UM-SJTU JOINT INSTITUTE
DISCRETE MATHEMATICS
(VE203)

ASSIGNMENT 7

Name: Pan Chongdan
ID: 516370910121

Date: November 23, 2017

1 Q1

Assume A only contains finite n prime numbers such as $p(1) = 3, p(2) = 7 \cdots p(n)$. Then assume $Q = 4 \cdot p(1) \cdot p(2) \cdots p(n) + 3 \in A$. It's clear that Q is odd and its divisor can be $4k+1$ because $(4k_1+1) \cdot (4k_2+1) = 4(4k_1k_2 + k_1 + k_2) + 1 \notin A$ So the only divisor of Q is 1 and itself, which means Q is another prime, so A contains infinity primes.

2 Q2

Assume $g = gcd(c, m), m = xg, c = yg \Rightarrow \frac{m}{g} = x$
$ac \equiv bc \mod m \Rightarrow ayg = byg + kxg \Rightarrow a \equiv b + \frac{k}{y}x$
$a - b \in \mathbb{Z} \Rightarrow \frac{kx}{y} \in \mathbb{Z}$
If $\frac{k}{y} \in \mathbb{Z} \Rightarrow a \equiv b \mod x$, else $\frac{x}{y} \in \mathbb{Z} \Rightarrow g \neq gcd(c, m)$
$\therefore a \equiv b \mod \frac{m}{gcd(c,m)}$

3 Q3

We can solve the equation by solve

$$75 = 36x + 1309y$$

$$1309 = 36 \cdot 36 + 13$$
$$36 = 2 \cdot 13 + 10$$
$$13 = 10 + 3$$
$$10 = 3 \cdot 3 + 1$$
$$1 = -11 \cdot 1309 + 400 \cdot 36$$
$$75 = -825 \cdot 139 + 30000 \cdot 36$$
$$\therefore x = 30000$$

4 Q4

$$2x \equiv 4 \mod 5 \Rightarrow 6x \equiv 12 \mod 15$$
$$3x \equiv 5 \mod 7 \Rightarrow 6x \equiv 10 \mod 14$$
$$\therefore 6x \equiv 192 \mod 210 \Rightarrow 7x \equiv 224 \mod 245$$
$$\because 7x \equiv 2 \mod 13 \Rightarrow 7x \equiv 1939 \mod 3185$$
$$\therefore x \equiv 277 \mod 455$$

5 Q5

$$x \equiv 5 \mod 6 \land x \equiv 8 \mod 15 \Rightarrow x \equiv 23 \mod 30$$
$$\because x \equiv 3 \mod 10 \Rightarrow x \equiv 23 \mod 30$$
$$\therefore x = 23 \mod 30$$

6 Q6

$$x \equiv 5 \mod 5 \land x \equiv 3 \mod 7 \Rightarrow x \equiv 10 \mod 35$$
$$x \equiv 8 \mod 11 \land x \equiv 2 \mod 17 \Rightarrow x \equiv 19 \mod 187$$
$$x \equiv 1515 \mod 6545$$

7 Q7

Assume $f = n\log_2(n), g = \log_2(n), f$ is $O(g) \Rightarrow |n\log_2(n)| \leq C|\log_2(n)|$ if $n \neq 1 \Rightarrow |n| \leq C \Rightarrow C$ doesn't exist since n can be any number.

8 Q8

They're all order $\log_2 n$, it's clear that $|\log_2 n| \leq |\log_2 n|$

$$|\log_{10} n| = |\frac{\log_2 n}{\log_2 10}| \leq |\log_2 n|$$

$$|\log_2 n| = |\frac{\log_{10} n}{\log_{10} 2}| \leq 4|\log_{10} n|$$

$\therefore \log_{10} n$ is order $\log_2 n$, similarly:

$$|\ln n| = |\frac{\log_2 n}{\log_2 e}| \leq |\log_2 n|$$

$$|\log_2 n| = |\frac{\ln n}{\ln 2}| \leq 2|\ln n|$$

$\therefore$ they have the same order $\log_2 n$

9 Q9

(i)

$$\frac{1}{n}=\int_{n-1}^{n}\frac{1}{n}\mathrm{d}x\Rightarrow\frac{1}{n}<\int_{n-1}^{n}\frac{1}{x}\mathrm{d}x\Rightarrow\sum_{j=2}^{n}\frac{1}{j}<\int_{2-1}^{2}\frac{1}{x}\mathrm{d}x+\cdots\int_{n-1}^{n}\frac{1}{x}\mathrm{d}x=\int_{1}^{n}\frac{1}{x}\mathrm{d}x$$

(ii)

$$H(n)=\frac{1}{n}+\frac{1}{n-1}\cdots+\frac{1}{1}=1+\sum_{j=2}^{n}\frac{1}{j}<1+\int_{1}^{n}\frac{1}{x}\mathrm{d}x=1+\ln(n)$$

$$\therefore\lim_{n\to\infty}|\frac{H(n)}{\ln(n)}|<\lim_{n\to\infty}|\frac{1}{\ln(n)}+1|=1$$

$$\frac{1}{n}=\int_{n}^{n+1}\frac{1}{n}\mathrm{d}x\Rightarrow\frac{1}{n}>\int_{n}^{n+1}\frac{1}{x}\mathrm{d}x\Rightarrow H(n)>\int_{1}^{n}\frac{1}{x}\mathrm{d}x=\ln(n)\Rightarrow\lim_{n\to\infty}|\frac{H(n)}{\ln(n)}|>1$$

$$\therefore\lim_{n\to\infty}|\frac{H(n)}{\ln(n)}|=1$$

$\therefore H(n)$ is $O(\ln(n))$

10 Q10

$$\lfloor x^3-4\rfloor=x^3-y-4(0\leq y<1)$$

$$\lim_{x\to\infty}\frac{\lfloor x^3-4\rfloor}{|x^3|}=\lim_{x\to\infty}1+|\frac{y+4}{x^3}|=1(0\leq y+4<5)$$

$\therefore\lfloor x^3-4\rfloor$ is $O(x^3)$

$$\lim_{x\to\infty}\frac{|x^3|}{\lfloor x^3-4\rfloor}=\lim_{x\to\infty}=|\frac{x^3}{x^3-y-4}|=|1+\frac{y+4}{x^3-y-4}|=|1|$$

$\therefore\lfloor x^3-4\rfloor$ is order x^3

11 Q11

$$\lim_{n\to\infty}\frac{|n^{n-k}|}{|n^n|}=\lim_{n\to\infty}\frac{1}{|n^k|}=0$$

$\therefore n^{n-k}$ is $O(n^n)$, if n^n is $O(n^{n-k})$ then there exists C such that $\forall n,|n^n|\leq C|n^{n-k}|$

$$\therefore\forall n\in\mathrm{dom},k>1,C\geq|n^k|$$

$\therefore$ if the two functions' domain has both upper bound a and lower bound b than $C\geq\max(|a^k|,|b^k|)$, otherwise, such as the domain is $\mathbb{R}$ or $\mathbb{N}$ they don't have the same order.