Assignment - 2

Q1] Find the value of $\phi(29)$, $\phi(32)$, $\phi(80)$, $\phi(100)$, $\phi(101)$

i) $\phi(29)$

↳ here, 29 is a prime number

∴ Using 2nd property of euler's phi function

i.e $\phi(p) = p-1$ where p is prime

∴ $\phi(29) = 29-1 = 28$

∴ $\boxed{\phi(29) = 28}$

ii) $\phi(32)$

here, ~~32 ≠ 2^5~~ 32 is not prime but it can be written as.

$32 = 2^5$

$\phi(32) = \phi(2^5)$

∴ Using 4th property of euler's phi function.

i.e $\phi(p^e) = p^e - p^{e-1}$ wher p is prime

∴ $\phi(32) = \phi(2^5) = 2^5 - 2^{5-1}$

$= 2^5 - 2^4 = 16$

$\boxed{\phi(32) = 16}$

iii) $\phi(80)$

↳ here, 80 is not prime no. but it can be written as,

$80 = 2^4 \times 5$

i.e $\phi(80) = \phi(2^4 \times 5)$

Using property ③ i.e

$\phi(m \times n) = \phi(m) \times \phi(n)$

$\therefore \phi(2^4 \times 5) = \phi(2^4) \times \phi(5)$ —①

Now, for finding $\phi(2^4)$ applying 4th property of Euler's phi function

i.e $\phi(p^e) = p^e - p^{e-1}$

$\therefore \phi(2^4) = 2^4 - 2^{4-1} = 2^4 - 2^3 = 8$

put this in eqn ①

$\phi(2^4 \times 5) = 8 \times \phi(5)$

Using property ①

$\phi(p) = p - 1$

$\phi(5) = 5 - 1 = 4$

$\therefore \phi(2^4 \times 5) = 8 \times 4 = 32$

$\boxed{\phi(80) = 32}$

iv) $\phi(100)$

↳ here, 100 can be written as,

$100 = 2^2 \times 5^2$

$\phi(100) = \phi(2^2 \times 5^2)$

By using the property ③

$\phi(m \times n) = \phi(m) \times \phi(n)$

$\phi(2^2 \times 5^2) = \phi(2^2) \times \phi(5^2)$

Now for calculating $\phi(2^2)$ & $\phi(5^2)$

Using property ④

$\phi(p^e) = p^e - p^{e-1}$

$\therefore \phi(2^2) = 2^2 - 2^{2-1} = 2^2 - 2^1 = 2$

$\phi(5^2) = 5^2 - 5^{2-1} = 5^2 - 5^1 = 20$

$\therefore \phi(2^2 \times 5^2) = 2 \times 20 = 40$

$\boxed{\phi(100) = 40}$

v) $\phi(101)$

↳ here 101 is prime number

∴ Using property ① of Euler's phi

$\phi(p) = p - 1$ where p is prime

$\phi(101) = 101 - 1 = 100$

$\boxed{\phi(101) = 100}$

Q2) Find the results of the following using Fermat's little theorem

i) $5^{15} \bmod 13$

↳ $5^{15} = 5^{12} \times 5^3$

$\therefore 5^{15} \bmod 13 = (5^{12} \times 5^3) \bmod 13$

$= ((5^{12} \bmod 13) \times (5^3 \bmod 13)) \bmod 13$ —— ①

$5^{12} \bmod 13$ can be written as, $5^{13-1} \bmod 13$.

$\therefore$ Using Fermat's little theorem,

i.e $\boxed{a^{p-1} \bmod p = 1}$

where p is prime & p does not divide a.

$\therefore \boxed{5^{13-1} \bmod 13 = 1}$

& $5^3 \bmod 13 = 125 \bmod 13 = 8$

$\therefore$ putting this value in above eq^n ①

$5^{15} \bmod 13 = 1 \times 8$

$\boxed{5^{15} \bmod 13 = 8}$

ii) $15^{18} \bmod 17$

↳ $15^{18} = 15^{16} \times 15^2$

$\therefore 15^{18} \bmod 17 = (15^{16} \times 15^2) \bmod 17$

$= ((15^{16} \bmod 17) \times (15^2 \bmod 17)) \bmod 17$ —— ①

Calculating $15^{16} \bmod 17$ & $15^2 \bmod 17$ seperately.

$15^{16} \bmod 17 = 15^{17-1} \bmod 17$

$\therefore$ Using Fermat's little theorem

$\boxed{a^{p-1} \bmod p = 1}$

$\therefore 15^{17-1} \bmod 17 = 1$

$\therefore \boxed{15^{16} \bmod 17 = 1}$

$15^2 \bmod 17 = 225 \bmod 17 = 8$

putting this value in eq^n ①

$\therefore 15^{18} \bmod 17 = 1 \times 8$

$\boxed{15^{18} \bmod 17 = 8}$

iii) $456^{17} \bmod 17$

↳ $456^{17} \bmod 17$

Using Fermat's little theorem second version.

i.e $\boxed{a^p \bmod p = a}$

where p is prime & a is integer

$\therefore 456^{17} \bmod 17 = 456$

but 456 is not in Z_{17}

$\therefore$ Taking mod. 17 $= 456 \bmod 17$

$= 14$

$\therefore \boxed{456^{17} \bmod 17 = 14}$

iv) $145^{102} \bmod 101$

↳ $145^{102} = 145^{100} \times 145^{2}$ ~~mod 101~~

$\therefore 145^{102} \bmod 101 = \left((145^{100} \bmod 101) \times (145^{2} \bmod 101)\right) \bmod 101$ —①

$\therefore 145^{100} \bmod 101 = 145^{101-1} \bmod 101$

∴ Using Fermat's little theorem,

$\boxed{a^{p-1} \bmod p = 1}$

$\therefore \boxed{145^{101-1} \bmod 101 = 1}$

$145^{2} \bmod 101 = 21025 \bmod 101$

$= 17$

putting this values in eq^n ①

$145^{102} \bmod 101 = 1 \times 17$

$\boxed{145^{102} \bmod 101 = 17}$

Q3) Find the results of the following using Fermat's little theorem.

a) $5^{-1} \bmod 13$

↳ ~~Using the Fermat~~

here, 13 is prime

∴ Using Fermat's little theorem for multiplicative inverse

$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$

$\therefore 5^{-1} \bmod 13 = 5^{13-2} \bmod 13$

$= 5^{11} \bmod 13$

$= 48828125 \bmod 13$

$= 8$

$\therefore \boxed{5^{-1} \bmod 13 = 8}$

b) $15^{-1} \bmod 17$

↳ here, 17 is prime

∴ Using Fermat's little theorem, for multiplicative inverse,

$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$

$\therefore 15^{-1} \bmod 17 = 15^{17-2} \bmod 17$

$= 15^{15} \bmod 17$

$= \left(15^{8} \cdot 15^{4} \cdot 15^{2} \cdot 15\right) \bmod 17$

$= \left((15^{8} \bmod 17)(15^{4} \bmod 17)(15^{2} \bmod 17)(15 \bmod 17)\right) \bmod 17$ —①

$\therefore 15 \bmod 17 = 15$

$15^{2} \bmod 17 = 225 \bmod 17 = 4$

$15^{4} \bmod 17 = \left((15^{2} \cdot \bmod 17)(15^{2} \bmod 17)\right) \bmod 17$

$= (4 \times 4) \bmod 17 = 16$

$15^{8} \bmod 17 = \left((15^{4} \bmod 17) \cdot (15^{4} \bmod 17)\right) \bmod 17$

$= (16 \times 16) \bmod 17 = 1$

From eq^n ①

$\therefore 15^{-1} \bmod 17 = (1 \times 16 \times 4 \times 15) \bmod 17 = 8$

$\boxed{15^{-1} \bmod 17 = 8}$

c) $27^{-1} \bmod 41$

↳ 41 is a prime no.

∴ Using Fermat's little theorem

$$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$$

$$27^{-1} \bmod 41 = 27^{41-2} \bmod 41$$
$$= 27^{39} \bmod 41$$

$$27^{39} \bmod 41 = (27^{32} \cdot 27^4 \cdot 27^2 \cdot 27^1) \bmod 41$$
$$= ((27^{32} \bmod 41)(27^4 \bmod 41) \cdot (27^2 \bmod 41) \cdot (27 \bmod 41)) \bmod 41 \quad \text{—— (1)}$$

$27 \bmod 41 = 27$

$27^2 \bmod 41 = 729 \bmod 41 = 32$

$27^4 \bmod 41 = ((27^2 \bmod 41)(27^2 \bmod 41)) \bmod 41$
$= (32 \times 32) \bmod 41 = 40$

$27^{32} \bmod 41 = 27^4 \cdot 27^4 \cdot 27^4 \cdot 27^4$

$27^8 \bmod 41 = ((27^4 \bmod 41)(27^4 \bmod 41)) \bmod 41$
$= (40 \times 40) \bmod 41 = 1$

$\therefore 27^{32} \bmod 41 = (27^8 \cdot 27^8 \cdot 27^8 \cdot 27^8) \bmod 41$
$= (1 \times 1 \times 1 \times 1) \bmod 41$
$= 1$

∴ From eqⁿ (1)

$27^{39} \bmod 41 = (1 \times 40 \times 32 \times 27) \bmod 41$
$= 38$

$\therefore \boxed{27^{-1} \bmod 41 = 38}$

d) $70^{-1} \bmod 101$

↳ 101 is a prime no.

∴ Using Fermat's little theorem,

$$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$$

$$70^{-1} \bmod 101 = 70^{101-2} \bmod 101$$
$$= 70^{99} \bmod 101$$

$$70^{99} \bmod 101 = (70^{64} \cdot 70^{32} \cdot 70^2 \cdot 70) \bmod 101$$
$$= ((70^{64} \bmod 101)(70^{32} \bmod 101)(70^2 \bmod 101)(70 \bmod 101)) \bmod 101 \quad \text{—— (1)}$$

Calculations :

$70 \bmod 101 = 70$

$70^2 \bmod 101 = 4900 \bmod 101 = 52$

$70^4 \bmod 101 = (52 \times 52) \bmod 101 = 78$

$70^8 \bmod 101 = (78 \times 78) \bmod 101 = 24$

$70^{16} \bmod 101 = (24 \times 24) \bmod 101 = 71$

$70^{32} \bmod 101 = (71 \times 71) \bmod 101 = 92$

$70^{64} \bmod 101 = (92 \times 92) \bmod 101 = 81$

∴ eqⁿ (1) becomes.

$70^{99} \bmod 101 = (81 \times 92 \times 52 \times 70) \bmod 101$
$= 13$

$\therefore \boxed{70^{-1} \bmod 101 = 13}$

Q4) Find the results of the following using Euler's theorem.

a) $12^{-1} \bmod 77$

↳ ~~77 is a prime no~~

& 12 & 77 are coprime.

∴ Using Euler's theorem for multiplicative inverse

$$\boxed{a^{-1} \bmod n = a^{\phi(n)-1} \bmod n}$$

$$12^{-1} \bmod 77 = 12^{\phi(77)-1} \bmod 77 \quad -①$$

$$\phi(77) = \phi(7 \times 11) = \phi(7) \times \phi(11)$$
$$= (7-1)(11-1)$$
$$= 6 \times 10 = 60$$

∴ eq^n ① becomes.

$$12^{-1} \bmod 77 = 12^{60-1} \bmod 77$$
$$= 12^{59} \bmod 77$$

$$12^{59} \bmod 77 = (12^{32} \cdot 12^{16} \cdot 12^{8} \cdot 12^{2} \cdot 12) \bmod 77$$
$$= ((12^{32} \bmod 77)(12^{16} \bmod 77)(12^{8} \bmod 77)$$
$$(12^{2} \bmod 77)(12 \bmod 77)) \bmod 77 \quad -②$$

Calculating mod values.

$12 \bmod 77 = 12$

$12^2 \bmod 77 = 67$

$12^8 \bmod 77 = (67 \times 67 \times 67 \times 67) \bmod 77 = 67$

$12^{16} \bmod 77 = (67 \times 67) \bmod 77 = 23$

$12^{32} \bmod 77 = (23 \times 23) \bmod 77 = 67$

∴ putting values in eq^n ②

$$12^{59} \bmod 77 = (67 \times 23 \times 67 \times 67 \times 12) \bmod 77$$
$$= 45$$

$$\therefore \boxed{12^{-1} \bmod 77 = 45}$$

b) $16^{-1} \bmod 323$

↳ ~~323 is a prime no.~~

& 16 & 323 are coprime.

∴ Using Euler's theorem for multiplicative inverse

$$\boxed{a^{-1} \bmod n = a^{\phi(n)-1} \bmod n}$$

$$16^{-1} \bmod 323 = 16^{\phi(323)-1} \bmod 323 \quad -①$$

$$\phi(323) = \phi(17 \times 19) = \phi(17) \times \phi(19)$$
$$= (17-1)(19-1)$$
$$= 16 \times 18 = 288$$

put this value in eq^n ①

$$16^{-1} \bmod 323 = 16^{288-1} \bmod 323$$
$$= 16^{287} \bmod 323$$

$16^{287} \bmod 323 = (16^{256} \cdot 16^{16} \cdot 16^{8} \cdot 16^{4} \cdot 16^{2} \cdot 16) \bmod 323$

$= (((16^{256} \bmod 323)(16^{16} \bmod 323)(16^{8} \bmod 323)(16^{4} \bmod 323)(16^{2} \bmod 323)(16 \bmod 323)) \bmod 323$

~~$16^{256} \bmod 323 =$~~

$16 \bmod 323 = 16$

$16^2 \bmod 323 = 256$

$16^4 \bmod 323 = (256 \times 256) \bmod 323 = 290$

$16^8 \bmod 323 = (290 \times 290) \bmod 323 = 120$

$16^{16} \bmod 323 = (120 \times 120) \bmod 323 = 188$

$16^{32} \bmod 323 = (188 \times 188) \bmod 323 = 137$

$16^{64} \bmod 323 = (137 \times 137 \bmod 323 = 85$

$16^{128} \bmod 323 = (35 \times 35) \bmod 323 = 256$

$16^{256} \bmod 323 = (256 \times 256) \bmod 323 = 290$

$16^{287} \bmod 323 = (290 \times 188 \times 120 \times 290 \times 256 \times 16) \bmod 323$

$= 101$

$\therefore \boxed{16^{-1} \bmod 323 = 101}$

c) $20^{-1} \bmod 403$

↳ ~~403~~ is a ~~prime~~ no.

& 20 & 403 are coprime

∴ Using Euler's theorem for multiplicative inverse

$\boxed{a^{-1} \bmod n = a^{\phi(n)-1} \bmod n}$

$\therefore 20^{-1} \bmod 403 = 20^{\phi(403)-1} \bmod 403$

$\phi(403) = \phi(13 \times 31) = \phi(t)$

$= (3-1)(31-1) = 12 \times 30 = 360$

$20^{-1} \bmod 403 = 20^{360-1} \bmod 403$

$= 20^{359} \bmod 403$

$20^{359} \bmod 403 = (20^{256} \cdot 20^{32} \cdot 20^{16} \cdot 20^{4} \cdot 20^{2} \cdot 20^{1}) \bmod 403$

$= ((20^{256} \bmod 403) \cdot (20^{32} \bmod 403) \cdot (20^{16} \bmod 403) \cdot (20^{4} \bmod 403) \cdot (20^{2} \bmod 403) \cdot (20 \bmod 403)) \bmod 403$

$= (20^{256} \cdot 20^{64} \cdot 20^{32} \cdot 20^{16} \cdot 20^{4} \cdot 20^{2} \cdot 20^{1}) \bmod 403$

Calculating mod value.

$20 \bmod 403 = 20$

$20^2 \bmod 403 = 400$

$20^4 \bmod 403 = (400 \times 400) \bmod 403 = 9$

$20^8 \bmod 403 = (9 \times 9) \bmod 403 = 81$

$20^{16} \bmod 403 = (81 \times 81) \bmod 403 = 113$

$20^{32} \bmod 403 = (113 \times 113) \bmod 403 = 276$

$20^{64} \bmod 403 = (276 \times 276) \bmod 403 = 9$

$20^{128} \bmod 403 = (9 \times 9) \bmod 403 = 81$

$20^{256} \bmod 403 = (81 \times 81) \bmod 403 = 113$

$\therefore 20^{359} \bmod 403 = (113 \times 9 \times 276 \times 113 \times 9 \times 400 \times 20) \bmod 403$

$= 187$

$\therefore \boxed{20^{-1} \bmod 403 = 187}$

d) $44^{-1} \bmod 667$

↳ Using Euler's theorem for multiplicative inverse,

$$\boxed{a^{-1} \bmod n = a^{\phi(n)-1} \bmod n}$$

$$44^{-1} \bmod 667 = 44^{\phi(667)-1} \bmod 667$$

$$\phi(667) = \phi(23 \times 29)$$
$$= \phi(23) \times \phi(29)$$
$$= (23-1)(29-1) = 22 \times 28 = 616$$

$$44^{-1} \bmod 667 = 44^{616-1} \bmod 667$$
$$= 44^{615} \bmod 667$$

$$44^{615} \bmod 667 = (44^{512} \cdot 44^{64} \cdot 44^{32} \cdot 44^{4} \cdot 44^{2} \cdot 44) \bmod 667$$

Calculating modulus value

$44 \bmod 667 = 44$

$44^2 \bmod 667 = 602$

$44^4 \bmod 667 = (602 \times 602) \bmod 667 = 223$

$44^8 \bmod 667 = (223 \times 223) \bmod 667 = 371$

$44^{16} \bmod 667 = (371 \times 371) \bmod 667 = 289$

$44^{32} \bmod 667 = (289 \times 289) \bmod 667 = 426$

$44^{64} \bmod 667 = (426 \times 426) \bmod 667 = 52$

$44^{128} \bmod 667 = (52 \times 52) \bmod 667 = 36$

$44^{256} \bmod 667 = (36 \times 36) \bmod 667 = 629$

$44^{512} \bmod 667 = (629 \times 629) \bmod 667 = 110$

$\therefore 44^{615} \bmod 667 = (110 \times 52 \times 426 \times 223 \times 602 \times 44) \bmod 667$

$= 379$

$\therefore \boxed{44^{-1} \bmod 667 = 379}$

Q5) Find the value of x for the following sets of congruence using the Chinese remainder theorem

a) $x \equiv 2 \bmod 7$, and $x \equiv 3 \bmod 9$

↳ Given:- $x \equiv 2 \bmod 7$

$x \equiv 3 \bmod 9$

From given eqn

$m_1 = 7$, $m_2 = 9$

$a_1 = 2$, $a_2 = 3$

Step 1:- Calculating M

$M = m_1 \times m_2$

$M = 7 \times 9 = 63$

Step 2:- Calculating M_1 & M_2

$M_1 = M/m_1 = 63/7 = 9$

$M_2 = M/m_2 = 63/9 = 7$

Steps: Calculating M_1^{-1} & M_2^{-1}

$M_1 = 9$

$9^{-1} \bmod 7$

here 7 is prime

Using Fermat's little theorem

$a^{-1} \bmod p = a^{p-2} \bmod p$

$9^{-1} \bmod 7 = 9^{7-2} \bmod 7$

$= 9^5 \bmod 7 = 4$

$\therefore \boxed{M_1^{-1} = 4}$

$M_2 = 7$

$7^{-1} \bmod 9$

7 & 9 ~~are prime~~ are coprime.

$\therefore$ Using Euler's theorem

$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$

$7^{-1} \bmod 9 = 7^{\phi(9)-1} \bmod 9$

$\phi(9) = \phi(3^2) = 3^2 - 3 = 6$

$\therefore 7^{-1} \bmod 9 = 7^{6-1} \bmod 9 = 7^5 \bmod 9$

$= 4$

$\boxed{M_2^{-1} = 4}$

Solution to simultaneous eq^n is,

$x = (a_1 \times M_1 \times M_1^{-1} + a_2 M_2 \times M_2^{-1}) \bmod M$

$= (2 \times 9 \times 4 + 3 \times 7 \times 4) \bmod 63$

$= (72 + 84) \bmod 63 = 30$

$\boxed{x = 30}$

b) $x \equiv 4 \bmod 5$ and $x \equiv 10 \bmod 11$

Given:- $x \equiv 4 \bmod 5$

$x \equiv 10 \bmod 11$

From the given eq^n

$a_1 = 4$, $a_2 = 10$, $m_1 = 5$, $m_2 = 11$

$M = m_1 \times m_2 = 5 \times 11 = 55$

$\boxed{M = 55}$

~~$M_1 = M/M =$~~

$M_1 = M/m_1 = 55/5 = 11$

$M_2 = M/m_2 = 55/11 = 5$

$M_1 = 11$

Calculating M_1^{-1},

$11^{-1} \bmod 5$

5 is prime no.

$\therefore$ Using Fermat's theorem,

$a^{-1} \bmod p = a^{p-2} \bmod p$

$11^{-1} \bmod 5 = 11^{5-2} \bmod 5$

$= 11^3 \bmod 5 = 1$

$\boxed{M_1^{-1} = 1}$

$M_2 = 5$

$5^{-1} \bmod 11$

11 is prime no.

$\therefore$ Using Fermat's theorem,

$5^{-1} \bmod 11 = 5^{11-2} \bmod 11$

$= 5^9 \bmod 11 = 9$

$\boxed{M_2^{-1} = 9}$

$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1}) \bmod M$
$= (4 \times 11 \times 1 + 10 \times 5 \times 9) \bmod 55$
$= (44 + 450) \bmod 55$
$\boxed{x = 54}$

c) $x \equiv 7 \bmod 13$, and $x \equiv 11 \bmod 12$

↳ Given:- $x \equiv 7 \bmod 13$
$x \equiv 11 \bmod 12$

From given eqn
$a_1 = 7$, $m_1 = 13$
$a_2 = 11$, $m_2 = 12$

$M = m_1 \times m_2 = 13 \times 12 = 156$

$M_1 = M/m_1 = 156/13 = 12$
$M_2 = M/m_2 = 156/12 = 13$

$M_1 = 12$

Calculating multiplicative inverses.

$M_1^{-1} = 12^{-1} \bmod 13$

13 is prime

∴ Using Fermat's little theorem
$a^{-1} \bmod p = a^{p-2} \bmod p$
$12^{-1} \bmod 13 = 12^{13-2} \bmod 13$
$= 12^{11} \bmod 13$
$= 12$

$\boxed{M_1^{-1} = 12}$

$M_2^{-1} = 13^{-1} \bmod 12$

13 & 12 are coprime

Using Euler's theorem
$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$
$13^{-1} \bmod 12 = 13^{\phi(12)-1} \bmod 12$
$\phi(12) = \phi(3 \times 2^2)$
$= \phi(3) \times \phi(2^2)$
$= (3-1)(2^2-2) = 2 \times 2 = 4$
$13^{-1} \bmod 12 = 13^{4-1} \bmod 12$
$= 13^3 \bmod 12$
$= 1$

$\boxed{M_2^{-1} = 1}$

$\therefore x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1}) \bmod M$
$= (7 \times 12 \times 12 + 11 \times 13 \times 1) \bmod 156$
$= (1008 + 143) \bmod 156$
$\boxed{x = 59}$

(Q2) ~~Find~~

Q6) Find the results of the following using the square & multiply method

a) $21^{24} \bmod 8$

↳ $21^{24} \bmod 8$

$24 \Rightarrow (11000)_2$

x_i	Multiplication (Initialization $y=1$)	Squaring (Initializing $a=21$)
0	→	$a = 21^2 \bmod 8 = 1$
0	→	$a = 1^2 \bmod 8 = 1$
0	→	$a = 1^2 \bmod 8 = 1$
1	$y = 1 \times 1 \bmod 8 = 1$	$a = 1^2 \bmod 8 = 1$
1	$y = 1 \times 1 \bmod 8 = 1$	

$\therefore \boxed{21^{24} \bmod 8 = 1}$

b) $320^{23} \bmod 461$

↳ $23 \Rightarrow 10111$

x_i	Multiplication (Initialization $y=1$)	Squaring (Initializing $a=320$)
1	$y = 1 \times 320 \bmod 461 = 320$	$a = 320^2 \bmod 461 = 58$
1	$y = 58 \times 320 \bmod 461 = 120$	$a = 58^2 \bmod 461 = 137$
1	$y = 120 \times 137 \bmod 461 = 305$	$a = 137^2 \bmod 461 = 324$
0	→	$a = 324^2 \bmod 461 = 367$
1	$y = 367 \times 305 \bmod 461 = 373$	

$\boxed{320^{23} \bmod 461 = 373}$

c) $1736^{41} \bmod 2134$

↳ $41 \Rightarrow 101001$

x_i	Multiplication (Initialization $y=1$)	Squaring (Initialization $a=1736$)
1	$y = 1 \times 1736 \bmod 2134 = 1736$	$a = 1736^2 \bmod 2134 = 488$
0	→	$a = 488^2 \bmod 2134 = 1270$
0	→	$a = 1270^2 \bmod 2134 = 1730$
1	$y = 1736 \times 1730 \bmod 2134 = 742$	$a = 1730^2 \bmod 2134 = 1032$
0	→	$a = 1032^2 \bmod 2134 = 158$
1	$y = 742 \times 158 \bmod 2134 = 2000$	

$\therefore \boxed{1736^{41} \bmod 2134 = 2000}$

d) $2001^{35} \bmod 2000$

↳ $35 \Rightarrow 100011$

x_i	Multiplication (Initialization $y=1$)	Squaring (Initialization $a=2001$)
1	$y = 2001 \times 1 \bmod 2000 = 1$	$a = 2001^2 \bmod 2000 = 1$
1	$y = 1 \times 1 \bmod 2000 = 1$	$a = 1^2 \bmod 2000 = 1$
0		$a = 1^2 \bmod 2000 = 1$
0		$a = 1^2 \bmod 2000 = 1$
0		$a = 1^2 \bmod 2000 = 1$
1	$y = 1 \times 1 \bmod 2000 = 1$	

$\boxed{2001^{35} \bmod 2000 = 1}$

Q7) In RSA:

a) Given $n = 221$ and $e = 5$ find d

↳ $n = 221$

We need to.

Factors of 221 are ⇒ 13 & 17

$\therefore n = p \times q$ where p & q are prime

$\therefore p = 13$, $q = 17$

d is the inverse modulo of e modulo $\phi(n)$

$\therefore d = e^{-1} \bmod \phi(n)$

$d = 5^{-1} \bmod \phi(221)$ — ①

$\therefore \phi(221) = \phi(17 \times 13)$

$= \phi(17) \times \phi(13)$

$= (17-1)(13-1) = 16 \times 12 = 192$

$\therefore$ eq^n ① becomes,

$d = 5^{-1} \bmod 192$

Using Euler's theorem

$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$

$\therefore 5^{-1} \bmod 192 = 5^{\phi(192)-1} \bmod 192$ — ②

$\phi(192) = \phi(2^6 \cdot 3)$

$= \phi(2^6) \cdot \phi(3)$

$= \phi(2^6 - 2^5) \times (3-1)$

$= 32 \times 2 = 64$

$\therefore$ eq^n ② becomes,

$5^{-1} \bmod 192 = 5^{64-1} \bmod 192$

$= 5^{63} \bmod 192$

$5^{63} \bmod 192 = (5^{32} \cdot 5^{16} \cdot 5^8 \cdot 5^4 \cdot 5^2 \cdot 5) \bmod 192$

$= ((5^{32} \bmod 192)(5^{16} \bmod 192)(5^8 \bmod 192)$

$(5^4 \bmod 192)(5^2 \bmod 192)(5 \bmod 192)) \bmod 192$ — ③

$\therefore$ Calculating values.

$5 \bmod 192 = 5$

$5^2 \bmod 192 = 25$

$5^4 \bmod 192 = 49$

$5^8 \bmod 192 = (49 \times 49) \bmod 192 = 97$

$5^{16} \bmod 192 = (97 \times 97) \bmod 192 = 1$

$5^{32} \bmod 192 = (1 \times 1) \bmod 192 = 1$

$\therefore 5^{63} \bmod 192 = (1 \times 1 \times 97 \times 49 \times 25 \times 5) \bmod 192$

$5^{63} \bmod 192 = 77$

i.e $5^{-1} \bmod 192 = 77$

$\therefore \boxed{d = 77}$

b) $n = 3937$ and $e = 17$, find d

$n = 3937$

$3937 = 31 \times 127$

$\therefore p = 31, \quad q = 127$

d is the inverse of e modulo $\phi(n)$

$d = e^{-1} \bmod \phi(n)$

$d = 17^{-1} \bmod \phi(3937) \quad - (1)$

$\phi(3937) = \phi(127 \times 31)$

$= \phi(127) \times \phi(31)$

$= (127-1)(31-1)$

$= 126 \times 30 = 3780$

$\therefore$ eqn (1) becomes,

$d = 17^{-1} \bmod 3780$

Using Euler's theorem

$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$

$\therefore 17^{-1} \bmod 3780 = 17^{\phi(3780)-1} \bmod n \quad - (2)$

$\phi(3780) = \phi(2^2 \cdot 5 \cdot 3^3 \cdot 7)$

$= \phi(2^2) \cdot \phi(5) \phi(3^3) \cdot \phi(7)$

$= (2^2-2)(5-1)(3^3-3^2) \cdot (7-1)$

$= 2 \times 4 \times 18 \times 6 = 864$

$\therefore$ eqn (2) becomes,

$\phi \; 17^{-1} \bmod 3780 = 17^{864-1} \bmod 3780$

$= 17^{863} \bmod 3780$

$17^{863} \bmod 3780 = (17^{512} \cdot 17^{256} \cdot 17^{64} \cdot 17^{16} \cdot 17^{8} \cdot 17^{4} \cdot 17^{2} \cdot 17^{1}) \bmod 3780$

~~$17^{512} \bmod$~~

Calculating values,

$17 \bmod 3780 = 17$

$17^2 \bmod 3780 = 289$

$17^4 \bmod 3780 = 361$

$17^8 \bmod 3780 = 1801$

$17^{16} \bmod 3780 = (1801 \times 1801) \bmod 3780 = 361$

$17^{32} \bmod 3780 = (361 \times 361) \bmod 3780 = 1801$

$17^{64} \bmod 3780 = (1801 \times 1801) \bmod 3780 = 361$

$17^{128} \bmod 3780 = (361 \times 361) \bmod 3780 = 1801$

$17^{256} \bmod 3780 = (1801 \times 1801) \bmod 3780 = 361$

$17^{512} \bmod 3780 = (361 \times 361) \bmod 3780 = 1801$

$\therefore 17^{863} \bmod 3780 = (1801 \times 361 \times 361 \times 361 \times 1801 \times 361 \times 289 \times 17) \bmod 3780$

$17^{863} \bmod 3780 = 3113$

$\therefore \boxed{d = 3113}$

c) Given $p = 19$, $q = 23$, and $e = 3$ find $\phi(n)$ & d.

↳ $p = 19$, $q = 23$

$n = p \times q$

$n = 19 \times 23 = 437$

$\boxed{n = 437}$

$\phi(n) = \phi(437) = \phi(19) \times \phi(23)$

$= (19-1)(23-1)$

$= 18 \times 22 = 396$

$\boxed{\phi(n) = 396}$

For finding d,

$d = e^{-1} \bmod \phi(n)$

$d = 3^{-1} \bmod \phi(437)$

$d = 3^{-1} \bmod 396$ — ①

Using Euler's theorem,

$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$

$\therefore 3^{-1} \bmod 396 = a^{\phi(396)-1} \bmod 396$

— ②

$\therefore \phi(396) = \phi(11 \cdot 2^2 \cdot 3^2)$

$= \phi(11) \times \phi(2^2) \times \phi(3^2)$

$= (11-1) \times (2^2 - 2^1) \times (3^2 - 3)$

$= 10 \times 2 \times 6$

$= 120$

$\therefore$ eqn ② becomes,

$3^{-1} \bmod 396 = 3^{120-1} \bmod 396$

$= 3^{119} \bmod 396$

$3^{119} \bmod 396 = (3^{64} \cdot 3^{32} \cdot 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3) \bmod 396$

$= ((3^{64} \bmod 396)(3^{32} \bmod 396)(3^{16} \bmod 396)(3^4 \bmod 396)(3^2 \bmod 396)(3 \bmod 396)) \bmod 396$

Calculating values

$3 \bmod 396 = 3$

$3^2 \bmod 396 = 9$

$3^4 \bmod 396 = 81$

$3^8 \bmod 396 = 225$

$3^{16} \bmod 396 = 333$

$3^{32} \bmod 396 = 9$

$3^{64} \bmod 396 = 81$

$\therefore 3^{119} \bmod 396 = (81 \times 9 \times 333 \times 81 \times 9 \times 3) \bmod 396$

$= 279$

$\boxed{d = 279}$

Q8) To understand the security of the RSA algorithm, find d if you know that e = 17 & n = 187

↳ n = 187

187 = 17 × 11

∴ p = 17, q = 11

$\phi(n) = \phi(187) = \phi(17 \times 11)$

$= \phi(17) \times \phi(11)$

$= 16 \times 10 = 160$

$d = e^{-1} \bmod \phi(n)$

$d = 17^{-1} \bmod \phi(187)$

$d = 17^{-1} \bmod 160$

Using Euler's theorem,

$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$

$17^{-1} \bmod 160 = 17^{\phi(160)-1} \bmod 160$

$\phi(160) = \phi(2^5 \cdot 5)$

$= \phi(2^5) \times \phi(5)$

$= \phi(2^5 - 2^4) \cdot (5-1)$

$= 16 \times 4 = 64$

$17^{-1} \bmod 160 = 17^{64-1} \bmod 160$

$17^{63} \bmod 160$

$17^{63} \bmod 160 = (17^{32} \cdot 17^{16} \cdot 17^{8} \cdot 17^{4} \cdot 17^{2} \cdot 17) \bmod 160$

$= ((17^{32} \bmod 160)(17^{16} \bmod 160)$

$(17^{8} \bmod 160)(17^{4} \bmod 160)(17^{2} \bmod 160)$

$(17 \bmod 160)) \bmod 160$

$17 \bmod 160 = 17$

$17^2 \bmod 160 = 129$

$17^4 \bmod 160 = 1$

$17^8 \bmod 160 = 1$

$17^{16} \bmod 160 = 1$

$17^{32} \bmod 160 = 1$

$17^{63} \bmod 160 = (1 \times 1 \times 1 \times 1 \times 129 \times 17) \bmod 160$

$17^{63} \bmod 160 = 113$