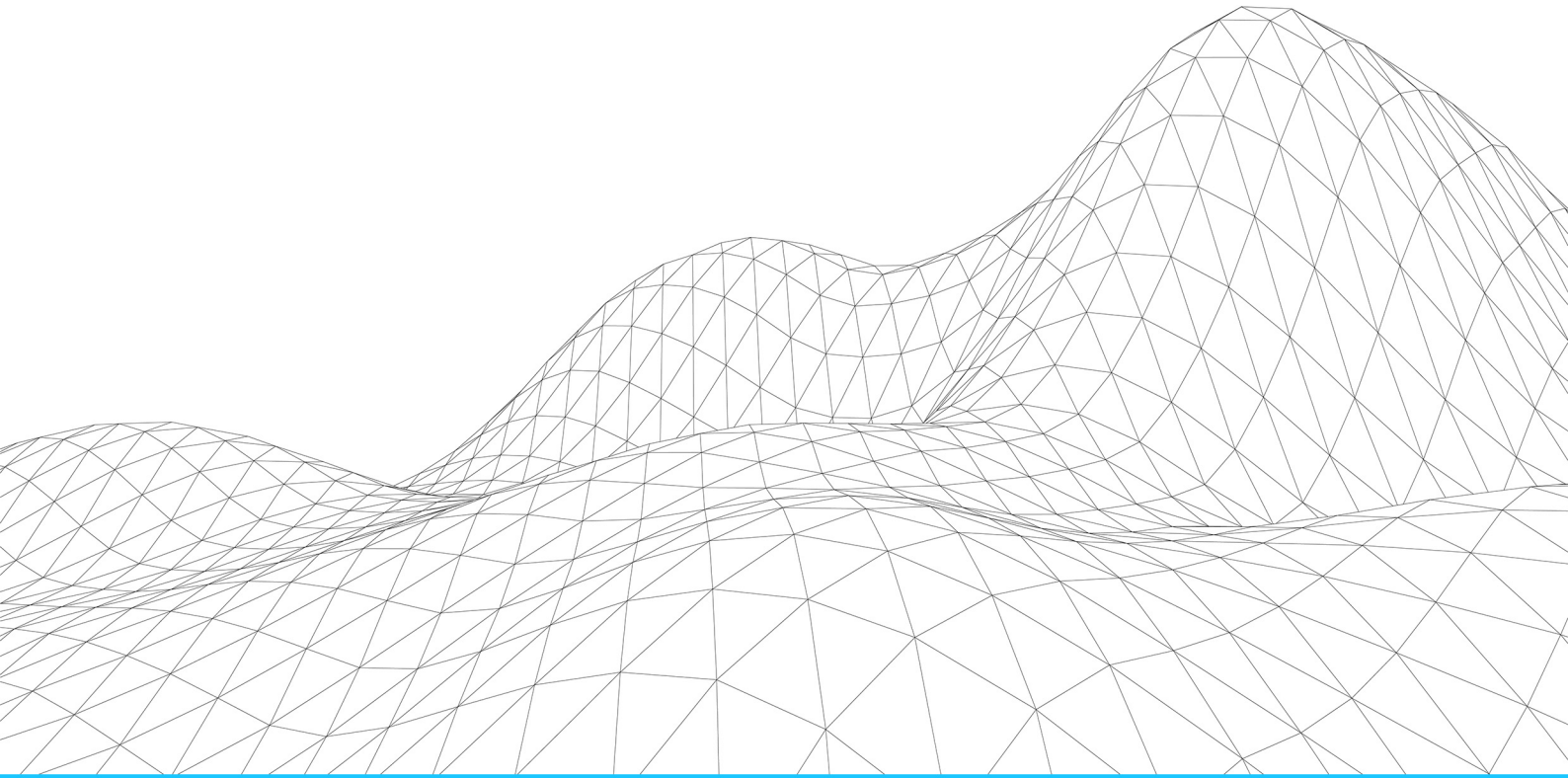
London Academy of Maths

Number Theory

Worked Solutions



1. (i) Use Fermat's Little Theorem to find the least positive residue of 6^{542} modulo 13

(5)

$$6^{542} = 6^{12\times 45+2}$$

$$= (6^{12})^{45} \times 6^2$$

$$\equiv 1^{45} \times 6^2 \mod 13$$

$$\equiv 36 \mod 13$$

$$\equiv 10 \mod 13$$

since $6^{12} \equiv 1 \mod 13$ by FLT

ignore the marks.

2. **In this question you must show detailed reasoning.**

Use Fermat's Little Theorem to determine the least positive residue of

$$21^{80} \pmod{23}$$

(4)

$21^{80} = 21^{3\times 22 + 14}$

$= (21^{22})^3 \times 21^{14}$

$\equiv 21^{14} \bmod 23$

$\equiv (-2)^{14} \bmod 23$

$\equiv (-2)^6 (-2)^6 (-2)^2 \bmod 23$

$\equiv 64 \times 64 \times 4 \bmod 23$

$\equiv 18 \times 18 \times 4 \bmod 23$

$\equiv -5 \times -5 \times 4 \bmod 23$

$\equiv 2 \times 4 \bmod 23$

$\equiv 8 \bmod 23$

Since $21^{22} \equiv 1 \bmod 23$ by FLT

**

3 **(a)** Solve $7x \equiv 6 \pmod{19}$. **[2]**

(b) Show that the following simultaneous linear congruences have no solution.

$x \equiv 3 \pmod{4}$, $x \equiv 4 \pmod{6}$. **[2]**

a) Find inverse of 7 mod 19

Method A

Back substitution using Euclid's Algorithm

Method B

Total and Error.

$7^{-1} \equiv 11 \mod 19$

$7x \equiv 6 \mod 19$ since hcf $(7, 19) = 1$

$\times 11$ ( ) $\times 11$

$x \equiv 66 \mod 19$

$\boxed{x \equiv 9 \mod 19}$

b) $x = 3 \mod 4$ (A) $x \equiv 4 \mod 6$ (B)

$x = 3 + 4a$ for some $a \in \mathbb{Z}$

Sub into (B):

$3 + 4a \equiv 4 \mod 6$

$4a \equiv 1 \mod 6$

Inverse of 4 mod 6 does not exist since hcf $(4, 6) = 2 \neq 1$

So no solutions.

4) Solve the simultaneous linear congruences

$$5x \equiv 3 \pmod 8 \quad \text{and} \quad x \equiv 4 \pmod 5.$$

(3)

Find inverse of 5 mod 8.

Note: inverse of 5 mod 8 exists because hcf(5,8)=1

$5 \times 5 \equiv 25 \bmod 8$

$\equiv 1 \bmod 8$

$5x \equiv 3 \bmod 8$

$\times 5 \left(\quad \right) \times 5$

$x \equiv 15 \bmod 8$

$\equiv 7 \bmod 8$

so $x = 7 + 8a$ where $a \in \mathbb{Z}$.

Sub this into $x \equiv 4 \bmod 5$

$7 + 8a \equiv 4 \bmod 5$

$2 + 3a \equiv 4 \bmod 5$

$3a \equiv 2 \bmod 5$

hcf(3,5)=1

$\times 2 \left(\quad \right) \times 2$

$a \equiv 4 \bmod 5$

$a = 4 + 5b$ where $b \in \mathbb{Z}$.

Sub $a = 4 + 5b$ into $x = 7 + 8a$:

$x = 7 + 8(4 + 5b)$

$= 39 + 40b$

So $\boxed{x \equiv 39 \bmod 40}$

5) Prove that $30n + 4$ and $20n + 3$ are always coprime, where $n \in \mathbb{N}$. (3)

let $h = hcf(30n+4, 20n+3)$

$h \mid 30n+4$ & $h \mid 20n+3$

So $h \mid a(30n+4) + b(20n+3)$ for all $a, b \in \mathbb{Z}$

$\Rightarrow h \mid -2(30n+4) + 3(20n+3)$

$h \mid -60n - 8 + 60n + 9$

$h \mid 1$

$\Rightarrow n = 1$

$\Rightarrow 30n+4$ and $20n+3$ are coprime

6) Solve the simultaneous linear congruences

$$7x \equiv 2 \pmod{25} \quad \text{and} \quad x \equiv 4 \pmod{19}.$$

(3)

$25 = 7(3) + 4$

$7 = 4(1) + 3$

$4 = 3(1) + 1$

$1 = 4 - 3$

$= 4 - (7 - 4)$

$= 2(4) - 7$

$= 2(25 - 7(3)) - 7$

$= 2 \times 25 - 7(7)$

$7x \equiv 2 \bmod 25$ $\quad hcf(7, 25) = 1$

$\times -7$ $\quad \times -7$

$x \equiv -14 \bmod 25$

$\equiv 11 \bmod 25$

$x = 11 + 25a$ where $a \in \mathbb{Z}$

sub into $x \equiv 4 \bmod 19$

$11 + 25a \equiv 4 \bmod 19$ $\quad hcf(6, 19) = 1$

$6a \equiv -7 \bmod 19$

$6a \equiv 12 \bmod 19$

$a \equiv 2 \bmod 19$

So $a = 2 + 19b$ where $b \in \mathbb{Z}$

$\Rightarrow x = 11 + 25(2 + 19b)$

$= 61 + 475b$

$x \equiv 61 \bmod 475$

7) Solve the simultaneous linear congruences

$$x \equiv a \pmod 4 \quad \text{and} \quad x \equiv b \pmod 5,$$

giving your answer in the form

$$x \equiv ha + kb \pmod{20},$$

where $h, k \in \mathbb{Z}$, $0 \leq h < 20$, and $0 \leq k < 20$. (4)

$x = a + 4n$ where $n \in \mathbb{Z}$

$a + 4n \equiv b \bmod 5$

$4n \equiv b - a \bmod 5$

$hcf(4,5) = 1$

$\times 4$ ( ) $\times 4$

$n \equiv 4b - 4a \bmod 5$

$\equiv 4b + a \bmod 5$

$n = 4b + a + 5m$ where $m \in \mathbb{Z}$

Sub into $x = a + 4n$

$\Rightarrow x = a + 4(4b + a + 5m)$

$= 5a + 16b + 20m$

so $x \equiv 5a + 16b \bmod 20$

8 Let N be the number 15 824 578.

(a) (i) Use a standard divisibility test to show that N is a multiple of 11. **[2]**

(ii) A student uses the following test for divisibility by 7.

> 'Throw away' multiples of 7 that appear either individually or within a pair of consecutive digits of the test number.
> Stop when the number obtained is 0, 1, 2, 3, 4, 5 or 6.
> The test number is only divisible by 7 if that obtained number is 0.

For example, for the number N, they first 'throw away' the "7" in the tens column, leaving the number $N_1 = 15824508$. At the second stage, they 'throw away' the "14" from the left-hand pair of digits of N_1, leaving $N_2 = 01824508$; and so on, until a number is obtained which is 0, 1, 2, 3, 4, 5 or 6.

- Justify the validity of this process.
- Continue the student's test to show that $7 \mid N$. **[2]**

(iii) Given that $N = 11 \times 1438598$, explain why $7 \mid 1438598$. **[1]**

(b) Let $M = N^2$.

(i) Express N in the unique form $101a + b$ for positive integers a and b, with $0 \leqslant b < 101$. **[2]**

(ii) Hence write M in the form $M \equiv r \pmod{101}$, where $0 < r < 101$. **[1]**

(iii) Deduce the order of N modulo 101. **[1]**

a) i $1 - 5 + 8 - 2 + 4 - 5 + 7 - 8 = 0$

$11 \mid 0$ so $11 \mid N$

ii) we know that if $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ for any $x, y \in \mathbb{Z}$.

So applying this here, if $7 \mid N$ (and $7 \mid 7k$) then

$7 \mid N - 7k$

When the student through away the 7 in the tens column it's the same as $k = 10$, i.e. $7 \mid N - 70$.

***

$N_2 = 0182\,4508$ ● : what I'm reducing

$N_3 = 0112\,4501$

$N_4 = 0040\,3011$

$N_5 = 0005\,0204$

$N_6 = 0000\,1064$

$N_7 = 0000\,0301$

$N_8 = 0000\,0021$

$N_9 = 0000\,0000$

(i) by Euclid's Lemma:

$7 \mid 111 \times 1438598 \Rightarrow 7 \mid 111$ or $7 \mid 1438598$

$\Rightarrow 7 \mid 1438598$ since $7 \nmid 11$.

b) i) $\frac{N}{101} = 156678.9901$

so $N = 101 \times 156678 + 100$

i.e $a = 156678$, $b = 100$

ii) $M = N^2 = (101 \times 156678 + 100)^2$

$= (101 \times 156678)^2 + 2 \times 101 \times 156678 + 100^2$

$\equiv 0 + 0 + 100^2 \mod 101$

$\equiv (-1)^2 \mod 101$

$\equiv 1 \mod 101$

(ii) if $N^2 \equiv 1 \mod 101$

then $\text{ord}(N) = 2$, since $\text{ord}(N) \neq 1$ as $N' \equiv 100 \mod 101$

9) Suppose

$$x \equiv 3 \pmod 7 \quad \text{and} \quad x \equiv 11 \pmod{17}.$$

Show that

$$x^2 \equiv 2 \pmod{119}.$$

(3)

$x^2 \equiv 9 \bmod 7$

$\equiv 2 \bmod 7$

$x^2 \equiv (-6)^2 \bmod 17$

$\equiv 36 \bmod 17$

$\equiv 2 \bmod 17$

$\Rightarrow x^2 \equiv 2 \bmod (7 \times 17)$

$\equiv 2 \bmod 119$

since $hcf(7,17) = 1$

will lose a mark if you don't state this.

10 Solve the simultaneous linear congruences $x \equiv 1 \pmod 3$, $x \equiv 5 \pmod{11}$, $2x \equiv 5 \pmod{17}$. **[6]**

$x \equiv 1 \bmod 3$ (A)

(D) $x = 1 + 3a$ for some $a \in \mathbb{Z}$

Sub into (B):

$1 + 3k \equiv 5 \bmod 11$

$3k \equiv 4 \bmod 11$

$\times 4 \left(\quad \right) \times 4$

$k \equiv 16 \bmod 11$

$\equiv 5 \bmod 11$

i.e. $a = 5 + 11b$ for some $b \in \mathbb{Z}$

Since hcf $(3, 11) = 1$

Sub into (D):

$x = 1 + 3(5 + 11b)$

$= 16 + 33b$ (E)

sub this into (C):

$16 + 33b \equiv 11 \bmod 17$

$-b \equiv -5 \bmod 17$

$b \equiv 5 \bmod 17$

$\Rightarrow b = 5 + 17c$ for some $c \in \mathbb{Z}$

Sub back into (E):

$x = 16 + 33(5 + 17c)$

$= 181 + 561c$

$\Rightarrow$ $\boxed{x \equiv 181 \bmod 561}$

(C) $x \equiv 45 \bmod 17$

$\equiv 11 \bmod 17$

$\times 9 \left(\quad \right) \times 9$

11 Determine all integers x for which $x \equiv 1 \pmod 7$ and $x \equiv 22 \pmod{37}$ and $x \equiv 7 \pmod{67}$.
Give your answer in the form $x = qn + r$ for integers n, q, r with $q > 0$ and $0 \leqslant r < q$. **[6]**

$x \equiv 1 \mod 7$

$x = 1 + 7a$ (A) for some $a \in \mathbb{Z}$

sub (A) into $x \equiv 22 \mod 37$

$\Rightarrow 1 + 7a \equiv 22 \mod 37$

$7a \equiv 21 \mod 37$

$\Rightarrow a \equiv 3 \mod 37$

$\Rightarrow a = 3 + 37b$ for some $b \in \mathbb{Z}$.

Sub this back into (A):

$x = 1 + 7(3 + 37b)$

$= 22 + 259b$ (C)

sub (C) into $x \equiv 7 \mod 67$

$22 + 259b \equiv 7 \mod 67$

$58b \equiv -15 \mod 67$

$58b \equiv 52 \mod 67$

Need to find $58^{-1} \mod 67$ (since $\text{hcf}(58, 67) = 1$)

$67 = 58(1) + 9$

$58 = 9(6) + 4$

$9 = 4(2) + 1$

$\Rightarrow 1 = 9 - 4(2)$

$= 9 - (58 - 9(6))(2)$

$= 13(9) - 2(58)$

$= 13(67 - 58) - 2(58)$

$= 13(67) - 15(58)$

$58x - 15 \equiv 1 \mod 67$

$b \equiv 52x - 15 \mod 67$

$\equiv -15x - 15 \mod 67$

$\equiv 24 \mod 67$

So $b = 24 + 67c$

$\Rightarrow x = 22 + 259(24 + 67c)$

$= 17353c + 6238$

12) Suppose

$$x^{109} \equiv 53 \pmod 7 \quad \text{and} \quad x^{131} \equiv 59 \pmod{11}.$$

Show that

$$x \equiv 4 \pmod{77}.$$

(3)

by FLT → $x^6 \equiv 1 \bmod 7$ provided $\gcd(x,7)=1$

& $x^{10} \equiv 1 \bmod 11$ provided $\gcd(x,11)=1$

or x is not a multiple of 7 or 11 — these statements are equivalent.

So $x^{109} \equiv 53 \bmod 7$

$\Rightarrow (x^6)^{18} x \equiv 4 \bmod 7$

$\Rightarrow x \equiv 4 \bmod 7$

& $(x^{10})^{13} x \equiv 4 \bmod 11$

$\Rightarrow x \equiv 4 \bmod 11$

So $x \equiv 4 \bmod (7 \times 11)$

$x \equiv 4 \bmod 77$

since hcf $(7,11) = 1$

13) Solve the simultaneous linear congruences

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 4 \pmod 7.$$

(4)

(A) $x = 2 + 3k$

Sub into $x \equiv 3 \bmod 5$

$2 + 3k \equiv 3 \bmod 5$

$3k \equiv 1 \bmod 5$ since $hcf(3,5) = 1$

$\times 2$ ( ) $\times 2$

$k \equiv 2 \bmod 5$

$k = 2 + 5a$

Sub into (A):

$x = 2 + 3(2 + 5a)$

$= 8 + 15a$ (B)

Sub (B) into $x \equiv 4 \bmod 7$

$8 + 15a \equiv 4 \bmod 7$

$1 + a \equiv 4 \bmod 7$

$a \equiv 3 \bmod 7$

So $a = 3 + 7b$ where $b \in \mathbb{Z}$

Sub this into (B):

$x = 8 + 15(3 + 7b)$

$= 53 + 105b$

$\boxed{x \equiv 53 \bmod 105}$

14. Let G be a group of order $46^{46} + 47^{47}$

Using Fermat's Little Theorem and explaining your reasoning, determine which of the following are possible orders for a subgroup of G

(i) 11

(ii) 21

(7)

by Lagrange's Theorem, order of subgroup divides order of group.

i.e. we need to check if $11 \mid 46^{46} + 47^{47}$

$$46^{46} + 47^{47} \equiv 2^{46} + 3^{47} \mod 11$$

$$\equiv 2^{4\times10+6} + 3^{4\times10+7} \mod 11$$

$$\equiv (2^{10})^4 (2)^6 + (3^{10})^4 3^7 \mod 11$$

by FLT

$$\equiv 2^6 + 3^7 \mod 11$$

$$\equiv 2^3 \times 2^3 + 3^3 \times 3^3 \times 3 \mod 11$$

$$\equiv -3 \times -3 + 5 \times 5 \times 3 \mod 11$$

$$\equiv 9 + 2 \times 3 \mod 11$$

$$\equiv 4 \mod 11$$

so $11 \nmid 46^{46} + 47$ so it's not a possible order of the subgroup.

15) Solve the simultaneous linear congruences

$$x \equiv 3 \pmod 6, \qquad x \equiv 5 \pmod 8, \qquad x \equiv 9 \pmod{14}.$$

(4)

$x \equiv 3 \bmod 6$

$\Rightarrow x = 3 + 6a$ (A) where $a \in \mathbb{Z}$

Sub (A) into $x \equiv 5 \bmod 8$

$3 + 6a \equiv 5 \bmod 8$

$6a \equiv 2 \bmod 8$

$3a \equiv 1 \bmod 4$ ($3a \equiv 1 \bmod 8$ is incorrect!)

$\times 3$ ( ) $\times 3$ $\quad$ hcf $(3,4) = 1$

$a \equiv 3 \bmod 4$

So $a = 3 + 4b$ (B) where $b \in \mathbb{Z}$

sub (B) into (A):

$x = 3 + 6(3 + 4b)$

$= 21 + 24b$ (C)

Sub (C) into $x \equiv 9 \bmod 14$

$21 + 24b \equiv 9 \bmod 14$

$7 + 10b \equiv 9 \bmod 14$

$10b \equiv 2 \bmod 14$

$5b \equiv 1 \bmod 7$

$\times 3$ ( ) $\times 3$

$b \equiv 3 \bmod 7$

$b = 3 + 7c$

Sub $b = 3 + 7c$ back into (C): $x = 21 + 24(3 + 7c) = 93 + 168c$

$\boxed{x \equiv 93 \bmod 168}$

16) Let $m, n \in \mathbb{N}$, and suppose $x, a, b \in \mathbb{Z}$ satisfy

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.$$

Prove that

$$a \equiv b \pmod{\gcd(m, n)}.$$

(4)

Suppose $x \equiv a \bmod m$ and $x \equiv b \bmod n$

then $x = a + tm$ and $x = b + pn$ where $t, p \in \mathbb{Z}$

(A) $x - a = tm$ and $x - b = pn$ (B)

(A) − (B) $b - a = tm - pn$

now let $d = hcf(n, m)$

$d \mid n$ and $d \mid m$ so $d \mid tm - pn$ by closure of divisibility

$\Rightarrow tm - pn \equiv 0 \bmod d$

$\Rightarrow b - a \equiv 0 \bmod d$

$\Rightarrow b \equiv a \bmod d$

$\Rightarrow b \equiv a \bmod (hcf(n, m))$

□

please note there's plenty of ways to prove this. There's actually more efficient ways to prove this but I have tried to make my proof as straightforward as possible

17 **(a)** The group G consists of the set $S = \{1, 9, 17, 25\}$ under $\times_{32}$, the operation of multiplication modulo 32.

(i) Complete the Cayley table for G given in the Printed Answer Booklet. **[2]**

(ii) Up to isomorphisms, there are only two groups of order 4.

- C_4, the cyclic group of order 4
- K_4, the non-cyclic (Klein) group of order 4

State, with justification, to which of these two groups G is isomorphic. **[2]**

(b) **(i)** List the odd quadratic residues modulo 32. **[2]**

(ii) Given that n is an odd integer, prove that $n^6 + 3n^4 + 7n^2 \equiv 11 \pmod{32}$. **[4]**

a) i)

$\times_{32}$	1	9	17	25
1	1	9	17	25
9	9	17	25	1
17	17	25	1	9
25	25	1	9	17

ii) Check if G is cyclic:

element	1	9	17	25
order	1	?	2	?

ord(9) & ord(25) must equal 4 because order of any element divides the order of the group by Lagrange's Theorem. So both 9 & 25 are generators so G is cyclic and thus isomorphic to C_4.

bi) To find Quadratic Residues check up to $\left(\frac{n-1}{2}\right)^2$ ****

i.e. here we would check $1^2, 2^2, 3^3, 4^2, \ldots, 15^2$.

Since we only want odd Quadratic Residues we only check the odd numbers squared.

$1^2 \equiv 1$

$3^2 \equiv 9$

$5^2 \equiv 25$

$7^2 \equiv (16-7)^2 \equiv 9^2 \equiv 17$ by ai)

$9^2 \equiv 17$ by ai)

$11^2 \equiv (16-11)^2 \equiv 5^2 \equiv 25$

$13^2 \equiv (16-13)^2 \equiv 3^2 \equiv 9$

$15^2 \equiv (16-15)^2 \equiv 1^2 \equiv 1$

So 1, 9, 17, 25 are the odd QRs.

Trick: $a^2 \equiv (16-a)^2 \bmod 32$

because if I expand RHS I get

$16^2 - 2\times 16 \times a + a^2$

$\equiv 0 \quad \equiv 0$

$\equiv a^2 \bmod 32$

ii) Let $A = n^6 + 3n^4 + 7n^2 = (n^2)^3 + 3(n^2)^2 + 7(n^2)$

if n is an odd integer then by bi) we know

$n^2 \equiv 1, 9, 17$ or $25 \bmod 32$

By Exhaustion,

if $n^2 \equiv 1 \bmod 32$ then $A \equiv 1^3 + 3(1)^2 + 7(1)$

$\equiv 11 \bmod 32$

if $n^2 \equiv 9 \bmod 32$ then $A \equiv 9^3 + 3(9)^2 + 7(9)$

$9^2 \equiv 17 \bmod 32$ by ai)

$\equiv 9^2 \times 9 + 3(17) + 63 \bmod 32$

see ai) $\equiv (17 \times 9) + 51 - 1 \bmod 32$

$\equiv 25 + 51 - 1 \bmod 32$

$\equiv 75 \bmod 32$

$\equiv 11 \bmod 32$

$17^2 \equiv 1 \bmod 32$ by ai ****

if $n^2 \equiv 17 \bmod 32$

then $A \equiv (17)^3 + 3(17)^2 + 7(17)$

$\equiv 17 + 3(17) + 23$

$\equiv 43$

$\equiv 11 \bmod 32$

if $n^2 \equiv 25 \bmod 32$

$A \equiv (25)^3 + 3(25)^2 + 7(25)$

$\equiv 25 \times 17 + 3 \times 17 + 7(-7)$

$\equiv 9 + 51 - 49$

$\equiv 11 \bmod 32$

18 Throughout this question, n is a positive integer.

(a) Explain why $n^5 \equiv n \pmod 5$. **[1]**

(b) By proving that $n^5 \equiv n \pmod 2$, show that $n^5 \equiv n \pmod{10}$. **[3]**

(c) **(i)** Prove that $n^5 - n$ is divisible by 30 for all positive integers n. **[5]**

(ii) Is there an integer N, greater than 30, such that $n^5 - n$ is divisible by N for all positive integers n? Justify your answer. **[1]**

a) by Fermat's Little theorem,

$n^4 \equiv 1 \bmod 5$

$\times n$ ( ) $\times n$

$n^5 \equiv n \bmod 5$

b) $0^5 = 0 \equiv 0 \bmod 2$

$1^5 = 1 \equiv 1 \bmod 2$

so $n^5 \equiv n \bmod 2$

we know that $n^5 \equiv n \bmod 5$ and $n^5 \equiv n \bmod 2$

since $hcf(5,2) = 1$ then $n^5 \equiv n \bmod (2 \times 5)$

i.e. $n^5 \equiv n \bmod 10$

If this doesn't make sense think about how you would check if a number, N, was divisible by 66 for example.

You'd check if $6 \mid N$ and if $11 \mid N$.

if N is a multiple of 6 and 11 then it must be a multiple of 66.

In our question, we're saying $n^5 - n$ is a multiple of 5 and of 2, so $n^5 - n$ is a multiple of 10

$\Rightarrow n^5 - n \equiv 0 \bmod 10$

$\Rightarrow n^5 \equiv n \bmod 10$

****

(c i) if $n \equiv 0 \bmod 3$, then $n^5 - n \equiv 0 \bmod 3$

if $n \equiv 1$ or $2 \bmod 3$ then $n^2 \equiv 1 \bmod 3$ by FLT

$\Rightarrow n^4 \equiv 1 \bmod 3$

$\Rightarrow n^5 \equiv n \bmod 3$

$\Rightarrow n^5 - n \equiv 0 \bmod 3$

So $n^5 - n \equiv 0 \bmod 3$ for all $n \in \mathbb{Z}$.

$n^5 \equiv n \bmod 10$ and $n^5 \equiv n \bmod 3$ and hcf $(3, 10) = 1$

$\Rightarrow n^5 \equiv n \bmod (10 \times 3)$

$\Rightarrow n^5 \equiv n \bmod 30$

(ii) No. if $n = 2$, $n^5 - n = 30$ which cannot be divisible by any number greater than 30.

19) Prove that

$$\gcd(12n+3,\ 20n+1) = \begin{cases} a, & \text{when } n \equiv b \pmod{c}, \\ d, & \text{otherwise,} \end{cases}$$

where $a, b, c, d \in \mathbb{Z}$ are to be found. (5)

let $h = \gcd(12n+3, 20n+1)$

$h \mid 12n+3$ & $h \mid 20n+1$

So $h \mid a(12n+3) + b(20n+1)$ for all $a, b \in \mathbb{Z}$

$\Rightarrow h \mid 5(12n+3) - 3(20n+1)$

$\Rightarrow h \mid 60n+15-60n-3$

$\Rightarrow h \mid 12$

$\Rightarrow h = 1, 2, 3, 4, 6$ or 12

now $20n+1$ is always odd $(20n+1 \equiv 1 \bmod 2)$

So $h \neq 2, 4, 6$ or 12

$\Rightarrow h = 1$ or 3

if $h=3$ then $20n+1 \equiv 0 \bmod 3$

$\Rightarrow 2n \equiv -1 \bmod 3$

$2n \equiv 2 \bmod 3$

$n \equiv 1 \bmod 3$ $\quad \text{hcf}(2,3) = 1$

so $\boxed{a=3,\ b=1,\ c=3 \text{ \& } d=1}$

20) Solve

$$x^9 \equiv 6 \pmod{77}.$$

(5)

$x^9 \equiv 6 \bmod 77$

$\Longleftrightarrow \quad x^9 \equiv 6 \bmod 7 \quad$ and $\quad x^9 \equiv 6 \bmod 11$

since $hcf(7,11)=1$

(A) $x^3 \equiv 6 \bmod 7 \quad$ and $\quad x^{-1} \equiv 6 \bmod 11$ (B)

Solve (A) by trial & error :

$x \equiv 3$ or 5 or $6 \bmod 7$

Solve (B) by raising both sides to "the minus one"

$x \equiv 6^{-1} \bmod 11$

6 inverse mod 11 is just 2

So $x \equiv 2 \bmod 11$

$x \equiv 3 \bmod 7$

$\Rightarrow x = 3 + 7k$

$3 + 7k \equiv 2 \bmod 11$

$7k \equiv 10 \bmod 11 \qquad hcf(7,11)=1$

$\times 8 \left(\quad \right) \times 8$

$k \equiv 3 \bmod 11$

$\Rightarrow k = 3 + 11a$

So $x = 3 + 7(3+11a)$

$= 24 + 77a$

$x \equiv 24 \bmod 77$

doing the same procedure for $x \equiv 5, 6 \bmod 7$ gives :

$x \equiv 13, 24$ or $68 \bmod 77$

21) Solve the congruence

$$x^{1351} \equiv 2024 \pmod{2027}.$$

(5)

Using FACT on calculator 2027 is prime

So $x^{2026} \equiv 1 \bmod 2027$ where $\gcd(x, 2027) = 1$

I want to find an integer k such that

$(x^{1351})^k = x^{2026a} x$ where a is an integer

i.e. $1351k = 2026a + 1$

$\Rightarrow 1351k \equiv 1 \bmod 2026$

so we look for inverse of 1351 mod 2026.

by Euclid's Algorithm,

$2026 = 1351(1) + 675$

$1351 = 675(2) + 1$

$\Rightarrow 1 = 1351 - 675(2)$

$= 1351 - (2026 - 1351)(2)$

$= 3(1351) - 2(2026)$

So $1351 \times 3 \equiv 1 \bmod 2026$

$x^{1351} \equiv -3 \bmod 2027$

$(x^{1351})^3 \equiv (-3)^3 \bmod 2027 \Rightarrow x \equiv -27 \bmod 2027$

$\equiv \boxed{2000 \bmod 2027}$

22 **(i)** **(a)** Prove that $p \equiv \pm 1 \pmod 6$ for all primes $p > 3$. **[2]**

(b) Hence or otherwise prove that $p^2 - 1 \equiv 0 \pmod{24}$ for all primes $p > 3$. **[3]**

(ii) Given that p is an odd prime, determine the residue of 2^{p^2-1} modulo p. **[4]**

(iii) Let p and q be distinct primes greater than 3. Prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. **[5]**

i) a) for all primes $p > 3$, $p = 2k+1$ for some $k \in \mathbb{Z}$, i.e. they're all odd. So $p \equiv 1, 3$ or $5 \bmod 6$

but if $p \equiv 3 \bmod 6$ then $p = 3 + 6m$ for some $m \in \mathbb{Z}$

$= 3(1+2m)$ i.e. $3 \mid p$

which is impossible since p is prime and $p > 3$.

$\therefore$ $p \equiv 1$ or $5 \bmod 6 \Rightarrow p \equiv \pm 1 \bmod 6$

b) $p \equiv \pm 1 \bmod 6$

$\Rightarrow p \pm 1 = 6k$ for some $k \in \mathbb{Z}$

$\Rightarrow p^2 - 1 = (6k \pm 1)^2 - 1$

$= 36k^2 \pm 12k + 1 - 1$

$= 36k^2 + 12k$

$\equiv 12k^2 + 12k \bmod 24$

$\equiv 12k(k+1) \bmod 24$

k & $k+1$ are consecutive integers so one is odd and one is even.

even $\times$ odd = even. So $k(k+1) = 2m$ for some $m \in \mathbb{Z}$

i.e. $p^2 - 1 \equiv 12k \times 2m \bmod 24$

$\equiv 24mk \bmod 24$

$\equiv 0 \bmod 24$

ii) From Fermat's Little Theorem, we know that ******

$a^{p-1} \equiv 1 \bmod p$ where a is not a multiple of p.

$\therefore 2^{p-1} \equiv 1 \bmod p$ for $p \neq 2$.

$$2^{p^2-1} = 2^{(p-1)(p+1)} = (2^{p-1})^{p+1}$$
$$\equiv (1)^{p+1} \bmod p$$
$$\equiv 1 \bmod p.$$

iii) (A) $p^{q-1} \equiv 1 \bmod q$ by FLT

(B) $q^{p-1} \equiv 1 \bmod p$ by FLT

Adding q^{p-1} to both sides of (A) gives:

$p^{q-1} + q^{p-1} \equiv 1 \bmod q$ since $q^{p-1} \equiv 0 \bmod q$

Similarly $q^{p-1} + p^{q-1} \equiv 1 \bmod p$

Now, since $hcf(p,q) = 1$ since they're both distinct primes

$p^{q-1} + q^{p-1} \equiv 1 \bmod pq$