Question 1

Problem a

Proof.

$$n \equiv n' \mod rs$$
$$\Rightarrow rs | n - n'$$
$$\Rightarrow r | n - n' \land s | n - n'$$
$$n \equiv n' \mod r \land n \equiv n' \mod s$$
$$\Rightarrow (n \mod r, n \mod s) = (n' \mod r, n' \mod s)$$
$$\Rightarrow \phi \text{ is well defined}$$

$\square$

Problem b

Proof.

Addition :

$\phi(m+n) = (m+n \mod r, m+n \mod s)$

$\phi(m) + \phi(n)$

$= (m \mod r, m \mod s) + (n \mod r, n \mod s)$

$= ((m \mod r + n \mod r) \mod r, (m \mod s + n \mod s) \mod s)$

$= (m+n \mod r, m+n \mod s)$

$= \phi(m+n)$

$\Rightarrow \phi(m) + \phi(n) = \phi(m+n)$

Multiplication :

$\phi(mn) = (mn \mod r, mn \mod s)$

$\phi(m)\phi(n)$

$= (m \mod r, m \mod s)(n \mod r, n \mod s)$

$= (((m \mod r)(n \mod r)) \mod r, ((m \mod s)(n \mod s)) \mod s)$

$= (mn \mod r, mn \mod s)$

$= \phi(mn)$

$\Rightarrow \phi(m)\phi(n) = \phi(mn)$

$\Rightarrow \phi$ is a homomorphism

$\square$

Problem c

Proof.

Injective :

$\exists m, n \in \mathbb{Z}_{rs} : \phi(m) = \phi(n)$

$(m \mod r, m \mod s) = (n \mod r, n \mod s)$

$\Rightarrow m \equiv n \mod r \wedge m \equiv n \mod s$

r, s are relatively prime

$\Rightarrow m \equiv n \mod rs$

$\Rightarrow m = n$

Surjective :

$\exists p \in \mathbb{Z}_{rs} : \phi(p) = (a, b)$

$p \equiv a \mod r, p \equiv b \mod s$

$\Rightarrow \exists m, n \in \mathbb{Z} : p = mr + a = ns + b$

$a - b = mr - ns$

r, s are relatively prime

$\Rightarrow \langle r, s \rangle = \mathbb{Z}$

$\Rightarrow a, b$ can be arbitrary

$\Rightarrow \forall (a, b) \in \mathbb{Z}_r \times \mathbb{Z}_s, \exists p \in \mathbb{Z}_{rs} : \phi(p) = (a, b)$

Homomorphism :

Problem b

$\Rightarrow \phi$ is an isomorphism

$\square$

Question 2

Problem a

Proof.

$$\exists n : (n-1)! \equiv -1 \mod n$$

Suppose n is not prime

$$\exists 1 < a < n : a | n$$

$$n := ak, k \in \mathbb{Z}$$

$$1 < a < n$$

$$\Rightarrow \exists a \text{ as a term in } (n-1)!$$

$$\Rightarrow a | (n-1)!$$

$$(n-1)! \equiv 0 \mod a$$

$$(n-1)! \equiv -1 \mod n$$

$$\Rightarrow (n-1)! = mn - 1, m \in \mathbb{Z}$$

$$n = ak$$

$$\Rightarrow (n-1)! = akm - 1$$

$$(n-1)! = a(km) - 1$$

$$\Rightarrow (n-1)! \equiv -1 \mod a \nLeftrightarrow (n-1)! \equiv 0 \mod a$$

$$\Rightarrow n \text{ is a prime}$$

□

Problem b

Proof.

$\forall a \in \mathbb{Z}_p$ are their own multiplicative inverses :

$a^2 \equiv 1 \mod p$

$a^2 - 1 \equiv 0 \mod p$

$(a-1)(a+1) \equiv 0 \mod p$

$(a-1)(a+1) = kp$

p is prime

$\Rightarrow a - 1 \equiv p \mod p \vee a + 1 \equiv p \mod p$

$\Rightarrow a = 1 \vee a = -1$

$\square$

Problem c

Proof.

p is prime

$\forall 1 < a < p - 1, \exists! 1 < b < p - 1 : ab \equiv 1 \mod p$

$\forall 1 < a < p - 1, \nexists a : a^2 \equiv 1 \mod p$

$\Rightarrow \forall 1 < a < p - 1 \wedge 1 < b < p - 1, ab \equiv 1 \mod p : a \neq b$

$\Rightarrow$ All elements of $(p-2)!/1$ can be paired to be congruent to $1 \mod p$

$\Rightarrow (p-2)!/1 \equiv 1 \mod p$

$(p-2)! \equiv 1 \mod p$

$(p-1)! \equiv 1(p-1) = p - 1 \equiv -1 \mod p$

$\square$

Problem d

31 is prime

$\Rightarrow (31-1)! \equiv -1 \mod 31$

$30! \equiv -1 \mod 30$

$28! \times 29 \times 30 \equiv -1 \mod 30$

$28! \equiv -1 \times 29^{-1} \times 30^{-1} \mod 30$

$29 \times 27 \equiv 1 \mod 31$

$30 \times 30 \equiv 1 \mod 31$

$\Rightarrow 28! \equiv -1 \times 27 \times 30 \mod 31$

$28! \equiv 27 \mod 31$

Question 3

Problem a

$$a^{p-1} \equiv 1 \mod p, \gcd(a, p) = 1$$
$$p = 17, a = 3$$
$$\Rightarrow 3^{16} \equiv 1 \mod 17$$
$$3^{2015} = 3^{16^{125}} \times 3^1 5 = 3^{16^{126}} \times 3^{-1}$$
$$3 \times 6 \equiv 1 \mod 17$$
$$\Rightarrow 3^{-1} \mod 17 = 6$$
$$3^{2015} = 3^{16^{126}} \times 3^{-1} \equiv 1 \times 6 \equiv 6 \mod 17$$

Problem b

$$a^{\varphi(n)} \equiv 1 \mod n, \gcd(a, n) = 1$$
$$a = 3, n = 16, \varphi(16) = 8$$
$$\Rightarrow 3^8 \equiv 1 \mod 16$$
$$3^{2015} = 3^{8^{251}} \times 3^7 = 3^{8^{252}} \times 3^{-1}$$
$$3 \times 11 \equiv 1 \mod 16$$
$$\Rightarrow 3^{-1} \mod 16 = 11$$
$$3^{2015} = 3^{8^{252}} \times 3^{-1} \equiv 1 \times 11 \equiv 11 \mod 16$$

Question 4

Problem a

Proof.

$\forall n \in \mathbb{Z}:$

n^{31} and n have the same parity

$\Rightarrow n^{31} \equiv n \mod 2$

$n^3 \equiv n \mod 3$

$n^{31} = n^{3^{10}} \times n$

$n^{31} = n^{3^{10}} \times n \equiv n^{10} \times n = n^{11} \mod 3$

$n^{11} = n^{3^3} \times n^2$

$n^{11} = n^{3^3} \times n^2 \equiv n^3 \times n^2 \equiv n \times n^2 = n^3 \equiv n \mod 3$

$\Rightarrow n^{31} \equiv n \mod 3$

$n^{11} \equiv n \mod 11$

$n^{31} = n^{11^2} \times n^9$

$n^{31} = n^{11^2} \times n^9 \equiv n^2 \times n^9 = n^1 1 \equiv n \mod 11$

$\Rightarrow n^{31} \equiv n \mod 11$

$n^{31} \equiv n \mod 31$

$\Rightarrow n^{31} \equiv n \mod 2 \wedge n^{31} \equiv n \mod 3 \wedge n^{31} \equiv n \mod 11 \wedge n^{31} \equiv n \mod 31$

$2 \times 3 \times 11 \times 31 = 2046$

$\Rightarrow \forall n \in \mathbb{Z}, n^{31} \equiv n \mod 2046$

$\square$

Problem b

$n^7 \equiv n \mod 7$

$n^{31} = (n^7)^4 \times n^3$

$n^{31} = (n^7)^4 \times n^3 \equiv n^4 \times n^3 = n^7 \equiv n \mod 7$

From part a :

$n^{31} \equiv n \mod 2 \wedge n^{31} \equiv n \mod 3 \wedge n^{31} \equiv n \mod 11 \wedge n^{31} \equiv n \mod 31$

$\Rightarrow n^{31} \equiv n \mod 2 \times 3 \times 7 \times 11 \times 31$

$n^{31} \equiv n \mod 14322$

$14322 > 2046$

Question 5

Problem 1

$$n = pq$$
$$\Rightarrow n = 15$$
$$\phi(n) = (3-1)(5-1) = 8$$
$$\Rightarrow s = 3, 5, 7$$
$$s = 3:$$
$$rs \equiv 1 \mod 8$$
$$3r \equiv 1 \mod 8$$
$$r \equiv 3 \mod 8$$
$$\Rightarrow (r, s) = (3, 3)$$
$$s = 5:$$
$$rs \equiv 1 \mod 8$$
$$5r \equiv 1 \mod 8$$
$$r \equiv 5 \mod 8$$
$$\Rightarrow (r, s) = (5, 5)$$
$$s = 7:$$
$$rs \equiv 1 \mod 8$$
$$7r \equiv 1 \mod 8$$
$$r \equiv 7 \mod 8$$
$$\Rightarrow (r, s) = (7, 7)$$
$$n = 15, \{(r, s)\} = \{(3, 3), (5, 5), (7, 7)\}$$

Problem 4

$$n = pq$$
$$\Rightarrow n = 35$$
$$\phi(n) = (5-1)(7-1) = 24$$
$$\Rightarrow s = 5, 7, 11, 13, 17, 19, 23$$
$$s = 5:$$
$$rs \equiv 1 \quad \mathrm{mod}\ 24$$
$$5s \equiv 1 \quad \mathrm{mod}\ 24$$
$$s \equiv 5 \quad \mathrm{mod}\ 24$$
$$\Rightarrow (r, s) = (5, 5)$$
$$s = 7:$$
$$rs \equiv 1 \quad \mathrm{mod}\ 24$$
$$7s \equiv 1 \quad \mathrm{mod}\ 24$$
$$s \equiv 7 \quad \mathrm{mod}\ 24$$
$$\Rightarrow (r, s) = (7, 7)$$
$$s = 11:$$
$$rs \equiv 1 \quad \mathrm{mod}\ 24$$
$$11s \equiv 1 \quad \mathrm{mod}\ 24$$
$$s \equiv 11 \quad \mathrm{mod}\ 24$$
$$\Rightarrow (r, s) = (11, 11)$$
$$s = 13:$$
$$rs \equiv 1 \quad \mathrm{mod}\ 24$$
$$13s \equiv 1 \quad \mathrm{mod}\ 24$$
$$s \equiv 13 \quad \mathrm{mod}\ 24$$
$$\Rightarrow (r, s) = (13, 13)$$
$$s = 17:$$
$$rs \equiv 1 \quad \mathrm{mod}\ 24$$
$$17s \equiv 1 \quad \mathrm{mod}\ 24$$
$$s \equiv 17 \quad \mathrm{mod}\ 24$$
$$\Rightarrow (r, s) = (17, 17)$$
$$s = 19:$$
$$rs \equiv 1 \quad \mathrm{mod}\ 24$$
$$19s \equiv 1 \quad \mathrm{mod}\ 24$$
$$s \equiv 19 \quad \mathrm{mod}\ 24$$
$$\Rightarrow (r, s) = (19, 19)$$
$$s = 23:$$
$$rs \equiv 1 \quad \mathrm{mod}\ 24$$
$$23s \equiv 1 \quad \mathrm{mod}\ 24$$
$$s \equiv 23 \quad \mathrm{mod}\ 24$$

$$\Rightarrow (r, s) = (23, 23)$$
$$n = 35, \{(r, s)\} = \{(5, 5), (7, 7), (11, 11), (13, 13), (17, 17), (19, 19), (23, 23)\}$$

Problem 8

a

$$y \equiv m^s \mod 1457$$
$$y \equiv 999^{239} \mod 1457$$
$$\Rightarrow y = 784$$

b

$$\phi(1457) = (31 - 1) \times (47 - 1) = 1380$$
$$sr \equiv 1 \mod 1380$$
$$239r \equiv 1 \mod 1380$$
$$r = 179$$

c

$$784^{179} \equiv m \mod 1457$$
$$m = 999$$

Problem 9

$$p = 257$$
$$q = 359$$
$$n = pq = 92263$$
$$\phi(n) = (257 - 1)(359 - 1) = 91648$$
$$sr \equiv 1 \mod 91648$$
$$1493s \equiv 1 \mod 91648$$
$$\Rightarrow s = 9085$$
$$\Rightarrow \text{Public key} : (n = 92263, r = 1493)$$
$$\text{Private key} : (n = 92263, s = 9085)$$

Reference

Jeffery Shu

Wolfram Mathematica