Exercise 1

(1) $x^5 \equiv 2 \mod 35$: Since $\gcd(5,24)=1$,

$\Rightarrow x \equiv 2^d \mod 35$ where $5d \equiv 1 \mod \varphi(35) \equiv 1 \mod 24$

24 5 4 1

4; 1 4 $\Rightarrow 5 \cdot 5 \equiv 1 \mod 25 \Rightarrow d = 5$

Therefore, $x \equiv 2^5 \mod 35 \equiv \boxed{32} \mod 35$

(2) $\gcd(11,24)=1 \Rightarrow \varphi(35)=24 \Rightarrow$ 24 11 2 1

2; 5 2 11/5

1/5

$\Rightarrow d = 11 \Rightarrow x \equiv 13^{11} \mod 35 \equiv \boxed{27} \mod 35$

~~(3) gcd(7, 48) = 1 ⇒ φ(63) = 48 ⇒ 48~~ ~~7×7 ≡ 1 mod 48~~

~~⇒ d = 7 ⇒ x ≡ 11^7 mod 63 ≡ 11 mod 63~~

(3) $\gcd(7,36)=1 \Rightarrow$ 36 7 1

5; 7 $7 \times 5 \equiv -1 \mod 36$

$\Rightarrow 7 \times 31 \equiv 1 \mod 36$

$\Rightarrow d = 31 \Rightarrow x \equiv 11^{31} \mod 63 \equiv \boxed{11} \mod 63$

(4) $\gcd(5,32)=1 \Rightarrow 5 \times 13 \equiv 1 \mod 32 \Rightarrow d = 13$

$\Rightarrow x \equiv 3^{13} \equiv \boxed{19} \mod 64$

EXERCISE 2

(1)

g	1	2	3	4	5	6	7	8	9	10	11	12
ord(g)	1	12	3	6	4	12	12	4	3	6	12	2

$\boxed{2, 6, 7, 11}$

(2)

e	1	2	3	4	5	6	7	8	9	10
2^e	2	4	8	5	10	9	7	3	6	1

(a) $\left.\begin{array}{l} 7 \equiv 2^7 \\ 6 \equiv 2^9 \end{array}\right\} \text{mod } 11 \Rightarrow 2^7 x \equiv 2^9 \text{ mod } 11 \Rightarrow x \equiv 2^2 \equiv \boxed{4} \text{ mod } 11$

(b) $\left.\begin{array}{l} 5 \equiv 2^4 \\ 3 \equiv 2^8 \end{array}\right\} \text{mod } 11 \Rightarrow 2^4 x \equiv 2^8 \text{ mod } 11 \Rightarrow x \equiv 2^4 \equiv \boxed{5} \text{ mod } 11$

(c) $\left.\begin{array}{l} 4 \equiv 2^2 \\ 9 \equiv 2^6 \end{array}\right\} \text{Mod } 11 \Rightarrow 2^2 x^2 \equiv 2^6 \text{ Mod } 11 \Rightarrow x^2 \equiv 2^4 \Rightarrow x \equiv 2^2 \equiv \boxed{4} \text{ mod } 11$

(3)

e	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^e	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

$x^5 \equiv 7 \text{ mod } 19 \equiv 2^6 \text{ mod } 19$. Since $2^{18} \equiv 1 \text{ mod } 19$,

$\Rightarrow x^5 \equiv 2^6 (2^{18})^3 \equiv 2^{60} \text{ mod } 19$

Therefore, $x \equiv \boxed{2^{12}} \text{ mod } 19$ because $(2^{12})^5 = 2^{60}$

$\Rightarrow x \equiv \boxed{11} \text{ mod } 19$