CHAPTER 2

Solutions to Chapter 2 exercises

Exercise 2.

(a) true **(b)** false **(c)** false
(d) true **(e)** false (a may be 0)
(f) true

Exercise 4. If $a \mid b$ then $b = an$ for some $n \in \mathbb{Z}$, hence $bc = anc$ so $a \mid bc$.

Exercise 6.

(a) prime **(b)** prime **(c)** composite
(d) prime **(e)** composite **(f)** composite

Exercise 8.

(a) $2 \cdot 13$ **(b)** $2^5 \cdot 3$ **(c)** 2^9
(d) $2^8 \cdot 5^2$ **(e)** $3^2 \cdot 7^2 \cdot 13^2$ **(f)** $13^3 \cdot 17^4$

Exercise 10. In the following q is the quotient and r is the remainder.

(a) $q = 22$, $r = 1$ **(b)** $r = 36$, $r = 0$
(c) $q = -7$, $r = 1$ **(d)** $q = -41$, $r = 10$
(e) $q = 30$, $r = 8$ **(f)** $q = -356$, $r = 12$

Exercise 12.

(a) 5 **(b)** 120 **(c)** 2
(d) 7 **(e)** 1050 **(f)** 45

Exercise 14. See the answers for problem 12.

Exercise 16. **(a)** $5 = (3)(15) + (-1)(40)$
(b) $2 = (-12)(136) + (19)(86)$
(c) $7 = (-101)(1925) + (124)(1568)$
(d) $45 = (908)(256500) + (-2129)(109395)$

Exercise 18.

(a) false **(b)** false **(c)** true
(d) false **(e)** true **(f)** true

Exercise 20.

(a) 33 **(b)** 42 **(c)** 47 **(d)** 3 **(e)** 15

Exercise 22. **(a)** Addition and multiplication in $\mathbb{Z}_3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Every element in $\mathbb{Z}_3$ has an additive inverse. Nonzero elements 1 and 2 have multiplicative inverses.

(b) Addition and multiplication in $\mathbb{Z}_9$

$+$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	0
2	3	4	5	6	7	8	9	0	1
3	4	5	6	7	8	9	0	1	2
4	5	6	7	8	9	0	1	2	3
5	6	7	8	9	0	1	2	3	4
6	7	8	9	0	1	2	3	4	5
7	8	9	0	1	2	3	4	5	6
8	9	0	1	2	3	4	5	6	7

$\times$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Every element has an additive inverse. Numbers that are not divisible by 3, that is 1,2,4,5,7,8, have multiplicative inverses.

Exercise 24. Multiplicative inverses in $\mathbb{Z}_{10}$

x	1	3	7	9
x^{-1}	1	7	3	9

Exercise 26. Multiplicative inverses in $\mathbb{Z}_{11}$

x	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10

Exercise 28. **(a)**

$$(7)(3x) \equiv (7)(5) \mod 10$$
$$x \equiv 5 \mod 10$$

(b)

$$(3)(7x+2) \equiv (3)(3) \mod 10$$
$$x+6 \equiv 9 \mod 10$$
$$x \equiv 3 \mod 10$$

(c)

$$(9)(9x-8) \equiv (9)(7) \mod 10$$
$$x-2 \equiv 3 \mod 10$$
$$x \equiv 5 \mod 10$$

Exercise 30. Multiplicative inverses in $\mathbb{Z}_{299}$.

(a) $2^{-1} \equiv 150$ **(b)** $\gcd(52, 299) = 13$ so 52 is not invertible.

(c) $80^{-1} \equiv 228$ **(d)** $199^{-1} \equiv 296$.

Exercise 32.

(a) $2^{-1} \equiv 1278 \mod 2555$ **(b)** $74^{-1} \equiv 1899 \mod 2555$

(c) not invertible $\gcd(98, 2555) = 7$ **(d)** $1972^{-1} \equiv 1753 \mod 2555$

Exercise 34. **(a)**

$$\begin{aligned}(150)(2x) &\equiv (150)(59) \mod 299\\ x &\equiv 179 \mod 299\end{aligned}$$

(b)

$$\begin{aligned}(296)(199x) &\equiv (296)(99) \mod 299\\ x &\equiv 2 \mod 299\end{aligned}$$

(c)

$$\begin{aligned}(1278)(2x) &\equiv (1278)(847) \mod 2555\\ x &\equiv 1701 \mod 2555\end{aligned}$$

(d)

$$\begin{aligned}(1753)(1972x) &\equiv (1753)(363) \mod 2555\\ x &\equiv 144 \mod 2555\end{aligned}$$

Exercise 36. **(a)**

$$\begin{aligned}2x &\equiv 6 \mod 16\\ \text{divide by 2:}\quad x &\equiv 3 \mod 8\end{aligned}$$

(b)

$$\begin{aligned}6x &\equiv 16 \mod 27\\ \text{iff}\quad 6x &= 16 + 27n \quad \text{for some integer } n\\ \text{iff}\quad 6x - 27n &= 16\end{aligned}$$

$3 \mid (6x - 27n)$ but $3 \nmid 16$ so no solution exists.

(c)

$$\begin{aligned}14x &\equiv 21 \mod 88\\ \text{iff}\quad 14x &= 21 + 88n \quad \text{for some integer } n\\ \text{iff}\quad 14x - 88n &= 21\end{aligned}$$

$2 \mid (14 - 88n)$ but $2 \nmid 21$ so no solution exists.

(d)

$$\begin{aligned}25x &\equiv 55 \mod 95\\ \text{divide by 5:}\quad 5x &\equiv 11 \mod 19\\ (4)(5x) &\equiv (4)(11) \mod 19\\ x &\equiv 6 \mod 19\end{aligned}$$

Exercise 38. **(a)**

$$\begin{aligned} & 8x \equiv 16 \mod 1196 \\ \text{divide by 4:} \quad & 2x \equiv 4 \mod 299 \\ & (150)(2x) \equiv (150)(4) \mod 299 \\ & x \equiv 2 \mod 299 \end{aligned}$$

(b)

$$\begin{aligned} & 400x \equiv 125 \mod 1495 \\ \text{divide by 5:} \quad & 80x \equiv 25 \mod 299 \\ & (228)(80x) \equiv (228)(25) \mod 299 \\ & x \equiv 19 \mod 299 \end{aligned}$$

(c)

$$\begin{aligned} & 1393x \equiv 175 \mod 2093 \\ \text{divide by 7:} \quad & 199x \equiv 25 \mod 299 \\ & (296)(199x) \equiv (296)(25) \mod 299 \\ & x \equiv 224 \mod 299 \end{aligned}$$

(d)

$$\begin{aligned} & 17748x \equiv 6642 \mod 22995 \\ \text{divide by 9:} \quad & 1972x \equiv 738 \mod 3285 \\ & (658)(1972x) \equiv (658)(738) \mod 3285 \\ & x \equiv 2709 \mod 3285 \end{aligned}$$

Exercise 40. **(a)** $(4)(4) + (-3)(5) = 1$ so

$$x \equiv (3)(-3)(5) + (4)(4)(4) \equiv 19 \mod 20$$

(b)

$$\begin{aligned} (-22)(2) + (1)(5)(9) &= 1 \\ (-7)(5) + (2)(2)(9) &= 1 \\ (-1)(9) + (1)(2)(5) &= 1 \end{aligned}$$

so

$$\begin{aligned} x &\equiv (0)(1)(5)(9) + (1)(2)(2)(9) + (6)(1)(2)(5) \\ &\equiv 6 \mod 90 \end{aligned}$$

(c)

$$\begin{aligned} (124)(4) + (-1)(5)(9)(11) &= 1 \\ (-79)(5) + (1)(4)(9)(11) &= 1 \\ (49)(9) + (-2)(4)(5)(11) &= 1 \\ (-49)(11) + (3)(4)(5)(9) &= 1 \end{aligned}$$

so

$$\begin{aligned} x \equiv & (1)(-1)(5)(9)(11) + (2)(1)(4)(9)(11) \\ & + (3)(-2)(4)(5)(11) + (1)(3)(4)(5)(9) \\ \equiv & 1497 \mod 1980 \end{aligned}$$

Exercise 42. Suppose the computer has x bytes of memory. If it runs j jobs, allocates b bytes to each job, and has r bytes left over then $x = jb + r$ so

$$x \equiv r \mod j.$$

Therefore

$$\begin{aligned} x &\equiv 86 \mod 95 \\ x &\equiv 13 \mod 98 \\ x &\equiv 46 \mod 99 \\ x &\equiv 0 \mod 101. \end{aligned}$$

Also

$$\begin{aligned} (-340387)(95) + (33)(98 * 99 * 101) &= 1 \\ (106622)(98) + (-11)(95 * 99 * 101) &= 1 \\ (351429)(99) + (-37)(95 * 98 * 101) &= 1 \\ (-127759)(101) + (14)(95 * 98 * 99) &= 1 \end{aligned}$$

so, using the Chinese remainder procedure, it follows that

$$\begin{aligned} x \equiv & (86)(33)(98 * 99 * 101) + (13)(-11)(95 * 99 * 101) \\ & + (46)(-37)(95 * 98 * 101) + (0)(14)(95 * 98 * 99) \\ \equiv & 20720251 \mod 93090690 \end{aligned}$$

$x < 10^9$ so $x = 20720251$ bytes exactly.

Exercise 44. **(a)** 4, 4, 2

(b) Suppose $x_1x_2 \cdots x_{10}$ and $y_1y_2 \cdots y_{10}$ are two ten-digit strings. Consider the sums

$$x_1 + 2x_2 + 3x_3 + 4x_4 + \cdots + 9x_9 - x_{10} \mod 11 \tag{1}$$

$$y_1 + 2y_2 + 3y_3 + 4y_4 + \cdots + 9y_9 - y_{10} \mod 11 \tag{2}$$

If the strings are correct ISBN-10 numbers then both sums will be 0 (mod 11). However suppose the x-string is correct and the y-string equals the x-string except for the kth digit. Subtracting the second sum from the first, we obtain

$$\begin{aligned} & (x_1 + 2x_2 + 3x_3 + 4x_4 + \cdots + 9x_9 - x_{10}) \\ & -(y_1 + 2y_2 + 3y_3 + 4y_4 + \cdots + 9y_9 - y_{10}) \\ & \equiv k(x_k - y_k) \mod 11 \end{aligned}$$

(If $k = 10$ use the fact that $-1 \equiv 10 \mod 11$).

The difference of the two sums cannot be 0 (mod 11) because $1 \leq |x_k - y_k| \leq 10$, $1 \leq k \leq 10$ and the product of such numbers is never 0 mod 11. Therefore $y_{10} \not\equiv y_1 + 2y_2 + 3y_3 + 4y_4 + \cdots + 9y_9 \mod 11$. This discrepancy shows that the y-string cannot be a correct ISBN-10 code.

(c) Using the notation from part (b) assume that the x-string is correct, $1 \le j < k \le 10$, and the y-string is obtained from the x-string by swapping y_j with y_k. Thus for each $i = 1, \ldots, 10$,

$$y_i = \begin{cases} x_i & \text{if } i \neq j \text{ and } i \neq k \\ x_k & \text{if } i = j \\ x_j & \text{if } i = k. \end{cases}$$

Then

$$\begin{aligned} &(x_1 + 2x_2 + 3x_3 + 4x_4 + \cdots + 9x_9 - x_{10}) \\ -&(y_1 + 2y_2 + 3y_3 + 4y_4 + \cdots + 9y_9 - y_{10}) \\ &\equiv j(x_j - x_k) + k(x_k - x_j) \mod 11 \\ &\equiv (j-k)(x_j - x_k) \mod 11. \end{aligned}$$

(If j or k is 10 use $-1 \equiv 10 \mod 11$).

If $x_j = x_k$ then swapping the digits does not change the string. But if $x_j \neq x_k$ then $(j-k)(x_j - x_k) \not\equiv 0 \mod 11$ because $1 \le |j-k|$ and $|x_j - x_k| \le 10$. Thus $y_{10} \not\equiv y_1 + 2y_2 + 3y_3 + 4y_4 + \cdots + 9y_9 \mod 11$ if $x_j \neq x_k$.

(d) For example let $x = 0000000000$, $y = 1000000000$, $z = 1000000001$. x and z are correct ISBN-10 strings that differ from y in only one digit. If someone received the garbled copy y it wouldn't be possible to decide which string, x or z, was the correct one, using only the ISBN-10 system as a guide.

Exercise 46. The tables in parts (a) and (b) show how the teams are paired against each other in each round. In round k, each team in the top line of the table plays against the team in the same column in the row labeled "round k", except when the teams are the same. If the teams are the same the team sits out the round.

(a)

	4	3	2	1
round 1	1	2	3	4
round 2	2	3	4	1
round 3	3	4	1	2
round 4	4	1	2	3

(b)

	6	5	4	3	2	1
round 1	1	2	3	4	5	6
round 2	2	3	4	5	6	1
round 3	3	4	5	6	1	2
round 4	4	5	6	1	2	3
round 5	5	6	1	2	3	4
round 6	6	1	2	3	4	5

(c) Team i plays against team j in round k iff $j \equiv (N-i) + k \mod N$, except when $i \equiv (N-i) + k$. When $i \equiv (N-i) + k$ the team sits out the round. Thus each team plays at most one other team in a given round.

Suppose team i plays against the same team in rounds k and k'. Then $(N-i)+k \equiv (N-i)+k' \mod N$ so, subtracting $N-i$ from both sides, we have $k \equiv k' \mod N$ hence $k = k'$ because $1 \le k, k' \le N$. Therefore each team plays every other team exactly once in the tournament.

Exercise 48. **(a)** Proof. Let $a \mid b$ and $c \mid d$. Then there exist $m, n \in \mathbb{Z}$ such that $am = b$ and $cn = d$. Hence $bd = amcn = (ac)(mn)$ so $ac \mid bd$.

(b) Proof. There exist integers x, y such that $\gcd(b, c) = xb + yc$. If $a \mid b$ and $a \mid c$ then there also exist integers r, s such that $b = ra$ and $c = sa$. Substitute these into the previous equation to obtain $\gcd(b, c) = xra + ysa = (xr + ys)a$. Hence $a \mid \gcd(b, c)$.

(c) Proof. $n^3 - n = n(n^2 - 1) = (n + 1)n(n - 1)$. If n is any integer then either $n - 1$ or n or $n + 1$ is a multiple of 3, hence $(n + 1)n(n - 1)$ is a multiple of 3.

Exercise 50. **(a)** Counterexample. let $a = b = 2$.

(b) Proof. Let a be an odd integer. Then $a = 2n + 1$ for some integer n. Hence $a^2 - 1 = (a - 1)(a + 1) = (2n)(2n + 2) = 4n(n + 1)$ is divisible by 4.

(c) Proof. In part (b) we showed that $a^2 = 4n(n + 1)$ for some integer n. Either n is even or $n + 1$ is even so in every case the product $n(n + 1)$ is even. Hence $n(n + 1) = 2k$ for some integer k. Hence $a^2 - 1 = 4n(n + 1) = (4)(2k) = 8k$ is divisible by 8.

Exercise 52. Proof. Let $a \mid bc$ and $\gcd(a, b) = 1$. Then there exists an integer n such that $bc = an$, and by theorem 2.6 there exist x, y such that $1 = ax + by$. Multiply the last equation by c to obtain $c = c(1) = c(ax + by) = acx + bcy$, then plug in $bc = an$ to obtain $c = acx + (an)y = a(cx + ny)$. Hence $a \mid c$.

Exercise 54. **(a)** Proof. Let n be a positive integer, written in the usual way as a string of base 10 digits $d_{D-1}d_{D-2}\dots d_2d_1d_0$ so $n = \sum_{k=0}^{D} d_k \cdot 10^k$. $10 \equiv 1 \mod 3$ so $10^k \equiv 1^k \equiv 1 \mod 3$ so

$$n \equiv \sum_{k=0}^{D} d_k \cdot 1 = \sum_{k=0}^{D} d_k \mod 3.$$

In particular $0 \equiv n \mod 3$ iff $0 \equiv \sum_{k=0}^{D} d_k \mod 3$.

(b) If $k \geq 2$ then $10^k = 100 \cdot 10^{k-2} = (4)(25)(10^{k-2})$ is divisible by 4 so $10^k \equiv 0 \mod 4$. Hence

$$n = d_0 + d_1 + \sum_{k=}^{D} d_k \cdot 10^k \equiv d_0 + d_1 \mod 4.$$

Exercise 56. Proof. $\sum_{k=1}^{m-1} = (m-1)(m)/2$. If m is odd then $m = 2n+1$ for some integer n so $(m - 1)(m)/2 = (2n)(m)/2 = nm$ is divisible by m.

Exercise 58. $x = 1$ is the unique (mod N) solution to the simultaneous congruences $x \equiv 1 \mod n_i, i = 1, \dots, k$. Setting $b_i = 1, i = 1, \dots, n$ in formula (8) on page 26 we have $x \equiv \sum_{i=1}^{k} e_i(N/n_i) \mod N$.

Exercise 60. **(a)** Let $0 \leq n \leq p - 1$. n has a square root mod p iff there exists $0 \leq k < p$ such that $n \equiv (\pm k)^2 \mod p$. $-k \equiv p - k \mod p$ so it's enough to prove the following

Claim. If p is odd and $(p - 1)/2 < k < p$ then $0 \leq (k - p) \leq (p - 1)/2$.

Proof. If $(p - 1)/2 < k < p$ then $(p - p) < p - k < p - (p - 1)/2$ so $0 < p-k < (p+1)/2$. If p is also odd then $(p+1)/2$ is an integer, so $p-k < (p+1)/2$ implies that $p - k \leq (p + 1)/2 - 1 = (p - 1)/2$. Hence $0 < p - k \leq (p - 1)/2$. □

(b) Suppose $j^2 \equiv k^2 \mod p$. Then $j^2 - k^2 = (j - k)(j + k) \equiv 0 \mod p$ so $p \mid (j - k)(j + k)$. p is prime so $p \mid j - k$ or $p \mid j + k$.

Suppose also that $0 \le j, k \le (p-1)/2$. $(p-1)/2 \le j+k \le p-1$ so $p \nmid j+k$. Thus $p \mid j-k$. But $-(p-1)/2 \le j-k \le (p-1)/2$ so $j-k=0$ because $p \mid j-k$. Hence $j=k$.

(c) Suppose $n = j^2 \equiv k^2 \mod p$. In part (b) we proved that $p \mid j-k$ or $p \mid j+k$, so $j-k \equiv 0$ or $j+k \equiv 0 \mod p$. Hence $j \equiv \pm k \mod p$. Thus n has at most two square roots: $\pm k \bmod p$. It has exactly two square roots iff $k \not\equiv -k \mod p$. Now $k \equiv -k \mod p$ iff $2k \equiv 0 \mod p$ iff $p \mid 2k$. p is prime so $p \mid 2k$ iff $p \mid 2$ or $p \mid k$ iff $p = 2$ or $k \equiv 0 \mod p$. So if $p > 2$ and $0 < k < p$ then $n = k^2$ has exactly two square roots.

(d) Below is a table of elements in $\mathbb{Z}_{11}$ and their squares.

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1

The squares are in the second row and the corresponding square roots are in the first row. Except for 0, every square in the second row appears twice so it has two corresonding square roots in the first row.

(e) Below is a table of squares in $\mathbb{Z}_{13}$. The squares are in row 2, corresponding square roots are in row 1.

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	3	12	10	10	12	3	9	4	1

(f) Both $0 \equiv 0^2$ and $1 \equiv 1^2$ are squares in $\mathbb{Z}_2$. The assertions in parts (a-c) don't make sense because $[(2-1)/2]^2 = 1/4$ is not in $\mathbb{Z}_2$.

Exercise 62.

(i) 19 and 40 (because $-19 \equiv 40 \mod 59$)

(ii) 402 and 206

(iii) $\left(10^{2144/4}\right)^2 \equiv 2133 \equiv -10 \mod 2143$ so 10 has no square root mod 2143.

Exercise 64. **(a)** Suppose $(n-1)! \equiv -1 \mod n$. Then $(n-1)!+1 \equiv 0 \mod n$ so $(n-1)!+1 = nx$ for some integer x.

Let $1 \le a < n$ be an integer factor of n, so $n = ab$ for some integer b. a is a factor of $(n-1)!$ because $1 \le a < n$, so $(n-1)! = ac$ for some integer c. Substituting these equations into the formula $(n-1)!+1 = nx$ we obtain $ac+1 = nx = (ab)x$ so $1 = abx - ac = a(bx-c)$ is divisible by a. Thus $a = 1$.

We have proved that 1 is the only factor of n that is between 1 and $n-1$. Therefore n is prime.

(b) $p \ge 3$ because p is an odd prime, so $(p-1)! = (p-3)!(p-2)(p-1)$. Consider the product $[2(p-3)!+1](p-2)(p-1)$.

$$\begin{aligned}[2(p-3)!+1](p-2)(p-1) &= 2(p-3)!(p-2)(p-1) + (p-2)(p-1) \\ &= 2(p-1)! + p^2 - 3p + 2 = 2[(p-1)!+1] + p(p-3)\end{aligned}$$

Wilson's theorem says $p \mid (p-1)!+1$ hence p divides $2[(p-1)!+1]+p(p-3)$, hence p divides $[2(p-3)!+1](p-2)(p-1)$. Since p is prime it must divide one of the factors $2(p-3)!+1$ or $p-2$ or $p-1$. p cannot divide $p-2$ or $p-1$ so it must divide $2(p-3)!+1$.

Exercise 66. **(a)** Let $R(k,\ell)$ be the remainder obtained by dividing $a^k - 1$ by $a^\ell - 1$ and $r(k,\ell)$ the remainder obtained by dividing k by ℓ.

CLAIM.

$$R(k,\ell) = a^{r(k,\ell)} - 1 \text{ for all integers } 1 \leq k, \ell$$

PROOF. If $k = \ell$ the claim is obviously true since both remainders are 0.
If $k < \ell$ then $r(k,\ell) = k$. Also $a^k - 1 < a^l - 1$ since $a > 1$, so $R(k,\ell) = a^k - 1$. Hence the claim is true if $k < \ell$.
Thus the claim is true if $k = 1$ because $k \leq \ell$.
The rest of the proof proceeds by induction on k.
Let $k > 1$. Assume the claim is true for all $1 \leq k'$ such that $k' < k$ (this is the induction hypothesis). Let $1 \leq \ell < k$. Then

$$a^k - 1 = a^{k-\ell}(a^\ell - 1) + a^{k-\ell} - 1$$

Therefore the remainder obtained by dividing $a^k - 1$ by $a^\ell - 1$ equals the remainder obtained by dividing $a^{k-\ell} - 1$ by $a^\ell - 1$, that is,

$$R(k,\ell) = R(k-\ell,\ell).$$

The remainder obtained by dividing k by ℓ equals the remainder obtained by dividing $k - \ell$ by ℓ so

$$r(k,\ell) = r(k-\ell,\ell).$$

Set $k' = k - \ell$. $1 \leq \ell < k$ so $1 \leq k' < k$. Applying the induction hypothesis we have

$$R(k-\ell,\ell) = a^{r(k-\ell,\ell)} - 1.$$

Combine the last three displayed equations to obtain

$$R(k,\ell) = R(k-\ell,\ell) = a^{r(k-\ell,\ell)} - 1 = a^{r(k,\ell)} - 1.$$

Hence claim is also true for k. This completes the proof by induction. □

(b) Assume $k \geq \ell$. Applying the Euclidean algorithm to compute $d = \gcd(k,\ell)$ we generate a sequence of remainders r_i:

$$\begin{aligned}
k &= q_1\ell + r_1 \\
\ell &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-2} + r_n \\
r_{n-1} &= q_n r_n + 0
\end{aligned}$$

where

$$\ell > r_1 > r_2 > \cdots > r_n > 0 \text{ and } r_n = \gcd(k,\ell)$$

(if $k = \ell$ then $n = 0$ and $r_0 = k$).
Applying the result from part (a), it follows that the sequence of steps for computing the GCD of $a^k - 1$ and $a^\ell - 1$ with the Euclidean algorithm is

$$\begin{aligned}
a^k - 1 &= Q_1(a^\ell - 1) + (a^{r_1} - 1) \\
a^\ell - 1 &= Q_2(a^{r_1} - 1) + (a^{r_2} - 1) \\
&\vdots \\
a^{r_{n-2}} - 1 &= Q_{n-1}(a^{r_{n-1}} - 1) + (a^{r_n} - 1) \\
a^{r_{n-1}} - 1 &= Q_n(a^{r_n} - 1) + 0
\end{aligned}$$

where

$$a^\ell - 1 > a^{r_1} - 1 > \cdots > a^{r_n} - 1$$

because $a > 1$.
Thus $a^{r_n} - 1$ is the GCD of $a^k - 1$ and $a^\ell - 1$. Since $r_n = \gcd(k, \ell)$ the proof is complete.