Part A

Question 1:

Let

$$A = \{1, 2, 3, 4, 5\}, \quad B = \{cat, dog, rabbit, hamster\}, \quad C = \mathbb{Z}, \quad D = \{\alpha, \beta, \gamma, \delta\}$$

a)

i.

$$f : A \to B,$$

$$f(1) = cat, f(2) = hamster, f(3) = dog, f(4) = rabbit, f(5) = cat$$

f is onto but not one-to-one.

ii.

$$g : A \to D,$$

$$g(1) = \alpha, g(2) = \delta, g(3) = \beta, g(4) = \beta, g(5) = \alpha$$

g is neither one-to-one nor onto

iii.

$$F : A \to C,$$

$$F(a) = 100a, \text{ for all } a \in A$$

$F(a) = 100a$ is one-to-one but not onto

iv.

$$\phi : B \to D,$$

$$\phi(cat) = \alpha, \phi(dog) = \gamma, \phi(rabbit) = \beta, \phi(hamster) = \delta$$

ϕ is a bijection.

b)

i.

Example of a map $S \to T$ that is not one-to-one:

$$2 \mapsto 1,\ 3 \mapsto 1,\ 5 \mapsto 5,\ 7 \mapsto 7$$

.

ii.

Example of a bijection $S \to T$:

$$2 \mapsto 1,\ 3 \mapsto 3,\ 5 \mapsto 5,\ 7 \mapsto 7$$

.

Question 2:

$$\text{for } n \geq 1, 7^{2n} - 6^n \text{ is divisible by } 43$$

Proof.
Using proof by induction we will first prove the basis of induction $n = 1$

$$\begin{aligned} P(1) &= 7^{2(1)} - 6^1 \\ &= 49 - 6 \\ &= 43 \end{aligned}$$

Hence P(1) is divisible by 43

Now we will assume that $P(k)$ is true for some arbitrary $k \geq 1$

$$\begin{aligned} P(k) &= 7^{2k} - 6^k \\ &= 43m \end{aligned}$$

for some integer m

Next we will use this as our inductive hypothesis to prove that $P(k+1)$ is true

$$\begin{aligned} P(k+1) &= 7^{2(k+1)} - 6^{k+1} \\ &= 7^{2k+2} - 6^{k+1} \\ &= 7^2 \cdot 7^{2k} - 6 \cdot 6^k \\ &= 49 \cdot 7^{2k} - 6 \cdot 6^k \end{aligned}$$

From our inductive hypothesis we know that $7^{2k} - 6^k = 43m$

$$\begin{aligned} &= 49(43m + 6^k) - 6 \cdot 6^k \\ &= 49 \cdot 43m + 49 \cdot 6^k - 6 \cdot 6^k \end{aligned}$$

Factorising out the 6^k

$$= 49 \cdot 43m + (49 - 6) \cdot 6^k$$

$$= 49 \cdot 43m + 43 \cdot 6^k$$

Factoring out the 43

$$= 43(49m + 6^k)$$

Since m and k are both integers, $49m + 6^k$ is also an integer

hence $P(k + 1)$ is divisible by 43

By the principle of mathematical induction we have shown that $P(n)$ is true for all $n \geq 1$

□

Question 3:

$$\text{hcf}(2025, 630) = 2025x + 630y$$

$$\begin{aligned} 2025 &= 3 \cdot 630 + 135 \\ 630 &= 4 \cdot 135 + 90 \\ 135 &= 1 \cdot 90 + 45 \\ 90 &= 2 \cdot 45 + 0 \end{aligned}$$

Hence,

$$\text{hcf}(2025, 630) = 45$$

rearranging to make the remainder the subject;

$$\begin{aligned} 45 &= 135 - 1 \cdot 90 \\ 90 &= 630 - 4 \cdot 135 \\ 135 &= 2025 - 3 \cdot 630 \end{aligned}$$

Substituting back up the chain we get;

$$\begin{aligned} 45 &= 135 - 1(630 - 4 \cdot 135) \\ &= 5 \cdot 135 - 1 \cdot 630 \\ &= 5(2025 - 3 \cdot 630) - 1 \cdot 630 \\ &= 5 \cdot 2025 - 15 \cdot 630 - 1 \cdot 630 \\ &= 5 \cdot 2025 - 16 \cdot 630 \end{aligned}$$

Hence one solution is

$$\boxed{x = 5, y = -16}$$

Question 4:

a)
If a and b are positive integers and p divides $\text{hcf}(a^2, b)$ if, and only if, p divides $\text{hcf}(a, b^2)$.

Proof.
Let p be a prime number.

Definition 4.5, Chapter 1 HB p15: Highest common factor(HCF), $\text{hcf}(a, b)$, of two integers a and b, not both of which are zero, is the natural number n satisfying

$(a) n \mid a$ and $n \mid b$;

if $d \mid a$ and $d \mid b$ then $d \leq n$

Forward direction ($\Rightarrow$): Suppose $p \mid \text{hcf}(a^2, b)$ then by Definition 4.5, HB p15,

$$p \mid a^2 \text{ and } p \mid b$$

Since p is a prime number, and $p \mid a^2$, by Euclid's Lemma for prime factors (Theorem 1.4, Chapter 2 HB p17),

$$p \mid a$$

Hence,

$$p \mid a \text{ and } p \mid b$$

Which implies, by Definition 4.5, HB p15,

$$p \mid \text{hcf}(a, b^2) \because p \mid b \implies p \mid b^2$$

Backward direction ($\Leftarrow$): conversely suppose $p \mid \text{hcf}(a, b^2)$ Then

$$p \mid a \text{ and } p \mid b^2$$

Again by Theorem 1.4, HB p17,

$$p \mid b^2 \implies p \mid b$$

Therefore,

$$p \mid a \text{ and } p \mid b \implies p \mid a^2 \text{ also}$$

Hence $p \mid (a^2, b)$

Thus, we have shown in both directions and so;

$$p \mid \text{hcf}(a^2, b) \iff p \mid \text{hcf}(a, b^2)$$

□

b)
If a and b are positive integers and m and n are defined by

$$m = 3a + b \quad \text{and} \quad n = 5a + 2b$$

then $\text{hcf}(m, n) = \text{hcf}(a, b)$

Proof.
Let $d = \text{hcf}(a, b)$ and $c = \text{hcf}(m, n)$.

Since d is the highest common factor of a and b, by Definition 4.5, HB p15,

$$d \mid a \text{ and } d \mid b$$

Then by Properties of division (Theorem 4.4, Chapter 1 p15),

$$d \mid (3a + b) \text{ and } d \mid (5a + 2b)$$

Hence,

$$d \mid m \text{ and } d \mid n$$

Therefore, by Definition 4.5,

$$d \mid c$$

And since c is the highest common factor of m and n, by Definition 4.5, HB p15,

$$c \mid m \text{ and } c \mid n$$

Then by Theorem 4.4,

$$c \mid (2m - n) \text{ and } c \mid (5m - 3n)$$

Hence,

$$c \mid a \text{ and } c \mid b$$

Therefore, by Definition 4.5, HB p15,

$$c \mid d$$

Thus, $d \mid c$ and $c \mid d \implies c = d$

$$\text{hcf}(m, n) = \text{hcf}(a, b)$$

□

c)
A number of the form $14a + 3$, where a is a non-negative integer, must have a prime divisor of this same form $14b + 3$, where b is a non-negative integer.

Proof.
Consider if n is prime, then n is a prime divisor of itself and since $n = 14a + 3$, n is of the form $14b + 3$ where $b = a$.

Now consider if n is composite, then by Fundamental theorem of arithmetic (Theorem 1.7, Chapter 2 HB p17), n can be expressed as;

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

thus having at least one prime factor such that $p \mid n$

Hence we will have to show that;

$$n \equiv 3 \pmod{14}$$

and

$$p \mid n, \text{such that } p \equiv 3 \pmod{14}$$

Consider the counter example where $n = 185$, that is;

$$n = 185 = 5 \times 37$$

$$5 \equiv 5 \pmod{14}$$

and

$$37 \equiv 9 \pmod{14}$$

As neither of these prime factors are of the form $14b + 3$ the statement is incorrect.

□

d)
If n is divisible by 15 but not divisible by 9 or 25, then $\tau(n)$ is divisible by 4.

Proof.
By Theorem 1.7, HB p17, we can express n as a product of its prime factors;

$$n = 3^{k_1} \cdot 5^{k_2} \cdot p_1^{k_1} \cdot p_2^{k_2} \dots$$

where $k_1, k_2 = 1$ as n is divisible by 15 but not by 9 or 25.

Hence,

$$n = 3^1 \cdot 5^1 \cdot p_1^{k_1} \cdot p_2^{k_2} \dots$$

Then by Proposition 2.3, Chapter 2 p17 (Formula for $\tau(n)$);

$$\begin{aligned}\tau(n) &= (1+1)(1+1)(k_1+1)(k_2+1)\dots \\ &= 2 \cdot 2 \cdot (k_1+1)(k_2+1)\dots \\ &= 4 \cdot (k_1+1)(k_2+1)\dots\end{aligned}$$

Since $(k_1+1)(k_2+1)\dots$ is an integer, $\tau(n)$ is divisible by 4

□

Question 5:

a)
i.

$$3x \equiv 4 \pmod 5$$

$\text{hcf}(3, 5) = 1$, hence 3 has a multiplicative inverse modulo 5

Hence, this will be the unique solution to the linear congruence

$$3v \equiv 1 \pmod 5$$

By trying values for v we find that;

$$3 \cdot 2 \equiv 1 \pmod 5$$

Thus, $v = 2$ is the multiplicative inverse of 3 modulo 5

Multiplying both sides of the original congruence by 2 gives;

$$6x \equiv 8 \pmod 5$$

Reducing 6 and 8 modulo 5 gives;

$$x \equiv 3 \pmod 5$$

Thus, the solution is;

$$\boxed{x \equiv 3 \pmod 5}$$

ii.

$$3x - 1 \equiv 2(4 + x) \pmod 7$$

distributing the 2 on the RHS;

$$3x - 1 \equiv 8 + 2x \pmod 7$$

subtracting $2x$ from both sides;

$$x - 1 \equiv 8 \pmod 7$$

adding 1 to both sides;

$$x \equiv 9 \pmod{7}$$

reducing 9 modulo 7 gives;

$$x \equiv 2 \pmod{7}$$

Thus, the solution is;

$$\boxed{x \equiv 2 \pmod{7}}$$

iii.

$$2(7 - x) \equiv 8 - x \pmod{17}$$

distributing the 2 on the LHS;

$$14 - 2x \equiv 8 - x \pmod{17}$$

adding $2x$ to both sides;

$$14 \equiv 8 + x \pmod{17}$$

subtracting 8 from both sides;

$$6 \equiv x \pmod{17}$$

Thus, the solution is;

$$\boxed{x \equiv 6 \pmod{17}}$$

b)

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$x \equiv 6 \pmod{17}$$

$$\text{hcf}(5,7) = \text{hcf}(5,17) = \text{hcf}(7,17) = 1$$

Since 5, 7, and 17 are coprime, by the Chinese Remainder Theorem (CRT, Theorem 4.2, Chapter 3 p20) there is a unique solution modulo $5 \times 7 \times 17 = 595$. Checking shows $x = 23$ satisfies all three congruences, so the least positive solution is;

$\boxed{x = 23}$.

Question 6:

a)

$$25^{60} \pmod{59}$$

Using Fermat's little theorem (FLT, Theorem 1.1, Chapter 4 p21);

$a^{p-1} \equiv 1 \pmod{p}$ where p is a prime and a is not divisible by p

$$25^{58} \equiv 1 \pmod{59}$$

Substitute this into the original expression, and using index laws;

$$\equiv 25^{58} \cdot 25^2 \pmod{59}$$

Reducing 25^{58} modulo 59 gives;

$$\equiv 1 \cdot 25^2 \pmod{59}$$

$$\equiv 625 \pmod{59}$$

Reducing 625 modulo 59 gives;

$$\equiv 35 \pmod{59}$$

Thus, the solution is;

$$\boxed{35}$$

b)

$$a^{25} \equiv \pmod{195}$$

Proof.
Since $195 = 3 \times 5 \times 13$ and these are coprime, we can use CRT and show;

$$a^{25} \equiv a \pmod{p}$$

For each of the primes divisors $p \in \{3, 5, 13\}$

Using FLT we need to check that $25 \equiv 1 \pmod{p-1}$ for each prime:

$$p = 3 : 25 \equiv 1 \pmod{2}$$

$$p = 5 : 25 \equiv 1 \pmod{4}$$

$$p = 13 : 25 \equiv 1 \pmod{12}$$

Hence, for each prime p dividing 195,

$$a^{25} \equiv a^1 \equiv a \pmod{p}$$

By the CRT, there is a unique solution modulo 195 and so;

$$a^{25} \equiv a \pmod{195}$$

for all integers a.

□

Question 7:

$$P(x) = x^3 + 23x^2 + 10x + 6$$

a)
The degree of $P(x)$ is 3.

b)
i.

$$P(x) \equiv \pmod 3$$

$$P(x) \equiv x^3 + 23x^2 + 10x + 6 \pmod 3$$
$$\equiv x^3 + 2x^2 + x \pmod 3$$

Factoring out an x gives;

$$\equiv x(x^2 + 2x + 1) \pmod 3$$

Factor out x and complete the square;

$$\equiv x\big(x^2 + 2x + 1\big) \pmod 3$$
$$\equiv x(x+1)^2 \pmod 3$$

Thus the roots satisfy $x \equiv 0$ or $x \equiv -1 \equiv 2 \pmod 3$.

$$\boxed{x \equiv 0, 2 \pmod 3}$$

ii.

$$P(x) \equiv 0 \pmod 7$$

$$P(x) \equiv x^3 + 23x^2 + 10x + 6 \pmod 7$$
$$\equiv x^3 + 2x^2 + 3x + 6 \pmod 7$$

Trying values for x from 0 to 6 gives;

$$x = 2 \equiv 0 \pmod 7$$
$$x = 5 \equiv 0 \pmod 7$$

Thus, the solutions are;

$$\boxed{x \equiv 2, 5 \pmod 7}$$

c)

$$P(x) \equiv 0 \pmod{63}$$

Using the CRT we can split this into two congruences;

$$P(x) \equiv 0 \pmod 7$$
$$P(x) \equiv 0 \pmod 9$$
$$\text{hcf}(7, 9) = 1$$

$$P(x) \equiv x^3 + 23x^2 + 10x + 6 \pmod 9$$
$$\equiv x^3 + 5x^2 + x + 6 \pmod 9$$

Trying values for x from 0 to 8 gives;

$$x = 2 \equiv 0 \pmod 9$$

$$x = 3 \equiv 0 \pmod 9$$

$$x = 5 \equiv 0 \pmod 9$$

$$x = 8 \equiv 0 \pmod 9$$

Thus, the solutions are;

$$\boxed{x \equiv 2, 3, 5, 8 \pmod 9}$$

Using the solutions from part (b) we have;

$$x \equiv 2, 5 \pmod 7$$

$$x \equiv 2, 3, 5, 8 \pmod 9$$

$$\text{hcf}(7, 9) = 1$$

Since 7 and 9 are coprime, by the CRT there is a unique solution modulo $7 \times 9 = 63$.

first pair

$$x \equiv 2 \pmod 7$$

$$x \equiv 2 \pmod 9$$

$$\implies x \equiv 2 \pmod{63}$$

Now using the multiplicative inverse v of $7 \pmod 9$;

$$v = 4, \text{ since } 7 \times 4 \equiv 1 \pmod 9$$

second pair

$$x \equiv 2 \pmod 7$$

$$x \equiv 3 \pmod 9$$

$$x = 7k + 2$$

$$7k + 2 \equiv 3 \pmod 9$$

Substituting v and multiplying both sides by 4 gives;

$$4(7k + 2) \equiv 4 \cdot 3 \pmod 9$$

$$k + 8 \equiv 12 \pmod 9$$

$$k \equiv 4 \pmod 9$$

Substituting back gives;

$$x = 7(9m + 4) + 2$$

$$= 63m + 30$$

$$\implies x \equiv 30 \pmod{63}$$

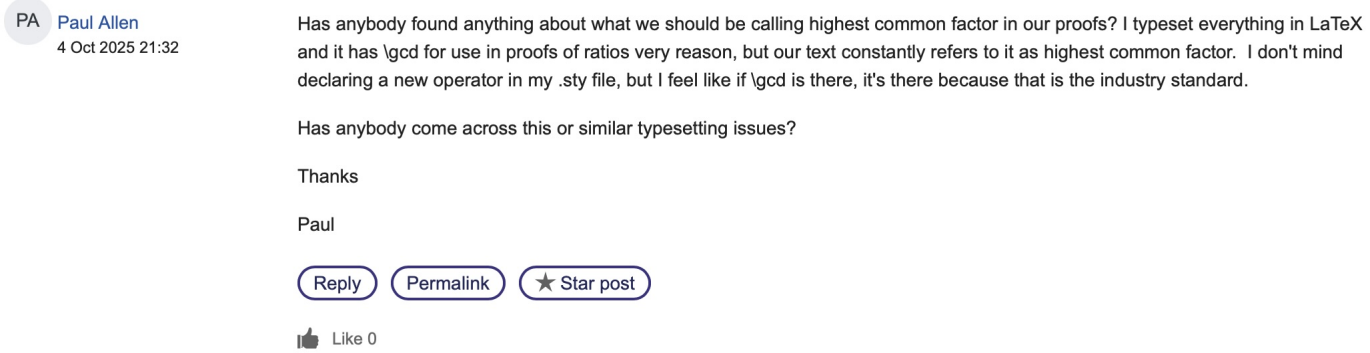
Checking the rest of the pairs, shows $x = 2, 5, 16, 23, 30, 37, 47, 54$ satisfy both congruences, so the least positive solutions are;

$\boxed{2, 5, 16, 23, 30, 37, 47, 54}$.

Question 8:

a)
I have watched the online session entitled "M303: Things you need to know".

b)


PA Paul Allen
4 Oct 2025 21:32

Has anybody found anything about what we should be calling highest common factor in our proofs? I typeset everything in LaTeX and it has \gcd for use in proofs of ratios very reason, but our text constantly refers to it as highest common factor. I don't mind declaring a new operator in my .sty file, but I feel like if \gcd is there, it's there because that is the industry standard.

Has anybody come across this or similar typesetting issues?

Thanks

Paul

Reply Permalink ★ Star post

Like 0

https://learn2.open.ac.uk/mod/forumng/discuss.php?d=5080556

Part B

Question 9: Question 10 from the TMA booklet

a)
For $k \geq 1$ let $P(n)$ be the statement;

"Let k be the number of blue eared aliens, all the aliens will leave at $6am$ on the k^{th} day."

b)
Base case:

$$P(1) : k = 1$$

If a blue eared alien does not see any other blue eared aliens, then they will know they are the only blued eared alien on the planetoid, and will leave at $6am$ on the next rotation, i.e the k^{th} day.

So $P(1)$ holds

Inductive step: Assume that the statement is true for some arbitrary $m \geq 1$, i.e if there are m blue eared aliens, they will all leave at $6am$ on the m^{th} day.

Now consider if there are $m + 1$ blue eared aliens. Each blue eared alien will see m other blue eared aliens. When on the m^{th} day no aliens leave, they will realise that they must also have blue ears, so all $m + 1 = k$ aliens will leave at $6am$ on the k^{th} day.

Thus, by the principle of mathematical induction, the statement is true for all $k \geq 1$.

Question 10: Question 12 from the TMA booklet

Let p and q be distinct odd primes.

a)
An integer x satisfied $x^2 \equiv 1 \pmod{pq}$ if, and only if, x satisfies both

$$x^2 \equiv 1 \pmod{p} \text{ and } x^2 \equiv 1 \pmod{q}$$

Forward direction ($\Rightarrow$):

$$\begin{aligned} x^2 &\equiv 1 \pmod{pq} \\ x^2 - 1 &\equiv 0 \pmod{pq} \\ (x-1)(x+1) &\equiv 0 \pmod{pq} \end{aligned}$$

Hence, $pq \mid (x-1)(x+1)$ Since p and q are distinct primes;

$$p \mid (x-1)(x+1) \text{ and } q \mid (x-1)(x+1)$$

Thus,

$$x^2 \equiv 1 \pmod{p} \text{ and } x^2 \equiv 1 \pmod{q}$$

Backward direction ($\Leftarrow$):

$$\begin{aligned} x^2 &\equiv 1 \pmod{p} \text{ and } x^2 \equiv 1 \pmod{q} \\ x^2 - 1 &\equiv 0 \pmod{p} \text{ and } x^2 - 1 \equiv 0 \pmod{q} \\ (x-1)(x+1) &\equiv 0 \pmod{p} \text{ and } (x-1)(x+1) \equiv 0 \pmod{q} \end{aligned}$$

Hence,

$$p \mid (x-1)(x+1) \text{ and } q \mid (x-1)(x+1)$$

Since p and q are distinct primes;

$$\begin{aligned} pq \mid (x-1)(x+1) \\ (x-1)(x+1) &\equiv 0 \pmod{pq} \\ x^2 - 1 &\equiv 0 \pmod{pq} \\ x^2 &\equiv 1 \pmod{pq} \end{aligned}$$

Therefore,

$$\boxed{x^2 \equiv 1 \pmod{pq} \iff x^2 \equiv 1 \pmod{p} \text{ and } x^2 \equiv 1 \pmod{q}}$$

b)

$$x^2 \equiv 1 \pmod{p}$$

As p is odd, $p-1$ is even, hence divisible by 2.

By Proposition 4.8, Chapter 4 p22, if p is prime and d is a textupof $p-1$ then the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.

Thus, $x^2 \equiv 1 \pmod{p}$ has exactly 2 solutions. These solutions are $x \equiv 1 \pmod{p}$ and $x \equiv -1 \equiv p-1 \pmod{p}$.

c)

$$x^2 \equiv 1 \pmod{pq}$$

$$x^2 \equiv 1 \pmod{p}$$
$$x^2 \equiv 1 \pmod{q}$$

$$x^2 \equiv 1 \pmod{p}$$
$$x^2 - 1 \equiv 0 \pmod{p}$$
$$(x-1)(x+1) \equiv 0 \pmod{p}$$

Hence, $p \mid (x-1)$ or $p \mid (x+1)$

Thus, the solutions are;

$$x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \equiv p-1 \pmod{p}$$

The same argument can be used for q. Hence,

$x^2 \equiv 1 \pmod{pq}$ has four solutions.

d)

$$x^2 \equiv 1 \pmod{95}$$

Using the CRT we can split this into two congruences;

$$x^2 \equiv 1 \pmod{5}$$

$$x^2 \equiv 1 \pmod{19}$$
$$\text{hcf}(5, 19) = 1$$

Since 5 and 19 are coprime, by the CRT there is a unique solution modulo $5 \times 19 = 95$.

The solutions to $x^2 \equiv 1 \pmod{5}$ are;

$$x \equiv 1 \pmod{5} \text{ or } x \equiv 4 \pmod{5}$$

The solutions to $x^2 \equiv 1 \pmod{19}$ are;

$$x \equiv 1 \pmod{19} \text{ or } x \equiv 18 \pmod{19}$$

Checking the four pairs of solutions shows $x = 1, 4, 16, 19$ satisfy both congruences, so the least positive solutions are;

$\boxed{1, 4, 16, 19}$.

e)
This does not contradict Lagrange's theorem (Theorem 4.3, Chapter 4 p22) as this theorem only applies to polynomials modulo a prime number, and 95 is not prime.