Modular Arithmetic

Type I: Congruence

Let a and b be integers and m a positive integer. The integer a is said to be congruent b modulo m if $m|(a-b)$. If $m \nmid (a-b)$ then we say a is incongruent to b modulo m.

$a \equiv b(mod\ m)$ if and only if $m|(a-b)$

$a \not\equiv b(mod\ m)$ if and only if $m \nmid (a-b)$

Some properties:

- $a \equiv a(mod\ m)$
- If $a \equiv b(mod\ m)$, then $b \equiv a(mod\ m)$
- If $a \equiv b(mod\ m), b \equiv c(mod\ m)$, then $a \equiv c(mod\ m)$
- If $a \equiv b(mod\ m)$ then $(a+c) \equiv (b+c)(mod\ m)$
- If $a \equiv b(mod\ m)$ then $(a-c) \equiv (b-c)(mod\ m)$
- If $a \equiv b(mod\ m)$ then $(ac) \equiv (bc)(mod\ m)$
- If $(a \pm c) \equiv (b \pm c)(mod\ m)$ then $a \equiv b(mod\ m)$
- Let $a \equiv b(mod\ m), c \equiv d(mod\ m)$ then $a + c \equiv (b+d)(mod\ m)$
- Let $a \equiv b(mod\ m), c \equiv d(mod\ m)$ then $a - c \equiv (b-d)(mod\ m)$
- Let $a \equiv b(mod\ m), c \equiv d(mod\ m)$ then $ac \equiv (bd)(mod\ m)$
- If $a \equiv b(mod\ m)$ then $a + mk \equiv b(mod\ m)$
- If $a \equiv b(mod\ m)$ then $a^k \equiv b^k(mod\ m)$

Solving Linear Congruences $\boldsymbol{ax \equiv b(mod\ m)}$

The linear congruence $ax \equiv b(mod\ m)$ has a solution if and only if $d|b$, where $d = (a, m)$. In that case, there are precisely d incongruent solutions modulo m which are $x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, x_0 + \frac{3m}{d}, \dots \dots \dots, x_0 + \frac{(d-1)m}{d}$

1. Find the remainder when 7 divides:

   (a) 2^{50}

   [M19/IT/5M]

   Solution:

   We see that,

   $2^3 \equiv 8 \equiv 1(mod\ 7)$

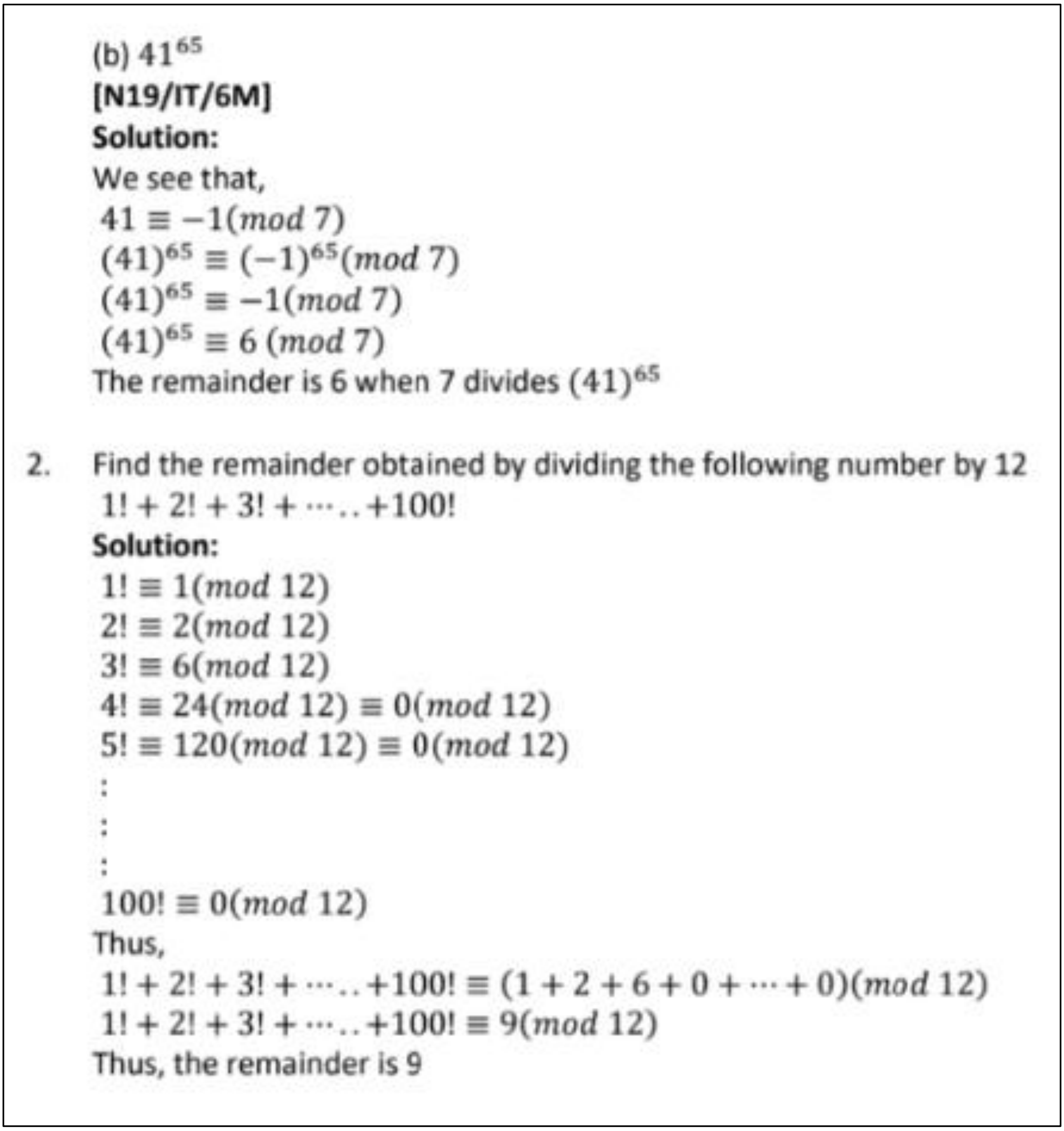
   $(2^3)^{16} \equiv 1^{16}(mod\ 7)$

   $2^{48} \equiv 1(mod\ 7)$

   $2^2.2^{48} \equiv 2^2.1\ (mod\ 7)$

   $2^{50} \equiv 4(mod\ 7)$

   The remainder is 4 when 7 divides 2^{50}



(b) 41^{65}

[N19/IT/6M]

Solution:

We see that,

$41 \equiv -1(mod\ 7)$

$(41)^{65} \equiv (-1)^{65}(mod\ 7)$

$(41)^{65} \equiv -1(mod\ 7)$

$(41)^{65} \equiv 6\ (mod\ 7)$

The remainder is 6 when 7 divides $(41)^{65}$

2. Find the remainder obtained by dividing the following number by 12

$1! + 2! + 3! + \cdots .. + 100!$

Solution:

$1! \equiv 1(mod\ 12)$

$2! \equiv 2(mod\ 12)$

$3! \equiv 6(mod\ 12)$

$4! \equiv 24(mod\ 12) \equiv 0(mod\ 12)$

$5! \equiv 120(mod\ 12) \equiv 0(mod\ 12)$

$\vdots$

$\vdots$

$\vdots$

$100! \equiv 0(mod\ 12)$

Thus,

$1! + 2! + 3! + \cdots .. + 100! \equiv (1 + 2 + 6 + 0 + \cdots + 0)(mod\ 12)$

$1! + 2! + 3! + \cdots .. + 100! \equiv 9(mod\ 12)$

Thus, the remainder is 9

3. Prove that 3 divides $1^3 + 2^3 + 3^3 + \cdots \ldots . +99^3$

Solution:

Let $S = 1^3 + 2^3 + 3^3 + \cdots \ldots . +99^3$

The integers 1,2, … …,99 can be divided into three sections

(i) $n = 3k, k = 1,2, \ldots .33$

(ii) $n = 3k + 1, k = 0,1,2,3, \ldots 32$

(iii) $n = 3k + 2, k = 0,1,2, \ldots . .32$

Now,

If $n = 3k$,

then $n^3 \equiv (3k)^3 (mod\ 3) \equiv 0 (mod\ 3)$ ……………………(1)

If $n = 3k + 1$,

then $n^3 \equiv (3k + 1)^3 (mod\ 3) \equiv 1^3 (mod\ 3) \equiv 1 (mod\ 3)$ …………(2)

If $n = 3k + 2$,

then $n^3 \equiv (3k + 2)^3 (mod\ 3) \equiv 2^3 (mod\ 3) \equiv 8 (mod\ 3)$ ………..(3)

Adding all three equations we get,

$S = (0 + 1 + 8)(mod\ 3)$

$S = 9\ (mod\ 3)$

$S = 0(mod\ 3)$

Thus, 3 divides $1^3 + 2^3 + 3^3 + \cdots \ldots . +99^3$

4. Using the congruence, prove that

(a) $97 | 2^{48} - 1$

[N18/IT/5M]

Solution:

We have,

$2^6 \equiv 64 (mod\ 97)$

$(2^6)^2 \equiv 64^2 (mod\ 97) \equiv 4096 (mod\ 97)$

$2^{12} \equiv 22 (mod\ 97)$

$(2^{12})^2 \equiv 22^2 (mod\ 97) \equiv 484 (mod\ 97) \equiv 96 (mod\ 97)$

$2^{24} \equiv -1 (mod\ 97)$

$(2^{24})^2 \equiv (-1)^2 (mod\ 97)$

$2^{48} \equiv 1 (mod\ 97)$

Thus, $97 | 2^{48} - 1$

(b) $17|\,(11^{104}+1)$

Solution:

$11 \equiv 11(mod\ 17) \equiv -6(mod\ 17)$
$11^2 \equiv (-6)^2(mod\ 17) \equiv 36(mod\ 17) \equiv 2(mod\ 17)$
$(11^2)^4 \equiv 2^4(mod\ 17) \equiv 16(mod\ 17)$
$11^8 \equiv -1(mod\ 17)$
$(11^8)^{13} \equiv (-1)^{13}(mod\ 17)$
$11^{104} \equiv -1(mod\ 17)$

Thus, $17|\,(11^{104}+1)$

(c) $13|\,(11^{12n+6}+1)$

Solution:

$11 \equiv 11(mod\ 13) \equiv -2(mod\ 13)$
$11^6 \equiv (-2)^6(mod\ 13) \equiv 64(mod\ 13) \equiv -1(mod\ 13)$
$(11^6)^{2n+1} \equiv (-1)^{2n+1}(mod\ 13)$
$11^{12n+6} \equiv -1(mod\ 13)$

Thus, $13|\,(11^{12n+6}+1)$

5. Prove that 39 divides $53^{103}+103^{53}$

[N18/IT/6M]

Solution:

We have,

$53 \equiv 14(mod\ 39)$
$(53)^2 \equiv 14^2(mod\ 39) \equiv 196(mod\ 39) \equiv 1(mod\ 39)$
$(53^2)^{51} \equiv 1^{51}(mod\ 39)$
$53^{102} \equiv 1(mod\ 39)$
$53^{102} \times 53 \equiv 1 \times 53(mod\ 39)$
$53^{103} \equiv 14(mod\ 39)$.................. (1)

And,

$103 \equiv 25(mod\ 39)$
$103^2 \equiv 25^2(mod\ 39) \equiv 625(mod\ 39) \equiv 1(mod\ 39)$
$(103^2)^{26} \equiv 1^{26}(mod\ 39)$
$103^{52} \equiv 1(mod\ 39)$
$103^{52} \times 103 \equiv 1 \times 103(mod\ 39)$
$103^{53} \equiv 25(mod\ 39)$......................... (2)

Adding (1) & (2), we get

$53^{103}+103^{53} = (14+25)(mod\ 39)$
$53^{103}+103^{53} = 39(mod\ 39) = 0(mod\ 39)$

Thus, $53^{103}+103^{53}$ is divisible by 39

6. Prove that $111^{333} + 333^{111}$ is divisible by 7

[M18/IT/6M][M19/IT/4M]

Solution:

We have,

$111 \equiv 6(mod\ 7)$ since $111 = 15 \times 7 + 6$

$111 \equiv -1(mod\ 7)$

$(111)^{333} \equiv (-1)^{333}(mod\ 7)$

$(111)^{333} \equiv -1(mod\ 7)$ .... (1)

And,

$111 \equiv -1(mod\ 7)$

$3 \times 111 = 3 \times -1(mod\ 7)$

$333 = -3(mod\ 7)$

$333 = 4(mod\ 7)$

$333^3 = (4)^3(mod\ 7)$

$333^3 = 64(mod\ 7)$

$333^3 = 1(mod\ 7)$

$(333^3)^{37} = (1)^{37}(mod\ 7)$

$333^{111} = 1(mod\ 7)$ .... (2)

Adding (1) & (2), we get

$111^{333} + 333^{111} = (-1 + 1)(mod\ 7)$

$111^{333} + 333^{111} = 0\ (mod\ 7)$

Thus, $111^{333} + 333^{111}$ is divisible by 7

7. Solve the following linear congruences:

a) $3x \equiv 2(mod\ 7)$

Solution:

$3x \equiv 2(mod\ 7)$

It is of the form $ax \equiv b(mod\ m)$ where $a = 3, b = 2, m = 7$

Now, gcd $(a, m) = (3,7) = 1$

Therefore there is exactly one solution of $3x \equiv 2(mod\ 7)$

Then,

$3x \equiv 2(mod\ 7)$

$2 \equiv 3x(mod\ 7)$

$2 \times 2 \equiv 2 \times 3x(mod\ 7)$

$4 \equiv 6x(mod\ 7)$

$4 \equiv -1x(mod\ 7)$

$x \equiv -4(mod\ 7)$

$x \equiv 3(mod\ 7)$

Thus, $x = 3$

b) $6x \equiv 3(mod\ 9)$

Solution:

$6x \equiv 3(mod\ 9)$

It is of the form $ax \equiv b(mod\ m)$ where $a = 6, b = 3, m = 9$

Now, gcd $(a, m) = (6,9) = 3$

Therefore there are exactly three solutions of $6x \equiv 3(mod\ 9)$

Then,

$6x \equiv 3(mod\ 9)$

$2x \equiv 1(mod\ 3)$ by the property if $a \equiv b(mod\ m)$ then $\frac{a}{n} \equiv \frac{b}{n}\left(mod\ \frac{m}{n}\right)$

$1 \equiv 2x(mod\ 3)$

$1 \equiv -1x(mod\ 3)$

$x \equiv -1(mod\ 3)$

$x \equiv 2(mod\ 3)$

Thus, $x_0 = 2$

Further solutions are

$x_1 = x_0 + \frac{m}{d} = 2 + \frac{9}{3} = 2 + 3 = 5$

$x_2 = x_0 + \frac{2m}{d} = 2 + \frac{2\times 9}{3} = 8$

Thus, the solutions are $x = 2, 5, 8$

c) $128x \equiv 833(mod\ 1001)$

Solution:

$128x \equiv 833(mod\ 1001)$

It is of the form $ax \equiv b(mod\ m)$ where $a = 128, b = 833, m = 1001$

Now, gcd $(a, m) = (128,1001) = 1$

Therefore there is exactly one solution of $128x \equiv 833(mod\ 1001)$

Then,

$128x \equiv 833(mod\ 1001)$

$128x \equiv -168(mod\ 1001)$

$16x \equiv -21(mod\ 1001)$ Dividing by 8

$16x \equiv 980(mod\ 1001)$

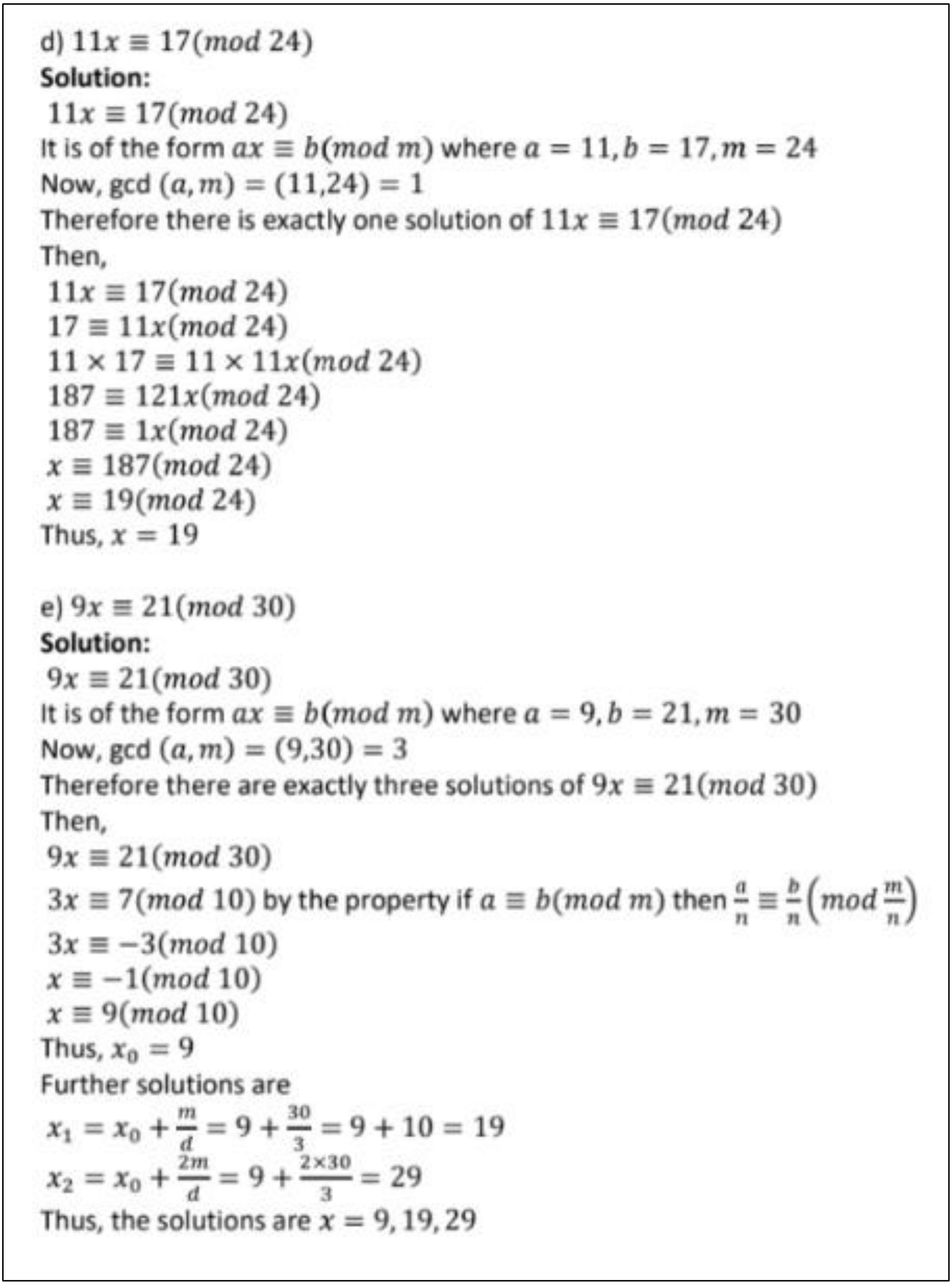
$4x \equiv 245(mod\ 1001)$ Dividing by 4

$4x \equiv -756(mod\ 1001)$

$x \equiv -189(mod\ 1001)$

$x \equiv 812(mod\ 1001)$

Thus, $x = 812$



d) $11x \equiv 17(mod\ 24)$

Solution:

$11x \equiv 17(mod\ 24)$

It is of the form $ax \equiv b(mod\ m)$ where $a = 11, b = 17, m = 24$

Now, gcd $(a, m) = (11,24) = 1$

Therefore there is exactly one solution of $11x \equiv 17(mod\ 24)$

Then,

$11x \equiv 17(mod\ 24)$

$17 \equiv 11x(mod\ 24)$

$11 \times 17 \equiv 11 \times 11x(mod\ 24)$

$187 \equiv 121x(mod\ 24)$

$187 \equiv 1x(mod\ 24)$

$x \equiv 187(mod\ 24)$

$x \equiv 19(mod\ 24)$

Thus, $x = 19$

e) $9x \equiv 21(mod\ 30)$

Solution:

$9x \equiv 21(mod\ 30)$

It is of the form $ax \equiv b(mod\ m)$ where $a = 9, b = 21, m = 30$

Now, gcd $(a, m) = (9,30) = 3$

Therefore there are exactly three solutions of $9x \equiv 21(mod\ 30)$

Then,

$9x \equiv 21(mod\ 30)$

$3x \equiv 7(mod\ 10)$ by the property if $a \equiv b(mod\ m)$ then $\frac{a}{n} \equiv \frac{b}{n}\left(mod\ \frac{m}{n}\right)$

$3x \equiv -3(mod\ 10)$

$x \equiv -1(mod\ 10)$

$x \equiv 9(mod\ 10)$

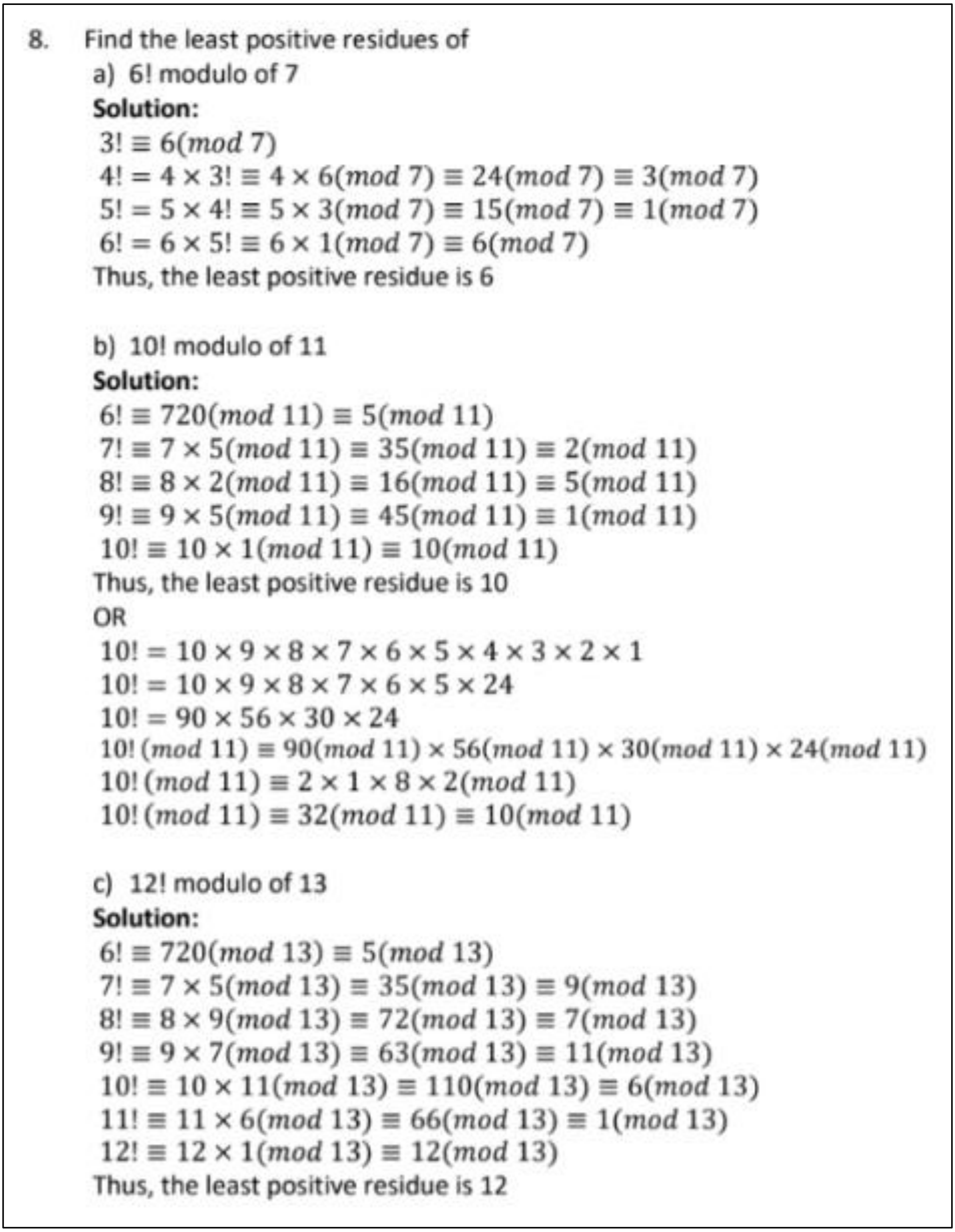
Thus, $x_0 = 9$

Further solutions are

$x_1 = x_0 + \frac{m}{d} = 9 + \frac{30}{3} = 9 + 10 = 19$

$x_2 = x_0 + \frac{2m}{d} = 9 + \frac{2 \times 30}{3} = 29$

Thus, the solutions are $x = 9, 19, 29$



8. Find the least positive residues of

a) 6! modulo of 7

Solution:

$3! \equiv 6(mod\ 7)$

$4! = 4 \times 3! \equiv 4 \times 6(mod\ 7) \equiv 24(mod\ 7) \equiv 3(mod\ 7)$

$5! = 5 \times 4! \equiv 5 \times 3(mod\ 7) \equiv 15(mod\ 7) \equiv 1(mod\ 7)$

$6! = 6 \times 5! \equiv 6 \times 1(mod\ 7) \equiv 6(mod\ 7)$

Thus, the least positive residue is 6

b) 10! modulo of 11

Solution:

$6! \equiv 720(mod\ 11) \equiv 5(mod\ 11)$

$7! \equiv 7 \times 5(mod\ 11) \equiv 35(mod\ 11) \equiv 2(mod\ 11)$

$8! \equiv 8 \times 2(mod\ 11) \equiv 16(mod\ 11) \equiv 5(mod\ 11)$

$9! \equiv 9 \times 5(mod\ 11) \equiv 45(mod\ 11) \equiv 1(mod\ 11)$

$10! \equiv 10 \times 1(mod\ 11) \equiv 10(mod\ 11)$

Thus, the least positive residue is 10

OR

$10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$

$10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 24$

$10! = 90 \times 56 \times 30 \times 24$

$10!\,(mod\ 11) \equiv 90(mod\ 11) \times 56(mod\ 11) \times 30(mod\ 11) \times 24(mod\ 11)$

$10!\,(mod\ 11) \equiv 2 \times 1 \times 8 \times 2(mod\ 11)$

$10!\,(mod\ 11) \equiv 32(mod\ 11) \equiv 10(mod\ 11)$

c) 12! modulo of 13

Solution:

$6! \equiv 720(mod\ 13) \equiv 5(mod\ 13)$

$7! \equiv 7 \times 5(mod\ 13) \equiv 35(mod\ 13) \equiv 9(mod\ 13)$

$8! \equiv 8 \times 9(mod\ 13) \equiv 72(mod\ 13) \equiv 7(mod\ 13)$

$9! \equiv 9 \times 7(mod\ 13) \equiv 63(mod\ 13) \equiv 11(mod\ 13)$

$10! \equiv 10 \times 11(mod\ 13) \equiv 110(mod\ 13) \equiv 6(mod\ 13)$

$11! \equiv 11 \times 6(mod\ 13) \equiv 66(mod\ 13) \equiv 1(mod\ 13)$

$12! \equiv 12 \times 1(mod\ 13) \equiv 12(mod\ 13)$

Thus, the least positive residue is 12

d) 16! modulo of 17

Solution:

$6! \equiv 720(mod\ 17) \equiv 6(mod\ 17)$
$7! \equiv 7 \times 6(mod\ 17) \equiv 42(mod\ 17) \equiv 8(mod\ 17)$
$8! \equiv 8 \times 8(mod\ 17) \equiv 64(mod\ 17) \equiv 13(mod\ 17)$
$9! \equiv 9 \times 13(mod\ 17) \equiv 117(mod\ 17) \equiv 15(mod\ 17)$
$10! \equiv 10 \times 15 \equiv 150(mod\ 17) \equiv 14(mod\ 17)$
$11! \equiv 11 \times 14 \equiv 154(mod\ 17) \equiv 1(mod\ 17)$
$12! \equiv 12 \times 1 \equiv 12(mod\ 17)$
$13! \equiv 13 \times 12(mod\ 17) \equiv 156(mod\ 17) \equiv 3(mod\ 17)$
$14! \equiv 14 \times 3(mod\ 17) \equiv 42(mod\ 17) \equiv 8(mod\ 17)$
$15! \equiv 15 \times 8(mod\ 17) \equiv 120(mod\ 17) \equiv 1(mod\ 17)$
$16! \equiv 16 \times 1(mod\ 17) \equiv 16(mod\ 17)$

Thus, the least positive residue is 16

OR

$6! \equiv 720(mod\ 17) \equiv 6(mod\ 17)$
$16 \times 15 \equiv 240(mod\ 17) \equiv 2(mod\ 17)$
$14 \times 13 \equiv 182(mod\ 17) \equiv 12(mod\ 17)$
$12 \times 11 \equiv 132(mod\ 17) \equiv 13(mod\ 17)$
$10 \times 9 \equiv 90(mod\ 17) \equiv 5(mod\ 17)$
$8 \times 7 \equiv 56(mod\ 17) \equiv 5(mod\ 17)$
$16! \equiv (2 \times 12 \times 13 \times 5 \times 5 \times 6)(mod\ 17)$
$16! \equiv 46800(mod\ 17) \equiv 16(mod\ 17)$

Thus, the least positive residue is 16

9. Find the remainder when $1! + 2! + 3! + \cdots . +200!$ divided by 15

Solution:

$1! \equiv 1(mod\ 15)$
$2! \equiv 2(mod\ 15)$
$3! \equiv 6(mod\ 15)$
$4! \equiv 24(mod\ 15) \equiv 9(mod\ 15)$
$5! \equiv 120(mod\ 15) \equiv 0(mod\ 15)$
$\vdots$
$\vdots$
$\vdots$
$200! \equiv 0(mod\ 15)$

Thus,

$1! + 2! + 3! + \cdots .. +200! \equiv (1 + 2 + 6 + 9 + \cdots + 0)(mod\ 15)$
$1! + 2! + 3! + \cdots .. +200! \equiv 18(mod\ 15) \equiv 3(mod\ 15)$

Thus, the remainder is 3

10. Prove that 4 divides $1^5 + 2^5 + \cdots .. + 99^5 + 100^5$

[M19/IT/4M]

Solution:

Let $S = 1^5 + 2^5 + \cdots .. + 99^5 + 100^5$

The integers $1,2, \dots \dots, 100$ can be divided into four sections

(i) $n = 4k, k = 1,2, \dots .25$

(ii) $n = 4k + 1, k = 0,12,3, \dots 24$

(iii) $n = 4k + 2, k = 0,1,2, \dots ..24$

(iv) $n = 4k + 3, k = 0,1,2,3, \dots .24$

Now,

If $n = 4k$,

then $n^5 \equiv (4k)^5 (mod\ 4) \equiv 0(mod 4)$ ....(1)

If $n = 4k + 1$,

then $n^5 \equiv (4k + 1)^5 (mod\ 4) \equiv 1^5 (mod4) \equiv 1(mod4)$ ....(2)

If $n = 4k + 2$,

then $n^5 \equiv (4k + 2)^5 (mod\ 4) \equiv 2^5 (mod4) \equiv 0(mod4)$ ....(3)

If $n = 4k + 3$,

then $n^5 \equiv (4k + 3)^5 (mod\ 4) \equiv 3^5 (mod4) \equiv -1(mod4)$ ....(4)

Adding all 4 equations we get,

$S = (0 + 1 + 0 - 1)(mod\ 4)$

$S = 0\ (mod\ 4)$

Thus, 4 divides $1^5 + 2^5 + \cdots .. + 99^5 + 100^5$

11. Using the congruence, prove that

(a) $89 | 2^{44} - 1$

Solution:

$2 \equiv 2(mod\ 89)$

$2^{11} \equiv 2048(mod\ 89) \equiv 1(mod\ 89)$

$(2^{11})^4 \equiv 1(mod\ 89)$

Thus, $89 | 2^{44} - 1$

(b) $41 | (2^{20} - 1)$

Solution:

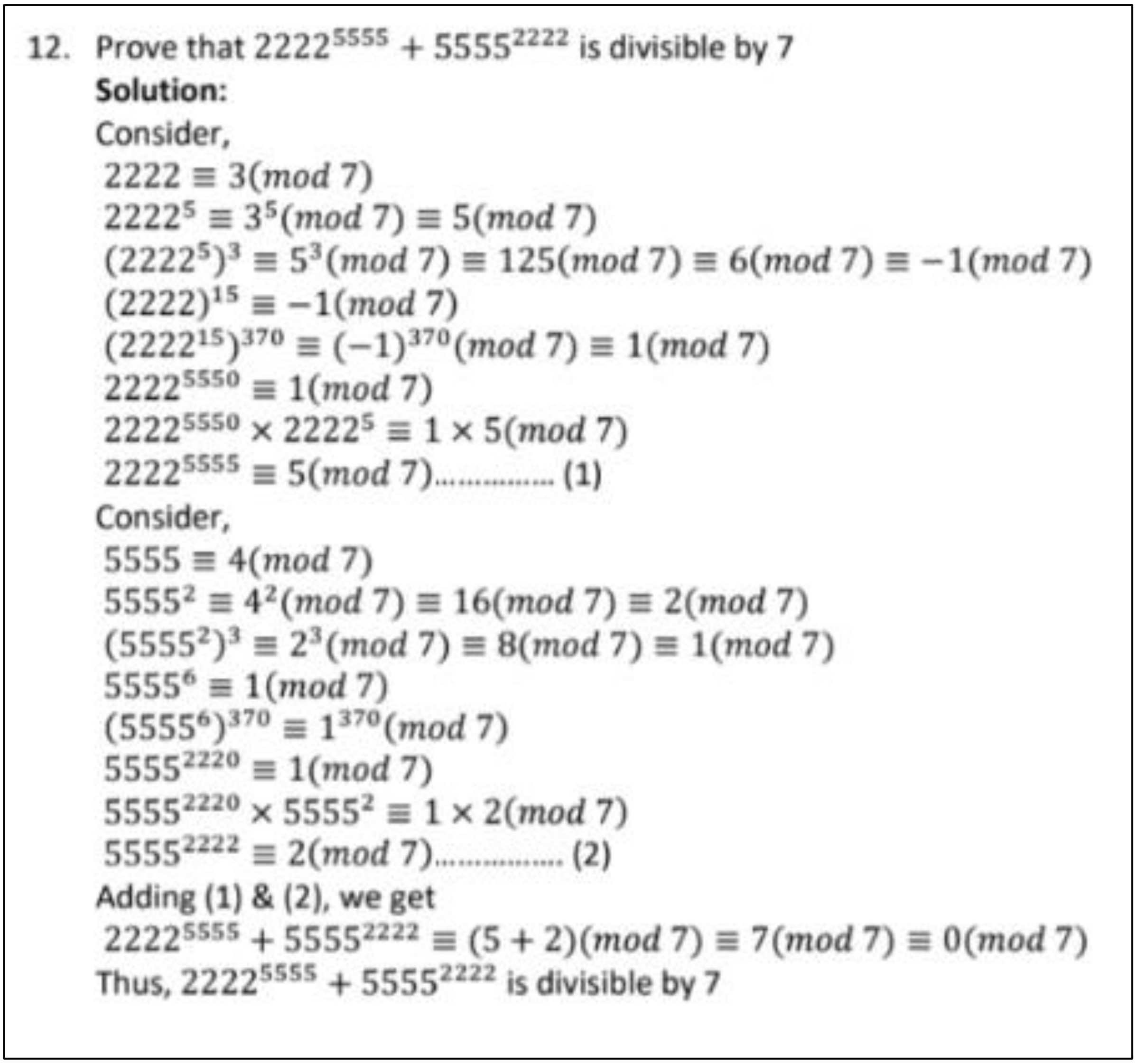
$2 \equiv 2(mod\ 41)$

$2^{10} \equiv 1024(mod\ 41) \equiv 40(mod\ 41) \equiv -1(mod\ 41)$

$(2^{10})^2 \equiv (-1)^2 (mod\ 41)$

$2^{20} \equiv 1(mod\ 41)$

Thus, $41 | (2^{20} - 1)$



12. Prove that $2222^{5555} + 5555^{2222}$ is divisible by 7

Solution:

Consider,

$2222 \equiv 3(mod\ 7)$

$2222^5 \equiv 3^5(mod\ 7) \equiv 5(mod\ 7)$

$(2222^5)^3 \equiv 5^3(mod\ 7) \equiv 125(mod\ 7) \equiv 6(mod\ 7) \equiv -1(mod\ 7)$

$(2222)^{15} \equiv -1(mod\ 7)$

$(2222^{15})^{370} \equiv (-1)^{370}(mod\ 7) \equiv 1(mod\ 7)$

$2222^{5550} \equiv 1(mod\ 7)$

$2222^{5550} \times 2222^5 \equiv 1 \times 5(mod\ 7)$

$2222^{5555} \equiv 5(mod\ 7)$................ (1)

Consider,

$5555 \equiv 4(mod\ 7)$

$5555^2 \equiv 4^2(mod\ 7) \equiv 16(mod\ 7) \equiv 2(mod\ 7)$

$(5555^2)^3 \equiv 2^3(mod\ 7) \equiv 8(mod\ 7) \equiv 1(mod\ 7)$

$5555^6 \equiv 1(mod\ 7)$

$(5555^6)^{370} \equiv 1^{370}(mod\ 7)$

$5555^{2220} \equiv 1(mod\ 7)$

$5555^{2220} \times 5555^2 \equiv 1 \times 2(mod\ 7)$

$5555^{2222} \equiv 2(mod\ 7)$................. (2)

Adding (1) & (2), we get

$2222^{5555} + 5555^{2222} \equiv (5 + 2)(mod\ 7) \equiv 7(mod\ 7) \equiv 0(mod\ 7)$

Thus, $2222^{5555} + 5555^{2222}$ is divisible by 7

13. Solve the following linear congruences:

a) $63x \equiv 110(mod\ 23)$

Solution:

$63x \equiv 110(mod\ 23)$

It is of the form $ax \equiv b(mod\ m)$ where $a = 63, b = 110, m = 23$

Now, gcd $(a, m) = (63,23) = 1$

Therefore there is exactly one solution of $63x \equiv 110(mod\ 23)$

Then, $63x \equiv 110(mod\ 23)$

$63x \equiv 18(mod\ 23)$

$18 \equiv 63x(mod\ 23)$

$18 \equiv 17x(mod\ 23)$

$18 \equiv -6x(mod\ 23)$

$4 \times 18 \equiv 4 \times -6x(mod\ 23)$

$72 \equiv -24x(mod\ 23)$

$72 \equiv -x(mod\ 23)$

$x \equiv -72(mod\ 23)$

$x \equiv -3(mod\ 23)$

$x \equiv 20(mod\ 23)$

Thus, $x = 20$

b) $9x \equiv 12(mod\ 15)$

Solution:

$9x \equiv 12(mod\ 15)$

It is of the form $ax \equiv b(mod\ m)$ where $a = 9, b = 12, m = 15$

Now, gcd $(a, m) = (9,15) = 3$

Therefore, there are exactly three solutions of $9x \equiv 12(mod\ 15)$

Then, $9x \equiv 12(mod\ 15)$

$3x \equiv 4(mod\ 5)$ by the property if $a \equiv b(mod\ m)$ then $\frac{a}{n} \equiv \frac{b}{n}\left(mod \frac{m}{n}\right)$

$3x \equiv -1(mod\ 5)$

$6x \equiv -2(mod\ 5)$

$6x \equiv 3(mod\ 5)$

$3 \equiv 6x(mod\ 5)$

$3 \equiv x(mod\ 5)$

$x \equiv 3(mod\ 5)$

Thus, $x_0 = 3$

Further solutions are

$x_1 = x_0 + \frac{m}{d} = 3 + \frac{15}{3} = 3 + 5 = 8$

$x_2 = x_0 + \frac{2m}{d} = 3 + \frac{2 \times 15}{3} = 13$

Thus, the solutions are $x = 3, 8, 13$

Type II: Fermat's Little theorem

$$\boxed{a^{p-1} \equiv 1(mod\ p)}$$

If p is prime and a is a positive integer, such that $p \nmid a$ then $a^{p-1} \equiv 1(mod\ p)$
Also, $a^p \equiv a(mod\ p)$

- a^{p-2} is the solution of $ax \equiv 1(mod\ p)$ i.e. a^{p-2} is inverse of a modulo p
- $a^{p-2}b$ is the solution of $ax \equiv b(mod\ p)$

Classwork Problems

1. Using Fermat's Little theorem, show that $5^{38} \equiv 4(mod\ 11)$

Solution:

Since 11 is a prime number,
We have by Fermat's little theorem, $a^{p-1} \equiv 1(mod\ p)$

$5^{11-1} \equiv 1(mod\ 11)$
$5^{10} \equiv 1(mod\ 11)$
$(5^{10})^3 \equiv 1^3(mod\ 11)$
$5^{30} \equiv 1(mod\ 11)$

Also,

$5^2 \equiv 25(mod\ 11) \equiv 3(mod\ 11)$
$(5^2)^4 \equiv 3^4(mod\ 11) \equiv 81(mod\ 11) \equiv 4(mod\ 11)$
$5^8 \equiv 4(mod\ 11)$

Thus,

$5^{30}.5^8 \equiv 1 \times 4(mod\ 11)$
$5^{38} \equiv 4(mod\ 11)$

2. Using Fermat's Little theorem, find the least positive residue of $2^{1000000}$ after dividing by 17

Solution:

Since 17 is a prime number,
We have by Fermat's little theorem,

$2^{17-1} \equiv 1(mod\ 17)$
$2^{16} \equiv 1(mod\ 17)$
$(2^{16})^{62500} \equiv 1^{62500}(mod\ 17)$
$2^{1000000} \equiv 1(mod\ 17)$

3. Find smallest positive integer modulo 5 to which $3^2.3^3.3^4.3^{10}$ is congruent **[M18/IT/5M]**

Solution:

$3^2.3^3.3^4.3^{10} = 3^{19}$

Since 5 is a prime number, we have by Fermat's little theorem,

$3^{5-1} \equiv 1(mod\ 5)$
$3^4 \equiv 1(mod\ 5)$
$(3^4)^4 \equiv 1^4(mod\ 5)$
$3^{16} \equiv 1(mod\ 5)$
$3^{16} \times 3^3 \equiv 1 \times 3^3(mod\ 5)$
$3^{19} \equiv 27(mod\ 5)$
$3^{19} \equiv 2(mod\ 5)$

4. Find the last digit of the base 7 expansion of 3^{100} using Fermat's Theorem **[N19/IT/4M]**

Solution:

Since 7 is a prime number,
We have by Fermat's little theorem,

$3^{7-1} \equiv 1(mod\ 7)$
$3^6 \equiv 1(mod\ 7)$
$(3^6)^{16} \equiv (1)^{16}(mod\ 7)$
$3^{96} \equiv 1(mod\ 7)$
$3^{96} \times 3^4 \equiv 1 \times 3^4(mod\ 7)$
$3^{100} \equiv 81(mod\ 7)$
$3^{100} \equiv 4(mod\ 7)$

The last digit is 4

5. Solve by Fermat's theorem

(a) $7^{222} mod\ 11$

Solution:

Since 11 is a prime number,
We have by Fermat's little theorem,

$7^{11-1} \equiv 1(mod\ 11)$
$7^{10} \equiv 1(mod\ 11)$
$(7^{10})^{22} \equiv 1^{22}(mod\ 11)$
$7^{220} \equiv 1(mod\ 11)$
$7^{220} \times 7^2 \equiv 1 \times 7^2(mod\ 11)$
$7^{222} \equiv 49(mod\ 11)$
$7^{222} \equiv 5(mod\ 11)$

(b) $3^{201} mod\ 11$

Solution:

Since 11 is a prime number,

We have by Fermat's little theorem,

$3^{11-1} \equiv 1(mod\ 11)$
$3^{10} \equiv 1(mod\ 11)$
$(3^{10})^{20} \equiv 1^{20}(mod\ 11)$
$3^{200} \equiv 1(mod\ 11)$
$3^{200} \times 3 \equiv 1 \times 3(mod\ 11)$
$3^{201} \equiv 3(mod\ 11)$

(c) $5^{15} mod\ 13$

Solution:

Since 13 is a prime number,

We have by Fermat's little theorem,

$5^{13-1} \equiv 1(mod\ 13)$
$5^{12} \equiv 1(mod\ 13)$
$5^{12} \times 5^{3} \equiv 1 \times 5^{3}(mod\ 13)$
$5^{15} \equiv 125(mod\ 13)$
$5^{15} \equiv 8(mod\ 13)$

6. Find solutions of the following congruences

(a) $7x \equiv 12(mod\ 17)$

Solution:

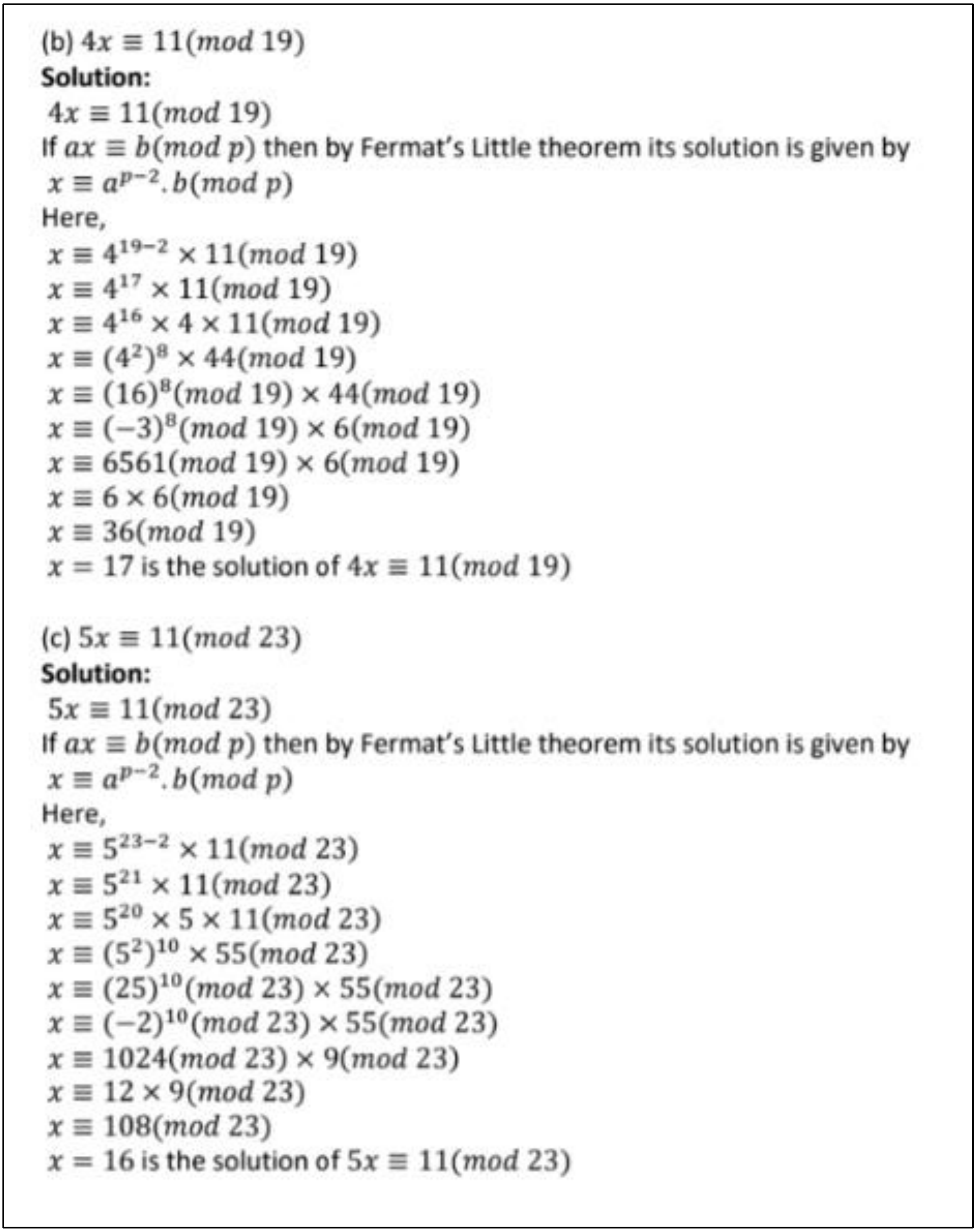
$7x \equiv 12(mod\ 17)$

If $ax \equiv b(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}.b(mod\ p)$

Here,

$x \equiv 7^{17-2} \times 12(mod\ 17)$
$x \equiv 7^{15} \times 12(mod\ 17)$
$x \equiv 7^{14} \times 7 \times 12(mod\ 17)$
$x \equiv (7^{2})^{7} \times 84(mod\ 17)$
$x \equiv (49)^{7}(mod\ 17) \times 84(mod\ 17)$
$x \equiv (15)^{7}(mod\ 17) \times 16(mod\ 17)$
$x \equiv (-2)^{7}(mod\ 17) \times -1(mod\ 17)$
$x \equiv -128 \times -1(mod\ 17)$
$x \equiv 128(mod\ 17)$
$x = 9$ is the solution of $7x \equiv 12(mod\ 17)$



(b) $4x \equiv 11(mod\ 19)$

Solution:

$4x \equiv 11(mod\ 19)$

If $ax \equiv b(mod\ p)$ then by Fermat's Little theorem its solution is given by
$x \equiv a^{p-2}.b(mod\ p)$

Here,

$x \equiv 4^{19-2} \times 11(mod\ 19)$
$x \equiv 4^{17} \times 11(mod\ 19)$
$x \equiv 4^{16} \times 4 \times 11(mod\ 19)$
$x \equiv (4^2)^8 \times 44(mod\ 19)$
$x \equiv (16)^8(mod\ 19) \times 44(mod\ 19)$
$x \equiv (-3)^8(mod\ 19) \times 6(mod\ 19)$
$x \equiv 6561(mod\ 19) \times 6(mod\ 19)$
$x \equiv 6 \times 6(mod\ 19)$
$x \equiv 36(mod\ 19)$
$x = 17$ is the solution of $4x \equiv 11(mod\ 19)$

(c) $5x \equiv 11(mod\ 23)$

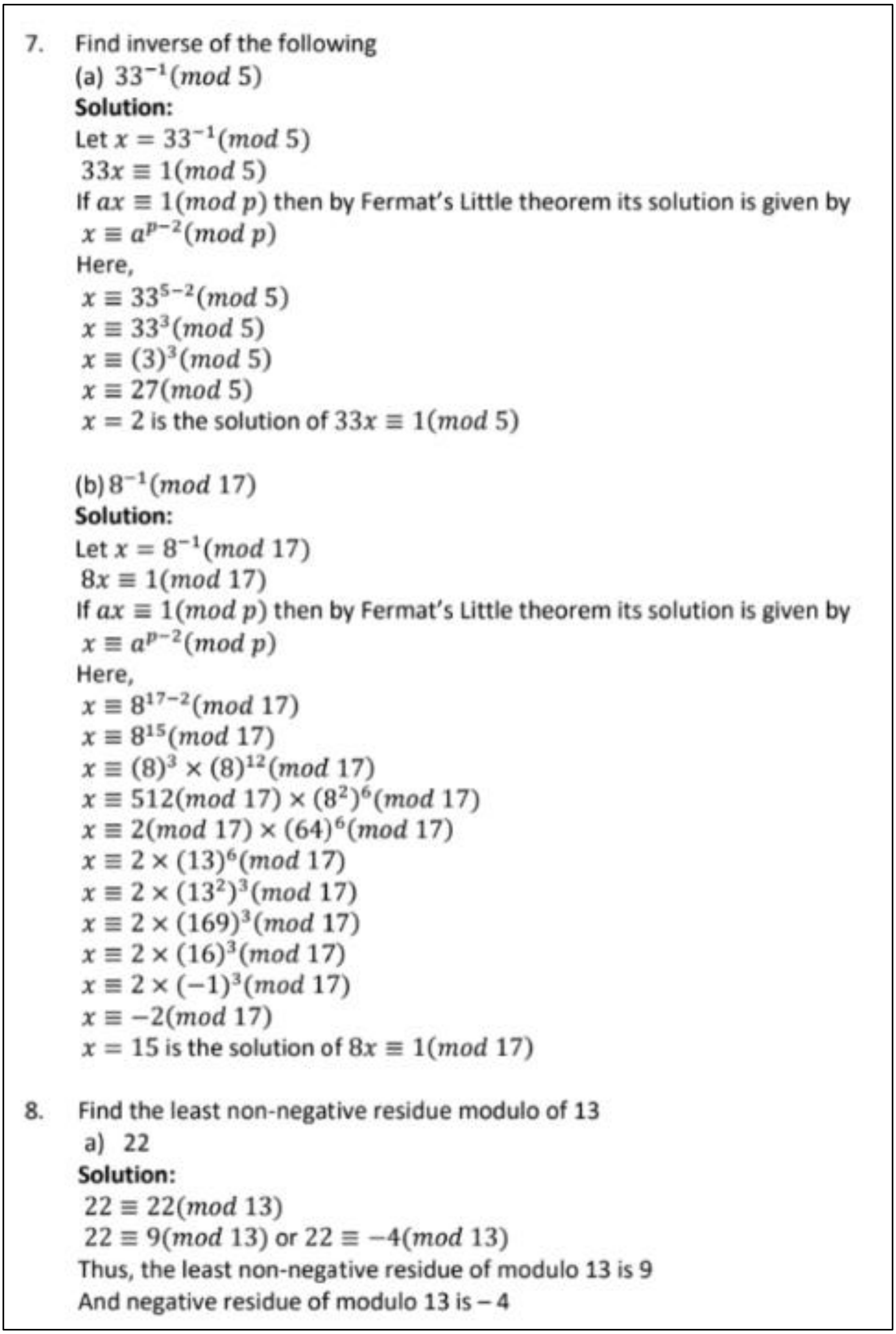
Solution:

$5x \equiv 11(mod\ 23)$

If $ax \equiv b(mod\ p)$ then by Fermat's Little theorem its solution is given by
$x \equiv a^{p-2}.b(mod\ p)$

Here,

$x \equiv 5^{23-2} \times 11(mod\ 23)$
$x \equiv 5^{21} \times 11(mod\ 23)$
$x \equiv 5^{20} \times 5 \times 11(mod\ 23)$
$x \equiv (5^2)^{10} \times 55(mod\ 23)$
$x \equiv (25)^{10}(mod\ 23) \times 55(mod\ 23)$
$x \equiv (-2)^{10}(mod\ 23) \times 55(mod\ 23)$
$x \equiv 1024(mod\ 23) \times 9(mod\ 23)$
$x \equiv 12 \times 9(mod\ 23)$
$x \equiv 108(mod\ 23)$
$x = 16$ is the solution of $5x \equiv 11(mod\ 23)$



7. Find inverse of the following

(a) $33^{-1}(mod\ 5)$

Solution:

Let $x = 33^{-1}(mod\ 5)$

$33x \equiv 1(mod\ 5)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 33^{5-2}(mod\ 5)$

$x \equiv 33^{3}(mod\ 5)$

$x \equiv (3)^{3}(mod\ 5)$

$x \equiv 27(mod\ 5)$

$x = 2$ is the solution of $33x \equiv 1(mod\ 5)$

(b) $8^{-1}(mod\ 17)$

Solution:

Let $x = 8^{-1}(mod\ 17)$

$8x \equiv 1(mod\ 17)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 8^{17-2}(mod\ 17)$

$x \equiv 8^{15}(mod\ 17)$

$x \equiv (8)^{3} \times (8)^{12}(mod\ 17)$

$x \equiv 512(mod\ 17) \times (8^{2})^{6}(mod\ 17)$

$x \equiv 2(mod\ 17) \times (64)^{6}(mod\ 17)$

$x \equiv 2 \times (13)^{6}(mod\ 17)$

$x \equiv 2 \times (13^{2})^{3}(mod\ 17)$

$x \equiv 2 \times (169)^{3}(mod\ 17)$

$x \equiv 2 \times (16)^{3}(mod\ 17)$

$x \equiv 2 \times (-1)^{3}(mod\ 17)$

$x \equiv -2(mod\ 17)$

$x = 15$ is the solution of $8x \equiv 1(mod\ 17)$

8. Find the least non-negative residue modulo of 13

a) 22

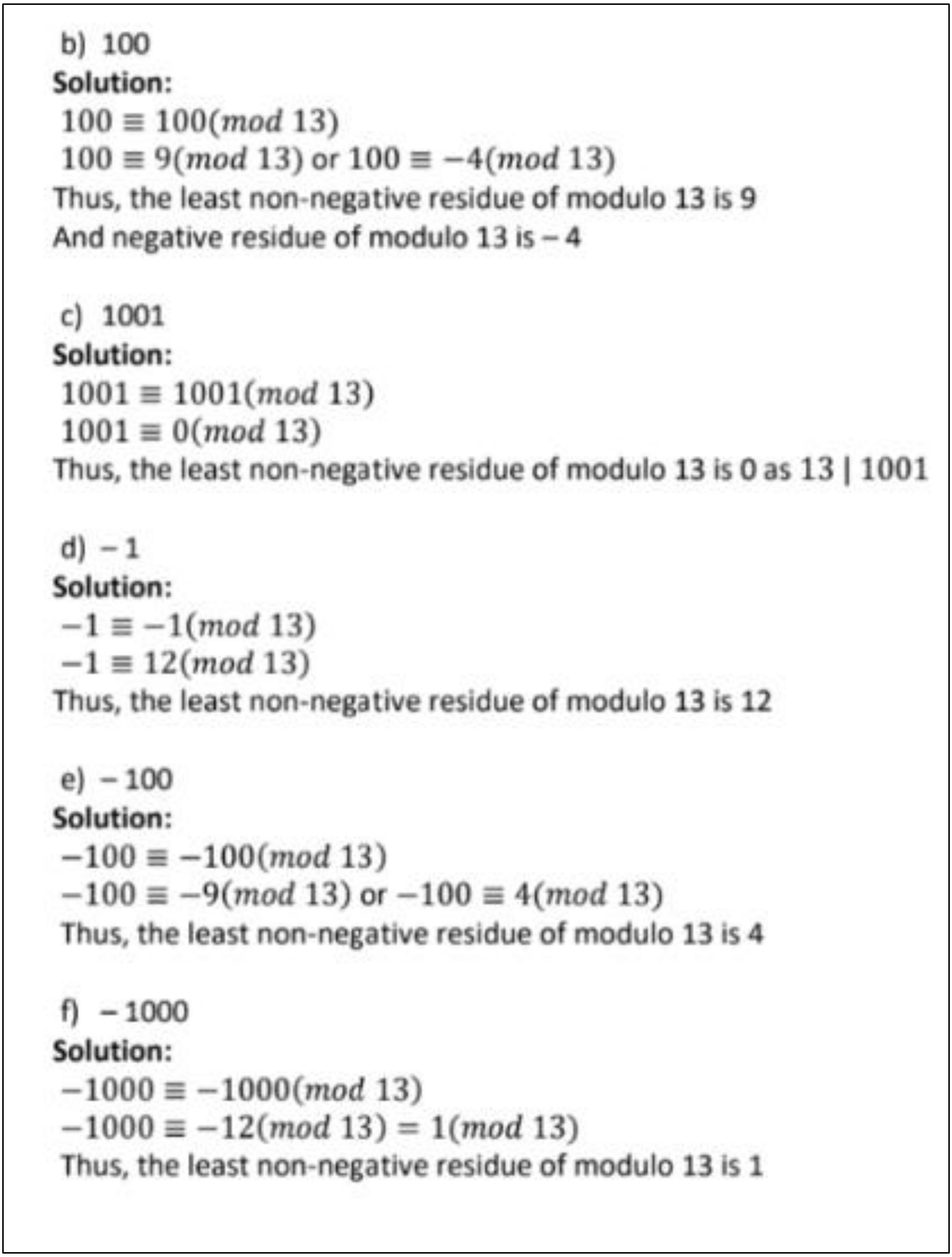
Solution:

$22 \equiv 22(mod\ 13)$

$22 \equiv 9(mod\ 13)$ or $22 \equiv -4(mod\ 13)$

Thus, the least non-negative residue of modulo 13 is 9

And negative residue of modulo 13 is -4



b) 100

Solution:

$100 \equiv 100(mod\ 13)$

$100 \equiv 9(mod\ 13)$ or $100 \equiv -4(mod\ 13)$

Thus, the least non-negative residue of modulo 13 is 9

And negative residue of modulo 13 is – 4

c) 1001

Solution:

$1001 \equiv 1001(mod\ 13)$

$1001 \equiv 0(mod\ 13)$

Thus, the least non-negative residue of modulo 13 is 0 as 13 | 1001

d) -1

Solution:

$-1 \equiv -1(mod\ 13)$

$-1 \equiv 12(mod\ 13)$

Thus, the least non-negative residue of modulo 13 is 12

e) – 100

Solution:

$-100 \equiv -100(mod\ 13)$

$-100 \equiv -9(mod\ 13)$ or $-100 \equiv 4(mod\ 13)$

Thus, the least non-negative residue of modulo 13 is 4

f) – 1000

Solution:

$-1000 \equiv -1000(mod\ 13)$

$-1000 \equiv -12(mod\ 13) = 1(mod\ 13)$

Thus, the least non-negative residue of modulo 13 is 1

9. Find the least positive residue of $3^{1000000}$ modulo 13

Solution:

Since 13 is a prime number,

We have by Fermat's little theorem,

$3^{13-1} \equiv 1(mod\ 13)$

$3^{12} \equiv 1(mod\ 13)$

$(3^{12})^{83333} \equiv 1^{83333}(mod\ 13)$

$3^{999996} \equiv 1(mod\ 13)$

$3^{999996} \times 3^4 \equiv 1 \times 3^4(mod\ 13)$

$3^{1000000} \equiv 81(mod\ 13)$

$3^{1000000} \equiv 3(mod\ 13)$

10. Solve by Fermat's theorem

(a) $15^{15} mod\ 17$

Solution:

Since 17 is a prime number,

We have by Fermat's little theorem,

$15^{17-1} \equiv 1(mod\ 17)$

$15^{16} \equiv 1(mod\ 17)$

But we need 15^{15}, Fermat's little theorem doesn't seem to work much here.

Now,

$15 \equiv 15(mod\ 17) \equiv -2(mod\ 17)$

$15^4 \equiv (-2)^4(mod\ 17) \equiv 16(mod\ 17) \equiv -1(mod\ 17)$

$(15^4)^3 \equiv (-1)^3(mod\ 17)$

$15^{12} \equiv -1(mod\ 17)$

$15^3 \times 15^{12} \equiv 15^3 \times -1(mod\ 17)$

$15^{15} \equiv (-2)^3 \times -1(mod\ 17)$

$15^{15} \equiv 8(mod\ 17)$

(b) $456^{17} mod\ 17$

Solution:

Since 17 is a prime number,

We have by Fermat's little theorem,

$456^{17-1} \equiv 1(mod\ 17)$

$456^{16} \equiv 1(mod\ 17)$

$456 \times 456^{16} \equiv 456 \times 1(mod\ 17)$

$456^{17} \equiv 14(mod\ 17)$

(c) $145^{102} mod\ 101$

Solution:

Since 101 is a prime number,

We have by Fermat's little theorem,

$145^{101-1} \equiv 1(mod\ 101)$

$145^{100} \equiv 1(mod\ 101)$

$145 \times 145^{100} \equiv 145 \times 1(mod\ 101)$

$145^{101} \equiv 44(mod\ 101)$

$145 \times 145^{101} \equiv 145 \times 44(mod\ 101)$

$145^{102} \equiv 44 \times 44(mod\ 101)$

$145^{102} \equiv 1936(mod\ 101)$

$145^{102} \equiv 17(mod\ 101)$

11. Find solutions of the following congruences

(a) $11x \equiv 5(mod\ 7)$

Solution:

$11x \equiv 5(mod\ 7)$

If $ax \equiv b(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}.b(mod\ p)$

Here,

$x \equiv 11^{7-2} \times 5(mod\ 7)$

$x \equiv 11^{5} \times 5(mod\ 7)$

$x \equiv 11^{4} \times 11 \times 5(mod\ 7)$

$x \equiv (-4)^{4} \times 55(mod\ 7)$

$x \equiv 256(mod\ 7) \times 55(mod\ 7)$

$x \equiv 4 \times 6(mod\ 7)$

$x \equiv 24(mod\ 7)$

$x \equiv 3(mod\ 7)$

$x = 3$ is the solution of $11x \equiv 5(mod\ 7)$

(b) $7x \equiv 3(mod\ 19)$

Solution:

$7x \equiv 3(mod\ 19)$

If $ax \equiv b(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}.b(mod\ p)$

Here,

$x \equiv 7^{19-2} \times 3(mod\ 19)$

$x \equiv 7^{17} \times 3(mod\ 19)$

$x \equiv 7^{16} \times 7 \times 3(mod\ 19)$

$x \equiv (7^2)^8 \times 21(mod\ 19)$

$x \equiv (49)^8(mod\ 19) \times 21(mod\ 19)$

$x \equiv (11)^8(mod\ 19) \times 2(mod\ 19)$

$x \equiv (-8)^8(mod\ 19) \times 2(mod\ 19)$

$x \equiv ((-8)^2)^4(mod\ 19) \times 2(mod\ 19)$

$x \equiv (64)^4(mod\ 19) \times 2(mod\ 19)$

$x \equiv (7)^4(mod\ 19) \times 2(mod\ 19)$

$x \equiv 2401(mod\ 19) \times 2(mod\ 19)$

$x \equiv 7 \times 2(mod\ 19)$

$x \equiv 14(mod\ 19)$

$x = 14$ is the solution of $7x \equiv 3(mod\ 19)$

12. Find the least positive residue of 3^{201} modulo 11

Solution:

Since 11 is a prime number,

We have by Fermat's little theorem,

$3^{11-1} \equiv 1(mod\ 11)$

$3^{10} \equiv 1(mod\ 11)$

$(3^{10})^{20} \equiv (1)^{20}(mod\ 11)$

$3^{200} \equiv 1(mod\ 11)$

$3^{200} \times 3 \equiv 1 \times 3(mod\ 11)$

$3^{201} \equiv 3(mod\ 11)$

The least positive residue is 3

13. Find the inverse of $2^{-1}(mod\ 31)$ using Fermat's theorem

[N18/IT/4M]

Solution:

Let $x = 2^{-1}(mod\ 31)$

$2x \equiv 1(mod\ 31)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 2^{31-2}(mod\ 31)$

$x \equiv 2^{29}(mod\ 31)$

$x \equiv (2)^9 \times (2)^{20}(mod\ 31)$

$x \equiv 512(mod\ 31) \times (2^5)^4(mod\ 31)$

$x \equiv 16(mod\ 31) \times (32)^4(mod\ 31)$

$x \equiv 16 \times (1)^4(mod\ 31)$

$x \equiv 16(mod\ 31)$

$x = 16$ is the solution of $2x \equiv 1(mod\ 31)$

14. Find inverse of the following

(a) $5^{-1}(mod\ 23)$

[M19/IT/4M]

Solution:

Let $x = 5^{-1}(mod\ 23)$

$5x \equiv 1(mod\ 23)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 5^{23-2}(mod\ 23)$

$x \equiv 5^{21}(mod\ 23)$

$x \equiv (5)^1 \times (5)^{20}(mod\ 23)$

$x \equiv 5 \times (5^2)^{10}(mod\ 23)$

$x \equiv 5 \times (25)^{10}(mod\ 23)$

$x \equiv 5 \times (2)^{10}(mod\ 23)$

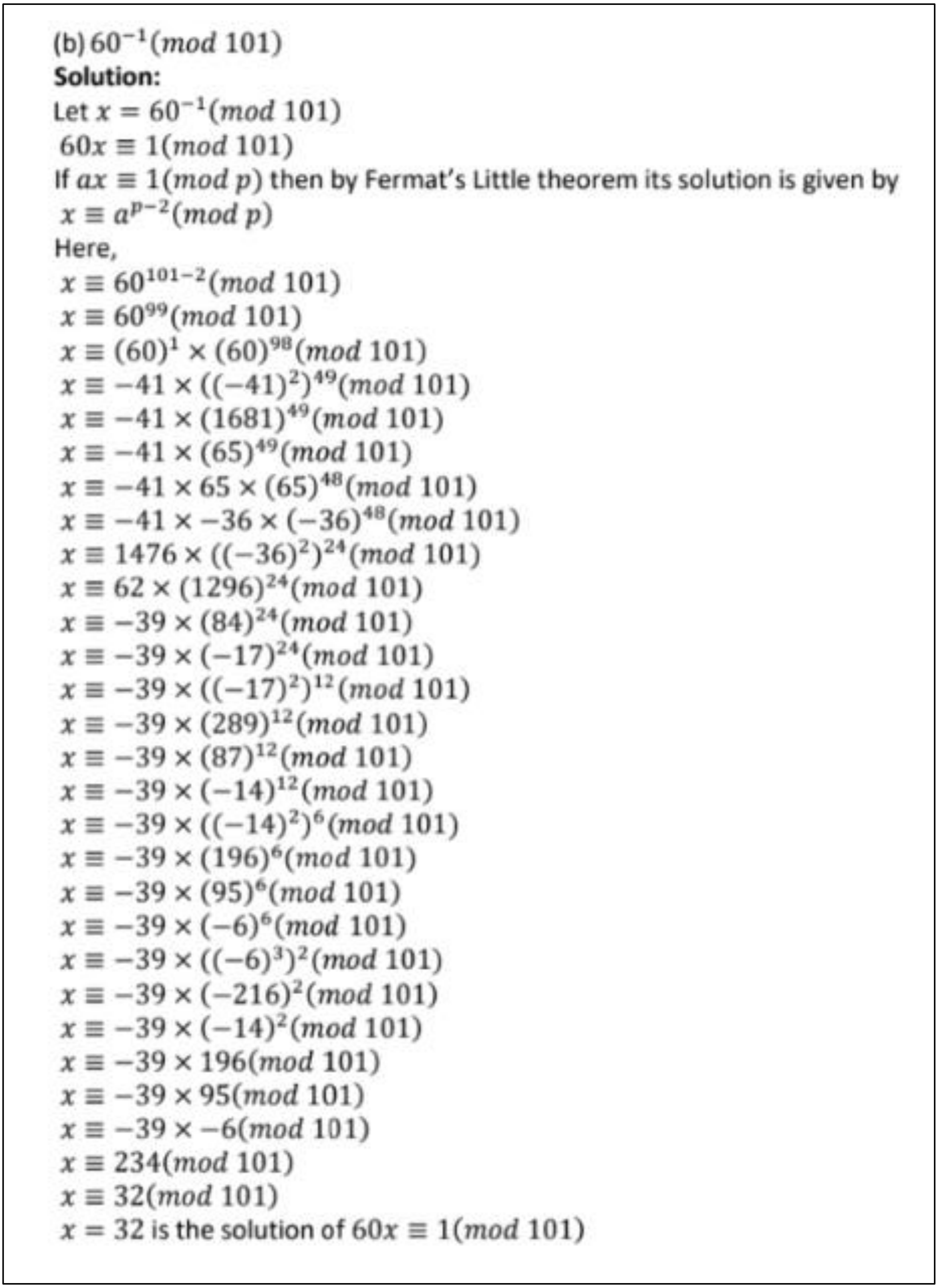
$x \equiv 5 \times 1024(mod\ 23)$

$x \equiv 5 \times 12(mod\ 23)$

$x \equiv 60(mod\ 23)$

$x \equiv 14(mod\ 23)$

$x = 14$ is the solution of $5x \equiv 1(mod\ 23)$



(b) $60^{-1}(mod\ 101)$

Solution:

Let $x = 60^{-1}(mod\ 101)$

$60x \equiv 1(mod\ 101)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 60^{101-2}(mod\ 101)$

$x \equiv 60^{99}(mod\ 101)$

$x \equiv (60)^1 \times (60)^{98}(mod\ 101)$

$x \equiv -41 \times ((-41)^2)^{49}(mod\ 101)$

$x \equiv -41 \times (1681)^{49}(mod\ 101)$

$x \equiv -41 \times (65)^{49}(mod\ 101)$

$x \equiv -41 \times 65 \times (65)^{48}(mod\ 101)$

$x \equiv -41 \times -36 \times (-36)^{48}(mod\ 101)$

$x \equiv 1476 \times ((-36)^2)^{24}(mod\ 101)$

$x \equiv 62 \times (1296)^{24}(mod\ 101)$

$x \equiv -39 \times (84)^{24}(mod\ 101)$

$x \equiv -39 \times (-17)^{24}(mod\ 101)$

$x \equiv -39 \times ((-17)^2)^{12}(mod\ 101)$

$x \equiv -39 \times (289)^{12}(mod\ 101)$

$x \equiv -39 \times (87)^{12}(mod\ 101)$

$x \equiv -39 \times (-14)^{12}(mod\ 101)$

$x \equiv -39 \times ((-14)^2)^6(mod\ 101)$

$x \equiv -39 \times (196)^6(mod\ 101)$

$x \equiv -39 \times (95)^6(mod\ 101)$

$x \equiv -39 \times (-6)^6(mod\ 101)$

$x \equiv -39 \times ((-6)^3)^2(mod\ 101)$

$x \equiv -39 \times (-216)^2(mod\ 101)$

$x \equiv -39 \times (-14)^2(mod\ 101)$

$x \equiv -39 \times 196(mod\ 101)$

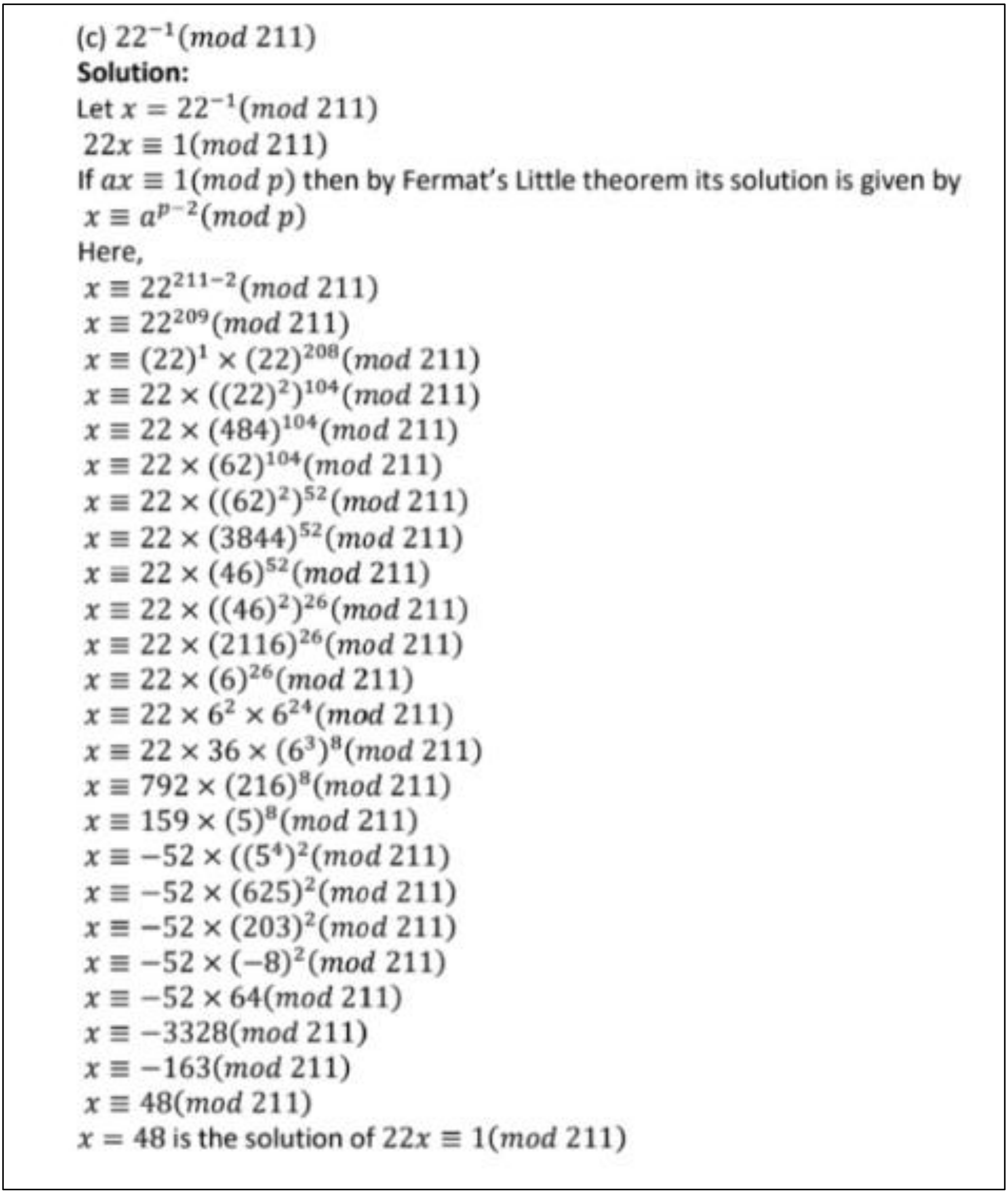
$x \equiv -39 \times 95(mod\ 101)$

$x \equiv -39 \times -6(mod\ 101)$

$x \equiv 234(mod\ 101)$

$x \equiv 32(mod\ 101)$

$x = 32$ is the solution of $60x \equiv 1(mod\ 101)$



(c) $22^{-1}(mod\ 211)$

Solution:

Let $x = 22^{-1}(mod\ 211)$

$22x \equiv 1(mod\ 211)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 22^{211-2}(mod\ 211)$

$x \equiv 22^{209}(mod\ 211)$

$x \equiv (22)^1 \times (22)^{208}(mod\ 211)$

$x \equiv 22 \times ((22)^2)^{104}(mod\ 211)$

$x \equiv 22 \times (484)^{104}(mod\ 211)$

$x \equiv 22 \times (62)^{104}(mod\ 211)$

$x \equiv 22 \times ((62)^2)^{52}(mod\ 211)$

$x \equiv 22 \times (3844)^{52}(mod\ 211)$

$x \equiv 22 \times (46)^{52}(mod\ 211)$

$x \equiv 22 \times ((46)^2)^{26}(mod\ 211)$

$x \equiv 22 \times (2116)^{26}(mod\ 211)$

$x \equiv 22 \times (6)^{26}(mod\ 211)$

$x \equiv 22 \times 6^2 \times 6^{24}(mod\ 211)$

$x \equiv 22 \times 36 \times (6^3)^8(mod\ 211)$

$x \equiv 792 \times (216)^8(mod\ 211)$

$x \equiv 159 \times (5)^8(mod\ 211)$

$x \equiv -52 \times ((5^4)^2(mod\ 211)$

$x \equiv -52 \times (625)^2(mod\ 211)$

$x \equiv -52 \times (203)^2(mod\ 211)$

$x \equiv -52 \times (-8)^2(mod\ 211)$

$x \equiv -52 \times 64(mod\ 211)$

$x \equiv -3328(mod\ 211)$

$x \equiv -163(mod\ 211)$

$x \equiv 48(mod\ 211)$

$x = 48$ is the solution of $22x \equiv 1(mod\ 211)$

(d) $5^{-1}(mod\ 13)$

Solution:

Let $x = 5^{-1}(mod\ 13)$

$5x \equiv 1(mod\ 13)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 5^{13-2}(mod\ 13)$

$x \equiv 5^{11}(mod\ 13)$

$x \equiv (5)^1 \times (5)^{10}(mod\ 13)$

$x \equiv 5 \times (5^2)^5(mod\ 13)$

$x \equiv 5 \times (25)^5(mod\ 13)$

$x \equiv 5 \times (12)^5(mod\ 13)$

$x \equiv 5 \times (-1)^5(mod\ 13)$

$x \equiv 5 \times -1(mod\ 13)$

$x \equiv -5(mod\ 13)$

$x \equiv 8(mod\ 13)$

$x = 8$ is the solution of $5x \equiv 1(mod\ 13)$

(e) $15^{-1}(mod\ 17)$

Solution:

Let $x = 15^{-1}(mod\ 17)$

$15x \equiv 1(mod\ 17)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 15^{17-2}(mod\ 17)$

$x \equiv 15^{15}(mod\ 17)$

$x \equiv (-2)^{15}(mod\ 17)$

$x \equiv ((-2)^5)^3(mod\ 17)$

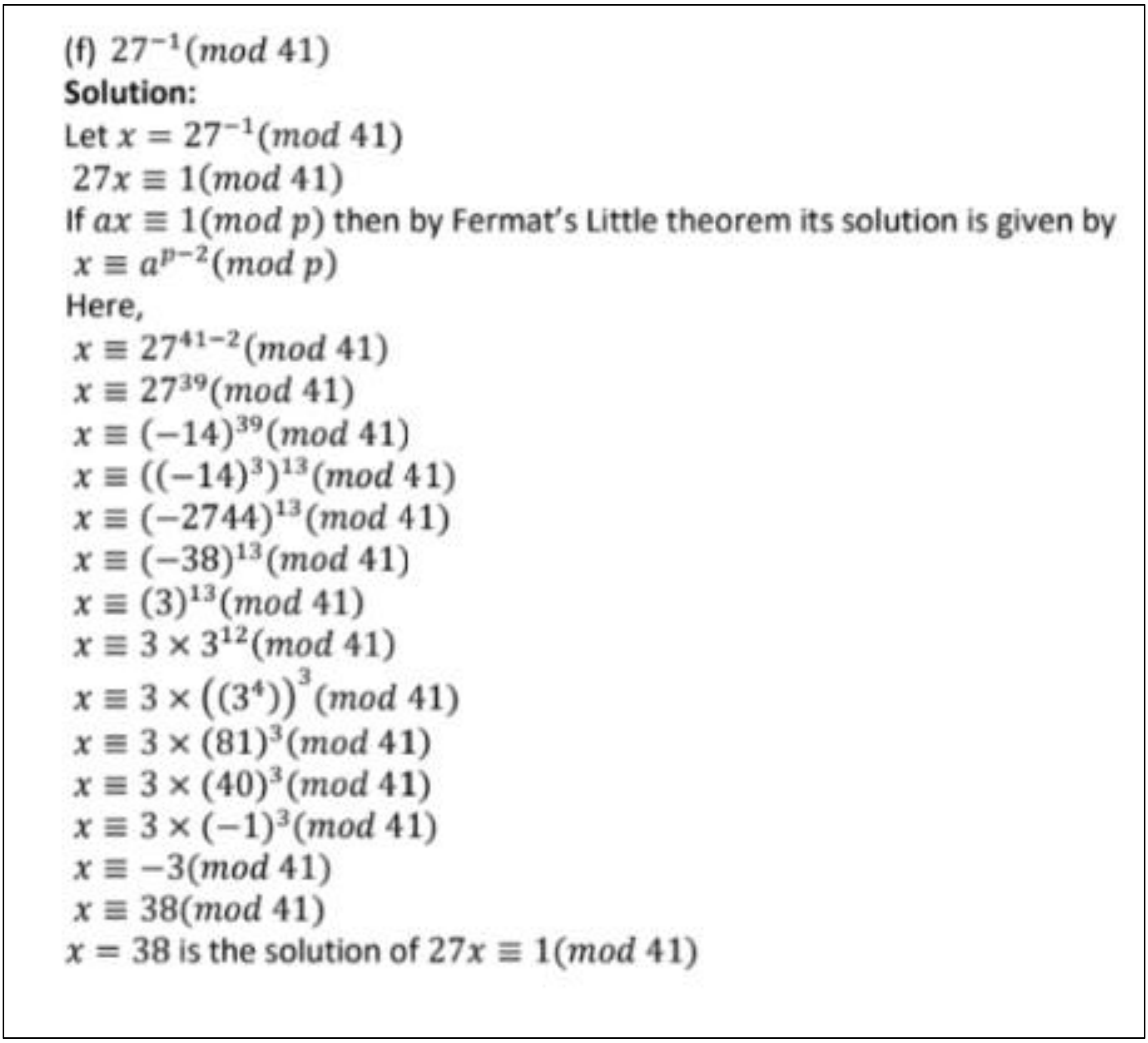
$x \equiv (-32)^3(mod\ 17)$

$x \equiv (-15)^3(mod\ 17)$

$x \equiv (2)^3(mod\ 17)$

$x \equiv 8(mod\ 17)$

$x = 8$ is the solution of $15x \equiv 1(mod\ 17)$



(f) $27^{-1}(mod\ 41)$

Solution:

Let $x = 27^{-1}(mod\ 41)$

$27x \equiv 1(mod\ 41)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 27^{41-2}(mod\ 41)$

$x \equiv 27^{39}(mod\ 41)$

$x \equiv (-14)^{39}(mod\ 41)$

$x \equiv ((-14)^{3})^{13}(mod\ 41)$

$x \equiv (-2744)^{13}(mod\ 41)$

$x \equiv (-38)^{13}(mod\ 41)$

$x \equiv (3)^{13}(mod\ 41)$

$x \equiv 3 \times 3^{12}(mod\ 41)$

$x \equiv 3 \times \left((3^{4})\right)^{3}(mod\ 41)$

$x \equiv 3 \times (81)^{3}(mod\ 41)$

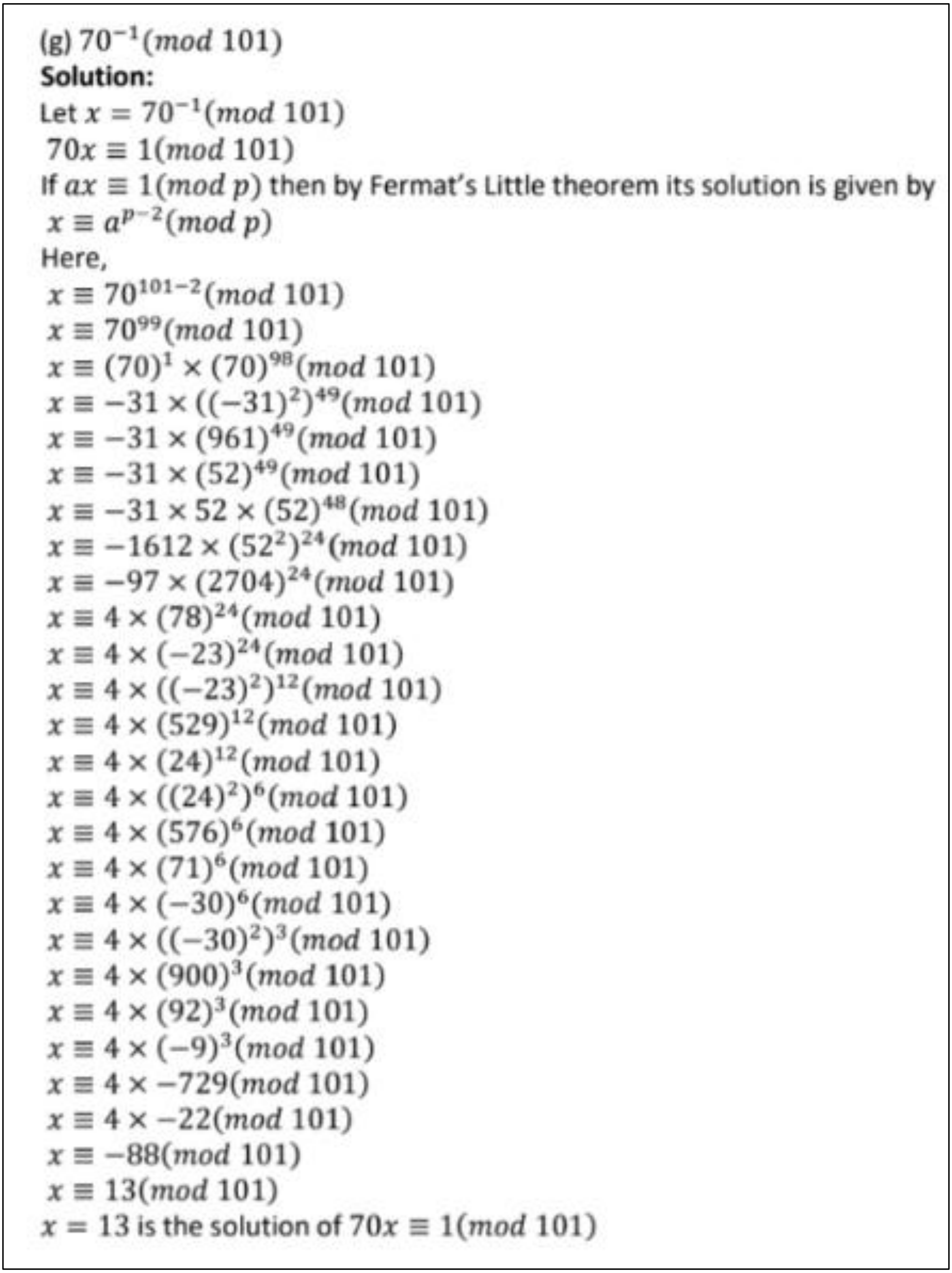
$x \equiv 3 \times (40)^{3}(mod\ 41)$

$x \equiv 3 \times (-1)^{3}(mod\ 41)$

$x \equiv -3(mod\ 41)$

$x \equiv 38(mod\ 41)$

$x = 38$ is the solution of $27x \equiv 1(mod\ 41)$



(g) $70^{-1}(mod\ 101)$

Solution:

Let $x = 70^{-1}(mod\ 101)$

$70x \equiv 1(mod\ 101)$

If $ax \equiv 1(mod\ p)$ then by Fermat's Little theorem its solution is given by

$x \equiv a^{p-2}(mod\ p)$

Here,

$x \equiv 70^{101-2}(mod\ 101)$

$x \equiv 70^{99}(mod\ 101)$

$x \equiv (70)^1 \times (70)^{98}(mod\ 101)$

$x \equiv -31 \times ((-31)^2)^{49}(mod\ 101)$

$x \equiv -31 \times (961)^{49}(mod\ 101)$

$x \equiv -31 \times (52)^{49}(mod\ 101)$

$x \equiv -31 \times 52 \times (52)^{48}(mod\ 101)$

$x \equiv -1612 \times (52^2)^{24}(mod\ 101)$

$x \equiv -97 \times (2704)^{24}(mod\ 101)$

$x \equiv 4 \times (78)^{24}(mod\ 101)$

$x \equiv 4 \times (-23)^{24}(mod\ 101)$

$x \equiv 4 \times ((-23)^2)^{12}(mod\ 101)$

$x \equiv 4 \times (529)^{12}(mod\ 101)$

$x \equiv 4 \times (24)^{12}(mod\ 101)$

$x \equiv 4 \times ((24)^2)^6(mod\ 101)$

$x \equiv 4 \times (576)^6(mod\ 101)$

$x \equiv 4 \times (71)^6(mod\ 101)$

$x \equiv 4 \times (-30)^6(mod\ 101)$

$x \equiv 4 \times ((-30)^2)^3(mod\ 101)$

$x \equiv 4 \times (900)^3(mod\ 101)$

$x \equiv 4 \times (92)^3(mod\ 101)$

$x \equiv 4 \times (-9)^3(mod\ 101)$

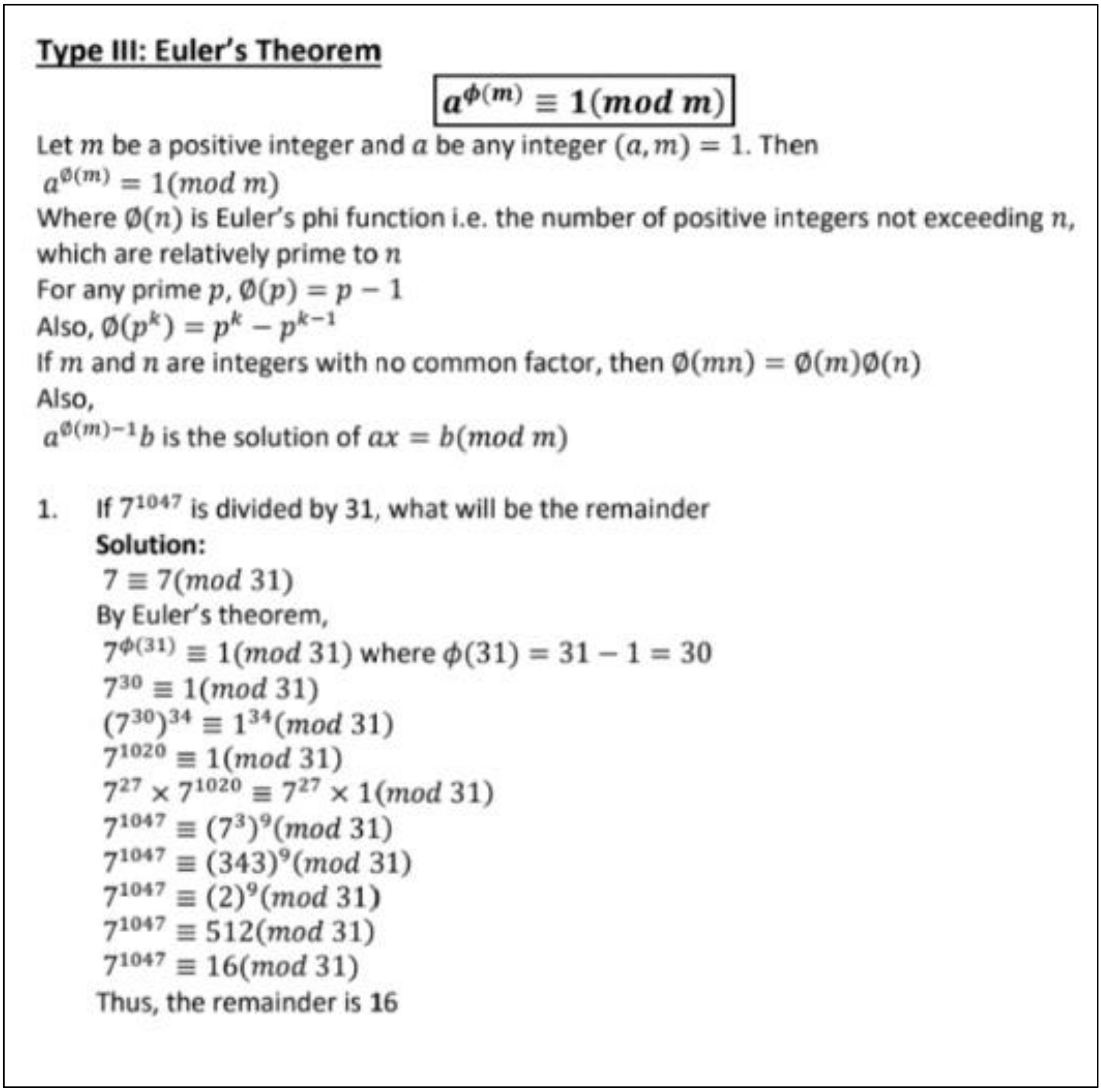
$x \equiv 4 \times -729(mod\ 101)$

$x \equiv 4 \times -22(mod\ 101)$

$x \equiv -88(mod\ 101)$

$x \equiv 13(mod\ 101)$

$x = 13$ is the solution of $70x \equiv 1(mod\ 101)$



Type III: Euler's Theorem

$$\boxed{\boldsymbol{a^{\phi(m)} \equiv 1(mod\ m)}}$$

Let m be a positive integer and a be any integer $(a, m) = 1$. Then

$a^{\emptyset(m)} = 1(mod\ m)$

Where $\emptyset(n)$ is Euler's phi function i.e. the number of positive integers not exceeding n, which are relatively prime to n

For any prime p, $\emptyset(p) = p - 1$

Also, $\emptyset(p^k) = p^k - p^{k-1}$

If m and n are integers with no common factor, then $\emptyset(mn) = \emptyset(m)\emptyset(n)$

Also,

$a^{\emptyset(m)-1}b$ is the solution of $ax = b(mod\ m)$

1. If 7^{1047} is divided by 31, what will be the remainder

   Solution:

   $7 \equiv 7(mod\ 31)$

   By Euler's theorem,

   $7^{\phi(31)} \equiv 1(mod\ 31)$ where $\phi(31) = 31 - 1 = 30$

   $7^{30} \equiv 1(mod\ 31)$

   $(7^{30})^{34} \equiv 1^{34}(mod\ 31)$

   $7^{1020} \equiv 1(mod\ 31)$

   $7^{27} \times 7^{1020} \equiv 7^{27} \times 1(mod\ 31)$

   $7^{1047} \equiv (7^3)^9(mod\ 31)$

   $7^{1047} \equiv (343)^9(mod\ 31)$

   $7^{1047} \equiv (2)^9(mod\ 31)$

   $7^{1047} \equiv 512(mod\ 31)$

   $7^{1047} \equiv 16(mod\ 31)$

   Thus, the remainder is 16

2. Find the last two digits in the decimal expression of 3^{100}

Solution:

To find the last two digits we have to find modulo 100 of a number

By Euler's theorem,

$3^{\phi(100)} \equiv 1(mod\ 100)$

Where

$\phi(100) = \phi(2^2.5^2) = \phi(2^2).\phi(5^2) = [2^2 - 2^{2-1}][5^2 - 5^{2-1}] = 40$

Thus,

$3^{40} \equiv 1(mod\ 100)$

$(3^{40})^2 \equiv 1^2(mod\ 100)$

$3^{80} \equiv 1(mod\ 100)$

$3^{80} \times 3^{20} \equiv 1 \times 3^{20}(mod\ 100)$

$3^{100} \equiv (3^5)^4(mod\ 100)$

$3^{100} \equiv (243)^4(mod\ 100)$

$3^{100} \equiv (43)^4(mod\ 100)$

$3^{100} \equiv (43^2)^2(mod\ 100)$

$3^{100} \equiv (1849)^2(mod\ 100)$

$3^{100} \equiv (49)^2(mod\ 100)$

$3^{100} \equiv 2401(mod\ 100)$

$3^{100} \equiv 1(mod\ 100)$

The last two digits are 01

3. Find smallest positive integer modulo 8 to which $3^2.3^3.3^4.3^{10}$ is congruent

Solution:

$3^2.3^3.3^4.3^{10} = 3^{19}$

By Euler's theorem,

$3^{\phi(8)} \equiv 1(mod\ 8)$ where $\phi(8) = \phi(2^3) = 2^3 - 2^{3-1} = 4$

$3^4 \equiv 1(mod\ 8)$

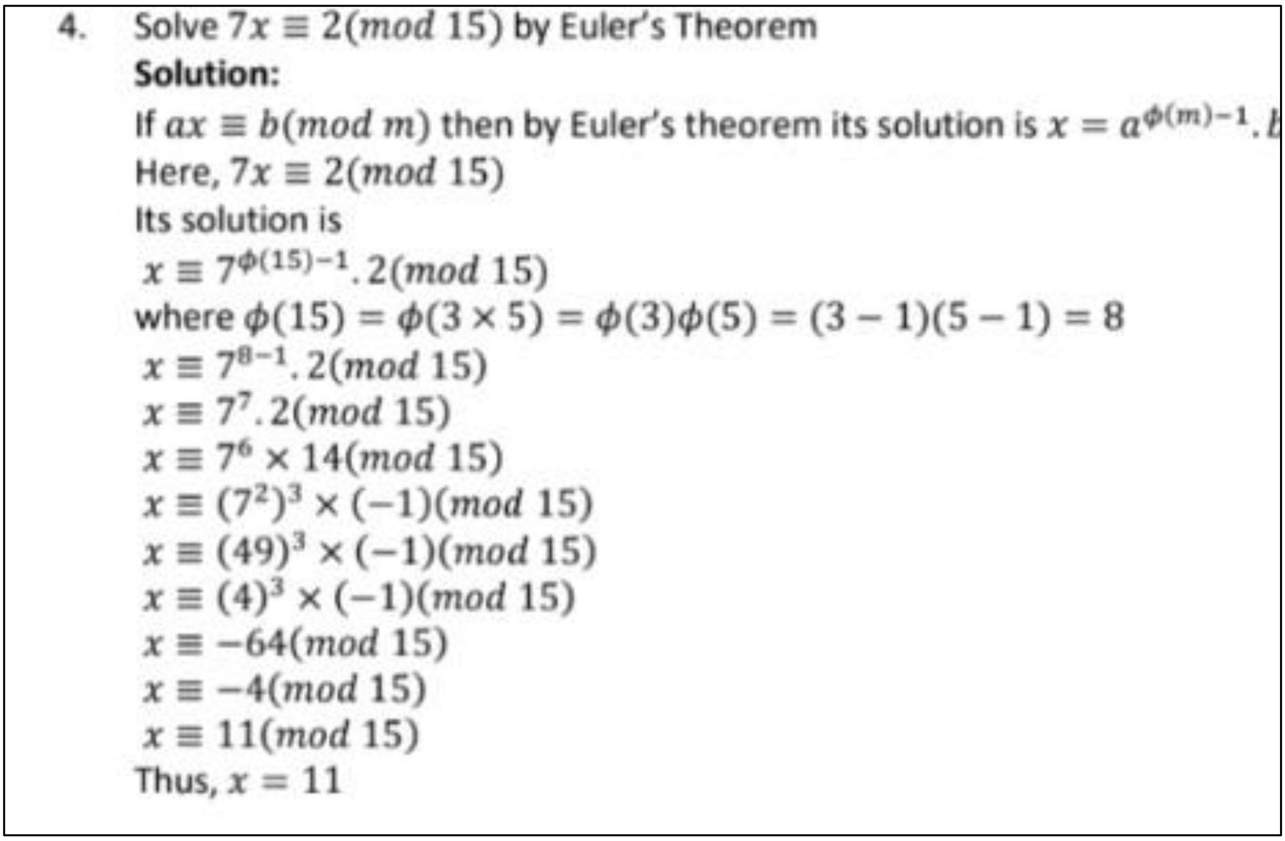
$(3^4)^4 \equiv 1^4(mod\ 8)$

$3^{16} \equiv 1(mod\ 8)$

$3^{16} \times 3^3 \equiv 1 \times 3^3(mod\ 8)$

$3^{19} \equiv 27(mod\ 8)$

$3^{19} \equiv 3(mod\ 8)$



4. Solve $7x \equiv 2(mod\ 15)$ by Euler's Theorem

Solution:

If $ax \equiv b(mod\ m)$ then by Euler's theorem its solution is $x = a^{\phi(m)-1}.b$

Here, $7x \equiv 2(mod\ 15)$

Its solution is

$x \equiv 7^{\phi(15)-1}.2(mod\ 15)$

where $\phi(15) = \phi(3 \times 5) = \phi(3)\phi(5) = (3-1)(5-1) = 8$

$x \equiv 7^{8-1}.2(mod\ 15)$

$x \equiv 7^{7}.2(mod\ 15)$

$x \equiv 7^{6} \times 14(mod\ 15)$

$x \equiv (7^{2})^{3} \times (-1)(mod\ 15)$

$x \equiv (49)^{3} \times (-1)(mod\ 15)$

$x \equiv (4)^{3} \times (-1)(mod\ 15)$

$x \equiv -64(mod\ 15)$

$x \equiv -4(mod\ 15)$

$x \equiv 11(mod\ 15)$

Thus, $x = 11$

5. Find inverse of $8^{-1}(mod\ 77)$ using Euler's theorem

[M18/IT/4M]

Solution:

We have, $8x \equiv 1(mod\ 77)$ i.e. $x \equiv 8^{-1}(mod\ 77)$

Using Euler's theorem, we have a solution

$x \equiv 8^{\emptyset(77)-1}\ (mod\ 77)$

We find, $\emptyset(77) = \emptyset(7 \times 11) = \emptyset(7) \times \emptyset(11) = (7-1)(11-1) = 60$

$x \equiv 8^{59}(mod\ 77)$

Now,

$8^2 = 64 \equiv -13(mod\ 77)$

$(8^2)^2 = (-13)^2(mod\ 77)$

$8^4 \equiv 169(mod\ 77) \equiv 15(mod\ 77)$

$(8^4)^2 = 15^2(mod\ 77) = 225\ (mod\ 77) = -6(mod\ 77)$

$8^8 = -6\ (mod\ 77)$

$(8^8)^7 = (-6)^7(mod\ 77)$

$8^{56} = -6^7(mod\ 77)$

$8^3.8^{56} = 50 \times -6^7\ (mod\ 77)$

$8^{59} = -300 \times 6^6(mod\ 77)$

$8^{59} \equiv -300(mod\ 77) \times 6^3(mod\ 77) \times 6^3(mod\ 77)$

$8^{59} = -8(mod\ 77) \times 216(mod\ 77) \times 216(mod\ 77)$

$8^{59} = -8 \times -15 \times -15(mod\ 77)$

$8^{59} = -8 \times 225\ (mod\ 77)$

$8^{59} = -8 \times 6\ (mod\ 77)$

$8^{59} = -48(mod\ 77)$

$8^{59} = 29(mod\ 77)$

Therefore, $x = 29$ so that $8x \equiv 1(mod\ 77)$

6. What time does a clock read

a) 29 hours after it reads 11 o' clock

Solution:

$11 + 29 \equiv 40\ (mod\ 12)$

$\equiv 4(mod\ 12)$

The clock will read 4 o' clock

b) 100 hours after it reads 2 o' clock

Solution:

$2 + 100 \equiv 102\ (mod\ 12)$

$\equiv 6(mod\ 12)$

The clock will read 6 o' clock

c) 50 hours after it reads 6 o' clock

Solution:

$6 + 50 \equiv 56\ (mod\ 12)$
$\equiv 8(mod\ 12)$

The clock will read 8 o' clock

d) 230 hours after it reads 9 o' clock

Solution:

$9 + 230 \equiv 239\ (mod\ 12)$
$\equiv 11(mod\ 12)$

The clock will read 11 o' clock

7. Find inverse of the following

(a) $7^{-1}(mod\ 15)$

Solution:

We have, $7x \equiv 1(mod\ 15)$ i.e. $x \equiv 7^{-1}(mod\ 15)$

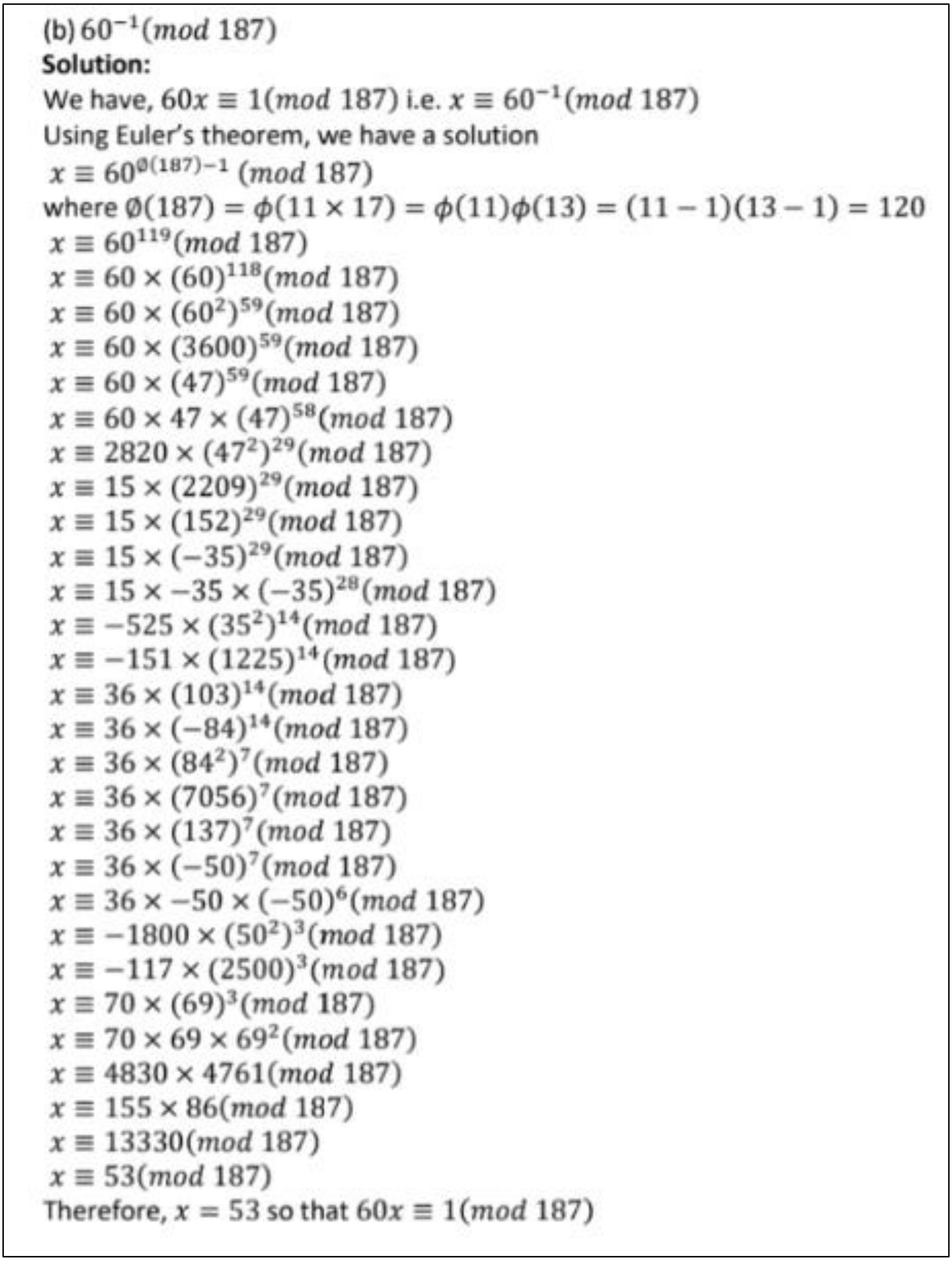
Using Euler's theorem, we have a solution

$x \equiv 7^{\emptyset(15)-1}\ (mod\ 15)$

where $\emptyset(15) = \phi(5 \times 3) = \phi(5)\phi(3) = (5-1)(3-1) = 8$

$x \equiv 7^7(mod\ 15)$
$x \equiv 7 \times 7^6(mod\ 15)$
$x \equiv 7 \times (7^2)^3(mod\ 15)$
$x \equiv 7 \times (49)^3(mod\ 15)$
$x \equiv 7 \times (4)^3(mod\ 15)$
$x \equiv 7 \times 64(mod\ 15)$
$x \equiv 7 \times 4(mod\ 15)$
$x \equiv 28(mod\ 15)$
$x \equiv 13(mod\ 15)$

Therefore, $x = 13$ so that $7x \equiv 1(mod\ 15)$



(b) $60^{-1}(mod\ 187)$

Solution:

We have, $60x \equiv 1(mod\ 187)$ i.e. $x \equiv 60^{-1}(mod\ 187)$

Using Euler's theorem, we have a solution

$x \equiv 60^{\emptyset(187)-1}\ (mod\ 187)$

where $\emptyset(187) = \phi(11 \times 17) = \phi(11)\phi(13) = (11-1)(13-1) = 120$

$x \equiv 60^{119}(mod\ 187)$

$x \equiv 60 \times (60)^{118}(mod\ 187)$

$x \equiv 60 \times (60^2)^{59}(mod\ 187)$

$x \equiv 60 \times (3600)^{59}(mod\ 187)$

$x \equiv 60 \times (47)^{59}(mod\ 187)$

$x \equiv 60 \times 47 \times (47)^{58}(mod\ 187)$

$x \equiv 2820 \times (47^2)^{29}(mod\ 187)$

$x \equiv 15 \times (2209)^{29}(mod\ 187)$

$x \equiv 15 \times (152)^{29}(mod\ 187)$

$x \equiv 15 \times (-35)^{29}(mod\ 187)$

$x \equiv 15 \times -35 \times (-35)^{28}(mod\ 187)$

$x \equiv -525 \times (35^2)^{14}(mod\ 187)$

$x \equiv -151 \times (1225)^{14}(mod\ 187)$

$x \equiv 36 \times (103)^{14}(mod\ 187)$

$x \equiv 36 \times (-84)^{14}(mod\ 187)$

$x \equiv 36 \times (84^2)^{7}(mod\ 187)$

$x \equiv 36 \times (7056)^{7}(mod\ 187)$

$x \equiv 36 \times (137)^{7}(mod\ 187)$

$x \equiv 36 \times (-50)^{7}(mod\ 187)$

$x \equiv 36 \times -50 \times (-50)^{6}(mod\ 187)$

$x \equiv -1800 \times (50^2)^{3}(mod\ 187)$

$x \equiv -117 \times (2500)^{3}(mod\ 187)$

$x \equiv 70 \times (69)^{3}(mod\ 187)$

$x \equiv 70 \times 69 \times 69^2(mod\ 187)$

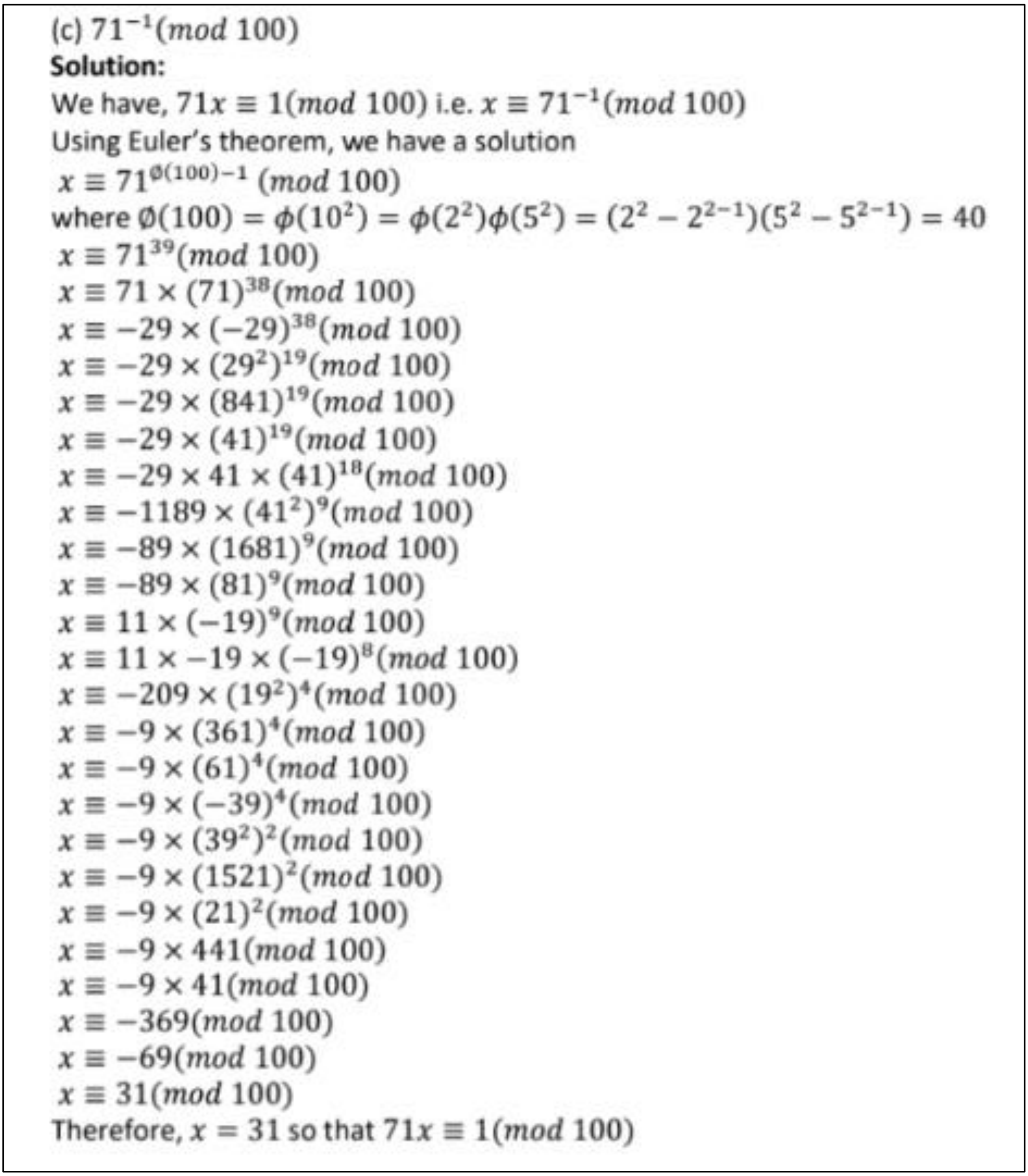
$x \equiv 4830 \times 4761(mod\ 187)$

$x \equiv 155 \times 86(mod\ 187)$

$x \equiv 13330(mod\ 187)$

$x \equiv 53(mod\ 187)$

Therefore, $x = 53$ so that $60x \equiv 1(mod\ 187)$



(c) $71^{-1}(mod\ 100)$

Solution:

We have, $71x \equiv 1(mod\ 100)$ i.e. $x \equiv 71^{-1}(mod\ 100)$

Using Euler's theorem, we have a solution

$x \equiv 71^{\emptyset(100)-1}\ (mod\ 100)$

where $\emptyset(100) = \phi(10^2) = \phi(2^2)\phi(5^2) = (2^2 - 2^{2-1})(5^2 - 5^{2-1}) = 40$

$x \equiv 71^{39}(mod\ 100)$

$x \equiv 71 \times (71)^{38}(mod\ 100)$

$x \equiv -29 \times (-29)^{38}(mod\ 100)$

$x \equiv -29 \times (29^2)^{19}(mod\ 100)$

$x \equiv -29 \times (841)^{19}(mod\ 100)$

$x \equiv -29 \times (41)^{19}(mod\ 100)$

$x \equiv -29 \times 41 \times (41)^{18}(mod\ 100)$

$x \equiv -1189 \times (41^2)^9(mod\ 100)$

$x \equiv -89 \times (1681)^9(mod\ 100)$

$x \equiv -89 \times (81)^9(mod\ 100)$

$x \equiv 11 \times (-19)^9(mod\ 100)$

$x \equiv 11 \times -19 \times (-19)^8(mod\ 100)$

$x \equiv -209 \times (19^2)^4(mod\ 100)$

$x \equiv -9 \times (361)^4(mod\ 100)$

$x \equiv -9 \times (61)^4(mod\ 100)$

$x \equiv -9 \times (-39)^4(mod\ 100)$

$x \equiv -9 \times (39^2)^2(mod\ 100)$

$x \equiv -9 \times (1521)^2(mod\ 100)$

$x \equiv -9 \times (21)^2(mod\ 100)$

$x \equiv -9 \times 441(mod\ 100)$

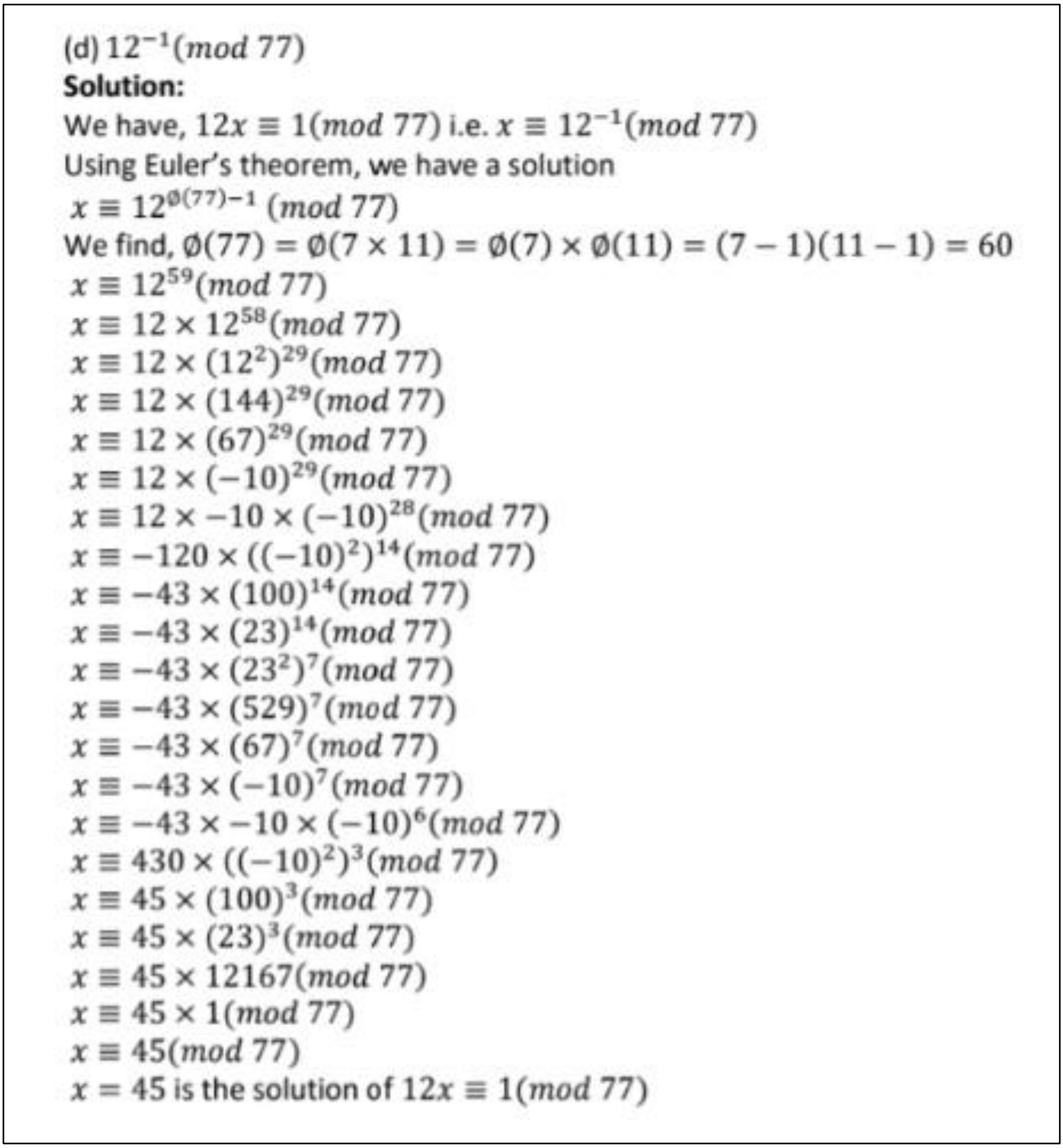
$x \equiv -9 \times 41(mod\ 100)$

$x \equiv -369(mod\ 100)$

$x \equiv -69(mod\ 100)$

$x \equiv 31(mod\ 100)$

Therefore, $x = 31$ so that $71x \equiv 1(mod\ 100)$



(d) $12^{-1}(mod\ 77)$

Solution:

We have, $12x \equiv 1(mod\ 77)$ i.e. $x \equiv 12^{-1}(mod\ 77)$

Using Euler's theorem, we have a solution

$x \equiv 12^{\emptyset(77)-1}\ (mod\ 77)$

We find, $\emptyset(77) = \emptyset(7 \times 11) = \emptyset(7) \times \emptyset(11) = (7-1)(11-1) = 60$

$x \equiv 12^{59}(mod\ 77)$

$x \equiv 12 \times 12^{58}(mod\ 77)$

$x \equiv 12 \times (12^2)^{29}(mod\ 77)$

$x \equiv 12 \times (144)^{29}(mod\ 77)$

$x \equiv 12 \times (67)^{29}(mod\ 77)$

$x \equiv 12 \times (-10)^{29}(mod\ 77)$

$x \equiv 12 \times -10 \times (-10)^{28}(mod\ 77)$

$x \equiv -120 \times ((-10)^2)^{14}(mod\ 77)$

$x \equiv -43 \times (100)^{14}(mod\ 77)$

$x \equiv -43 \times (23)^{14}(mod\ 77)$

$x \equiv -43 \times (23^2)^{7}(mod\ 77)$

$x \equiv -43 \times (529)^{7}(mod\ 77)$

$x \equiv -43 \times (67)^{7}(mod\ 77)$

$x \equiv -43 \times (-10)^{7}(mod\ 77)$

$x \equiv -43 \times -10 \times (-10)^{6}(mod\ 77)$

$x \equiv 430 \times ((-10)^2)^{3}(mod\ 77)$

$x \equiv 45 \times (100)^{3}(mod\ 77)$

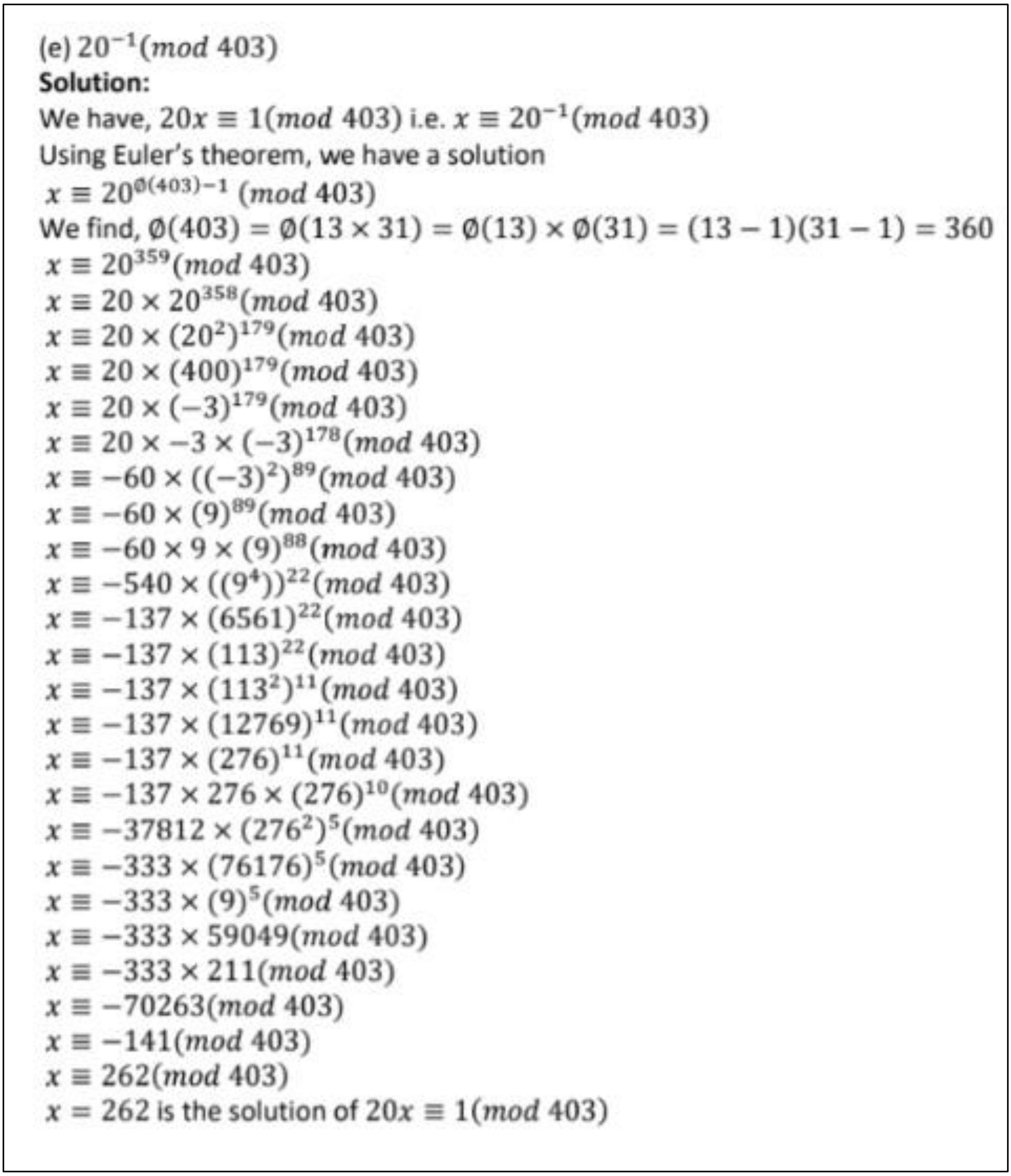
$x \equiv 45 \times (23)^{3}(mod\ 77)$

$x \equiv 45 \times 12167(mod\ 77)$

$x \equiv 45 \times 1(mod\ 77)$

$x \equiv 45(mod\ 77)$

$x = 45$ is the solution of $12x \equiv 1(mod\ 77)$



(e) $20^{-1}(mod\ 403)$

Solution:

We have, $20x \equiv 1(mod\ 403)$ i.e. $x \equiv 20^{-1}(mod\ 403)$

Using Euler's theorem, we have a solution

$x \equiv 20^{\emptyset(403)-1}\ (mod\ 403)$

We find, $\emptyset(403) = \emptyset(13 \times 31) = \emptyset(13) \times \emptyset(31) = (13-1)(31-1) = 360$

$x \equiv 20^{359}(mod\ 403)$

$x \equiv 20 \times 20^{358}(mod\ 403)$

$x \equiv 20 \times (20^2)^{179}(mod\ 403)$

$x \equiv 20 \times (400)^{179}(mod\ 403)$

$x \equiv 20 \times (-3)^{179}(mod\ 403)$

$x \equiv 20 \times -3 \times (-3)^{178}(mod\ 403)$

$x \equiv -60 \times ((-3)^2)^{89}(mod\ 403)$

$x \equiv -60 \times (9)^{89}(mod\ 403)$

$x \equiv -60 \times 9 \times (9)^{88}(mod\ 403)$

$x \equiv -540 \times ((9^4))^{22}(mod\ 403)$

$x \equiv -137 \times (6561)^{22}(mod\ 403)$

$x \equiv -137 \times (113)^{22}(mod\ 403)$

$x \equiv -137 \times (113^2)^{11}(mod\ 403)$

$x \equiv -137 \times (12769)^{11}(mod\ 403)$

$x \equiv -137 \times (276)^{11}(mod\ 403)$

$x \equiv -137 \times 276 \times (276)^{10}(mod\ 403)$

$x \equiv -37812 \times (276^2)^5(mod\ 403)$

$x \equiv -333 \times (76176)^5(mod\ 403)$

$x \equiv -333 \times (9)^5(mod\ 403)$

$x \equiv -333 \times 59049(mod\ 403)$

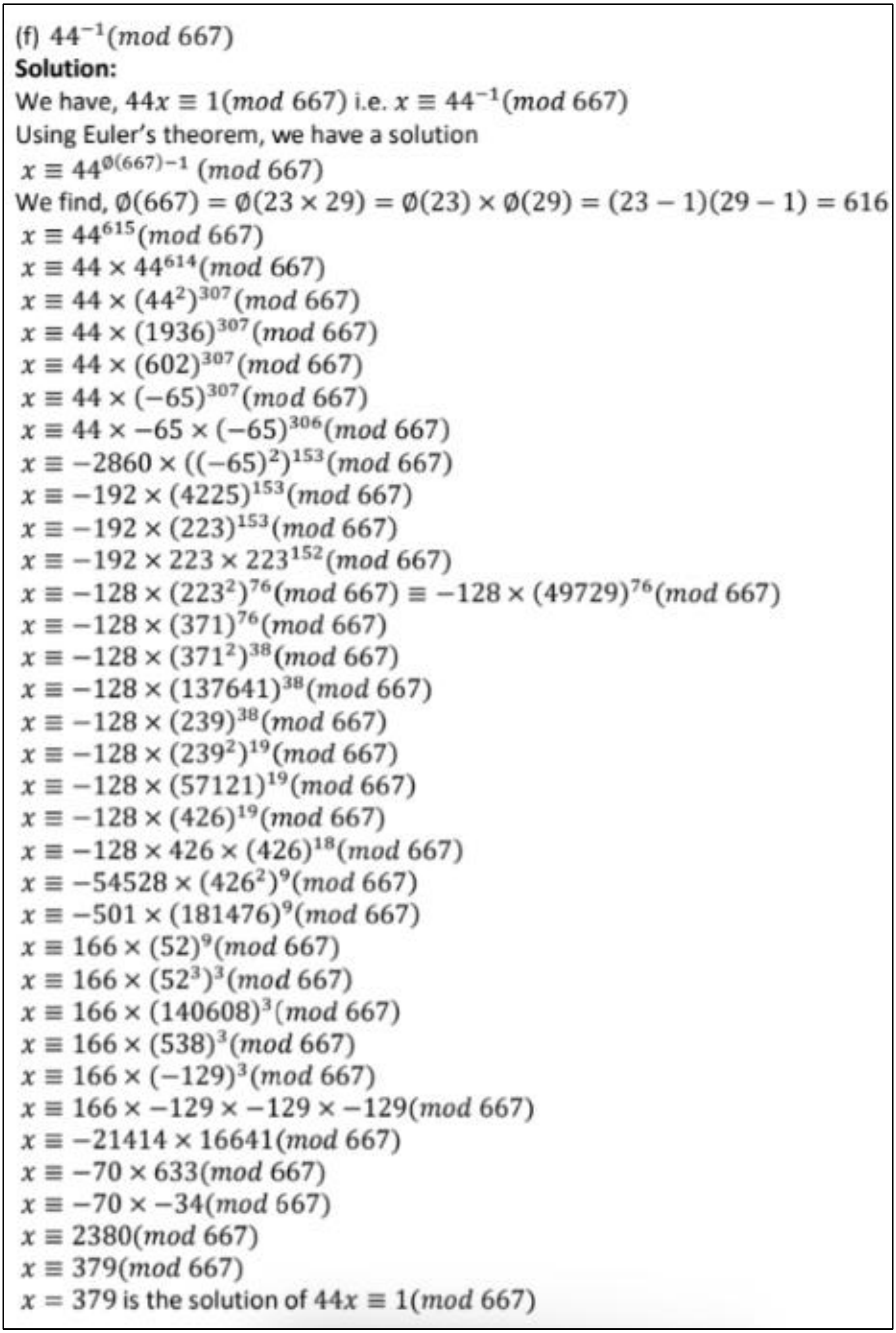
$x \equiv -333 \times 211(mod\ 403)$

$x \equiv -70263(mod\ 403)$

$x \equiv -141(mod\ 403)$

$x \equiv 262(mod\ 403)$

$x = 262$ is the solution of $20x \equiv 1(mod\ 403)$



(f) $44^{-1}(mod\ 667)$

Solution:

We have, $44x \equiv 1(mod\ 667)$ i.e. $x \equiv 44^{-1}(mod\ 667)$

Using Euler's theorem, we have a solution

$x \equiv 44^{\emptyset(667)-1}\ (mod\ 667)$

We find, $\emptyset(667) = \emptyset(23 \times 29) = \emptyset(23) \times \emptyset(29) = (23-1)(29-1) = 616$

$x \equiv 44^{615}(mod\ 667)$

$x \equiv 44 \times 44^{614}(mod\ 667)$

$x \equiv 44 \times (44^2)^{307}(mod\ 667)$

$x \equiv 44 \times (1936)^{307}(mod\ 667)$

$x \equiv 44 \times (602)^{307}(mod\ 667)$

$x \equiv 44 \times (-65)^{307}(mod\ 667)$

$x \equiv 44 \times -65 \times (-65)^{306}(mod\ 667)$

$x \equiv -2860 \times ((-65)^2)^{153}(mod\ 667)$

$x \equiv -192 \times (4225)^{153}(mod\ 667)$

$x \equiv -192 \times (223)^{153}(mod\ 667)$

$x \equiv -192 \times 223 \times 223^{152}(mod\ 667)$

$x \equiv -128 \times (223^2)^{76}(mod\ 667) \equiv -128 \times (49729)^{76}(mod\ 667)$

$x \equiv -128 \times (371)^{76}(mod\ 667)$

$x \equiv -128 \times (371^2)^{38}(mod\ 667)$

$x \equiv -128 \times (137641)^{38}(mod\ 667)$

$x \equiv -128 \times (239)^{38}(mod\ 667)$

$x \equiv -128 \times (239^2)^{19}(mod\ 667)$

$x \equiv -128 \times (57121)^{19}(mod\ 667)$

$x \equiv -128 \times (426)^{19}(mod\ 667)$

$x \equiv -128 \times 426 \times (426)^{18}(mod\ 667)$

$x \equiv -54528 \times (426^2)^9(mod\ 667)$

$x \equiv -501 \times (181476)^9(mod\ 667)$

$x \equiv 166 \times (52)^9(mod\ 667)$

$x \equiv 166 \times (52^3)^3(mod\ 667)$

$x \equiv 166 \times (140608)^3(mod\ 667)$

$x \equiv 166 \times (538)^3(mod\ 667)$

$x \equiv 166 \times (-129)^3(mod\ 667)$

$x \equiv 166 \times -129 \times -129 \times -129(mod\ 667)$

$x \equiv -21414 \times 16641(mod\ 667)$

$x \equiv -70 \times 633(mod\ 667)$

$x \equiv -70 \times -34(mod\ 667)$

$x \equiv 2380(mod\ 667)$

$x \equiv 379(mod\ 667)$

$x = 379$ is the solution of $44x \equiv 1(mod\ 667)$

8. Use Euler's theorem to compute

(a) $7^{1615}(mod\ 31)$

Solution:

By Euler's theorem,

$7^{\phi(31)} \equiv 1(mod\ 31)$ where $\phi(31) = 31 - 1 = 30$

$7^{30} \equiv 1(mod\ 31)$

$(7^{30})^{53} \equiv 1^{53}(mod\ 31)$

$7^{1590} \equiv 1(mod\ 31)$

$7^{1590} \times 7^{25} \equiv 1 \times 7^{25}(mod\ 31)$

$7^{1615} \equiv 7 \times 7^{24}(mod\ 31)$

$7^{1615} \equiv 7 \times (7^2)^{12}(mod\ 31) \equiv 7 \times (49)^{12}(mod\ 31)$

$7^{1615} \equiv 7 \times (18)^{12}(mod\ 31)$

$7^{1615} \equiv 7 \times (18^2)^6(mod\ 31)$

$7^{1615} \equiv 7 \times (324)^6(mod\ 31)$

$7^{1615} \equiv 7 \times (14)^6(mod\ 31)$

$7^{1615} \equiv 7 \times (14^2)^3(mod\ 31)$

$7^{1615} \equiv 7 \times (196)^3(mod\ 31)$

$7^{1615} \equiv 7 \times (10)^3(mod\ 31)$

$7^{1615} \equiv 7 \times 1000(mod\ 31)$

$7^{1615} \equiv 7 \times 8(mod\ 31)$

$7^{1615} \equiv 56(mod\ 31)$

$7^{1615} \equiv 25(mod\ 31)$

(b) $11^{100000}(mod\ 54)$

Solution:

By Euler's theorem,

$11^{\phi(54)} \equiv 1(mod\ 54)$

where $\phi(54) = \phi(3^3.2) = \phi(3^3)\phi(2) = [3^3 - 3^{3-1}][2 - 1] = 18$

$11^{18} \equiv 1(mod\ 54)$

$(11^{18})^{5555} \equiv 1^{5555}(mod\ 54)$

$11^{99990} \equiv 1(mod\ 54)$

$11^{99990} \times 11^{10} \equiv 1 \times 11^{10}(mod\ 54)$

$11^{100000} \equiv (11^2)^5(mod\ 54)$

$11^{100000} \equiv (121)^5(mod\ 54)$

$11^{100000} \equiv (13)^5(mod\ 54)$

$11^{100000} \equiv 13 \times 13^4(mod\ 54)$

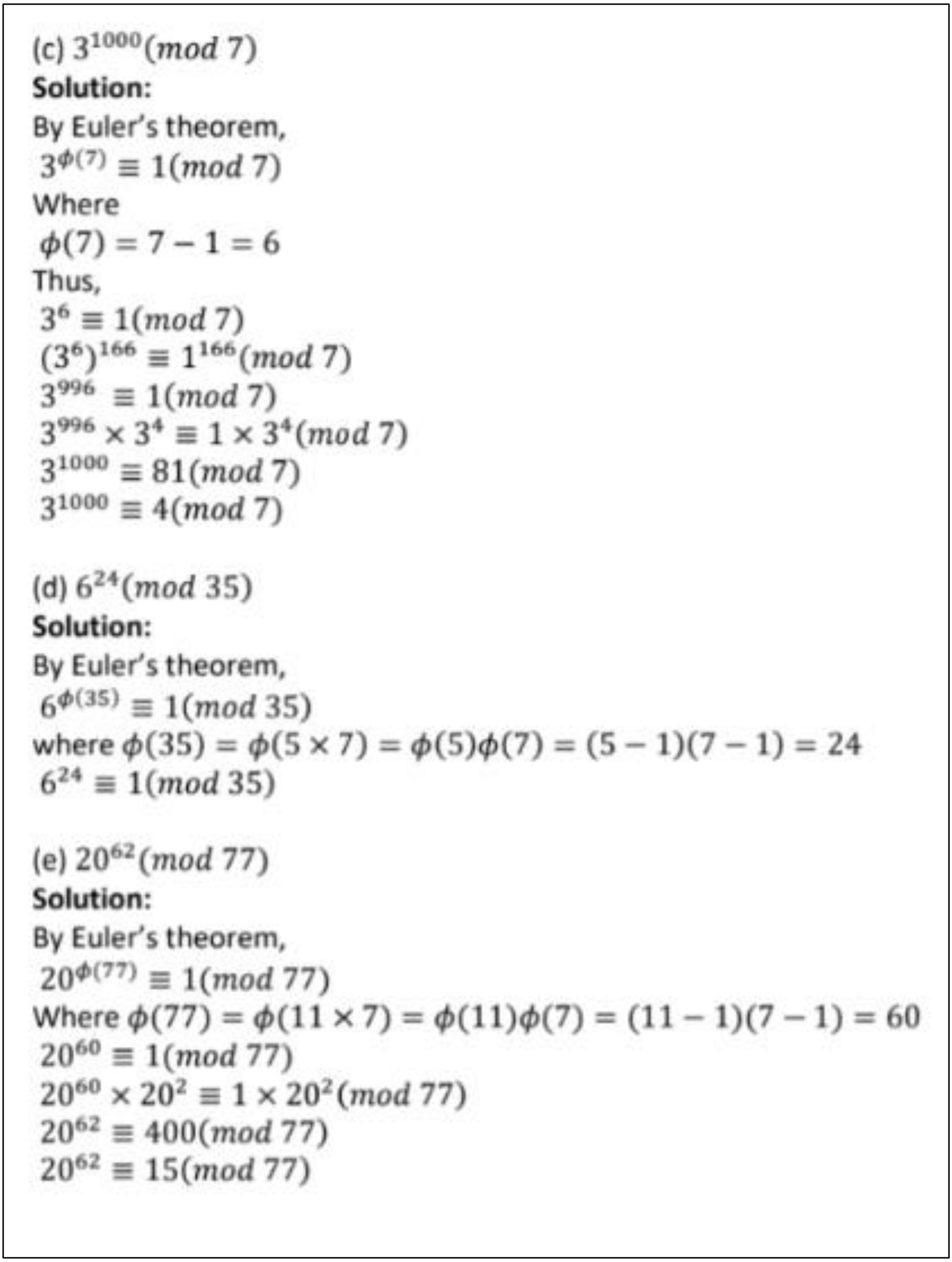
$11^{100000} \equiv 13 \times (13^2)^2(mod\ 54)$

$11^{100000} \equiv 13 \times (169)^2(mod\ 54)$

$11^{100000} \equiv 13 \times 7^2(mod\ 54)$

$11^{100000} \equiv 13 \times 49(mod\ 54)$

$11^{100000} \equiv 43(mod\ 54)$



(c) $3^{1000}(mod\ 7)$

Solution:

By Euler's theorem,

$3^{\phi(7)} \equiv 1(mod\ 7)$

Where

$\phi(7) = 7 - 1 = 6$

Thus,

$3^{6} \equiv 1(mod\ 7)$

$(3^{6})^{166} \equiv 1^{166}(mod\ 7)$

$3^{996} \equiv 1(mod\ 7)$

$3^{996} \times 3^{4} \equiv 1 \times 3^{4}(mod\ 7)$

$3^{1000} \equiv 81(mod\ 7)$

$3^{1000} \equiv 4(mod\ 7)$

(d) $6^{24}(mod\ 35)$

Solution:

By Euler's theorem,

$6^{\phi(35)} \equiv 1(mod\ 35)$

where $\phi(35) = \phi(5 \times 7) = \phi(5)\phi(7) = (5-1)(7-1) = 24$

$6^{24} \equiv 1(mod\ 35)$

(e) $20^{62}(mod\ 77)$

Solution:

By Euler's theorem,

$20^{\phi(77)} \equiv 1(mod\ 77)$

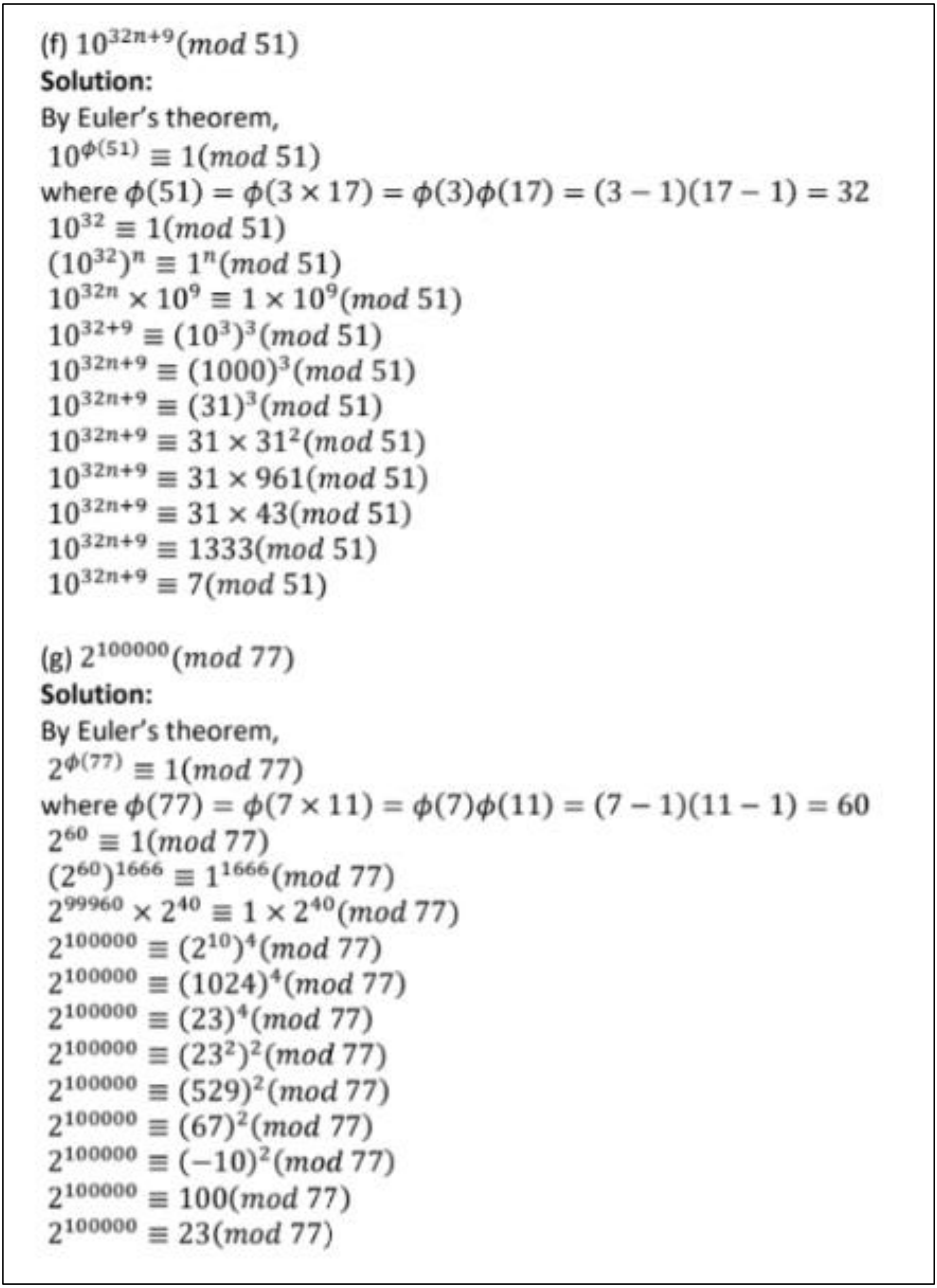
Where $\phi(77) = \phi(11 \times 7) = \phi(11)\phi(7) = (11-1)(7-1) = 60$

$20^{60} \equiv 1(mod\ 77)$

$20^{60} \times 20^{2} \equiv 1 \times 20^{2}(mod\ 77)$

$20^{62} \equiv 400(mod\ 77)$

$20^{62} \equiv 15(mod\ 77)$



(f) $10^{32n+9}(mod\ 51)$

Solution:

By Euler's theorem,

$10^{\phi(51)} \equiv 1(mod\ 51)$

where $\phi(51) = \phi(3 \times 17) = \phi(3)\phi(17) = (3-1)(17-1) = 32$

$10^{32} \equiv 1(mod\ 51)$

$(10^{32})^n \equiv 1^n(mod\ 51)$

$10^{32n} \times 10^9 \equiv 1 \times 10^9(mod\ 51)$

$10^{32+9} \equiv (10^3)^3(mod\ 51)$

$10^{32n+9} \equiv (1000)^3(mod\ 51)$

$10^{32n+9} \equiv (31)^3(mod\ 51)$

$10^{32n+9} \equiv 31 \times 31^2(mod\ 51)$

$10^{32n+9} \equiv 31 \times 961(mod\ 51)$

$10^{32n+9} \equiv 31 \times 43(mod\ 51)$

$10^{32n+9} \equiv 1333(mod\ 51)$

$10^{32n+9} \equiv 7(mod\ 51)$

(g) $2^{100000}(mod\ 77)$

Solution:

By Euler's theorem,

$2^{\phi(77)} \equiv 1(mod\ 77)$

where $\phi(77) = \phi(7 \times 11) = \phi(7)\phi(11) = (7-1)(11-1) = 60$

$2^{60} \equiv 1(mod\ 77)$

$(2^{60})^{1666} \equiv 1^{1666}(mod\ 77)$

$2^{99960} \times 2^{40} \equiv 1 \times 2^{40}(mod\ 77)$

$2^{100000} \equiv (2^{10})^4(mod\ 77)$

$2^{100000} \equiv (1024)^4(mod\ 77)$

$2^{100000} \equiv (23)^4(mod\ 77)$

$2^{100000} \equiv (23^2)^2(mod\ 77)$

$2^{100000} \equiv (529)^2(mod\ 77)$

$2^{100000} \equiv (67)^2(mod\ 77)$

$2^{100000} \equiv (-10)^2(mod\ 77)$

$2^{100000} \equiv 100(mod\ 77)$

$2^{100000} \equiv 23(mod\ 77)$

Type IV: Chinese Remainder Theorem

Let $M = m_1.m_2.m_3$

$\therefore M_1 = m_2.m_3$

$\therefore M_2 = m_1.m_3$

$\therefore M_3 = m_1.m_2$

Solve for x_1, x_2, x_3 by using these equations

$M_1x_1 \equiv 1(mod\ m_1), M_2x_2 \equiv 1(mod\ m_2), M_3x_3 \equiv 1(mod\ m_3)$

Thus, $x = [R_1M_1x_1 + R_2M_2x_2 + R_3M_3x_3](mod\ M)$

Classwork Problems

1. Find a positive integer which leaves remainder 1, if divided by 3; remainder 2, if divided by 5; and remainder 3, if divided by 7

Solution:

We have,

$x \equiv 1(mod\ 3)$

$x \equiv 2(mod\ 5)$

$x \equiv 3(mod\ 7)$

Let $M = 3 \times 5 \times 7 = 105$

$M_1 = 5 \times 7 = 35, M_2 = 3 \times 7 = 21, M_3 = 3 \times 5 = 15$

Consider the following congruences,

$35x_1 \equiv 1(mod\ 3)$

$21x_2 \equiv 1(mod\ 5)$

$15x_3 \equiv 1(mod\ 7)$

By Chinese remainder theorem,

$x = [1M_1x_1 + 2M_2x_2 + 3M_3x_3](mod\ M)$

Now,

$35x_1 \equiv 1(mod\ 3)$	$21x_2 \equiv 1(mod\ 5)$	$15x_3 \equiv 1(mod\ 7)$
$1 \equiv 35x_1(mod\ 3)$	$1 \equiv 21x_2(mod\ 5)$	$1 \equiv 15x_3(mod\ 7)$
$1 \equiv 2x_1(mod\ 3)$	$1 \equiv x_2(mod\ 5)$	$1 \equiv x_3(mod\ 7)$
$2 \equiv 4x_1(mod\ 3)$	$x_2 \equiv 1(mod\ 5)$	$x_3 \equiv 1(mod\ 7)$
$2 \equiv x_1(mod\ 3)$	$\therefore x_2 = 1$	$\therefore x_3 = 1$
$x_1 \equiv 2(mod\ 3)$		
$\therefore x_1 = 2$		

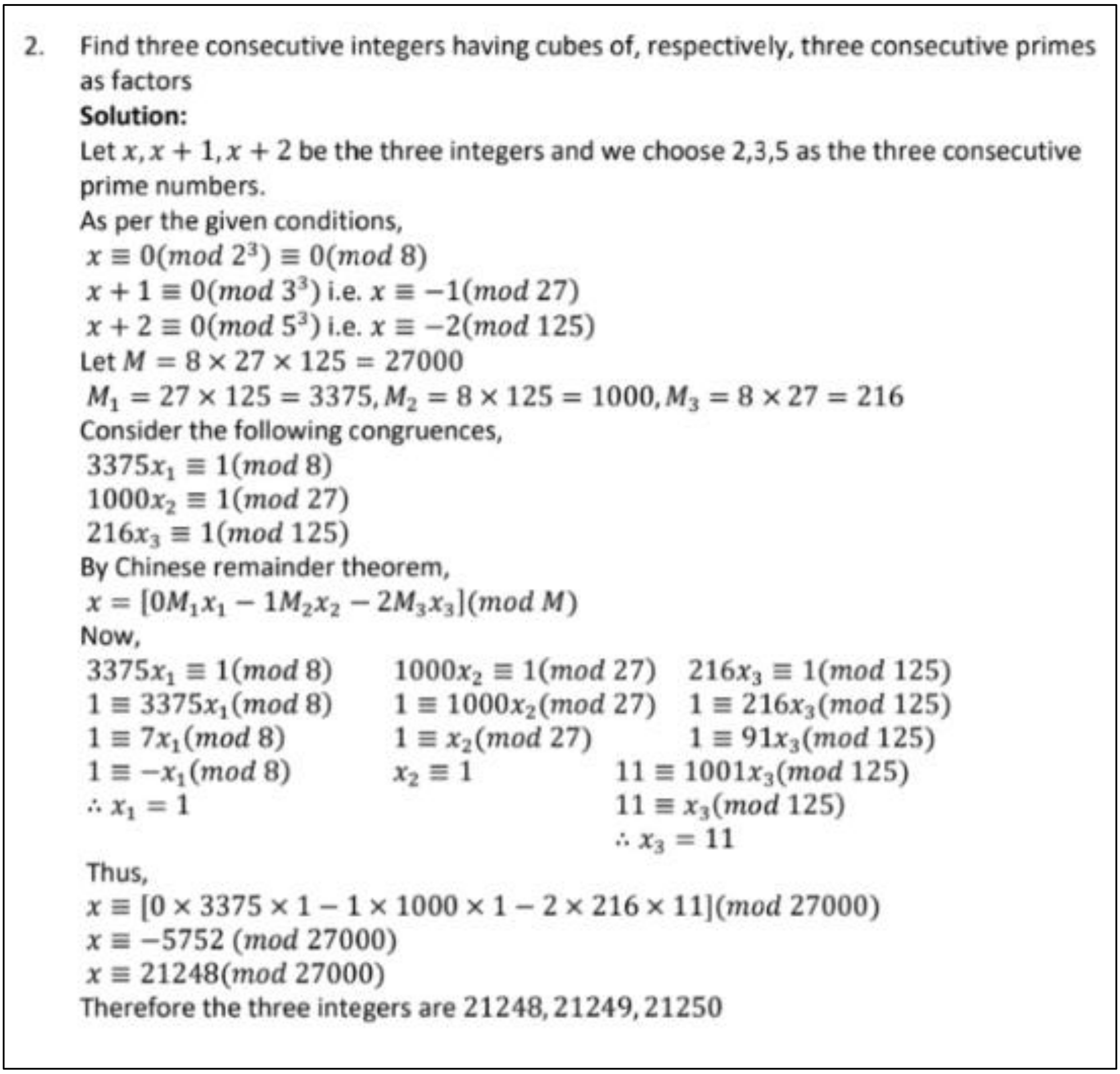
Thus,

$x \equiv [1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1](mod\ 105)$

$x \equiv 157\ (mod\ 105)$

$x \equiv 52\ (mod\ 105)$

Therefore 52 is a number that leaves remainder 1, 2 and 3 when divided by 3, 5 and 7 respectively



2. Find three consecutive integers having cubes of, respectively, three consecutive primes as factors

Solution:

Let $x, x+1, x+2$ be the three integers and we choose 2,3,5 as the three consecutive prime numbers.

As per the given conditions,

$x \equiv 0(mod\ 2^3) \equiv 0(mod\ 8)$

$x+1 \equiv 0(mod\ 3^3)$ i.e. $x \equiv -1(mod\ 27)$

$x+2 \equiv 0(mod\ 5^3)$ i.e. $x \equiv -2(mod\ 125)$

Let $M = 8 \times 27 \times 125 = 27000$

$M_1 = 27 \times 125 = 3375, M_2 = 8 \times 125 = 1000, M_3 = 8 \times 27 = 216$

Consider the following congruences,

$3375x_1 \equiv 1(mod\ 8)$

$1000x_2 \equiv 1(mod\ 27)$

$216x_3 \equiv 1(mod\ 125)$

By Chinese remainder theorem,

$x = [0M_1x_1 - 1M_2x_2 - 2M_3x_3](mod\ M)$

Now,

$3375x_1 \equiv 1(mod\ 8)$

$1 \equiv 3375x_1(mod\ 8)$

$1 \equiv 7x_1(mod\ 8)$

$1 \equiv -x_1(mod\ 8)$

$\therefore x_1 = 1$

$1000x_2 \equiv 1(mod\ 27)$

$1 \equiv 1000x_2(mod\ 27)$

$1 \equiv x_2(mod\ 27)$

$x_2 \equiv 1$

$216x_3 \equiv 1(mod\ 125)$

$1 \equiv 216x_3(mod\ 125)$

$1 \equiv 91x_3(mod\ 125)$

$11 \equiv 1001x_3(mod\ 125)$

$11 \equiv x_3(mod\ 125)$

$\therefore x_3 = 11$

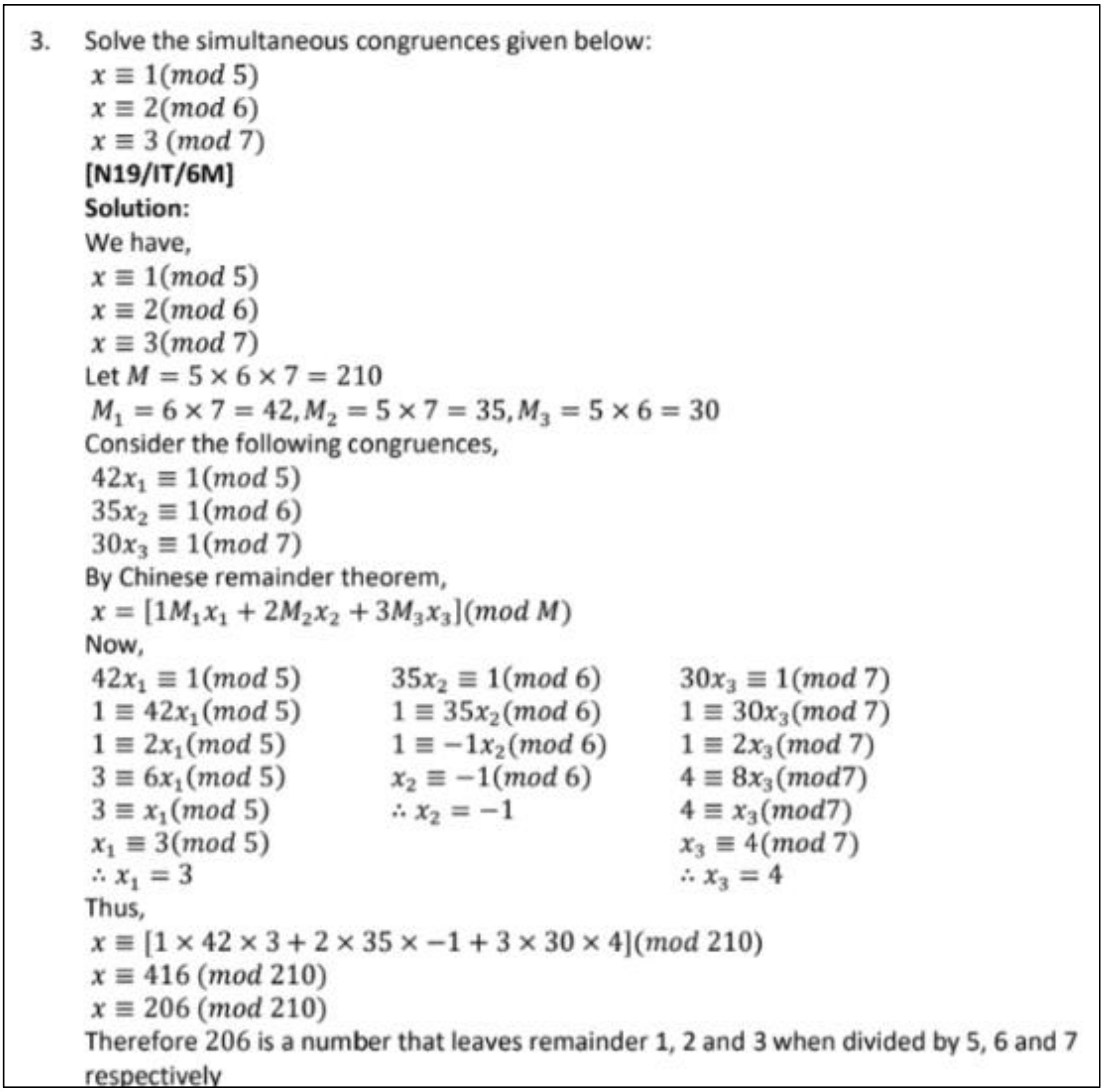
Thus,

$x \equiv [0 \times 3375 \times 1 - 1 \times 1000 \times 1 - 2 \times 216 \times 11](mod\ 27000)$

$x \equiv -5752\ (mod\ 27000)$

$x \equiv 21248(mod\ 27000)$

Therefore the three integers are $21248, 21249, 21250$



3. Solve the simultaneous congruences given below:

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

[N19/IT/6M]

Solution:

We have,

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

Let $M = 5 \times 6 \times 7 = 210$

$M_1 = 6 \times 7 = 42, M_2 = 5 \times 7 = 35, M_3 = 5 \times 6 = 30$

Consider the following congruences,

$42x_1 \equiv 1(mod\ 5)$
$35x_2 \equiv 1(mod\ 6)$
$30x_3 \equiv 1(mod\ 7)$

By Chinese remainder theorem,

$x = [1M_1x_1 + 2M_2x_2 + 3M_3x_3](mod\ M)$

Now,

$42x_1 \equiv 1(mod\ 5)$
$1 \equiv 42x_1(mod\ 5)$
$1 \equiv 2x_1(mod\ 5)$
$3 \equiv 6x_1(mod\ 5)$
$3 \equiv x_1(mod\ 5)$
$x_1 \equiv 3(mod\ 5)$
$\therefore x_1 = 3$

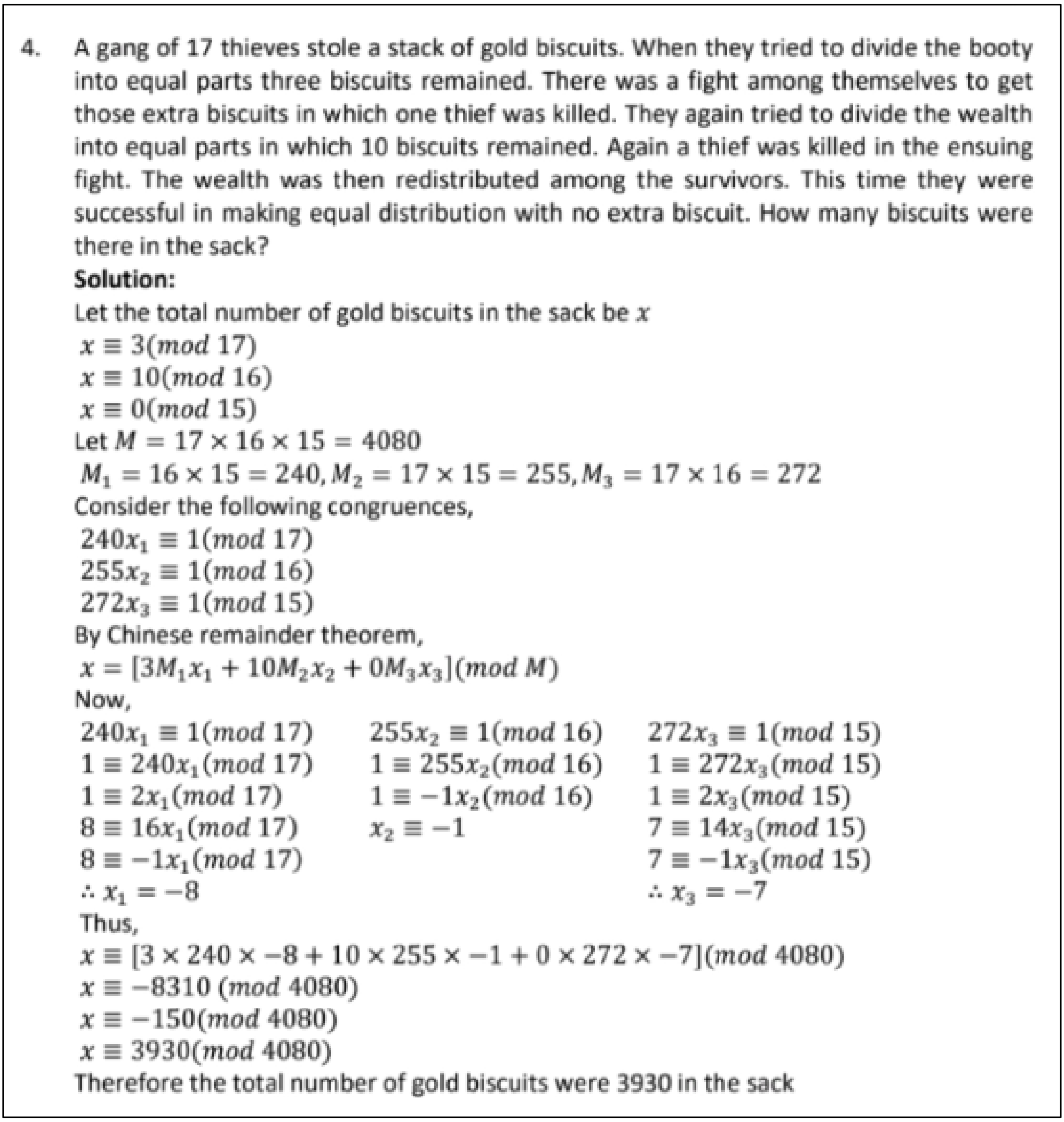
$35x_2 \equiv 1(mod\ 6)$
$1 \equiv 35x_2(mod\ 6)$
$1 \equiv -1x_2(mod\ 6)$
$x_2 \equiv -1(mod\ 6)$
$\therefore x_2 = -1$

$30x_3 \equiv 1(mod\ 7)$
$1 \equiv 30x_3(mod\ 7)$
$1 \equiv 2x_3(mod\ 7)$
$4 \equiv 8x_3(mod7)$
$4 \equiv x_3(mod7)$
$x_3 \equiv 4(mod\ 7)$
$\therefore x_3 = 4$

Thus,

$x \equiv [1 \times 42 \times 3 + 2 \times 35 \times -1 + 3 \times 30 \times 4](mod\ 210)$
$x \equiv 416\ (mod\ 210)$
$x \equiv 206\ (mod\ 210)$

Therefore 206 is a number that leaves remainder 1, 2 and 3 when divided by 5, 6 and 7 respectively



4. A gang of 17 thieves stole a stack of gold biscuits. When they tried to divide the booty into equal parts three biscuits remained. There was a fight among themselves to get those extra biscuits in which one thief was killed. They again tried to divide the wealth into equal parts in which 10 biscuits remained. Again a thief was killed in the ensuing fight. The wealth was then redistributed among the survivors. This time they were successful in making equal distribution with no extra biscuit. How many biscuits were there in the sack?

Solution:

Let the total number of gold biscuits in the sack be x

$x \equiv 3(mod\ 17)$

$x \equiv 10(mod\ 16)$

$x \equiv 0(mod\ 15)$

Let $M = 17 \times 16 \times 15 = 4080$

$M_1 = 16 \times 15 = 240, M_2 = 17 \times 15 = 255, M_3 = 17 \times 16 = 272$

Consider the following congruences,

$240x_1 \equiv 1(mod\ 17)$

$255x_2 \equiv 1(mod\ 16)$

$272x_3 \equiv 1(mod\ 15)$

By Chinese remainder theorem,

$x = [3M_1x_1 + 10M_2x_2 + 0M_3x_3](mod\ M)$

Now,

$240x_1 \equiv 1(mod\ 17)$

$1 \equiv 240x_1(mod\ 17)$

$1 \equiv 2x_1(mod\ 17)$

$8 \equiv 16x_1(mod\ 17)$

$8 \equiv -1x_1(mod\ 17)$

$\therefore x_1 = -8$

$255x_2 \equiv 1(mod\ 16)$

$1 \equiv 255x_2(mod\ 16)$

$1 \equiv -1x_2(mod\ 16)$

$x_2 \equiv -1$

$272x_3 \equiv 1(mod\ 15)$

$1 \equiv 272x_3(mod\ 15)$

$1 \equiv 2x_3(mod\ 15)$

$7 \equiv 14x_3(mod\ 15)$

$7 \equiv -1x_3(mod\ 15)$

$\therefore x_3 = -7$

Thus,

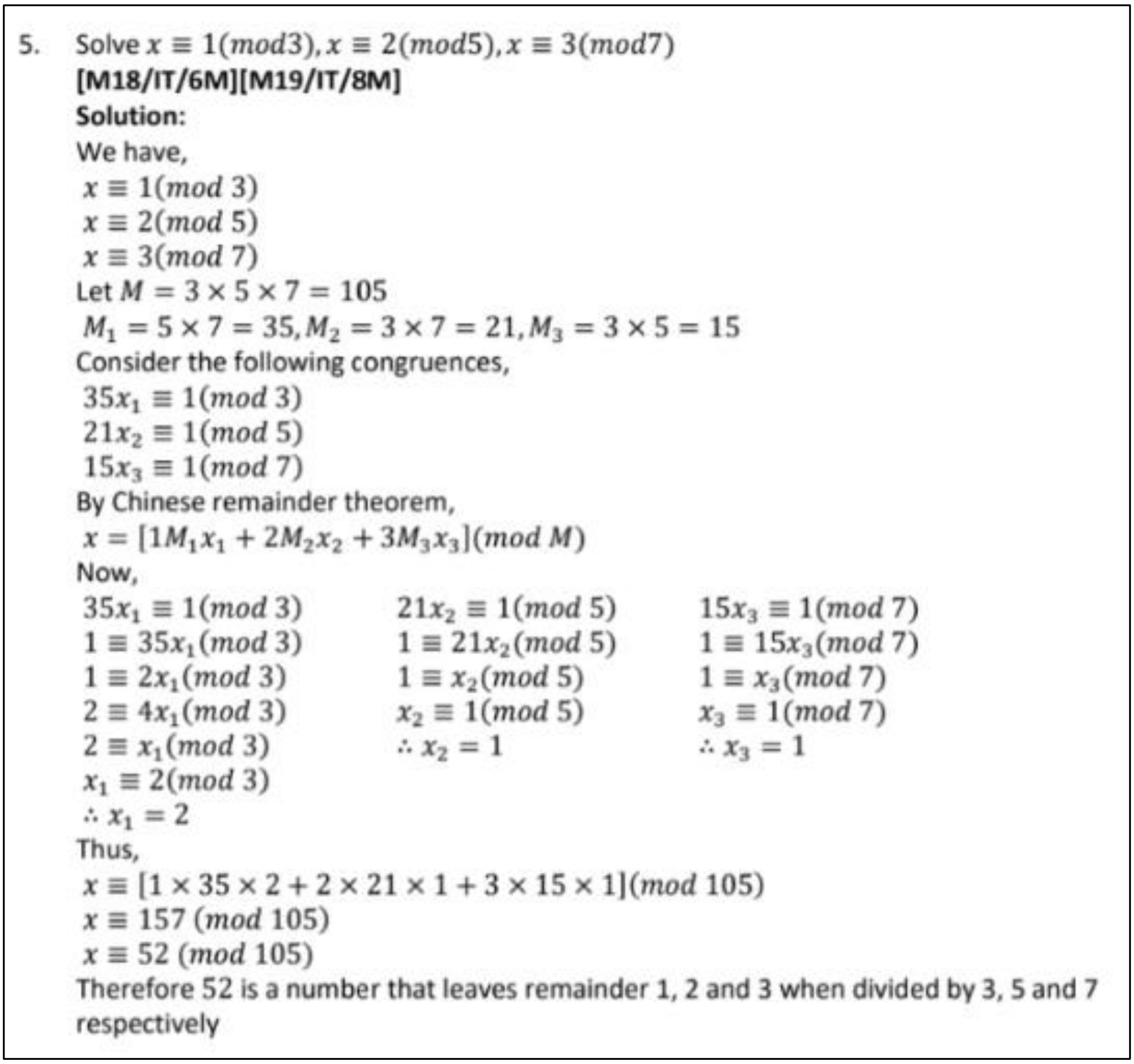
$x \equiv [3 \times 240 \times -8 + 10 \times 255 \times -1 + 0 \times 272 \times -7](mod\ 4080)$

$x \equiv -8310\ (mod\ 4080)$

$x \equiv -150(mod\ 4080)$

$x \equiv 3930(mod\ 4080)$

Therefore the total number of gold biscuits were 3930 in the sack



5. Solve $x \equiv 1(mod3), x \equiv 2(mod5), x \equiv 3(mod7)$

[M18/IT/6M][M19/IT/8M]

Solution:

We have,

$x \equiv 1(mod\ 3)$
$x \equiv 2(mod\ 5)$
$x \equiv 3(mod\ 7)$

Let $M = 3 \times 5 \times 7 = 105$

$M_1 = 5 \times 7 = 35, M_2 = 3 \times 7 = 21, M_3 = 3 \times 5 = 15$

Consider the following congruences,

$35x_1 \equiv 1(mod\ 3)$
$21x_2 \equiv 1(mod\ 5)$
$15x_3 \equiv 1(mod\ 7)$

By Chinese remainder theorem,

$x = [1M_1x_1 + 2M_2x_2 + 3M_3x_3](mod\ M)$

Now,

$35x_1 \equiv 1(mod\ 3)$
$1 \equiv 35x_1(mod\ 3)$
$1 \equiv 2x_1(mod\ 3)$
$2 \equiv 4x_1(mod\ 3)$
$2 \equiv x_1(mod\ 3)$
$x_1 \equiv 2(mod\ 3)$
$\therefore x_1 = 2$

$21x_2 \equiv 1(mod\ 5)$
$1 \equiv 21x_2(mod\ 5)$
$1 \equiv x_2(mod\ 5)$
$x_2 \equiv 1(mod\ 5)$
$\therefore x_2 = 1$

$15x_3 \equiv 1(mod\ 7)$
$1 \equiv 15x_3(mod\ 7)$
$1 \equiv x_3(mod\ 7)$
$x_3 \equiv 1(mod\ 7)$
$\therefore x_3 = 1$

Thus,

$x \equiv [1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1](mod\ 105)$
$x \equiv 157\ (mod\ 105)$
$x \equiv 52\ (mod\ 105)$

Therefore 52 is a number that leaves remainder 1, 2 and 3 when divided by 3, 5 and 7 respectively

6. Solve $x \equiv 5(mod6), x \equiv 4(mod11), x \equiv 3(mod17)$

[N18/IT/6M]

Solution:

We have,

$x \equiv 5(mod\ 6)$

$x \equiv 4(mod\ 11)$

$x \equiv 3(mod\ 17)$

Let $M = 6 \times 11 \times 17 = 1122$

$M_1 = 11 \times 17 = 187, M_2 = 6 \times 17 = 102, M_3 = 6 \times 11 = 66$

Consider the following congruences,

$187x_1 \equiv 1(mod\ 6)$

$102x_2 \equiv 1(mod\ 11)$

$66x_3 \equiv 1(mod\ 17)$

By Chinese remainder theorem,

$x = [5M_1x_1 + 4M_2x_2 + 3M_3x_3](mod\ M)$

Now,

$187x_1 \equiv 1(mod\ 6)$

$1 \equiv 187x_1(mod\ 6)$

$1 \equiv x_1(mod\ 6)$

$x_1 \equiv 1(mod\ 6)$

$\therefore x_1 = 1$

$102x_2 \equiv 1(mod\ 11)$

$1 \equiv 102x_2(mod\ 11)$

$1 \equiv 3x_2(mod\ 11)$

$4 \equiv 12x_2(mod11)$

$4 \equiv x_2(mod11)$

$\therefore x_2 = 4$

$66x_3 \equiv 1(mod\ 17)$

$1 \equiv 66x_3(mod\ 17)$

$1 \equiv 15x_3(mod\ 17)$

$1 \equiv -2x_3(mod\ 17)$

$9 \equiv -18x_3(mod17)$

$9 \equiv -x_3(mod17)$

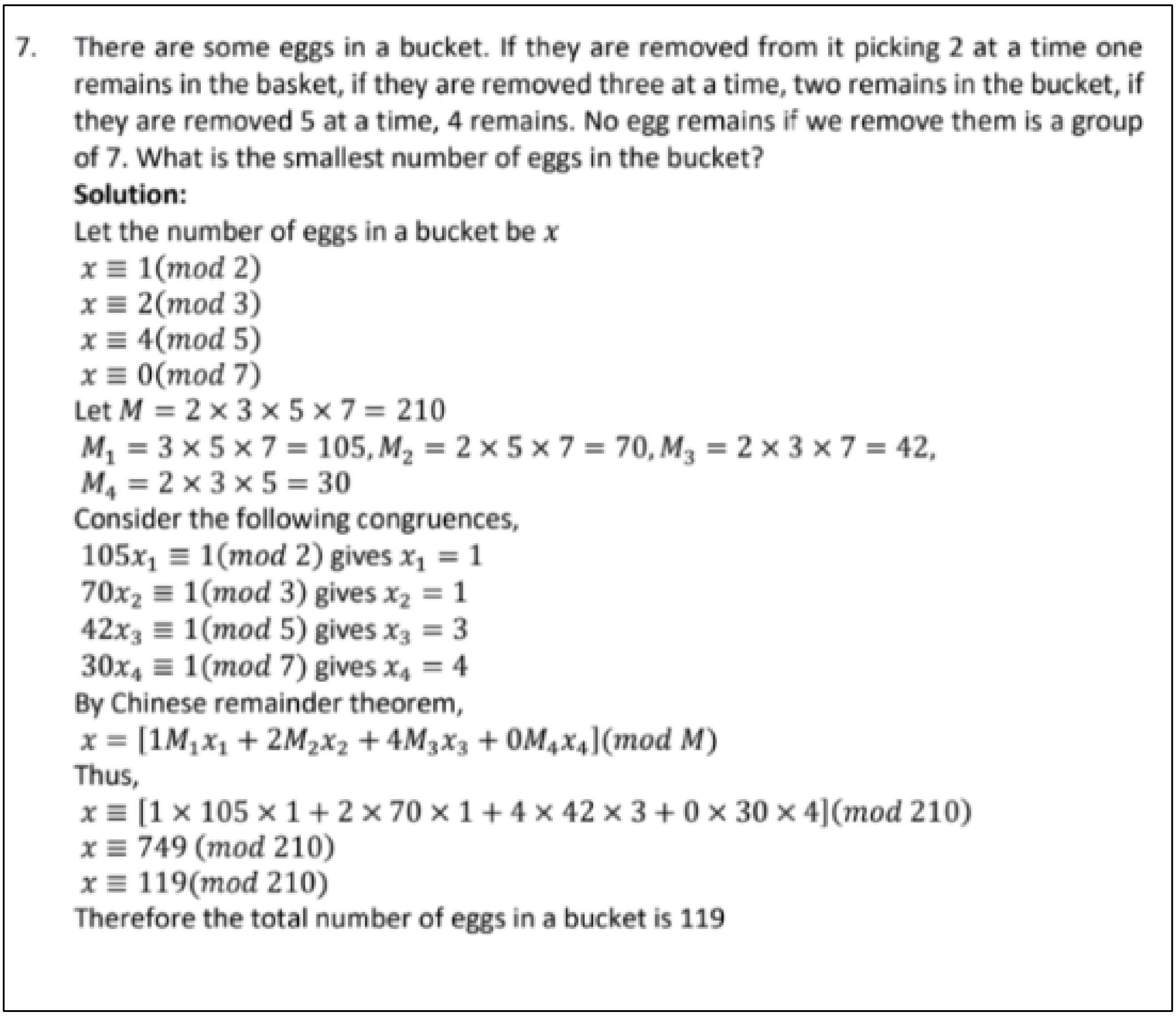
$\therefore x_3 = -9$

Thus,

$x \equiv [5 \times 187 \times 1 + 4 \times 102 \times 4 + 3 \times 66 \times -9](mod\ 1122)$

$x \equiv 785\ (mod\ 1122)$

Therefore 785 is a number that leaves remainder 5, 4 and 3 when divided by 6, 11 and 17 respectively



7. There are some eggs in a bucket. If they are removed from it picking 2 at a time one remains in the basket, if they are removed three at a time, two remains in the bucket, if they are removed 5 at a time, 4 remains. No egg remains if we remove them is a group of 7. What is the smallest number of eggs in the bucket?

Solution:

Let the number of eggs in a bucket be x

$x \equiv 1(mod\ 2)$

$x \equiv 2(mod\ 3)$

$x \equiv 4(mod\ 5)$

$x \equiv 0(mod\ 7)$

Let $M = 2 \times 3 \times 5 \times 7 = 210$

$M_1 = 3 \times 5 \times 7 = 105, M_2 = 2 \times 5 \times 7 = 70, M_3 = 2 \times 3 \times 7 = 42,$

$M_4 = 2 \times 3 \times 5 = 30$

Consider the following congruences,

$105x_1 \equiv 1(mod\ 2)$ gives $x_1 = 1$

$70x_2 \equiv 1(mod\ 3)$ gives $x_2 = 1$

$42x_3 \equiv 1(mod\ 5)$ gives $x_3 = 3$

$30x_4 \equiv 1(mod\ 7)$ gives $x_4 = 4$

By Chinese remainder theorem,

$x = [1M_1x_1 + 2M_2x_2 + 4M_3x_3 + 0M_4x_4](mod\ M)$

Thus,

$x \equiv [1 \times 105 \times 1 + 2 \times 70 \times 1 + 4 \times 42 \times 3 + 0 \times 30 \times 4](mod\ 210)$

$x \equiv 749\ (mod\ 210)$

$x \equiv 119(mod\ 210)$

Therefore the total number of eggs in a bucket is 119

Type V: RSA Algorithm

RSA (Rivest-Shamir-Adleman) Algorithm is an asymmetric or public key cryptography algorithm, which means it works on two different keys: Public Key and Private Key.

The Public Key is used for encryption and is known to everyone, while the Private Key is used for decryption and must be kept secret by the receiver.

RSA Algorithm is named after Ron Rivest, Adi Shamir and Leonard Adleman, who published the algorithm in 1977.

Example of Asymmetric Cryptography:

If Person A wants to send a message securely to Person B:

- Person A encrypts the message using Person B's Public Key.
- Person B decrypts the message using their Private Key.

Use of the RSA algorithm typically consists of four stages: key generation, key distribution, encryption and decryption:

1. Key generation. Two large prime numbers are selected and used to generate the public and private keys.
2. Key distribution. The public key can be shared with anyone who needs to send encrypted messages to the recipient. The private key is kept secure and only known to the recipient.
3. Encryption. To encrypt a message, the sender uses the recipient's public key to transform the message into cipher text. That makes the message unreadable to anyone who doesn't have the private key.
4. Decryption. The recipient uses their private key to decrypt the cipher text back into the original message. That way, only the intended recipient is able to read the message.

Steps to solve:

- Choose two large prime numbers, say p and q. These prime numbers should be kept secret.
- Calculate the product of primes, $n = p \times q$. This product is part of the public as well as the private key.
- Calculate Euler Totient Function $\phi(n)$ as
  $\phi(n) = \phi(p \times q) = \phi(p) \times \phi(q) = (p-1)(q-1)$
- Choose encryption exponent e, such that $1 < e < \phi(n)$ and $(e, \phi(n)) = 1$, that is e should be co-prime with $\phi(n)$.
- Calculate decryption exponent d, such that $de \equiv 1 \left(mod\phi(n)\right)$, that is d is modular multiplicative inverse of $e \left(mod\phi(n)\right)$.

  We can have multiple values of d satisfying $de \equiv 1 \left(mod\phi(n)\right)$ but it does not matter which value we choose as all of them are valid keys and will result into same message on decryption.

  Finally, the Public Key $= (n, e)$ and the Private Key $= (n, d)$.

5. Decryption Formula

Decrypt the cipher text using the Private Key $(n, d) = (33, 3)$

$M \equiv C^d (mod\ n)$

$M \equiv 7^3 (mod\ 33)$

$M \equiv 343 (mod\ 33)$

$M = 13$

1. p and q are two prime numbers $p = 7$ and $q = 17$. Take public key $e = 5$. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Also calculate plain text value from cipher text.

Solution:

Here, $p = 7, q = 17. n = p \times q = 7 \times 17 = 119$

$\phi(n) = \phi(119) = \phi(7 \times 17) = \phi(7)\phi(17) = (7 - 1)(17 - 1)$

$\therefore \phi(n) = 96$

Given that $e = 5$

Thus $de \equiv 1 \left(mod\phi(n)\right)$ gives

$5d \equiv 1 (mod\ 96)$

$d \equiv 5^{-1} (mod\ 96)$

$d \equiv 5^{\phi(96)-1} (mod\ 96)$ By Euler's theorem

Where $\phi(96) = \phi(3 \times 2^5) = \phi(3)\phi(2^5) = (3 - 1)(2^5 - 2^4) = 32$

$d \equiv 5^{32-1} (mod\ 96)$

$d \equiv 5^{31} (mod\ 96)$

$d \equiv 5^4 \times 5^{27} (mod\ 96)$

$d \equiv 625 (mod\ 96) \times (5^3)^9 (mod\ 96)$

$d \equiv 49 (mod\ 96) \times (125)^9 (mod\ 96)$

$d \equiv 49 \times (29)^9 (mod\ 96)$

$d \equiv 49 \times (29^3)^3 (mod\ 96)$

$d \equiv 49 \times (24389)^3 (mod\ 96)$

$d \equiv 49 \times (5)^3 (mod\ 96)$

$d \equiv 49 \times 125 (mod\ 96)$

$d \equiv 49 \times 29 (mod\ 96)$

$d \equiv 1421 (mod\ 96)$

$d = 77$

Public Key $= (n, e) = (119, 5)$ and the Private Key $= (n, d) = (119, 77)$

Sender's message, $M = 6$

Thus, encrypting

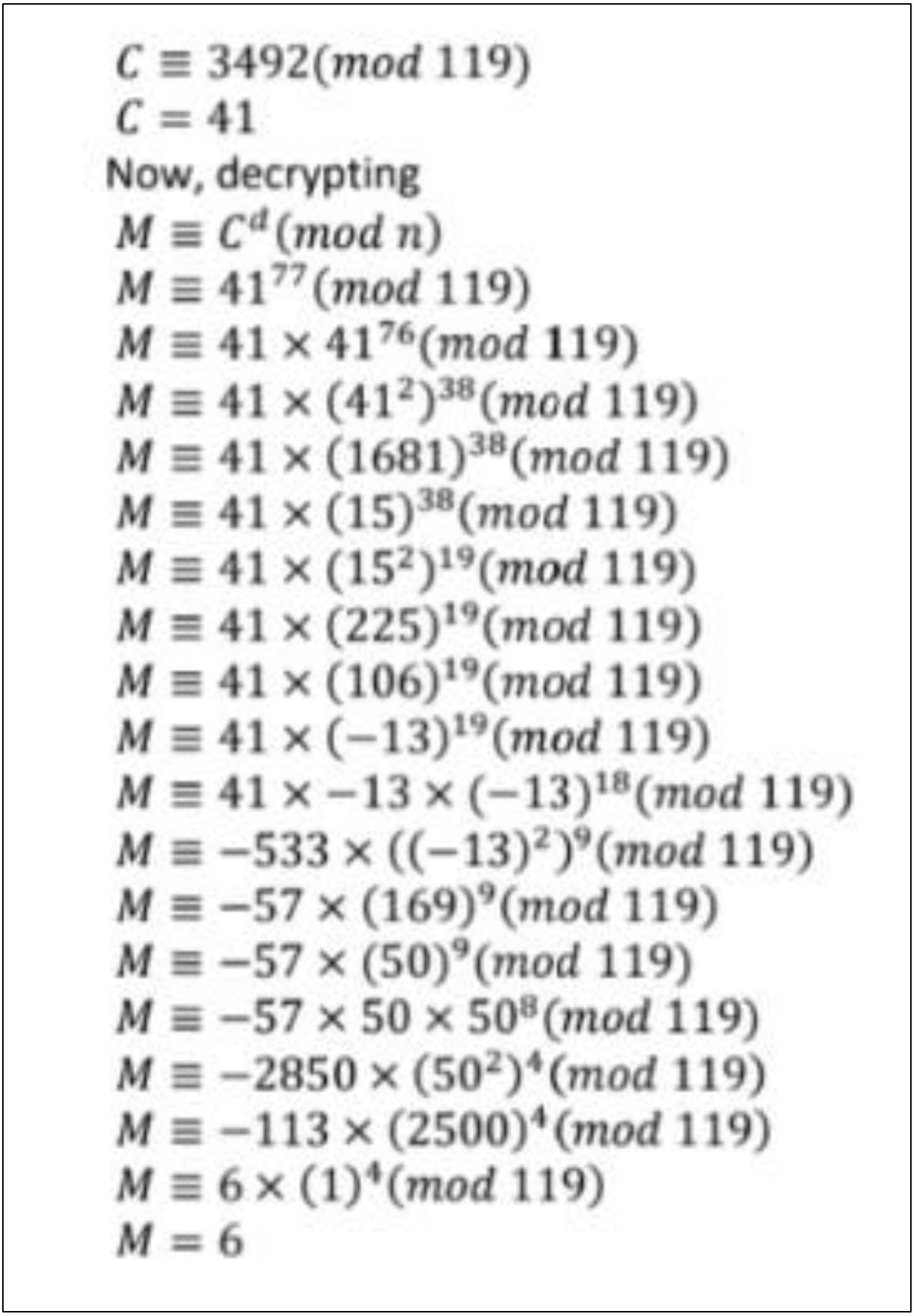
$C \equiv M^e (mod\ n)$

$C \equiv 6^5 (mod\ 119)$

$C \equiv 6^2 \times 6^3 (mod\ 119)$

$C \equiv 36 \times 216 (mod\ 119)$

$C \equiv 36 \times 97 (mod\ 119)$



$C \equiv 3492(mod\ 119)$

$C = 41$

Now, decrypting

$M \equiv C^{d}(mod\ n)$

$M \equiv 41^{77}(mod\ 119)$

$M \equiv 41 \times 41^{76}(mod\ 119)$

$M \equiv 41 \times (41^{2})^{38}(mod\ 119)$

$M \equiv 41 \times (1681)^{38}(mod\ 119)$

$M \equiv 41 \times (15)^{38}(mod\ 119)$

$M \equiv 41 \times (15^{2})^{19}(mod\ 119)$

$M \equiv 41 \times (225)^{19}(mod\ 119)$

$M \equiv 41 \times (106)^{19}(mod\ 119)$

$M \equiv 41 \times (-13)^{19}(mod\ 119)$

$M \equiv 41 \times -13 \times (-13)^{18}(mod\ 119)$

$M \equiv -533 \times ((-13)^{2})^{9}(mod\ 119)$

$M \equiv -57 \times (169)^{9}(mod\ 119)$

$M \equiv -57 \times (50)^{9}(mod\ 119)$

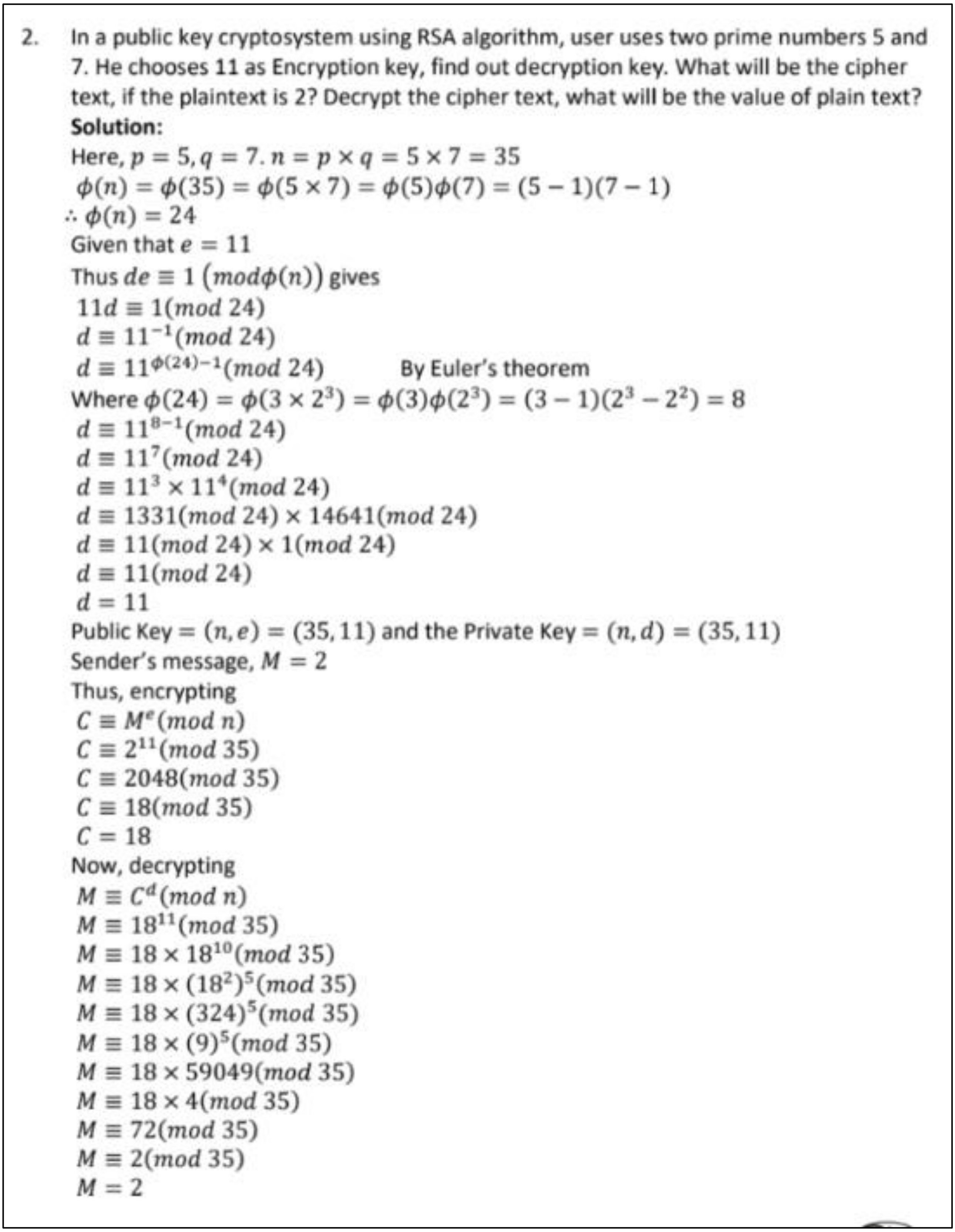
$M \equiv -57 \times 50 \times 50^{8}(mod\ 119)$

$M \equiv -2850 \times (50^{2})^{4}(mod\ 119)$

$M \equiv -113 \times (2500)^{4}(mod\ 119)$

$M \equiv 6 \times (1)^{4}(mod\ 119)$

$M = 6$



2. In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key, find out decryption key. What will be the cipher text, if the plaintext is 2? Decrypt the cipher text, what will be the value of plain text?

Solution:

Here, $p = 5, q = 7. n = p \times q = 5 \times 7 = 35$

$\phi(n) = \phi(35) = \phi(5 \times 7) = \phi(5)\phi(7) = (5-1)(7-1)$

$\therefore \phi(n) = 24$

Given that $e = 11$

Thus $de \equiv 1\left(mod\phi(n)\right)$ gives

$11d \equiv 1(mod\ 24)$

$d \equiv 11^{-1}(mod\ 24)$

$d \equiv 11^{\phi(24)-1}(mod\ 24)$ By Euler's theorem

Where $\phi(24) = \phi(3 \times 2^3) = \phi(3)\phi(2^3) = (3-1)(2^3 - 2^2) = 8$

$d \equiv 11^{8-1}(mod\ 24)$

$d \equiv 11^7(mod\ 24)$

$d \equiv 11^3 \times 11^4(mod\ 24)$

$d \equiv 1331(mod\ 24) \times 14641(mod\ 24)$

$d \equiv 11(mod\ 24) \times 1(mod\ 24)$

$d \equiv 11(mod\ 24)$

$d = 11$

Public Key $= (n, e) = (35, 11)$ and the Private Key $= (n, d) = (35, 11)$

Sender's message, $M = 2$

Thus, encrypting

$C \equiv M^e(mod\ n)$

$C \equiv 2^{11}(mod\ 35)$

$C \equiv 2048(mod\ 35)$

$C \equiv 18(mod\ 35)$

$C = 18$

Now, decrypting

$M \equiv C^d(mod\ n)$

$M \equiv 18^{11}(mod\ 35)$

$M \equiv 18 \times 18^{10}(mod\ 35)$

$M \equiv 18 \times (18^2)^5(mod\ 35)$

$M \equiv 18 \times (324)^5(mod\ 35)$

$M \equiv 18 \times (9)^5(mod\ 35)$

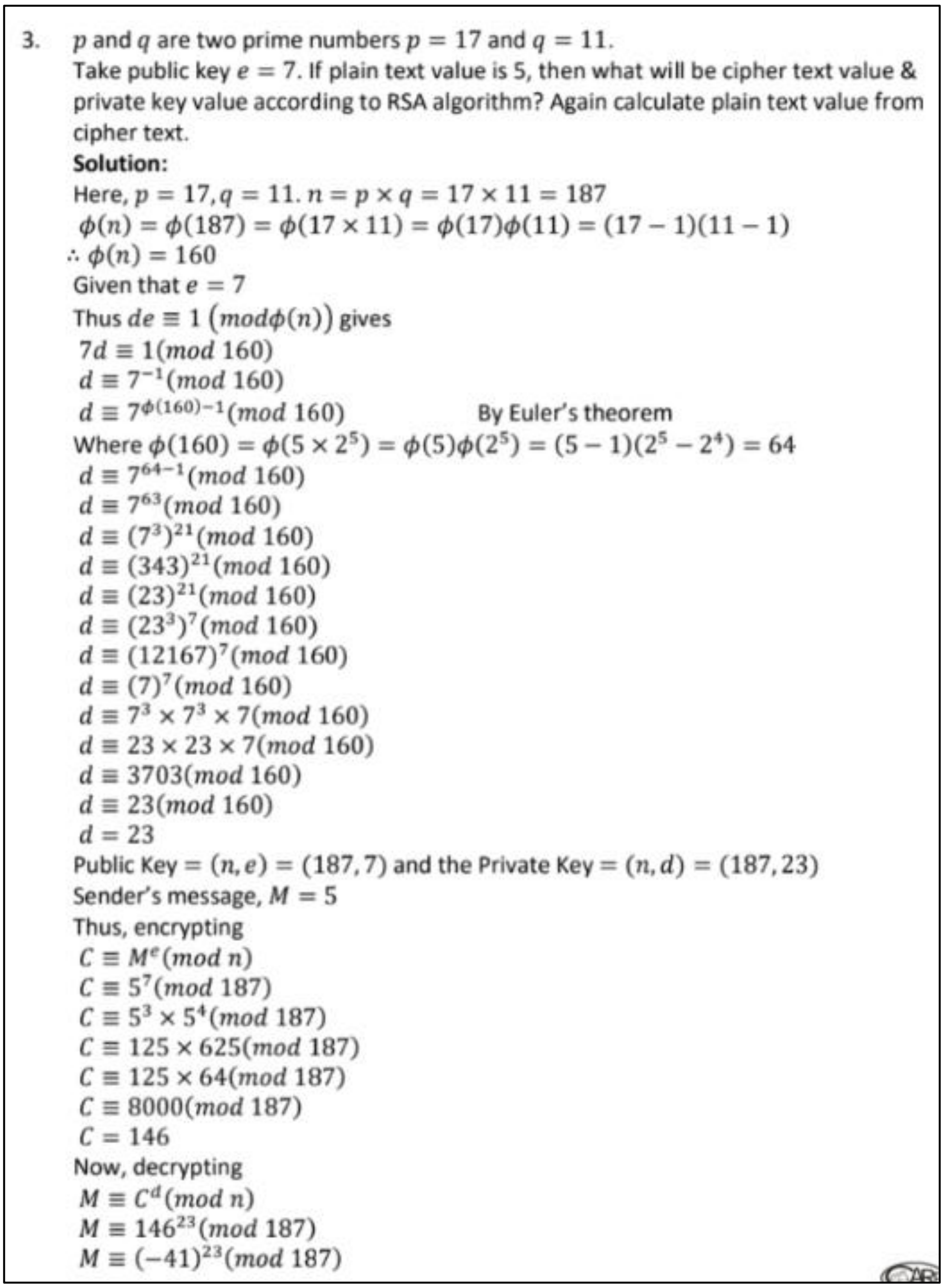
$M \equiv 18 \times 59049(mod\ 35)$

$M \equiv 18 \times 4(mod\ 35)$

$M \equiv 72(mod\ 35)$

$M \equiv 2(mod\ 35)$

$M = 2$



3. p and q are two prime numbers $p = 17$ and $q = 11$.
Take public key $e = 7$. If plain text value is 5, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

Here, $p = 17, q = 11. n = p \times q = 17 \times 11 = 187$

$\phi(n) = \phi(187) = \phi(17 \times 11) = \phi(17)\phi(11) = (17 - 1)(11 - 1)$

$\therefore \phi(n) = 160$

Given that $e = 7$

Thus $de \equiv 1\left(mod\phi(n)\right)$ gives

$7d \equiv 1(mod\ 160)$

$d \equiv 7^{-1}(mod\ 160)$

$d \equiv 7^{\phi(160)-1}(mod\ 160)$ By Euler's theorem

Where $\phi(160) = \phi(5 \times 2^5) = \phi(5)\phi(2^5) = (5 - 1)(2^5 - 2^4) = 64$

$d \equiv 7^{64-1}(mod\ 160)$

$d \equiv 7^{63}(mod\ 160)$

$d \equiv (7^3)^{21}(mod\ 160)$

$d \equiv (343)^{21}(mod\ 160)$

$d \equiv (23)^{21}(mod\ 160)$

$d \equiv (23^3)^7(mod\ 160)$

$d \equiv (12167)^7(mod\ 160)$

$d \equiv (7)^7(mod\ 160)$

$d \equiv 7^3 \times 7^3 \times 7(mod\ 160)$

$d \equiv 23 \times 23 \times 7(mod\ 160)$

$d \equiv 3703(mod\ 160)$

$d \equiv 23(mod\ 160)$

$d = 23$

Public Key $= (n, e) = (187, 7)$ and the Private Key $= (n, d) = (187, 23)$

Sender's message, $M = 5$

Thus, encrypting

$C \equiv M^e(mod\ n)$

$C \equiv 5^7(mod\ 187)$

$C \equiv 5^3 \times 5^4(mod\ 187)$

$C \equiv 125 \times 625(mod\ 187)$

$C \equiv 125 \times 64(mod\ 187)$

$C \equiv 8000(mod\ 187)$

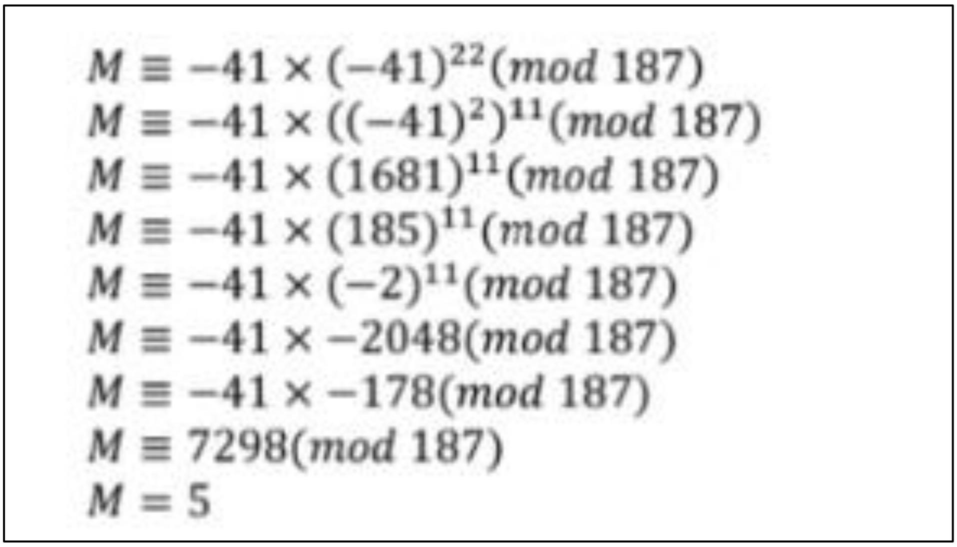
$C = 146$

Now, decrypting

$M \equiv C^d(mod\ n)$

$M \equiv 146^{23}(mod\ 187)$

$M \equiv (-41)^{23}(mod\ 187)$



$M \equiv -41 \times (-41)^{22}(mod\ 187)$

$M \equiv -41 \times ((-41)^2)^{11}(mod\ 187)$

$M \equiv -41 \times (1681)^{11}(mod\ 187)$

$M \equiv -41 \times (185)^{11}(mod\ 187)$

$M \equiv -41 \times (-2)^{11}(mod\ 187)$

$M \equiv -41 \times -2048(mod\ 187)$

$M \equiv -41 \times -178(mod\ 187)$

$M \equiv 7298(mod\ 187)$

$M = 5$