Solution 11

4.1

22.

$$\because a \equiv b \pmod m$$
$$\therefore a - b = km$$
$$\therefore a = km + b$$
$$\because \exists c, t,\ b = tm + c,\ c < m$$
$$\therefore a = km + tm + c = (k+t)m + c$$
$$\therefore a \mod m = c = b \mod m$$

26. a) $-17 = 2 \cdot (-9) + 1$, $-17 \mod 2 = 1$

b) $144 = 7 \cdot 20 + 4$, $144 \mod 7 = 4$

c) $-101 = 13 \cdot (-8) + 3$, $-101 \mod 13 = 3$

d) $199 = 19 \cdot 10 + 9$, $199 \mod 19 = 9$

38. a) $(19^2 \mod 41) \mod 9 = (361 \mod 41) \mod 9 = 33 \mod 9 = 6$

b) $(32^3 \mod 13)^2 \mod 11 = (32768 \mod 13)^2 \mod 11 = 64 \mod 11 = 9$

c) $(7^3) \mod 23^2 \mod 31 = (343 \mod 23)^2 \mod 31 = 441 \mod 31 = 7$

d) $(21^2 \mod 15)^3 \mod 22 = (441 \mod 15)^3 \mod 22 = 216 \mod 22 = 18$

40.

$$\because a \equiv b \pmod m,\ c \equiv d \pmod m$$
$$\therefore b = a + km,\ d = c + tm$$
$$\therefore b - d = (a - c) + (k - t)m$$
$$\therefore a - c \equiv b - d \pmod m$$

4.2

26.

$644 = (10\,1000\,0100)_2$

$i = 0 : a_0 = 0,\ x = 1,\ power = 11^2 \mod 645 = 121$

$i = 1 : a_1 = 0,\ x = 1,\ power = 121^2 \mod 645 = 451$

$i = 2 : a_2 = 1,\ x = 451 \mod 645 = 451,\ power = 451^2 \mod 645 = 226$

$i = 3 : a_3 = 0,\ x = 451,\ power = 226^2 \mod 645 = 121$

$i = 4 : a_4 = 0,\ x = 451,\ power = 121^2 \mod 645 = 451$

$i = 5 : a_5 = 0,\ x = 451,\ power = 451^2 \mod 645 = 226$

$i = 6 : a_6 = 0,\ x = 451,\ power = 226^2 \mod 645 = 121$

$i = 7 : a_7 = 1,\ x = 451 \cdot 121 \mod 645 = 391,\ power = 121^2 \mod 645 = 451$

$i = 8 : a_8 = 0,\ x = 391,\ power = 451^2 \mod 645 = 226$

$i = 9 : a_9 = 1,\ x = 391 \cdot 226 \mod 645 = 1$

$11^{644} \mod 645 = 1$

4.3

22. If n is prime, then all inegers from 1 to $n - 1$ are relatively prime to n. So $\phi(n) = n - 1$

    if $n > 1$ and n is not prime, then $n = ab,\ 1 < an,\ 1 < b < n$, then a and b are not relatively prime to n. So $\phi(n) \neq n - 1$

    If $n = 1$, then $\phi(1) = 1 \neq 0 = 1 - 1$

32. a) $\gcd(1, 5) = \gcd(1, 0) = 1$

    b) $\gcd(100, 101) = \gcd(100, 1) = \gcd(0, 1) = 1$

    c) $\gcd(123, 277) = \gcd(133, 31) = \gcd(31, 30) = \gcd(1, 30) = \gcd(1, 0) = 1$

    d) $\gcd(1529, 14039) = \gcd(1529, 278) = \gcd(139, 278) = \gcd(139, 0) = 139$

    e) $\gcd(1529, 14038) = \gcd(1529, 277) = \gcd(144, 277) = \gcd(144, 133) = \gcd(11, 133) = \gcd(11, 1) = \gcd(0, 1) = 1$

    f) $\gcd(11111, 111111) = \gcd(11111, 1) = \gcd(0, 1) = 1$