use the following:

Lemma: $\lim_{n \to \infty} \frac{\log n}{n} = 0.$

This can be easily proven by using L'Hôpital's rule:

$$\lim_{n\to\infty} \frac{\log n}{n} = \lim_{n\to\infty} \frac{(\log n)'}{n'} = \lim_{n\to\infty} \frac{1}{n} = 0.$$

By using the definition of the limit of a sequence (in our case the sequence $a_n = \frac{\log n}{n}$, where $\lim_{n\to\infty} a_n = 0$), we get:

$(\forall)\ \varepsilon > 0\ (\exists)\ N(\varepsilon) \in \mathbb{N}_+$ such that $(\forall)\ n \geq N(\varepsilon)$ we have $\left| \frac{\log n}{n} \right| < \varepsilon$ (as $\frac{\log n}{n} \geq 0$, for $n \geq 1$ we can use $\frac{\log n}{n} < \varepsilon$ instead)

So, if we take $\varepsilon = \frac{\log b}{a}$ and use the definition above, we get that there exists an $N(\varepsilon) = N\left(\frac{\log b}{a}\right)$ (and as b is a constant $\Rightarrow$ log b is a constant $\Rightarrow$ N depends only on a, so we can use $N(a)$ instead) such that $(\forall)\ n \geq N(a)$ we have $\frac{\log n}{n} < \varepsilon = \frac{\log b}{a}$.

Therefore, we proved the existence of $N(a) \in \mathbb{Z}$ and $c=1$, therefore

$$n^a = O(b^n).$$

From Case 1, Case 2 and Case 3 we draw the conclusion that $(\forall)\ a \in \mathbb{R}$ we have

$$n^a = O(b^n) \text{ is } \underline{\text{TRUE}}.$$

$\boxed{4.6}$ We consider the recurrence relation:

$$x_0 = 0$$
$$x_m = x_{\lfloor \frac{n}{3} \rfloor} + 3\, x_{\lfloor \frac{n}{5} \rfloor} + m, \quad \text{for } m \geq 1$$

We want to prove that $x_m = O(m)$.

We will do that by strong induction on m (Let $P(n)$: $x_m \leq cm$, where c will be determined)

<u>Base Case</u>: $P(0)$: $x_0 \leq c \cdot 0$

$0 \leq c \cdot 0$ YES

<u>Inductive Step</u>:

<u>Inductive Hypothesis</u>:

We assume that for all $i \in \{0, 1, 2, \dots, m\}$ $P(i)$ is true i.e. $x_i \leq ci$ and we want to prove that $P(n+1)$: $x_{n+1} \leq c(n+1)$ is also true.

From the definition of the sequence we get:

$$x_{n+1} = x_{\lfloor \frac{n+1}{3} \rfloor} + 3\, x_{\lfloor \frac{n+1}{5} \rfloor} + (n+1)$$

Now, we know that $\lfloor \frac{n+1}{3} \rfloor, \lfloor \frac{n+1}{5} \rfloor \in \{0, 1, 2, \dots, m\} \overset{IH}{\Rightarrow} P(\lfloor \frac{n+1}{3} \rfloor)$ and $P(\lfloor \frac{n+1}{5} \rfloor)$ are true, so

$x_{\lfloor \frac{n+1}{3} \rfloor} \leq c \lfloor \frac{n+1}{3} \rfloor$ and $x_{\lfloor \frac{n+1}{5} \rfloor} \leq c \lfloor \frac{n+1}{5} \rfloor$

Hence, $x_{n+1} \leq c \lfloor \frac{n+1}{3} \rfloor + 3c \lfloor \frac{n+1}{5} \rfloor + (n+1)$

Now, we use the fact that $\lfloor \frac{n+1}{3} \rfloor \leq \frac{n+1}{3}$ and $\lfloor \frac{n+1}{5} \rfloor \leq \frac{n+1}{5}$ to obtain

$$x_{n+1} \leq c\,\frac{n+1}{3} + 3c\,\frac{n+1}{5} + (n+1) = (n+1)\left(\overset{5}{\frac{c}{3}} + \overset{3}{\frac{3c}{5}} + 1\right) = (m+1)\left(\frac{14c}{15} + 1\right)$$

We want to find the $c \in \mathbb{R}$ for which $x_{n+1} \leq c(n+1)$.

By solving the inequality $(n+1)\left(\frac{14c}{15} + 1\right) \leq c(n+1)$, we obtain that

$$\cancel{(n+1)}\left(\frac{14c}{15} + 1\right) \leq c\,\cancel{(n+1)}$$
$$\frac{14c}{15} + 1 \leq c$$
$$1 \leq \frac{c}{15}$$
$$15 \leq c$$

So, by choosing $\boxed{c = 15}$ we get that $x_{n+1} \leq c(m+1) \Rightarrow P(n)$ is true for all $n \geq 0 \Rightarrow$

$\Rightarrow x_m \leq 15m \ (\forall)\ m \in \mathbb{N} \Rightarrow x_m = O(m)$.

$\boxed{4.7}$ Let's suppose that $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$

We want to prove that $f_1(n)\, f_2(n) = O(g_1(n)\, g_2(n))$.

$f_1(n) = O(g_1(n)) \Rightarrow (\exists)\ c_1 \in \mathbb{R}$ and $N_1 \in \mathbb{Z}$ such that $|f_1(n)| \leq c_1 |g_1(n)|$ for all $n \geq N_1$ ①

$f_2(n) = O(g_2(n)) \Rightarrow (\exists)\ c_2 \in \mathbb{R}$ and $N_2 \in \mathbb{Z}$ such that $|f_2(n)| \leq c_2 |g_2(n)|$ for all $n \geq N_2$ ②

Now,

$$|f_1(n) f_2(n)| \overset{\text{property of the module}}{=} |f_1(n)| \cdot |f_2(n)| \overset{\text{① and ②}}{\leq} c_1 |g_1(n)| \cdot c_2 |g_2(n)| \text{ for all } n \geq N_1 \text{ and } n \geq N_2$$

Continuing the reasoning we get

$$c_1 |g_1(n)| \cdot c_2 |g_2(n)| = (c_1 \cdot c_2)\, |g_1(n)| \cdot |g_2(n)| \overset{\text{property of the module}}{=} (c_1 \cdot c_2)\, |g_1(n) \cdot g_2(n)|$$

So, we obtained that

$|f_1(n) \cdot f_2(n)| \leq (c_1 \cdot c_2)\, |g_1(n) \cdot g_2(n)|$ for all $n \geq N_1$ and $n \geq N_2$, which can be written as:

$|f_1(n) f_2(n)| \leq c\, |g_1(n) g_2(n)|$ for all $n \geq N$, where $\boxed{c = c_1 c_2}$ and $\boxed{N = \max\{N_1, N_2\}}$.

Therefore, we can conclude that $f_1(n) f_2(n) = O(g_1(n)\, g_2(n))$.

Now, we choose $f_1(n) = n^3$, $g_1(n) = n^3 \Rightarrow f_1(n) = O(g_1(n))$, obviously and $f_2(n) = n$, $g_2(n) = n^2 \Rightarrow f_2(n) = O(g_2(n))$, obviously.

However, $\dfrac{f_1(n)}{f_2(n)} = \dfrac{n^3}{n} = n^2$ and $\dfrac{g_1(n)}{g_2(n)} = n$ and since $n^2 \neq O(n)$, we conclude that the statement $\dfrac{f_1(n)}{f_2(n)} = O\left(\dfrac{g_1(n)}{g_2(n)}\right)$ is not true for all functions f_1, f_2, g_1, g_2 which have $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$.