DETAILED SOLUTIONS

Q1]. . . [15 points] Find three consecutive positive integers which are divisible by 2^2, 3^2 and 5^2 respectively. Hint: If we denote the consecutive integers by x, $x+1$ and $x+2$ respectively, then the divisibility conditions can be written as $x \equiv 0 \mod 4$, $x+1 \equiv 0 \mod 9$ and $x+2 \equiv 0 \mod 25$. This rewrites as the following system of congruences:

$$\begin{aligned} x &\equiv 0 && \mod 4 \\ x &\equiv -1 && \mod 9 \\ x &\equiv -2 && \mod 25 \end{aligned}$$

Find a positive integer simultaneous solution to these congruences, and hence solutions to the original problem.

Solve $9(25)x_1 \equiv 1 \mod 4$

$x_1 \equiv 1 \mod 4$ $\quad x_1 = 1$

Solve $4(25)x_2 \equiv 1 \mod 9$

$x_2 \equiv 1 \mod 9$ $\quad x_2 = 1$

Solve $4(9)\,x_3 \equiv 1 \mod 25$

$11x_3 \equiv 1 \mod 25$ $\quad 4(25) - 9(11) = 1$

$x_3 = -9$

Chinese Remainder Th^{m}

$$\begin{aligned} x &= (1)(9)(25)(0) + (1)(4)(25)(-1) + (-9)(4)(9)(-2) \\ &= -100 + 648 \\ &= 548 \end{aligned}$$

$$\begin{array}{r} 81 \\ 8 \\ \hline 648 \end{array}$$

$\boxed{x = 548}$ $\boxed{x+1 = 549}$ $\boxed{x+2 = 550}$ are (the) 3 consecutive (+) integers which are divisible by 4, 9, 25 respectively.

Q2]... [10 points] Prove that there are *arbitrarily long* strings of consecutive integers $x, x+1, \ldots, x+N$ so that every one of them is divisible by a perfect square. Different integers in the strings may be divisible by different perfect squares.

Note that a *perfect square* is an integer which is the square of another integer.

Hint: Look at Q1 again.

We use 2 facts:

① Th^{m} [Euclid]: There are infinitely many primes.

② Th^{m} [CRT]: If $M_1, \ldots, M_N$ are pairwise relatively primes positive integers then

$$\left.\begin{array}{l} x \equiv a_1 \pmod{M_1} \\ \vdots \\ x \equiv a_N \pmod{M_N} \end{array}\right] \longrightarrow$$ has a solution. Hence it has a positive solution (by adding appropriate multiple of $(M_1 \cdots M_N)$).

Given a length N, we look at 1st N primes

$2 = p_1,\ 3 = p_2, \ldots, p_N$ (can do this by ①)

Since p_i are prime then $\gcd(p_i^2, p_j^2) = 1$ for $i \neq j$.

Thus ② $\Rightarrow$ there is a positive integer solution to the system

$$\begin{aligned} x &\equiv 0 \mod p_1^2 \\ x &\equiv -1 \mod p_2^2 \\ &\vdots \\ x &\equiv -N+1 \mod p_N^2 \end{aligned}$$

$\Rightarrow p_1^2 \mid x,\ p_2^2 \mid (x+1), \ldots, p_N^2 \mid (x+N)$

& we have the desired string of N consecutive positive integers. But N was arbitrary! $\Rightarrow$ done ☑

Q3]... [10 points] Solve the system

$$\begin{aligned} 3x &\equiv 1 \mod 5 \\ 4x &\equiv 2 \mod 7. \end{aligned}$$

Hint: Convert each congruence to ones of the form $x \equiv a \mod 5$ and $x \equiv b \mod 7$ and then solve.

Rewrite! $3X \equiv 1 \mod 5$ $\quad 5(2) - 3(3) = 1 \quad \Rightarrow 3(-3) \equiv 1 \mod 5$

$X \equiv -3 \mod 5$

$X \equiv 2 \mod 5$

Rewrite! $4X \equiv 2 \mod 7$ $\quad 2X \equiv 1 \mod 7$ $\quad 2(4) - 1(7) = 1$

$X \equiv 4 \mod 7$

$(X \equiv 4 \mod 7)$

Our original system becomes

$$X \equiv 2 \pmod 5$$
$$X \equiv 4 \pmod 7$$

to which we apply CRT.

solve $7x_1 \equiv 1 \mod 5$ .... $7(3) - 4(5) = 1$

$x_1 \equiv 3$

solve $5x_2 \equiv 1 \mod 7$ .... $5(3) - 2(7) = 1$

$x_2 \equiv 3$

Solution by CRT is $X = (7)(3)(2) + (5)(3)(4) = 42 + 60$
$= 102$

General solution $\boxed{X = 102 + t(35), \quad t \in \mathbb{Z}}$

Q4]... [10 points] Prove that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

where A, B, C are all finite sets, and where $|X|$ denotes the cardinality of the set X. You may assume the easier case $|A \cup B| = |A| + |B| - |A \cap B|$. (*)

$$|A \cup B \cup C| = |A \cup (B \cup C)|$$

$$= |A| + |B \cup C| - |A \cap (B \cup C)| \quad \text{.... by (*)}$$

$$= |A| + |B| + |C| - |B \cap C| - |A \cap (B \cup C)| \quad \text{..... by (*)}$$

$$= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| \quad \text{--- distrib}$$

$$= |A| + |B| + |C| - |B \cap C| - \Big[|A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)| \Big] \quad \text{... by (*)}$$

$$= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + \underbrace{|A \cap B \cap A \cap C|}_{= |A \cap B \cap C|}.$$

done

Q5]... **[10 points]** State the division algorithm.

Given $a, b \in \mathbb{Z}$, $a > 0$. $\exists!\ r, q \in \mathbb{Z}$ such that

$$\boxed{b = aq + r, \quad 0 \le r < a}$$

[Note: Uniqueness only holds since we require $0 \le r < a$]

Define what we mean by the *greatest common divisor*, gcd(a, b), of two integers a and b.

$d = \gcd(a,b)$ means ① $d \mid a$ and $d \mid b$, and

② d is largest such integer.

Give a proof *using well-ordering* of the following fact.

$$\forall a, b \in \mathbb{Z}, \exists x, y \in \mathbb{Z} \text{ such that } \gcd(a, b) = xa + yb$$

(Also assume ~~[illegible]~~ $a, b \neq 0$)

Let $S = \{pa + qb \mid p, q \in \mathbb{Z},\ pa + qb > 0\}$

Note $|a| = \begin{cases} 1.a + 0.b & \text{if } a > 0 \\ -1.a + 0.b & \text{if } a < 0 \end{cases}$

$\Rightarrow |a| \in S \quad \Rightarrow S \neq \emptyset$

Well ordering $\Rightarrow$ S has a least element, d (say).

Note: $d = xa + yb$ for some $x, y \in \mathbb{Z}$.

Claim ① $d \mid a$

Division algorithm $\Rightarrow \exists\, q, r$ so that $a = qd + r$, $0 \le r < d$.

(~~if $r > 0$ then~~) Note $r = a - qd$

$= a - q(xa + yb)$

$= (1 - qx)a + (-qy)b$

Thus if $r > 0$, then r would be an element of S which is strictly less than d. This contradicts the fact that $d =$ least element of S.

Thus $r = 0$. $\Rightarrow a = qd \Rightarrow d \mid a$ ☒

Claim (2) $d \mid b$

Proof: Exactly as for proof of claim (1), replacing a by b throughout.

Thus
- d is a common divisor of a and b
- d is positive.

Also any other integer m which divides a & b also divides $xa + yb$ & hence divides d.

$\Rightarrow$ d is $\gcd(a,b)$.

But since $d \in S$ we know $d = xa + yb$ for some $x, y \in \mathbb{Z}$.

Q6]... [15 points] State the principle of induction.

$P(n)$ = statement about positive integer n.

$$\left.\begin{array}{l} \bullet\ P(1) \text{ true} \\ \bullet\ P(k) \text{ true} \Rightarrow P(k+1) \text{ true} \end{array}\right] \Rightarrow P(n) \text{ true } \forall n \in \mathbb{Z}^+$$

Use induction to prove the following fact:
"$n^2 - 1$ is divisible by 8 whenever n is an *odd, positive integer.*"

Rephrase slightly....

$P(n)$: "the nth odd positive integer, l_n, satisfies

$$8 \mid l_n^2 - 1 \text{"}.$$

$\underline{P(1) \text{ true}}$: $\quad l_1 = 1 \qquad l_1^2 - 1 = 1^2 - 1 = 0$

& $8 \mid 0 \quad \Rightarrow \quad P(1)$ true!

$\underline{P(k) \text{ true} \Rightarrow P(k+1) \text{ true}}$:

Given $\quad 8 \mid (l_k^2 - 1)$

Note $\quad l_{k+1} = l_k + 2 \qquad$ (~~(positive)~~ odd numbers increase in 2's.

$$\Rightarrow \quad l_{k+1}^2 - 1 = (l_k + 2)^2 - 1$$
$$= l_k^2 + 2(2)(l_k) + 2^2 - 1$$
$$= (l_k^2 - 1) + 4(l_k) + 4$$

We know that $8 \mid (l_k^2 - 1)$ by inductive hypothesis ($P(k)$ true),

So we will have $8 \mid (l_{k+1}^2 - 1)$ provided we can show

that $8 \mid (4(l_k) + 4)$.

But $\quad 4(l_k)+4 = 4(l_k+1)$

$= 4$ (even #) ... since l_k is odd

which is clearly divisible by 8.

So $\quad P(k)$ true $\Rightarrow P(k+1)$ true.

By Induction $P(n)$ is true $\forall n \in \mathbb{Z}^+$.

Q7]...[15 points] State the *Schröder-Bernstein Theorem.*

A, B sets. If $f: A \longrightarrow B$ is injective and $g: B \to A$ is injective, then there exists a bijection $h: A \longrightarrow B$.

Use the Schröder-Bernstein Theorem to prove that the open interval $(0, 1)$ has the same cardinality as the power set, $\mathcal{P}(\mathbb{Z}^+)$, of the set of positive integers.

$\mathcal{P}(\mathbb{Z}^+)$ has same cardinality as $(0,1)$

means $\exists$ bijection $: \mathcal{P}(\mathbb{Z}^+) \longrightarrow (0,1)$. .... def^n of cardinality.

By S-B we only have to exhibit two injections;

$$f: \mathcal{P}(\mathbb{Z}^+) \longrightarrow (0,1)$$

and $g: (0,1) \longrightarrow \mathcal{P}(\mathbb{Z}^+)$.

$\boxed{f: P(\mathbb{Z}^+) \longrightarrow (0,1)}$

We know $P(\mathbb{Z}^+) \xleftrightarrow{\text{bijective (class notes)}} \{\infty \text{ binary strings}\}$

$A \longmapsto$ string where n^{th} place is $\begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$

So it suffices to produce an injection

$$\{\infty \text{ binary strings}\} \xrightarrow{f} (0,1)$$

$$00111\ldots \longmapsto 0.33444\ldots$$

string $\longmapsto$ decimal of the form $0.a_1a_2a_3\ldots$

where $a_i = \begin{cases} 3 & \text{if } i^{th} \text{ position of string} = 0 \\ 4 & \text{if } i^{th} \text{ position of string} = 1 \end{cases}$

Note decimals don't end in ∞ string of 9's ~~OR~~ 0's
$\Rightarrow$ we have uniqueness of decimal representations.

$$f(\text{string}_1) = f(\text{string}_2)$$

$\Rightarrow$ ith decimal place of $f(\text{string}_1)$ = ith decimal place of $f(\text{string}_2)$ $\forall i$

$\Rightarrow$ ith place of string 1 = ith place of string 2 $\forall i$

$\Rightarrow$ $\text{string}_1 = \text{string}_2$ $\boxed{f \text{ injective}}$

Remark We could have skipped the $\{\infty$ binary strings$\}$ step above & defined

$$f : P(\mathbb{Z}^+) \longrightarrow (0,1)$$
$$: A \longmapsto 0.a_1a_2\ldots \quad \text{where}$$
$$a_i = \begin{cases} 3 & \text{if } i \notin A \\ 4 & \text{if } i \in A \end{cases}$$

directly.

$\boxed{g : (0,1) \longrightarrow \{\infty \text{ binary strings}\}}$

$x \longmapsto g(x)$ defined as follows

Step (i) choose the unique ~~decimal~~ binary representation for x which does not ~~(?)~~ end in an infinite string of 1's.

$$x = (0.a_1a_2a_3\ldots)_{\text{base } 2}$$ $a_i \in \{0,1\}$ $\forall i$

Step (2) $g(x) = a_1a_2a_3\ldots$ ∞ binary string.

$g(x_1) = g(x_2) \Rightarrow$

$x_1 = (0.a_1a_2\ldots)_{base\ 2}$ & $x_2 = (0.b_1b_2\ldots)_{base\ 2}$

where $a_1 = b_1$, $a_2 = b_2$, ...

$$\Rightarrow x_1 = \sum_{i=1}^{\infty} \frac{a_i}{2^i} = \sum_{i=1}^{\infty} \frac{b_i}{2^i} = x_2$$

$\Rightarrow$ g is injective!

Q8]... **[15 points]** True/False. Give brief reasons or examples to support your answers.

1. $\mathbb{Z}$ and $\mathbb{R}$ have the same cardinality.

$\boxed{\text{FALSE}}$

$\mathbb{Z}$ is countable.

$\mathbb{R}$ is uncountable.

2. If $f : X \to Y$ is a function, and $A, B \subset Y$, then $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

$\boxed{\text{TRUE}}$

$$\begin{aligned} f^{-1}(A) \cup f^{-1}(B) &= \{x \mid x \in f^{-1}(A) \ \underline{\text{OR}} \ x \in f^{-1}(B)\} && \text{... def}^{n} \text{ of } \cup \\ &= \{x \mid f(x) \in A \ \underline{\text{OR}} \ f(x) \in B\} && \text{-- def}^{n} \text{ of } f^{-1}(A) \text{ etc} \\ &= \{x \mid f(x) \in A \cup B\} && \text{--- def}^{n} \text{ of } \cup \\ &= f^{-1}(A \cup B) && \text{--- def}^{n} \text{ of } f^{-1}(A \cup B). \end{aligned}$$

3. $P \to Q$ is equivalent to $\neg P \wedge Q$.

$\boxed{\text{FALSE}}$

$P = F, Q = F \Rightarrow P \to Q$ is TRUE while $\neg P \wedge Q$ is FALSE.

4. $P \to Q$ is equivalent to $Q \to P$.

CONVERSE

$\boxed{\text{FALSE}}$

$\left.\begin{matrix} P = F \\ Q = T \end{matrix}\right) \Rightarrow$ $P \to Q$ is TRUE while $Q \to P$ is False.

5. $P \to Q$ is equivalent to $\neg Q \to \neg P$.

CONTRAPOSITIVE

$\boxed{\text{TRUE}}$

$$P \to Q \equiv \neg P \vee Q \equiv \neg(\neg Q) \vee (\neg P) \equiv \neg Q \to \neg P$$

6. $\mathbb{Z}^+ \subset \mathcal{P}(\mathbb{Z}^+)$

$\boxed{\text{FALSE}}$

$P(\mathbb{Z}^+)$ = powerset.

$= \{\text{subsets of } \mathbb{Z}^+\}$

$1 \in \mathbb{Z}^+$, but $1 \notin P(\mathbb{Z}^+)$

7. $\mathbb{Z}^+ \in \mathcal{P}(\mathbb{Z}^+)$

$\boxed{\text{TRUE}}$

$P(\mathbb{Z}^+) = \{\text{subsets of } \mathbb{Z}^+\}$, and $\mathbb{Z}^+ \subseteq \mathbb{Z}^+$.

8. $(A \cap \overline{B}) \cup (B \cap \overline{A}) = (A \cup B) \cap \overline{(A \cap B)}$

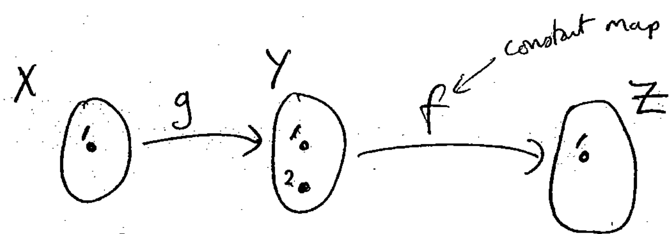
$\boxed{\text{TRUE}}$

$$\begin{aligned}
RHS &= (A \cup B) \cap (\bar{A} \cup \bar{B}) \text{ --- de Morgan} \\
&= (A \cap \bar{A}) \cup (B \cap \bar{A}) \cup (A \cap \bar{B}) \cup (B \cap \bar{B}) \text{ -- distrib Laws} \\
&= \emptyset \cup (B \cap \bar{A}) \cup (A \cap \bar{B}) \cup \emptyset \\
&= LHS
\end{aligned}$$

9. If $f \circ g$ is injective, then f must be injective.

$\boxed{\text{FALSE}}$

$f(1) = f(2) = 1$



$g(1)=1$

10. If $f \circ g$ is injective, then g must be injective.

$\boxed{\text{TRUE}}$

Prove contrapositive.

g not injective $\Rightarrow \exists\, x_1 \neq x_2 \in X$ so that $g(x_1) = g(x_2)$

$\Rightarrow f(g(x_1)) = f(g(x_2))$

$\Rightarrow (f \circ g)(x_1) = (f \circ g)(x_2)$

$\Rightarrow (f \circ g)$ not injective.

11. $(236)^{127} \equiv 1 \mod 16$

236 is <u>even</u> $\Rightarrow (236)^4 \equiv 0 \mod 16$ $\leftarrow 2^4$

$\boxed{\text{FALSE}}$

$$\Rightarrow (236)^{127} = (236)^4 (236)^{123} \equiv 0 \pmod{16}$$
$$\not\equiv 1 \pmod{16}$$

12. $(12)^{345} \equiv 6 \mod 7$

$12 \equiv 5 \mod 7$

$5^1 \equiv 5 \mod 7$
$5^2 \equiv 4 \mod 7$
$5^3 \equiv 5(4) \equiv 6 \mod 7$
$5^4 \equiv 5(6) \equiv 2 \mod 7$
$5^5 \equiv 5(2) \equiv 3 \mod 7$
$5^6 \equiv 5(3) \equiv 1 \mod 7$

So look at powers mod 6

$345 \equiv 6(57) + 3$

$$\Rightarrow (12)^{345} \equiv 1^{57} \cdot (5)^3 \pmod 7$$
$$\equiv 6 \pmod 7$$

$\boxed{\text{TRUE}}$

13. $(12345)^2 = (13542)$

$1 \to 2 \to 3$
$2 \to 3 \to 4$
$3 \to 4 \to 5$
$4 \to 5 \to 1$
$5 \to 1 \to 2$

composite

$1 \to 3 \to 5 \to 2 \to 4 \to 1$

Ans $= (13524) \neq (13542)$

$\boxed{\text{FALSE}}$

14. $(13)(1234)(13) = (3214)$

$1 \to 3 \to 4 \to 4$
$2 \to 2 \to 3 \to 1$
$3 \to 1 \to 2 \to 2$
$4 \to 4 \to 1 \to 3$

$\leftarrow$ composite

$1 \to 4 \to 3 \to 2 \to 1$

START

(3214)

$\boxed{\text{TRUE}}$

15. The composition of reflections in two lines which intersect in a point P is a rotation about the point P.

$\boxed{\text{TRUE}}$

Books =

Computer stuff — (Cont'd) Laptop)