99 Routine exercises

99.1 Elementary number theory

Greatest common divisors

Exercise 99.1. Use the Euclidean Algorithm to find $d = \gcd(330, 219)$, and find integers u and v such that $330u + 219v = d$.

Exercise 99.2. Use the Euclidean Algorithm to find $d = \gcd(544, 153)$, and find integers u and v such that $544u + 153v = d$.

Exercise 99.3. Use the Euclidean Algorithm to find $d = \gcd(462, 223)$, and find integers u and v such that $462u + 223v = d$.

Exercise 99.4. Use the Euclidean Algorithm to find $d = \gcd(865, 345)$, and find integers u and v such that $865u + 345v = d$.

Chinese Remainder Theorem

Exercise 99.5. Find the unique solution modulo 221 of the system of congruences

$$x \equiv 4 \pmod{13}, \qquad x \equiv 9 \pmod{17}.$$

Exercise 99.6. Find the unique solution modulo 840 of the system of congruences

$$x \equiv 11 \pmod{24}, \qquad x \equiv 3 \pmod{35}.$$

Exercise 99.7. Find the unique solution modulo 1189 of the system of congruences

$$x \equiv 17 \pmod{29}, \qquad x \equiv 30 \pmod{41}.$$

Exercise 99.8. Find the unique solution modulo 1440 of the system of congruences

$$x \equiv 25 \pmod{32}, \qquad x \equiv 40 \pmod{45}.$$

Parameters for RSA

Exercise 99.9. Let $N = pq = 3233$, where $p = 61$ and $q = 53$, and let $e = 17$.

(a) Check that e is a multiplicative unit in $\mathbf{Z}/\phi(N)\mathbf{Z}$.

(b) Compute the multiplicative inverse d of e in $\mathbf{Z}/\phi(N)\mathbf{Z}$, giving the representative with $0 < d < \phi(N)$.

Exercise 99.10. Let $N = pq = 2773$, where $p = 47$ and $q = 59$, and let $e = 37$.

(a) Check that e is a multiplicative unit in $\mathbf{Z}/\phi(N)\mathbf{Z}$.

(b) Compute the multiplicative inverse d of e in $\mathbf{Z}/\phi(N)\mathbf{Z}$, giving the representative with $0 < d < \phi(N)$.

Exercise 99.11. Let $N = pq = 1591$, where $p = 37$ and $q = 43$, and let $e = 65$.

(a) Check that e is a multiplicative unit in $\mathbf{Z}/\phi(N)\mathbf{Z}$.

(b) Compute the multiplicative inverse d of e in $\mathbf{Z}/\phi(N)\mathbf{Z}$, giving the representative with $0 < d < \phi(N)$.

Exercise 99.12. Let $N = pq = 2407$, where $p = 29$ and $q = 83$, and let $e = 53$.

(a) Check that e is a multiplicative unit in $\mathbf{Z}/\phi(N)\mathbf{Z}$.

(b) Compute the multiplicative inverse d of e in $\mathbf{Z}/\phi(N)\mathbf{Z}$, giving the representative with $0 < d < \phi(N)$.

Exponentiation by repeated squaring

Exercise 99.13. Use repeated squaring to compute 6^{23} mod 71.

Exercise 99.14. Use repeated squaring to compute 8^{29} mod 77.

Exercise 99.15. Use repeated squaring to compute 3^{31} mod 95.

Exercise 99.16. Use repeated squaring to compute 5^{26} mod 87.

Compositeness tests

Exercise 99.17. Let $n = 341$ and $a = 2$.

(a) Is 2 a Fermat witness for n?

(b) Show that 2 is a Miller–Rabin witness for n, and conclude that n is composite.

Exercise 99.18. Let $n = 561$ and $a = 5$.

(a) Is 5 a Fermat witness for n?

(b) Show that 5 is a Miller–Rabin witness for n, and conclude that n is composite.

Exercise 99.19. Let $n = 177$ and $a = 2$.

(a) Is 2 a Fermat witness for n?

(b) Show that 2 is a Miller–Rabin witness for n, and conclude that n is composite.

Exercise 99.20. Let $n = 289$ and $a = 3$.

(a) Is 3 a Fermat witness for n?

(b) Show that 3 is a Miller–Rabin witness for n, and conclude that n is composite.

Exercise 99.21. Let $n = 121$ and $a = 3$. Prove that a is not a Miller–Rabin witness for n.

Exercise 99.22. Let $n = 325$ and $a = 7$. Prove that a is not a Miller–Rabin witness for n.

Exercise 99.23. Let $n = 137$ and $a = 3$. Prove that a is not a Miller–Rabin witness for n.

Exercise 99.24. Let $n = 257$ and $a = 3$. Prove that a is not a Miller–Rabin witness for n.

99.2 Discrete logarithms

Solving non-linear congruences

Exercise 99.25. Let $p = 17$, and note that $g = 3$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$6x^4 \equiv 11 \pmod{17},$$

or show that it has no solutions.

Exercise 99.26. Let $p = 19$, and note that $g = 2$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$12x^2 \equiv 17 \pmod{19},$$

or show that it has no solutions.

Exercise 99.27. Let $p = 23$, and note that $g = 5$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$20x^7 \equiv 13 \pmod{23},$$

or show that it has no solutions.

Exercise 99.28. Let $p = 29$, and note that $g = 2$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$8x^{12} \equiv 12 \pmod{29},$$

or show that it has no solutions.

Exercise 99.29. Let $p = 13$, and note that $g = 2$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$5^x \equiv 12 \pmod{13},$$

or show that it has no solutions.

Exercise 99.30. Let $p = 17$, and note that $g = 3$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$13^x \equiv 4 \pmod{17},$$

or show that it has no solutions.

Exercise 99.31. Let $p = 19$, and note that $g = 2$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$17^x \equiv 14 \pmod{19},$$

or show that it has no solutions.

Exercise 99.32. Let $p = 23$, and note that $g = 5$ is a primitive root modulo p. Use discrete logarithms to solve the congruence

$$6^x \equiv 4 \pmod{23},$$

or show that it has no solutions.

Quadratic residues

Exercise 99.33. Let $p = 157$, which is prime. Use quadratic reciprocity and Jacobi symbols to evaluate $\left(\frac{57}{157}\right)$, and decide whether 57 is a quadratic residue modulo 157.

Exercise 99.34. Let $p = 941$, which is prime. Use quadratic reciprocity and Jacobi symbols to evaluate $\left(\frac{299}{941}\right)$, and decide whether 299 is a quadratic residue modulo 941.

Exercise 99.35. Let $p = 313$, which is prime. Use quadratic reciprocity and Jacobi symbols to evaluate $\left(\frac{101}{313}\right)$, and decide whether 101 is a quadratic residue modulo 313.

Exercise 99.36. Let $p = 463$, which is prime. Use quadratic reciprocity and Jacobi symbols to evaluate $\left(\frac{330}{463}\right)$, and decide whether 330 is a quadratic residue modulo 463.

Sums of squares

Exercise 99.37. Write 397 as a sum of two squares of integers.

Exercise 99.38. Write 493 as a sum of two squares of integers.

Exercise 99.39. Write 637 as a sum of two squares of integers.

Exercise 99.40. Write 754 as a sum of two squares of integers.

99.3 Elliptic curves

Points of finite order

Exercise 99.41. Let E be the elliptic curve $E : \ y^2 = x^3 + 3x - 11$ over $\mathbf{Q}$, and let $P = (3, 5) \in E(\mathbf{Q})$. Find the order of P, or prove that P has infinite order.

Exercise 99.42. Let E be the elliptic curve $E : \ y^2 = x^3 - 43x + 166$ over $\mathbf{Q}$, and let $P = (3, 8) \in E(\mathbf{Q})$. Find the order of P, or prove that P has infinite order.

Exercise 99.43. Let E be the elliptic curve $E : \ y^2 = x^3 + 17$ over $\mathbf{Q}$, and let $P = (-2, 3) \in E(\mathbf{Q})$. Find the order of P, or prove that P has infinite order.

Exercise 99.44. Let E be the elliptic curve $E : \ y^2 = x^3 - 4x + 4$ over $\mathbf{Q}$, and let $P = (2, 2) \in E(\mathbf{Q})$. Find the order of P, or prove that P has infinite order.

Curves over finite fields

Exercise 99.45. Let E be the elliptic curve $E : \ y^2 = x^3 + x + 2$ over $\mathbf{F}_5$.

(a) Find $\#E(\mathbf{F}_5)$.

(b) Determine the group structure of $E(\mathbf{F}_5)$.

Exercise 99.46. Let E be the elliptic curve $E : \ y^2 = x^3 + 1$ over $\mathbf{F}_5$.

(a) Find $\#E(\mathbf{F}_5)$.

(b) Determine the group structure of $E(\mathbf{F}_5)$.

Exercise 99.47. Let E be the elliptic curve $E:\ y^2 = x^3 + x + 6$ over $\mathbf{F}_7$.

(a) Find $\#E(\mathbf{F}_7)$.

(b) Determine the group structure of $E(\mathbf{F}_7)$.

Exercise 99.48. Let E be the elliptic curve $E:\ y^2 = x^3 + 2$ over $\mathbf{F}_7$.

(a) Find $\#E(\mathbf{F}_7)$.

(b) Determine the group structure of $E(\mathbf{F}_7)$.

99.4 Lattices

Lagrange–Gauss reduction in dimension two

Given vectors v_1 and v_2 spanning a two-dimensional lattice L in $\mathbf{R}^2$, find a Lagrange–Gauss reduced basis and use it to solve the SVP for L.

Exercise 99.49. Let $L \subset \mathbf{R}^2$ be the lattice with basis

$$v_1 = \begin{bmatrix} -5 \\ -6 \end{bmatrix}, \qquad v_2 = \begin{bmatrix} 8 \\ 8 \end{bmatrix}.$$

(a) Use Lagrange–Gauss reduction to find a reduced basis of L.

(b) Hence solve the shortest vector problem (SVP) for L.

Exercise 99.50. Let $L \subset \mathbf{R}^2$ be the lattice with basis

$$v_1 = \begin{bmatrix} 7 \\ 2 \end{bmatrix}, \qquad v_2 = \begin{bmatrix} -11 \\ -4 \end{bmatrix}.$$

(a) Use Lagrange–Gauss reduction to find a reduced basis of L.

(b) Hence solve the shortest vector problem (SVP) for L.

Exercise 99.51. Let $L \subset \mathbf{R}^2$ be the lattice with basis

$$v_1 = \begin{bmatrix} -2 \\ 8 \end{bmatrix}, \qquad v_2 = \begin{bmatrix} -2 \\ 11 \end{bmatrix}.$$

(a) Use Lagrange–Gauss reduction to find a reduced basis of L.

(b) Hence solve the shortest vector problem (SVP) for L.

Exercise 99.52. Let $L \subset \mathbf{R}^2$ be the lattice with basis

$$v_1 = \begin{bmatrix} -5 \\ -3 \end{bmatrix}, \qquad v_2 = \begin{bmatrix} -5 \\ -8 \end{bmatrix}.$$

(a) Use Lagrange–Gauss reduction to find a reduced basis of L.

(b) Hence solve the shortest vector problem (SVP) for L.

Answers

Solution 99.1. The Euclidean Algorithm gives

$$\begin{aligned} 330 &= 1 \cdot 219 + 111 \\ 219 &= 1 \cdot 111 + 108 \\ 111 &= 1 \cdot 108 + 3 \\ 108 &= 36 \cdot 3 + 0 \end{aligned}$$

so $d = 3$, the last nonzero remainder.

To find u and v we isolate 3 in the second-to-last step, then work our way back up, substituting for each remainder in turn:

$$\begin{aligned} 3 &= 111 - 108 \\ &= 111 - (219 - 111) = -219 + 2 \cdot 111 \\ &= -219 + 2(330 - 219) = 2 \cdot 330 - 3 \cdot 219. \end{aligned}$$

So we can take $u = 2$ and $v = -3$. (The general solution is $u = 2 + 73k$, $v = -3 - 110k$ with $k \in \mathbf{Z}$.)

Solution 99.2. The Euclidean Algorithm gives

$$\begin{aligned} 544 &= 3 \cdot 153 + 85 \\ 153 &= 1 \cdot 85 + 68 \\ 85 &= 1 \cdot 68 + 17 \\ 68 &= 4 \cdot 17 + 0 \end{aligned}$$

so $d = 17$, the last nonzero remainder.

To find u and v we isolate 17 in the second-to-last step, then work our way back up, substituting for each remainder in turn:

$$\begin{aligned} 17 &= 85 - 68 \\ &= 85 - (153 - 85) = -153 + 2 \cdot 85 \\ &= -153 + 2(544 - 3 \cdot 153) = 2 \cdot 544 - 7 \cdot 153. \end{aligned}$$

So we can take $u = 2$ and $v = -7$. (The general solution is $u = 2 + 9k$, $v = -7 - 32k$ with $k \in \mathbf{Z}$.)

Solution 99.3. The Euclidean Algorithm gives

$$\begin{aligned} 462 &= 2 \cdot 223 + 16 \\ 223 &= 13 \cdot 16 + 15 \\ 16 &= 1 \cdot 15 + 1 \\ 15 &= 15 \cdot 1 + 0 \end{aligned}$$

so $d = 1$, the last nonzero remainder.

To find u and v we isolate 1 in the second-to-last step, then work our way back up, substituting for each remainder in turn:

$$\begin{aligned} 1 &= 16 - 15 \\ &= 16 - (223 - 13 \cdot 16) = -223 + 14 \cdot 16 \\ &= -223 + 14(462 - 2 \cdot 223) = 14 \cdot 462 - 29 \cdot 223. \end{aligned}$$

So we can take $u = 14$ and $v = -29$. (The general solution is $u = 14 + 223k$, $v = -29 - 462k$ with $k \in \mathbf{Z}$.)

Solution 99.4. The Euclidean Algorithm gives

$$\begin{aligned} 865 &= 2 \cdot 345 + 175 \\ 345 &= 1 \cdot 175 + 170 \\ 175 &= 1 \cdot 170 + 5 \\ 170 &= 34 \cdot 5 + 0 \end{aligned}$$

so $d = 5$, the last nonzero remainder.

To find u and v we isolate 5 in the second-to-last step, then work our way back up, substituting for each remainder in turn:

$$\begin{aligned} 5 &= 175 - 170 \\ &= 175 - (345 - 175) = -345 + 2 \cdot 175 \\ &= -345 + 2(865 - 2 \cdot 345) = 2 \cdot 865 - 5 \cdot 345. \end{aligned}$$

So we can take $u = 2$ and $v = -5$. (The general solution is $u = 2 + 69k$, $v = -5 - 173k$ with $k \in \mathbf{Z}$.)

Solution 99.5. The first congruence says $x = 4 + 13t$ for some $t \in \mathbf{Z}$. Substituting into the second congruence gives

$$13t \equiv 9 - 4 = 5 \pmod{17}.$$

Since $1 = 4 \cdot 13 - 3 \cdot 17$ (extended Euclidean algorithm), we have $13^{-1} \equiv 4 \pmod{17}$. Therefore

$$t \equiv 4 \cdot 5 = 20 \equiv 3 \pmod{17},$$

that is, $t = 3 + 17s$ with $s \in \mathbf{Z}$, and then $x = 4 + 13(3 + 17s) = 43 + 221s$. Hence

$$x \equiv 43 \pmod{221}.$$

Check: $43 = 3 \cdot 13 + 4$ and $43 = 2 \cdot 17 + 9$.

Solution 99.6. The first congruence says $x = 11 + 24t$ for some $t \in \mathbf{Z}$. Substituting into the second congruence gives

$$24t \equiv 3 - 11 = -8 \equiv 27 \pmod{35}.$$

Since $1 = (-16) \cdot 24 + 11 \cdot 35$ (extended Euclidean algorithm), we have $24^{-1} \equiv -16 \equiv 19 \pmod{35}$. Therefore

$$t \equiv 19 \cdot 27 = 513 \equiv 23 \pmod{35},$$

that is, $t = 23 + 35s$ with $s \in \mathbf{Z}$, and then $x = 11 + 24(23 + 35s) = 563 + 840s$. Hence

$$x \equiv 563 \pmod{840}.$$

Check: $563 = 23 \cdot 24 + 11$ and $563 = 16 \cdot 35 + 3$.

Solution 99.7. The first congruence says $x = 17 + 29t$ for some $t \in \mathbf{Z}$. Substituting into the second congruence gives

$$29t \equiv 30 - 17 = 13 \pmod{41}.$$

Since $1 = 17 \cdot 29 - 12 \cdot 41$ (extended Euclidean algorithm), we have $29^{-1} \equiv 17 \pmod{41}$. Therefore

$$t \equiv 17 \cdot 13 = 221 \equiv 16 \pmod{41},$$

that is, $t = 16 + 41s$ with $s \in \mathbf{Z}$, and then $x = 17 + 29(16 + 41s) = 481 + 1189s$. Hence

$$x \equiv 481 \pmod{1189}.$$

Check: $481 = 16 \cdot 29 + 17$ and $481 = 11 \cdot 41 + 30$.

Solution 99.8. The first congruence says $x = 25 + 32t$ for some $t \in \mathbf{Z}$. Substituting into the second congruence gives

$$32t \equiv 40 - 25 = 15 \pmod{45}.$$

Since $1 = (-7) \cdot 32 + 5 \cdot 45$ (extended Euclidean algorithm), we have $32^{-1} \equiv -7 \equiv 38 \pmod{45}$. Therefore

$$t \equiv 38 \cdot 15 = 570 \equiv 30 \pmod{45},$$

that is, $t = 30 + 45s$ with $s \in \mathbf{Z}$, and then $x = 25 + 32(30 + 45s) = 985 + 1440s$. Hence

$$x \equiv 985 \pmod{1440}.$$

Check: $985 = 30 \cdot 32 + 25$ and $985 = 21 \cdot 45 + 40$.

Solution 99.9.

(a) We have $\phi(N) = (p-1)(q-1) = 60 \cdot 52 = 3120$, and e is a unit in $\mathbf{Z}/3120\mathbf{Z}$ if and only if $\gcd(17, 3120) = 1$. The Euclidean Algorithm gives

$$\begin{aligned} 3120 &= 183 \cdot 17 + 9 \\ 17 &= 1 \cdot 9 + 8 \\ 9 &= 1 \cdot 8 + 1 \\ 8 &= 8 \cdot 1 + 0 \end{aligned}$$

so $\gcd(17, 3120) = 1$ and $e \in (\mathbf{Z}/3120\mathbf{Z})^\times$.

(b) Working back up the Euclidean Algorithm from part (a):

$$\begin{aligned} 1 &= 9 - 8 \\ &= 9 - (17 - 9) = -17 + 2 \cdot 9 \\ &= -17 + 2(3120 - 183 \cdot 17) = 2 \cdot 3120 - 367 \cdot 17. \end{aligned}$$

Reducing modulo 3120 gives $17 \cdot (-367) \equiv 1 \pmod{3120}$, so $17^{-1} \equiv -367 \equiv 2753 \pmod{3120}$, that is, $d = 2753$. Check: $ed = 17 \cdot 2753 = 46801 = 15 \cdot 3120 + 1$.

Solution 99.10.

(a) We have $\phi(N) = (p-1)(q-1) = 46 \cdot 58 = 2668$, and e is a unit in $\mathbf{Z}/2668\mathbf{Z}$ if and only if $\gcd(37, 2668) = 1$. The Euclidean Algorithm gives

$$\begin{aligned} 2668 &= 72 \cdot 37 + 4 \\ 37 &= 9 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

so $\gcd(37, 2668) = 1$ and $e \in (\mathbf{Z}/2668\mathbf{Z})^\times$.

(b) Working back up the Euclidean Algorithm from part (a):

$$\begin{aligned} 1 &= 37 - 9 \cdot 4 \\ &= 37 - 9(2668 - 72 \cdot 37) = -9 \cdot 2668 + 649 \cdot 37. \end{aligned}$$

Reducing modulo 2668 gives $37 \cdot 649 \equiv 1 \pmod{2668}$, so $d = 649$. Check: $ed = 37 \cdot 649 = 24013 = 9 \cdot 2668 + 1$.

Solution 99.11.

(a) We have $\phi(N) = (p-1)(q-1) = 36 \cdot 42 = 1512$, and e is a unit in $\mathbf{Z}/1512\mathbf{Z}$ if and only if $\gcd(65, 1512) = 1$. The Euclidean Algorithm gives

$$\begin{aligned} 1512 &= 23 \cdot 65 + 17 \\ 65 &= 3 \cdot 17 + 14 \\ 17 &= 1 \cdot 14 + 3 \\ 14 &= 4 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

so $\gcd(65, 1512) = 1$ and $e \in (\mathbf{Z}/1512\mathbf{Z})^\times$.

(b) Working back up the Euclidean Algorithm from part (a):

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (14 - 4 \cdot 3) = -14 + 5 \cdot 3 \\ &= -14 + 5(17 - 14) = 5 \cdot 17 - 6 \cdot 14 \\ &= 5 \cdot 17 - 6(65 - 3 \cdot 17) = -6 \cdot 65 + 23 \cdot 17 \\ &= -6 \cdot 65 + 23(1512 - 23 \cdot 65) = 23 \cdot 1512 - 535 \cdot 65. \end{aligned}$$

Reducing modulo 1512 gives $65 \cdot (-535) \equiv 1 \pmod{1512}$, so $65^{-1} \equiv -535 \equiv 977 \pmod{1512}$, that is, $d = 977$. Check: $ed = 65 \cdot 977 = 63505 = 42 \cdot 1512 + 1$.

Solution 99.12.

(a) We have $\phi(N) = (p-1)(q-1) = 28 \cdot 82 = 2296$, and e is a unit in $\mathbf{Z}/2296\mathbf{Z}$ if and only if $\gcd(53, 2296) = 1$. The Euclidean Algorithm gives

$$\begin{aligned} 2296 &= 43 \cdot 53 + 17 \\ 53 &= 3 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

so $\gcd(53, 2296) = 1$ and $e \in (\mathbf{Z}/2296\mathbf{Z})^\times$.

(b) Working back up the Euclidean Algorithm from part (a):

$$\begin{aligned} 1 &= 17 - 8 \cdot 2 \\ &= 17 - 8(53 - 3 \cdot 17) = -8 \cdot 53 + 25 \cdot 17 \\ &= -8 \cdot 53 + 25(2296 - 43 \cdot 53) = 25 \cdot 2296 - 1083 \cdot 53. \end{aligned}$$

Reducing modulo 2296 gives $53 \cdot (-1083) \equiv 1 \pmod{2296}$, so $53^{-1} \equiv -1083 \equiv 1213 \pmod{2296}$, that is, $d = 1213$. Check: $ed = 53 \cdot 1213 = 64289 = 28 \cdot 2296 + 1$.

Solution 99.13. In base 2 we have $23 = (10111)_2$, so $r = 4$. Set $m_0 = 6$ and, for $j \geqslant 1$, let $m_j \equiv m_{j-1}^2$ if $e_{r-j} = 0$ and $m_j \equiv m_{j-1}^2 \cdot 6$ if $e_{r-j} = 1$, reducing modulo 71 at each step:

j	e_{r-j}		m_j
0	1	—	6
1	0	$6^2 = 36$	36
2	1	$36^2 = 1296 \equiv 18$, $\quad 18 \cdot 6 = 108 \equiv 37$	37
3	1	$37^2 = 1369 \equiv 20$, $\quad 20 \cdot 6 = 120 \equiv 49$	49
4	1	$49^2 = 2401 \equiv 58$, $\quad 58 \cdot 6 = 348 \equiv 64$	64

Hence $6^{23} \equiv m_4 = 64 \pmod{71}$.

Solution 99.14. In base 2 we have $29 = (11101)_2$, so $r = 4$. Set $m_0 = 8$ and, for $j \geqslant 1$, let $m_j \equiv m_{j-1}^2$ if $e_{r-j} = 0$ and $m_j \equiv m_{j-1}^2 \cdot 8$ if $e_{r-j} = 1$, reducing modulo 77 at each step:

j	e_{r-j}		m_j
0	1	—	8
1	1	$8^2 = 64$, $\quad 64 \cdot 8 = 512 \equiv 50$	50
2	1	$50^2 = 2500 \equiv 36$, $\quad 36 \cdot 8 = 288 \equiv 57$	57
3	0	$57^2 = 3249 \equiv 15$	15
4	1	$15^2 = 225 \equiv 71$, $\quad 71 \cdot 8 = 568 \equiv 29$	29

Hence $8^{29} \equiv m_4 = 29 \pmod{77}$.

Solution 99.15. In base 2 we have $31 = (11111)_2$, so $r = 4$. Set $m_0 = 3$ and, for $j \geqslant 1$, let $m_j \equiv m_{j-1}^2$ if $e_{r-j} = 0$ and $m_j \equiv m_{j-1}^2 \cdot 3$ if $e_{r-j} = 1$, reducing modulo 95 at each step:

j	e_{r-j}		m_j
0	1	—	3
1	1	$3^2 = 9, \quad 9 \cdot 3 = 27$	27
2	1	$27^2 = 729 \equiv 64, \quad 64 \cdot 3 = 192 \equiv 2$	2
3	1	$2^2 = 4, \quad 4 \cdot 3 = 12$	12
4	1	$12^2 = 144 \equiv 49, \quad 49 \cdot 3 = 147 \equiv 52$	52

Hence $3^{31} \equiv m_4 = 52 \pmod{95}$.

Solution 99.16. In base 2 we have $26 = (11010)_2$, so $r = 4$. Set $m_0 = 5$ and, for $j \geqslant 1$, let $m_j \equiv m_{j-1}^2$ if $e_{r-j} = 0$ and $m_j \equiv m_{j-1}^2 \cdot 5$ if $e_{r-j} = 1$, reducing modulo 87 at each step:

j	e_{r-j}		m_j
0	1	—	5
1	1	$5^2 = 25, \quad 25 \cdot 5 = 125 \equiv 38$	38
2	0	$38^2 = 1444 \equiv 52$	52
3	1	$52^2 = 2704 \equiv 7, \quad 7 \cdot 5 = 35$	35
4	0	$35^2 = 1225 \equiv 7$	7

Hence $5^{26} \equiv m_4 = 7 \pmod{87}$.

Solution 99.17.

(a) We have $n - 1 = 340 = 2^2 \cdot 85$, so $k = 2$ and $m = 85$ in the notation $n - 1 = 2^k m$ with m odd. Also $\gcd(2, 341) = 1$, so 2 is a Fermat witness for 341 if and only if $2^{340} \not\equiv 1 \pmod{341}$.

We compute $2^{85} \bmod 341$ by repeated squaring. In base 2, $85 = (1010101)_2$; set $a_0 = 2$ and $a_j \equiv a_{j-1}^2$ or $a_{j-1}^2 \cdot 2$ according as the next bit is 0 or 1:

j	bit		a_j
0	1	—	2
1	0	$2^2 = 4$	4
2	1	$4^2 = 16, \quad 16 \cdot 2 = 32$	32
3	0	$32^2 = 1024 \equiv 1$	1
4	1	$1^2 = 1, \quad 1 \cdot 2 = 2$	2
5	0	$2^2 = 4$	4
6	1	$4^2 = 16, \quad 16 \cdot 2 = 32$	32

So $2^{85} \equiv 32 \pmod{341}$. Squaring repeatedly, we reach $2^{340} = 2^{2^2 \cdot 85}$:

$$\begin{aligned} 2^{85} &\equiv 32 \\ 2^{2 \cdot 85} &\equiv 32^2 = 1024 \equiv 1 \\ 2^{2^2 \cdot 85} &\equiv 1^2 = 1 \pmod{341}. \end{aligned}$$

Thus $2^{340} \equiv 1 \pmod{341}$, so 2 is **not** a Fermat witness for 341.

(b) We use the values $2^{2^j m} \bmod 341$ computed in (a). Every power $2^{2^j m}$ with $j \geqslant 1$ is 1 (once a square is 1, all later ones are). We see that $2^{85} \not\equiv 1 \pmod{341}$, and that $2^{2^j m} \not\equiv -1 \equiv 340 \pmod{341}$ for $j = 0, 1$. Hence 2 is a Miller–Rabin witness for 341, and by the Miller–Rabin Compositeness Test, 341 is composite.

Remark. Here $b = 32$ satisfies $b^2 \equiv 1$ but $b \not\equiv \pm 1 \pmod{341}$, so $\gcd(b-1, n) = \gcd(31, 341) = 31$ is a nontrivial factor of n: $341 = 11 \cdot 31$.

Solution 99.18.

(a) We have $n - 1 = 560 = 2^4 \cdot 35$, so $k = 4$ and $m = 35$ in the notation $n - 1 = 2^k m$ with m odd. Also $\gcd(5, 561) = 1$, so 5 is a Fermat witness for 561 if and only if $5^{560} \not\equiv 1 \pmod{561}$.

We compute $5^{35} \bmod 561$ by repeated squaring. In base 2, $35 = (100011)_2$; set $a_0 = 5$ and $a_j \equiv a_{j-1}^2$ or $a_{j-1}^2 \cdot 5$ according as the next bit is 0 or 1:

j	bit			a_j
0	1	—		5
1	0	$5^2 = 25$		25
2	0	$25^2 = 625 \equiv 64$		64
3	0	$64^2 = 4096 \equiv 169$		169
4	1	$169^2 = 28561 \equiv 511,$	$511 \cdot 5 = 2555 \equiv 311$	311
5	1	$311^2 = 96721 \equiv 229,$	$229 \cdot 5 = 1145 \equiv 23$	23

So $5^{35} \equiv 23 \pmod{561}$. Squaring repeatedly, we reach $5^{560} = 5^{2^4 \cdot 35}$:

$$\begin{aligned} 5^{35} &\equiv 23 \\ 5^{2 \cdot 35} &\equiv 23^2 = 529 \\ 5^{2^2 \cdot 35} &\equiv 529^2 = 279841 \equiv 463 \\ 5^{2^3 \cdot 35} &\equiv 463^2 = 214369 \equiv 67 \\ 5^{2^4 \cdot 35} &\equiv 67^2 = 4489 \equiv 1 \pmod{561}. \end{aligned}$$

Thus $5^{560} \equiv 1 \pmod{561}$, so 5 is **not** a Fermat witness for 561.

(b) We use the values $5^{2^j m} \bmod 561$ computed in (a). We see that $5^{35} \not\equiv 1 \pmod{561}$, and that $5^{2^j m} \not\equiv -1 \equiv 560 \pmod{561}$ for all $j \in \{0, 1, \ldots, 3\}$. Hence 5 is a Miller–Rabin witness for 561, and by the Miller–Rabin Compositeness Test, 561 is composite.

Remark. Here $b = 67$ satisfies $b^2 \equiv 1$ but $b \not\equiv \pm 1 \pmod{561}$, so $\gcd(b-1, n) = \gcd(66, 561) = 33$ is a nontrivial factor of n: $561 = 17 \cdot 33$.

Solution 99.19.

(a) We have $n-1 = 176 = 2^4 \cdot 11$, so $k = 4$ and $m = 11$ in the notation $n-1 = 2^k m$ with m odd. Also $\gcd(2, 177) = 1$, so 2 is a Fermat witness for 177 if and only if $2^{176} \not\equiv 1 \pmod{177}$.

We compute $2^{11} \bmod 177$ by repeated squaring. In base 2, $11 = (1011)_2$; set $a_0 = 2$ and $a_j \equiv a_{j-1}^2$ or $a_{j-1}^2 \cdot 2$ according as the next bit is 0 or 1:

j	bit		a_j
0	1	—	2
1	0	$2^2 = 4$	4
2	1	$4^2 = 16, \quad 16 \cdot 2 = 32$	32
3	1	$32^2 = 1024 \equiv 139, \quad 139 \cdot 2 = 278 \equiv 101$	101

So $2^{11} \equiv 101 \pmod{177}$. Squaring repeatedly, we reach $2^{176} = 2^{2^4 \cdot 11}$:

$$\begin{aligned} 2^{11} &\equiv 101 \\ 2^{2 \cdot 11} &\equiv 101^2 = 10201 \equiv 112 \\ 2^{2^2 \cdot 11} &\equiv 112^2 = 12544 \equiv 154 \\ 2^{2^3 \cdot 11} &\equiv 154^2 = 23716 \equiv 175 \\ 2^{2^4 \cdot 11} &\equiv 175^2 = 30625 \equiv 4 \pmod{177}. \end{aligned}$$

Thus $2^{176} \equiv 4 \not\equiv 1 \pmod{177}$, so 2 is a Fermat witness for 177 (and in particular 177 is composite).

(b) We use the values $2^{2^j m} \bmod 177$ computed in (a). We see that $2^{11} \not\equiv 1 \pmod{177}$, and that $2^{2^j m} \not\equiv -1 \equiv 176 \pmod{177}$ for all $j \in \{0, 1, \ldots, 3\}$. Hence 2 is a Miller–Rabin witness for 177, and by the Miller–Rabin Compositeness Test, 177 is composite.

Solution 99.20.

(a) We have $n - 1 = 288 = 2^5 \cdot 9$, so $k = 5$ and $m = 9$ in the notation $n - 1 = 2^k m$ with m odd. Also $\gcd(3, 289) = 1$, so 3 is a Fermat witness for 289 if and only if $3^{288} \not\equiv 1 \pmod{289}$.

We compute $3^9 \bmod 289$ by repeated squaring. In base 2, $9 = (1001)_2$; set $a_0 = 3$ and $a_j \equiv a_{j-1}^2$ or $a_{j-1}^2 \cdot 3$ according as the next bit is 0 or 1:

j	bit		a_j
0	1	—	3
1	0	$3^2 = 9$	9
2	0	$9^2 = 81$	81
3	1	$81^2 = 6561 \equiv 203, \quad 203 \cdot 3 = 609 \equiv 31$	31

So $3^9 \equiv 31 \pmod{289}$. Squaring repeatedly, we reach $3^{288} = 3^{2^5 \cdot 9}$:

$$\begin{aligned} 3^9 &\equiv 31 \\ 3^{2\cdot 9} &\equiv 31^2 = 961 \equiv 94 \\ 3^{2^2\cdot 9} &\equiv 94^2 = 8836 \equiv 166 \\ 3^{2^3\cdot 9} &\equiv 166^2 = 27556 \equiv 101 \\ 3^{2^4\cdot 9} &\equiv 101^2 = 10201 \equiv 86 \\ 3^{2^5\cdot 9} &\equiv 86^2 = 7396 \equiv 171 \pmod{289}. \end{aligned}$$

Thus $3^{288} \equiv 171 \not\equiv 1 \pmod{289}$, so 3 is a Fermat witness for 289 (and in particular 289 is composite).

(b) We use the values $3^{2^j m} \bmod 289$ computed in (a). We see that $3^9 \not\equiv 1 \pmod{289}$, and that $3^{2^j m} \not\equiv -1 \equiv 288 \pmod{289}$ for all $j \in \{0, 1, \ldots, 4\}$. Hence 3 is a Miller–Rabin witness for 289, and by the Miller–Rabin Compositeness Test, 289 is composite.

Solution 99.21. We have $n - 1 = 120 = 2^3 \cdot 15$, so $k = 3$ and $m = 15$ in the notation $n - 1 = 2^k m$ with m odd.

We compute $3^{15} \bmod 121$ by repeated squaring. In base 2, $15 = (1111)_2$; set $a_0 = 3$ and $a_j \equiv a_{j-1}^2$ or $a_{j-1}^2 \cdot 3$ according as the next bit is 0 or 1:

j	bit		a_j
0	1	—	3
1	1	$3^2 = 9, \quad 9 \cdot 3 = 27$	27
2	1	$27^2 = 729 \equiv 3, \quad 3 \cdot 3 = 9$	9
3	1	$9^2 = 81, \quad 81 \cdot 3 = 243 \equiv 1$	1

So $3^{15} \equiv 1 \pmod{121}$. Since $a^m = 3^{15} \equiv 1 \pmod{121}$, the first condition in the definition of a Miller–Rabin witness fails. Hence 3 is not a Miller–Rabin witness for 121.

Remark. Nevertheless $121 = 11^2$ is composite: the Miller–Rabin test with $a = 3$ is inconclusive for this n.

Solution 99.22. We have $n - 1 = 324 = 2^2 \cdot 81$, so $k = 2$ and $m = 81$ in the notation $n - 1 = 2^k m$ with m odd.

We compute $7^{81} \bmod 325$ by repeated squaring. In base 2, $81 = (1010001)_2$; set $a_0 = 7$ and $a_j \equiv a_{j-1}^2$ or $a_{j-1}^2 \cdot 7$ according as the next bit is 0 or 1:

j	bit		a_j
0	1	—	7
1	0	$7^2 = 49$	49
2	1	$49^2 = 2401 \equiv 126, \quad 126 \cdot 7 = 882 \equiv 232$	232
3	0	$232^2 = 53824 \equiv 199$	199
4	0	$199^2 = 39601 \equiv 276$	276
5	0	$276^2 = 76176 \equiv 126$	126
6	1	$126^2 = 15876 \equiv 276, \quad 276 \cdot 7 = 1932 \equiv 307$	307

So $7^{81} \equiv 307 \pmod{325}$. Squaring repeatedly gives

$$\begin{aligned} 7^{81} &\equiv 307 \\ 7^{2\cdot 81} &\equiv 307^2 = 94249 \equiv 324 \pmod{325}. \end{aligned}$$

Since $324 \equiv -1 \pmod{325}$, this says $a^{2^j m} \equiv -1 \pmod{325}$ for $j = 1$, which lies in the range $0 \leqslant j \leqslant k-1 = 1$. So the second condition in the definition of a Miller–Rabin witness fails, and hence 7 is not a Miller–Rabin witness for 325.

Remark. Nevertheless $325 = 5^2 \cdot 13$ is composite: the Miller–Rabin test with $a = 7$ is inconclusive for this n.

Solution 99.23. We have $n - 1 = 136 = 2^3 \cdot 17$, so $k = 3$ and $m = 17$ in the notation $n - 1 = 2^k m$ with m odd.

We compute $3^{17} \bmod 137$ by repeated squaring. In base 2, $17 = (10001)_2$; set $a_0 = 3$ and $a_j \equiv a_{j-1}^2$ or $a_{j-1}^2 \cdot 3$ according as the next bit is 0 or 1:

j	bit		a_j
0	1	—	3
1	0	$3^2 = 9$	9
2	0	$9^2 = 81$	81
3	0	$81^2 = 6561 \equiv 122$	122
4	1	$122^2 = 14884 \equiv 88$, $\quad 88 \cdot 3 = 264 \equiv 127$	127

So $3^{17} \equiv 127 \pmod{137}$. Squaring repeatedly gives

$$\begin{aligned} 3^{17} &\equiv 127 \\ 3^{2\cdot 17} &\equiv 127^2 = 16129 \equiv 100 \\ 3^{2^2\cdot 17} &\equiv 100^2 = 10000 \equiv 136 \pmod{137}. \end{aligned}$$

Since $136 \equiv -1 \pmod{137}$, this says $a^{2^j m} \equiv -1 \pmod{137}$ for $j = 2$, which lies in the range $0 \leqslant j \leqslant k-1 = 2$. So the second condition in the definition of a Miller–Rabin witness fails, and hence 3 is not a Miller–Rabin witness for 137.

Remark. This is as it must be: 137 is prime, so it has no Miller–Rabin witnesses at all.

Solution 99.24. We have $n - 1 = 256 = 2^8 \cdot 1$, so $k = 8$ and $m = 1$ in the notation $n - 1 = 2^k m$ with m odd.

Squaring repeatedly gives

$$\begin{aligned} 3^1 &\equiv 3 \\ 3^2 &\equiv 3^2 = 9 \\ 3^{2^2} &\equiv 9^2 = 81 \\ 3^{2^3} &\equiv 81^2 = 6561 \equiv 136 \\ 3^{2^4} &\equiv 136^2 = 18496 \equiv 249 \\ 3^{2^5} &\equiv 249^2 = 62001 \equiv 64 \\ 3^{2^6} &\equiv 64^2 = 4096 \equiv 241 \\ 3^{2^7} &\equiv 241^2 = 58081 \equiv 256 \pmod{257}. \end{aligned}$$

Since $256 \equiv -1 \pmod{257}$, this says $a^{2^j m} \equiv -1 \pmod{257}$ for $j = 7$, which lies in the range $0 \leqslant j \leqslant k-1 = 7$. So the second condition in the definition of a Miller–Rabin witness fails, and hence 3 is not a Miller–Rabin witness for 257.

Remark. This is as it must be: 257 is prime, so it has no Miller–Rabin witnesses at all.

Solution 99.25. We tabulate the powers of 3 modulo 17; reading the table backwards gives $\log_3(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7
$3^k \bmod 17$	1	3	9	10	13	5	15	11

k	8	9	10	11	12	13	14	15
$3^k \bmod 17$	16	14	8	7	4	12	2	6

From the table, $\log_3(6) = 15$ and $\log_3(11) = 7$. Since $11 \not\equiv 0 \pmod{17}$, any solution satisfies $x \not\equiv 0 \pmod{17}$. Taking $\log_3$ of both sides, the congruence $6x^4 \equiv 11 \pmod{17}$ is equivalent to

$$15 + 4\log_3(x) \equiv 7 \pmod{16}, \qquad \text{that is,} \qquad 4\log_3(x) \equiv 7 - 15 \equiv 8 \pmod{16}.$$

Here $d = \gcd(4, 16) = 4$ divides 8, so this linear congruence has exactly 4 solutions modulo 16. Dividing through by $d = 4$ gives $\log_3(x) \equiv 2 \pmod{4}$. Hence, modulo 16,

$$\log_3(x) \in \{2, 6, 10, 14\},$$

and reading off the table, $3^2 \equiv 9$, $3^6 \equiv 15$, $3^{10} \equiv 8$, $3^{14} \equiv 2$. Hence the solutions are

$$x \equiv 2, 8, 9, 15 \pmod{17}.$$

Check (for instance): $6 \cdot 9^4 \equiv 11 \pmod{17}$.

Solution 99.26. We tabulate the powers of 2 modulo 19; reading the table backwards gives $\log_2(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7	8
$2^k \bmod 19$	1	2	4	8	16	13	7	14	9

k	9	10	11	12	13	14	15	16	17
$2^k \bmod 19$	18	17	15	11	3	6	12	5	10

From the table, $\log_2(12) = 15$ and $\log_2(17) = 10$. Since $17 \not\equiv 0 \pmod{19}$, any solution satisfies $x \not\equiv 0 \pmod{19}$. Taking $\log_2$ of both sides, the congruence $12x^2 \equiv 17 \pmod{19}$ is equivalent to

$$15 + 2\log_2(x) \equiv 10 \pmod{18}, \qquad \text{that is,} \qquad 2\log_2(x) \equiv 10 - 15 \equiv 13 \pmod{18}.$$

Here $\gcd(2, 18) = 2$, which does not divide 13. Since $2\log_2(x)$ is always congruent modulo 18 to a multiple of 2, this linear congruence has no solutions, and hence

$$12x^2 \equiv 17 \pmod{19}$$

has no solutions.

Solution 99.27. We tabulate the powers of 5 modulo 23; reading the table backwards gives $\log_5(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7	8	9	10
$5^k \bmod 23$	1	5	2	10	4	20	8	17	16	11	9

k	11	12	13	14	15	16	17	18	19	20	21
$5^k \bmod 23$	22	18	21	13	19	3	15	6	7	12	14

From the table, $\log_5(20) = 5$ and $\log_5(13) = 14$. Since $13 \not\equiv 0 \pmod{23}$, any solution satisfies $x \not\equiv 0 \pmod{23}$. Taking $\log_5$ of both sides, the congruence $20x^7 \equiv 13 \pmod{23}$ is equivalent to

$$5 + 7\log_5(x) \equiv 14 \pmod{22}, \qquad \text{that is,} \qquad 7\log_5(x) \equiv 14 - 5 = 9 \pmod{22}.$$

Since $\gcd(7, 22) = 1$, this linear congruence has a unique solution modulo 22: we have $7^{-1} \equiv 19 \pmod{22}$, since $7 \cdot 19 = 133 = 6 \cdot 22 + 1$, so

$$\log_5(x) \equiv 19 \cdot 9 = 171 \equiv 17 \pmod{22}.$$

From the table, $5^{17} \equiv 15 \pmod{23}$. Hence the congruence has the unique solution

$$x \equiv 15 \pmod{23}.$$

Check: $20 \cdot 15^7 \equiv 13 \pmod{23}$.

Solution 99.28. We tabulate the powers of 2 modulo 29; reading the table backwards gives $\log_2(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7	8	9
$2^k \bmod 29$	1	2	4	8	16	3	6	12	24	19

k	10	11	12	13	14	15	16	17	18	19
$2^k \bmod 29$	9	18	7	14	28	27	25	21	13	26

k	20	21	22	23	24	25	26	27
$2^k \bmod 29$	23	17	5	10	20	11	22	15

From the table, $\log_2(8) = 3$ and $\log_2(12) = 7$. Since $12 \not\equiv 0 \pmod{29}$, any solution satisfies $x \not\equiv 0 \pmod{29}$. Taking $\log_2$ of both sides, the congruence $8x^{12} \equiv 12 \pmod{29}$ is equivalent to

$$3 + 12\log_2(x) \equiv 7 \pmod{28}, \qquad \text{that is,} \qquad 12\log_2(x) \equiv 7 - 3 = 4 \pmod{28}.$$

Here $d = \gcd(12, 28) = 4$ divides 4, so this linear congruence has exactly 4 solutions modulo 28. Dividing through by $d = 4$ gives $3\log_2(x) \equiv 1 \pmod{7}$. Here $3^{-1} \equiv 5 \pmod{7}$, since $3 \cdot 5 = 15 = 2 \cdot 7 + 1$, so $\log_2(x) \equiv 5 \cdot 1 = 5 \pmod{7}$. Hence, modulo 28,

$$\log_2(x) \in \{5, 12, 19, 26\},$$

and reading off the table, $2^5 \equiv 3$, $2^{12} \equiv 7$, $2^{19} \equiv 26$, $2^{26} \equiv 22$. Hence the solutions are

$$x \equiv 3, 7, 22, 26 \pmod{29}.$$

Check (for instance): $8 \cdot 3^{12} \equiv 12 \pmod{29}$.

Solution 99.29. We tabulate the powers of 2 modulo 13; reading the table backwards gives $\log_2(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7	8	9	10	11
$2^k \bmod 13$	1	2	4	8	3	6	12	11	9	5	10	7

From the table, $\log_2(5) = 9$ and $\log_2(12) = 6$. Taking $\log_2$ of both sides, the congruence $5^x \equiv 12 \pmod{13}$ is equivalent to $x\log_2(5) \equiv \log_2(12) \pmod{12}$, that is,

$$9x \equiv 6 \pmod{12}.$$

Here $\gcd(9, 12) = 3$ divides 6; dividing through by 3 gives $3x \equiv 2 \pmod{4}$. Now $3^{-1} \equiv 3 \pmod{4}$, since $3 \cdot 3 = 9 = 2 \cdot 4 + 1$, so $x \equiv 3 \cdot 2 = 6 \equiv 2 \pmod{4}$. So the solutions of the original congruence are all integers x with

$$x \equiv 2 \pmod{4}.$$

(Note that $4 = 12/3$ is the order of 5 modulo 13.) Check: $5^2 \equiv 2^{9 \cdot 2} = 2^{18} \equiv 2^6 \equiv 12 \pmod{13}$.

Solution 99.30. We tabulate the powers of 3 modulo 17; reading the table backwards gives $\log_3(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7
$3^k \bmod 17$	1	3	9	10	13	5	15	11

k	8	9	10	11	12	13	14	15
$3^k \bmod 17$	16	14	8	7	4	12	2	6

From the table, $\log_3(13) = 4$ and $\log_3(4) = 12$. Taking $\log_3$ of both sides, the congruence $13^x \equiv 4 \pmod{17}$ is equivalent to $x \log_3(13) \equiv \log_3(4) \pmod{16}$, that is,

$$4x \equiv 12 \pmod{16}.$$

Here $\gcd(4, 16) = 4$ divides 12; dividing through by 4 gives $x \equiv 3 \pmod 4$. So the solutions of the original congruence are all integers x with

$$x \equiv 3 \pmod 4.$$

(Note that $4 = 16/4$ is the order of 13 modulo 17.) Check: $13^3 \equiv 3^{4\cdot 3} = 3^{12} \equiv 4 \pmod{17}$.

Solution 99.31. We tabulate the powers of 2 modulo 19; reading the table backwards gives $\log_2(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7	8
$2^k \bmod 19$	1	2	4	8	16	13	7	14	9

k	9	10	11	12	13	14	15	16	17
$2^k \bmod 19$	18	17	15	11	3	6	12	5	10

From the table, $\log_2(17) = 10$ and $\log_2(14) = 7$. Taking $\log_2$ of both sides, the congruence $17^x \equiv 14 \pmod{19}$ is equivalent to $x \log_2(17) \equiv \log_2(14) \pmod{18}$, that is,

$$10x \equiv 7 \pmod{18}.$$

But $\gcd(10, 18) = 2$ does not divide 7, so this linear congruence has no solutions. Hence the congruence $17^x \equiv 14 \pmod{19}$ has no solutions. (Equivalently: 17 has order $18/2 = 9$, and 14 is not one of the 9 powers of 17.)

Solution 99.32. We tabulate the powers of 5 modulo 23; reading the table backwards gives $\log_5(y)$ for $y \not\equiv 0$:

k	0	1	2	3	4	5	6	7	8	9	10
$5^k \bmod 23$	1	5	2	10	4	20	8	17	16	11	9

k	11	12	13	14	15	16	17	18	19	20	21
$5^k \bmod 23$	22	18	21	13	19	3	15	6	7	12	14

From the table, $\log_5(6) = 18$ and $\log_5(4) = 4$. Taking $\log_5$ of both sides, the congruence $6^x \equiv 4 \pmod{23}$ is equivalent to $x \log_5(6) \equiv \log_5(4) \pmod{22}$, that is,

$$18x \equiv 4 \pmod{22}.$$

Here $\gcd(18, 22) = 2$ divides 4; dividing through by 2 gives $9x \equiv 2 \pmod{11}$. Now $9^{-1} \equiv 5 \pmod{11}$, since $9 \cdot 5 = 45 = 4 \cdot 11 + 1$, so $x \equiv 5 \cdot 2 = 10 \pmod{11}$. So the solutions of the original congruence are all integers x with

$$x \equiv 10 \pmod{11}.$$

(Note that $11 = 22/2$ is the order of 6 modulo 23.) Check: $6^{10} \equiv 5^{18\cdot 10} = 5^{180} \equiv 5^4 \equiv 4 \pmod{23}$.

Solution 99.33. All the symbols below are Jacobi symbols, so we may use Quadratic Reciprocity (for Jacobi symbols) and the formula for $\left(\frac{2}{b}\right)$ without factoring the numerators, other than removing powers of 2:

$$\begin{aligned}
\left(\frac{57}{157}\right) &= \left(\frac{157}{57}\right) && \text{Quadratic Reciprocity, as } 57 \equiv 1 \pmod 4 \\
&= \left(\frac{43}{57}\right) && \text{since } 157 \equiv 43 \pmod{57} \\
&= \left(\frac{57}{43}\right) && \text{Quadratic Reciprocity, as } 57 \equiv 1 \pmod 4 \\
&= \left(\frac{14}{43}\right) && \text{since } 57 \equiv 14 \pmod{43} \\
&= \left(\frac{2}{43}\right)\left(\frac{7}{43}\right) && \text{as } 14 = 2 \cdot 7 \\
&= -\left(\frac{7}{43}\right) && \text{since } 43 \equiv 3 \pmod 8, \text{ so } \left(\frac{2}{43}\right) = -1 \\
&= \left(\frac{43}{7}\right) && \text{Quadratic Reciprocity, as } 7 \equiv 43 \equiv 3 \pmod 4 \\
&= \left(\frac{1}{7}\right) && \text{since } 43 \equiv 1 \pmod 7 \\
&= 1.
\end{aligned}$$

Since 157 is prime, the Jacobi symbol $\left(\frac{57}{157}\right)$ is the Legendre symbol, so $\left(\frac{57}{157}\right) = 1$ and 57 is a quadratic residue modulo 157.

Solution 99.34. All the symbols below are Jacobi symbols, so we may use Quadratic Reciprocity (for Jacobi symbols) and the formula for $\left(\frac{2}{b}\right)$ without factoring the numerators, other than removing powers of 2:

$$\begin{aligned}
\left(\frac{299}{941}\right) &= \left(\frac{941}{299}\right) && \text{Quadratic Reciprocity, as } 941 \equiv 1 \pmod 4 \\
&= \left(\frac{44}{299}\right) && \text{since } 941 \equiv 44 \pmod{299} \\
&= \left(\frac{2}{299}\right)^2\left(\frac{11}{299}\right) && \text{as } 44 = 2^2 \cdot 11 \\
&= \left(\frac{11}{299}\right) && \text{since } 299 \equiv 3 \pmod 8, \text{ so } \left(\frac{2}{299}\right) = -1 \\
&= -\left(\frac{299}{11}\right) && \text{Quadratic Reciprocity, as } 11 \equiv 299 \equiv 3 \pmod 4 \\
&= -\left(\frac{2}{11}\right) && \text{since } 299 \equiv 2 \pmod{11} \\
&= -\left(\frac{2}{11}\right) && \text{as } 2 = 2 \\
&= \left(\frac{1}{11}\right) && \text{since } 11 \equiv 3 \pmod 8, \text{ so } \left(\frac{2}{11}\right) = -1 \\
&= 1.
\end{aligned}$$

Since 941 is prime, the Jacobi symbol $\left(\frac{299}{941}\right)$ is the Legendre symbol, so $\left(\frac{299}{941}\right) = 1$ and 299 is a quadratic residue modulo 941.

Solution 99.35. All the symbols below are Jacobi symbols, so we may use Quadratic Reciprocity (for Jacobi symbols) and the formula for $\left(\frac{2}{b}\right)$ without factoring the numerators, other than removing powers of 2:

$$\begin{aligned}
\left(\frac{101}{313}\right) &= \left(\frac{313}{101}\right) && \text{Quadratic Reciprocity, as } 101 \equiv 1 \pmod 4 \\
&= \left(\frac{10}{101}\right) && \text{since } 313 \equiv 10 \pmod{101} \\
&= \left(\frac{2}{101}\right)\left(\frac{5}{101}\right) && \text{as } 10 = 2 \cdot 5 \\
&= -\left(\frac{5}{101}\right) && \text{since } 101 \equiv -3 \pmod 8, \text{ so } \left(\frac{2}{101}\right) = -1 \\
&= -\left(\frac{101}{5}\right) && \text{Quadratic Reciprocity, as } 5 \equiv 1 \pmod 4 \\
&= -\left(\frac{1}{5}\right) && \text{since } 101 \equiv 1 \pmod 5 \\
&= -1.
\end{aligned}$$

Since 313 is prime, the Jacobi symbol $\left(\frac{101}{313}\right)$ is the Legendre symbol, so $\left(\frac{101}{313}\right) = -1$ and 101 is not a quadratic residue modulo 313.

Solution 99.36. All the symbols below are Jacobi symbols, so we may use Quadratic Reciprocity (for Jacobi symbols) and the formula for $\left(\frac{2}{b}\right)$ without factoring the numerators, other than removing powers of 2:

$$\begin{aligned}
\left(\frac{330}{463}\right) &= \left(\frac{2}{463}\right)\left(\frac{165}{463}\right) && \text{as } 330 = 2 \cdot 165 \\
&= \left(\frac{165}{463}\right) && \text{since } 463 \equiv -1 \pmod 8, \text{ so } \left(\frac{2}{463}\right) = 1 \\
&= \left(\frac{463}{165}\right) && \text{Quadratic Reciprocity, as } 165 \equiv 1 \pmod 4 \\
&= \left(\frac{133}{165}\right) && \text{since } 463 \equiv 133 \pmod{165} \\
&= \left(\frac{165}{133}\right) && \text{Quadratic Reciprocity, as } 133 \equiv 1 \pmod 4 \\
&= \left(\frac{32}{133}\right) && \text{since } 165 \equiv 32 \pmod{133} \\
&= \left(\frac{2}{133}\right)^5 && \text{as } 32 = 2^5 \\
&= -\left(\frac{1}{133}\right) && \text{since } 133 \equiv -3 \pmod 8, \text{ so } \left(\frac{2}{133}\right) = -1 \\
&= -1.
\end{aligned}$$

Since 463 is prime, the Jacobi symbol $\left(\frac{330}{463}\right)$ is the Legendre symbol, so $\left(\frac{330}{463}\right) = -1$ and 330 is not a quadratic residue modulo 463.

Solution 99.37. The number 397 is prime and $397 \equiv 1 \pmod 4$, so it is a sum of two squares, $397 = x^2 + y^2$ with (say) $0 < x < y$. Then $2x^2 < 397$, so $x \leqslant 14$, and we test the values of x in turn: for $x = 1, 2, \dots, 6$ the numbers $397 - x^2$ are

$$396, 393, 388, 381, 372, 361,$$

and the last of these is $361 = 19^2$ (the others are not squares). Hence

$$397 = 6^2 + 19^2 = 36 + 361.$$

Solution 99.38. We factor $n = 493 = 17 \cdot 29$. This is squarefree. Every prime dividing n is 2 or congruent to 1 modulo 4, so n is a sum of two squares. By inspection, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$. Using the identity

$$(x^2 + y^2)(v^2 + w^2) = (xv + yw)^2 + (xw - yv)^2$$

we get

$$17 \cdot 29 = (1^2 + 4^2)(2^2 + 5^2) = (1 \cdot 2 + 4 \cdot 5)^2 + (1 \cdot 5 - 4 \cdot 2)^2 = 22^2 + (-3)^2.$$

Hence

$$493 = 3^2 + 22^2 = 9 + 484.$$

(This representation is not unique: the representations of 493 as $x^2 + y^2$ with $0 \leqslant x \leqslant y$ are $3^2 + 22^2$, $13^2 + 18^2$.)

Solution 99.39. We factor $n = 637 = 7^2 \cdot 13$. Writing $n = s^2 n_0$ with n_0 squarefree, we have $s = 7$ and $n_0 = 13$. Every prime dividing n_0 is 2 or congruent to 1 modulo 4, so n is a sum of two squares. By inspection, $13 = 2^2 + 3^2$. Multiplying by $s^2 = 7^2$ gives $637 = 7^2(2^2 + 3^2) = (7 \cdot 2)^2 + (7 \cdot 3)^2$. Hence

$$637 = 14^2 + 21^2 = 196 + 441.$$

Solution 99.40. We factor $n = 754 = 2 \cdot 13 \cdot 29$. This is squarefree. Every prime dividing n is 2 or congruent to 1 modulo 4, so n is a sum of two squares. By inspection, $2 = 1^2 + 1^2$, $13 = 2^2 + 3^2$, $29 = 2^2 + 5^2$. Using the identity

$$(x^2 + y^2)(v^2 + w^2) = (xv + yw)^2 + (xw - yv)^2$$

we get

$$\begin{aligned} 2 \cdot 13 &= (1^2 + 1^2)(2^2 + 3^2) = (1 \cdot 2 + 1 \cdot 3)^2 + (1 \cdot 3 - 1 \cdot 2)^2 = 5^2 + 1^2 \\ 26 \cdot 29 &= (1^2 + 5^2)(2^2 + 5^2) = (1 \cdot 2 + 5 \cdot 5)^2 + (1 \cdot 5 - 5 \cdot 2)^2 = 27^2 + (-5)^2. \end{aligned}$$

Hence

$$754 = 5^2 + 27^2 = 25 + 729.$$

(This representation is not unique: the representations of 754 as $x^2 + y^2$ with $0 \leqslant x \leqslant y$ are $5^2 + 27^2$, $15^2 + 23^2$.)

Solution 99.41. We compute multiples of P until we recognise $\mathcal{O}$ or the negative of a point already computed. We use the addition and duplication formulas from the notes: the slope m of the line through the two points (the tangent line, when doubling), its intercept $n = y_1 - mx_1$, and then $x_3 = m^2 - x_1 - x_2$ (or $m^2 - 2x_1$ when doubling) and $y_3 = -(mx_3 + n)$.

Duplication formula for $P = (x_1, y_1) = (3, 5)$:

$$\begin{aligned} m &= \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 3^2 + 3}{2 \cdot 5} = 3 \\ n &= y_1 - mx_1 = 5 - 3 \cdot 3 = -4 \\ x([2]P) &= m^2 - 2x_1 = 3^2 - 2 \cdot 3 = 3 \\ y([2]P) &= -(m\,x([2]P) + n) = -\left(3 \cdot 3 + (-4)\right) = -5, \end{aligned}$$

so $[2]P = (3, -5)$.

Thus $[2]P = -P$ (same x-coordinate, opposite y-coordinate), so $[3]P = [2]P + P = \mathcal{O}$. Since 3 is prime and $P \neq \mathcal{O}$, the order of P is exactly 3.

Solution 99.42. We compute multiples of P until we recognise $\mathcal{O}$ or the negative of a point already computed. We use the addition and duplication formulas from the notes: the slope m of the line through the two points (the tangent line, when doubling), its intercept $n = y_1 - mx_1$, and then $x_3 = m^2 - x_1 - x_2$ (or $m^2 - 2x_1$ when doubling) and $y_3 = -(mx_3 + n)$.

Duplication formula for $P = (x_1, y_1) = (3, 8)$:

$$\begin{aligned} m &= \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 3^2 - 43}{2 \cdot 8} = -1 \\ n &= y_1 - mx_1 = 8 - (-1) \cdot 3 = 11 \\ x([2]P) &= m^2 - 2x_1 = (-1)^2 - 2 \cdot 3 = -5 \\ y([2]P) &= -(m\,x([2]P) + n) = -\left((-1) \cdot (-5) + 11\right) = -16, \end{aligned}$$

so $[2]P = (-5, -16)$.

Addition formula for $P = (x_1, y_1) = (3, 8)$ and $[2]P = (x_2, y_2) = (-5, -16)$:

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1} = \frac{-16 - 8}{-5 - 3} = 3 \\ n &= y_1 - mx_1 = 8 - 3 \cdot 3 = -1 \\ x([3]P) &= m^2 - x_1 - x_2 = 3^2 - 3 - (-5) = 11 \\ y([3]P) &= -(m\,x([3]P) + n) = -\left(3 \cdot 11 + (-1)\right) = -32, \end{aligned}$$

so $[3]P = (11, -32)$.

Duplication formula for $[2]P = (x_1, y_1) = (-5, -16)$:

$$\begin{aligned} m &= \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot (-5)^2 - 43}{2 \cdot (-16)} = -1 \\ n &= y_1 - mx_1 = -16 - (-1) \cdot (-5) = -21 \\ x([4]P) &= m^2 - 2x_1 = (-1)^2 - 2 \cdot (-5) = 11 \\ y([4]P) &= -(m\,x([4]P) + n) = -\left((-1) \cdot 11 + (-21)\right) = 32, \end{aligned}$$

so $[4]P = (11, 32)$.

Thus $[4]P = -[3]P$ (same x-coordinate, opposite y-coordinate), so $[7]P = [4]P + [3]P = \mathcal{O}$. Since 7 is prime and $P \neq \mathcal{O}$, the order of P is exactly 7.

Solution 99.43. By the Lutz–Nagell Theorem, if $Q = (x, y) \in E(\mathbf{Q})$ is a torsion point then $x, y \in \mathbf{Z}$ and either $y = 0$ or $y^2 \mid 4a^3 + 27b^2$. Here $a = 0$, $b = 17$, and $4a^3 + 27b^2 = 7803 = 3^3 \cdot 17^2$. For P itself, $y^2 = 9$ divides 7803, so this gives no information yet, and we compute multiples of P. We use the addition and duplication formulas from the notes: the slope m of the line through the two points (the tangent line, when doubling), its intercept $n = y_1 - mx_1$, and then $x_3 = m^2 - x_1 - x_2$ (or $m^2 - 2x_1$ when doubling) and $y_3 = -(mx_3 + n)$.

Duplication formula for $P = (x_1, y_1) = (-2, 3)$:

$$\begin{aligned} m &= \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot (-2)^2}{2 \cdot 3} = 2 \\ n &= y_1 - mx_1 = 3 - 2 \cdot (-2) = 7 \\ x([2]P) &= m^2 - 2x_1 = 2^2 - 2 \cdot (-2) = 8 \\ y([2]P) &= -(m\, x([2]P) + n) = -\,(2 \cdot 8 + 7) = -23, \end{aligned}$$

so $[2]P = (8, -23)$.

The point $[2]P$ has integer coordinates, but $y^2 = 529$ does not divide 7803, so by the Lutz–Nagell Theorem $[2]P$ is not a torsion point. If P had finite order n, then $[n]([2]P) = [2]([n]P) = \mathcal{O}$ and $[2]P$ would have finite order too. Hence P has infinite order.

Solution 99.44. By the Lutz–Nagell Theorem, if $Q = (x, y) \in E(\mathbf{Q})$ is a torsion point then $x, y \in \mathbf{Z}$ and either $y = 0$ or $y^2 \mid 4a^3 + 27b^2$. Here $a = -4$, $b = 4$, and $4a^3 + 27b^2 = 176 = 2^4 \cdot 11$. For P itself, $y^2 = 4$ divides 176, so this gives no information yet, and we compute multiples of P. We use the addition and duplication formulas from the notes: the slope m of the line through the two points (the tangent line, when doubling), its intercept $n = y_1 - mx_1$, and then $x_3 = m^2 - x_1 - x_2$ (or $m^2 - 2x_1$ when doubling) and $y_3 = -(mx_3 + n)$.

Duplication formula for $P = (x_1, y_1) = (2, 2)$:

$$\begin{aligned} m &= \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 2^2 - 4}{2 \cdot 2} = 2 \\ n &= y_1 - mx_1 = 2 - 2 \cdot 2 = -2 \\ x([2]P) &= m^2 - 2x_1 = 2^2 - 2 \cdot 2 = 0 \\ y([2]P) &= -(m\, x([2]P) + n) = -\,(2 \cdot 0 + (-2)) = 2, \end{aligned}$$

so $[2]P = (0, 2)$. This has integer coordinates and $y^2 = 4$ divides 176, so we continue.

Addition formula for $P = (x_1, y_1) = (2, 2)$ and $[2]P = (x_2, y_2) = (0, 2)$:

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1} = \frac{2 - 2}{0 - 2} = 0 \\ n &= y_1 - mx_1 = 2 - 0 \cdot 2 = 2 \\ x([3]P) &= m^2 - x_1 - x_2 = 0^2 - 2 - 0 = -2 \\ y([3]P) &= -(m\, x([3]P) + n) = -\,(0 \cdot (-2) + 2) = -2, \end{aligned}$$

so $[3]P = (-2, -2)$. This has integer coordinates and $y^2 = 4$ divides 176, so we continue.

Duplication formula for $[2]P = (x_1, y_1) = (0, 2)$:

$$\begin{aligned} m &= \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 0^2 - 4}{2 \cdot 2} = -1 \\ n &= y_1 - mx_1 = 2 - (-1) \cdot 0 = 2 \\ x([4]P) &= m^2 - 2x_1 = (-1)^2 - 2 \cdot 0 = 1 \\ y([4]P) &= -(m\,x([4]P) + n) = -\left((-1) \cdot 1 + 2\right) = -1, \end{aligned}$$

so $[4]P = (1, -1)$. This has integer coordinates and $y^2 = 1$ divides 176, so we continue.

Addition formula for $P = (x_1, y_1) = (2, 2)$ and $[4]P = (x_2, y_2) = (1, -1)$:

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1} = \frac{-1 - 2}{1 - 2} = 3 \\ n &= y_1 - mx_1 = 2 - 3 \cdot 2 = -4 \\ x([5]P) &= m^2 - x_1 - x_2 = 3^2 - 2 - 1 = 6 \\ y([5]P) &= -(m\,x([5]P) + n) = -\left(3 \cdot 6 + (-4)\right) = -14, \end{aligned}$$

so $[5]P = (6, -14)$.

The point $[5]P$ has integer coordinates, but $y^2 = 196$ does not divide 176, so by the Lutz–Nagell Theorem $[5]P$ is not a torsion point. If P had finite order n, then $[n]([5]P) = [5]([n]P) = \mathcal{O}$ and $[5]P$ would have finite order too. Hence P has infinite order.

Solution 99.45.

(a) The nonzero squares modulo 5 are $1, 4$, since $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$ modulo 5. For each $x \in \mathbf{F}_5$ we compute $f(x) = x^3 + x + 2$: there are two points $(x, \pm y)$ if $f(x)$ is a nonzero square, one point $(x, 0)$ if $f(x) = 0$, and none if $f(x)$ is a non-residue.

x	$x^3 + x + 2 \bmod 5$	y	points
0	2	—	0
1	4	± 2	2
2	2	—	0
3	2	—	0
4	0	0	1

Adding the point at infinity $\mathcal{O}$, we get $\#E(\mathbf{F}_5) = 1 + 3 = 4$.

(b) Up to isomorphism, the abelian groups of order 4 are $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. The first has exactly one element of order 2 (namely 2), while the second has three (namely $(1,0)$, $(0,1)$, $(1,1)$). The points of order 2 are the points with $y = 0$; from the table, $E(\mathbf{F}_5)$ has exactly one point of order 2, namely $(4, 0)$. Hence

$$E(\mathbf{F}_5) \cong \mathbf{Z}/4\mathbf{Z}.$$

Solution 99.46.

(a) The nonzero squares modulo 5 are $1, 4$, since $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$ modulo 5. For each $x \in \mathbf{F}_5$ we compute $f(x) = x^3 + 1$: there are two points $(x, \pm y)$ if $f(x)$ is a nonzero square, one point $(x, 0)$ if $f(x) = 0$, and none if $f(x)$ is a non-residue.

x	$x^3 + 1 \bmod 5$	y	points
0	1	± 1	2
1	2	—	0
2	4	± 2	2
3	3	—	0
4	0	0	1

Adding the point at infinity $\mathcal{O}$, we get $\#E(\mathbf{F}_5) = 1 + 5 = 6$.

(b) Since $\#E(\mathbf{F}_5) = 6 = 2 \cdot 3$ is squarefree, the only abelian group of order 6 up to isomorphism is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, which is cyclic by the Chinese Remainder Theorem. Hence

$$E(\mathbf{F}_5) \cong \mathbf{Z}/6\mathbf{Z}.$$

Solution 99.47.

(a) The nonzero squares modulo 7 are $1, 2, 4$, since $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$, $(\pm 3)^2 \equiv 2$ modulo 7. For each $x \in \mathbf{F}_7$ we compute $f(x) = x^3 + x + 6$: there are two points $(x, \pm y)$ if $f(x)$ is a nonzero square, one point $(x, 0)$ if $f(x) = 0$, and none if $f(x)$ is a non-residue.

x	$x^3 + x + 6 \bmod 7$	y	points
0	6	—	0
1	1	± 1	2
2	2	± 3	2
3	1	± 1	2
4	4	± 2	2
5	3	—	0
6	4	± 2	2

Adding the point at infinity $\mathcal{O}$, we get $\#E(\mathbf{F}_7) = 1 + 10 = 11$.

(b) Since $\#E(\mathbf{F}_7) = 11$ is prime, every point other than $\mathcal{O}$ has order 11 (the order of an element divides the cardinality of the group). Hence $E(\mathbf{F}_7)$ is cyclic, generated by any point other than $\mathcal{O}$:

$$E(\mathbf{F}_7) \cong \mathbf{Z}/11\mathbf{Z}.$$

Solution 99.48.

(a) The nonzero squares modulo 7 are $1, 2, 4$, since $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$, $(\pm 3)^2 \equiv 2$ modulo 7. For each $x \in \mathbf{F}_7$ we compute $f(x) = x^3 + 2$: there are two points $(x, \pm y)$ if $f(x)$ is a nonzero square, one point $(x, 0)$ if $f(x) = 0$, and none if $f(x)$ is a non-residue.

x	$x^3+2 \bmod 7$	y	points
0	2	± 3	2
1	3	—	0
2	3	—	0
3	1	± 1	2
4	3	—	0
5	1	± 1	2
6	1	± 1	2

Adding the point at infinity $\mathcal{O}$, we get $\#E(\mathbf{F}_7) = 1 + 8 = 9$.

(b) Up to isomorphism, the abelian groups of order 9 are $\mathbf{Z}/9\mathbf{Z}$, which has exactly two elements of order 3, and $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, in which all eight non-identity elements have order 3. Working modulo 7 with the duplication formula: for $Q = (0,3)$ we get $m \equiv (3 \cdot 0^2)/(2 \cdot 3) \equiv 0$, $n \equiv 3 - 0 \cdot 0 \equiv 3$, hence $x([2]Q) \equiv 0^2 - 2 \cdot 0 \equiv 0$ and $y([2]Q) \equiv -(0 \cdot 0 + 3) \equiv 4$, so $[2]Q = (0,4) = -Q$ and Q has order 3; and for $Q = (3,1)$ we get $m \equiv (3 \cdot 3^2)/(2 \cdot 1) \equiv 3$, $n \equiv 1 - 3 \cdot 3 \equiv 6$, hence $x([2]Q) \equiv 3^2 - 2 \cdot 3 \equiv 3$ and $y([2]Q) \equiv -(3 \cdot 3 + 6) \equiv 6$, so again $[2]Q = (3,6) = -Q$ has order 3. Together with their negatives this gives four points of order 3, namely $(0,3)$, $(0,4)$, $(3,1)$, $(3,6)$, so $E(\mathbf{F}_7)$ is not cyclic. Hence

$$E(\mathbf{F}_7) \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

(In fact every one of the eight points other than $\mathcal{O}$ has order 3.)

Solution 99.49.

(a) We have $\|v_1\|^2 = 61$, $\|v_2\|^2 = 128$, $\langle v_1, v_2 \rangle = -88$. Therefore $t = 88/61 \approx 1.443$, $\lfloor t \rceil = 1$, so the new v_2 is $(8,8)^\mathsf{T} + (-5,-6)^\mathsf{T} = (3,2)^\mathsf{T}$.

Now $\|v_2\|^2 = 13$ so we swap v_1, v_2.

We have $\|v_1\|^2 = 13$, $\|v_2\|^2 = 61$, $\langle v_1, v_2 \rangle = -27$. Therefore $t = 27/13 \approx 2.077$, $\lfloor t \rceil = 2$, so the new v_2 is $(-5,-6)^\mathsf{T} + 2(3,2)^\mathsf{T} = (1,-2)^\mathsf{T}$.

Now $\|v_2\|^2 = 5$ so we swap v_1, v_2.

step	v_1	v_2	$\|v_1\|^2$	$\|v_2\|^2$	$\langle v_1, v_2 \rangle$	$\lfloor t \rceil$
1	$\left[\begin{smallmatrix}-5\\-6\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}8\\8\end{smallmatrix}\right]$	61	128	-88	1
2	$\left[\begin{smallmatrix}3\\2\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-5\\-6\end{smallmatrix}\right]$	13	61	-27	2
3	$\left[\begin{smallmatrix}1\\-2\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}3\\2\end{smallmatrix}\right]$	5	13	-1	0

(b) For a Lagrange–Gauss reduced basis, v_1 is a shortest nonzero vector of L. So a solution to SVP is $v_1 = \left[\begin{smallmatrix}1\\-2\end{smallmatrix}\right]$, with $\|v_1\| = \sqrt{5}$.

Solution 99.50.

(a) We have $\|v_1\|^2 = 53$, $\|v_2\|^2 = 137$, $\langle v_1, v_2\rangle = -85$. Therefore $t = 85/53 \approx 1.604$, $\lfloor t \rceil = 2$, so the new v_2 is $(-11,-4)^\mathsf{T} + 2(7,2)^\mathsf{T} = (3,0)^\mathsf{T}$.

Now $\|v_2\|^2 = 9$ so we swap v_1, v_2.

We have $\|v_1\|^2 = 9$, $\|v_2\|^2 = 53$, $\langle v_1, v_2\rangle = 21$. Therefore $t = -21/9 \approx -2.333$, $\lfloor t \rceil = -2$, so the new v_2 is $(7,2)^\mathsf{T} - 2(3,0)^\mathsf{T} = (1,2)^\mathsf{T}$.

Now $\|v_2\|^2 = 5$ so we swap v_1, v_2.

We have $\|v_1\|^2 = 5$, $\|v_2\|^2 = 9$, $\langle v_1, v_2\rangle = 3$. Therefore $t = -3/5 = -0.6$, $\lfloor t \rceil = -1$, so the new v_2 is $(3,0)^\mathsf{T} - (1,2)^\mathsf{T} = (2,-2)^\mathsf{T}$. Since $\|v_2\|^2 = 8$ we stop and the output is

$$\left(\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}2\\-2\end{bmatrix}\right).$$

step	v_1	v_2	$\|v_1\|^2$	$\|v_2\|^2$	$\langle v_1, v_2\rangle$	$\lfloor t \rceil$
1	$\left[\begin{smallmatrix}7\\2\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-11\\-4\end{smallmatrix}\right]$	53	137	-85	2
2	$\left[\begin{smallmatrix}3\\0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}7\\2\end{smallmatrix}\right]$	9	53	21	-2
3	$\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}3\\0\end{smallmatrix}\right]$	5	9	3	-1
4	$\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}2\\-2\end{smallmatrix}\right]$	5	8	-2	0

(b) For a Lagrange–Gauss reduced basis, v_1 is a shortest nonzero vector of L. So a solution to SVP is $v_1 = \left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]$, with $\|v_1\| = \sqrt{5}$.

Solution 99.51.

(a) We have $\|v_1\|^2 = 68$, $\|v_2\|^2 = 125$, $\langle v_1, v_2\rangle = 92$. Therefore $t = -92/68 \approx -1.353$, $\lfloor t \rceil = -1$, so the new v_2 is $(-2,11)^\mathsf{T} - (-2,8)^\mathsf{T} = (0,3)^\mathsf{T}$.

Now $\|v_2\|^2 = 9$ so we swap v_1, v_2.

We have $\|v_1\|^2 = 9$, $\|v_2\|^2 = 68$, $\langle v_1, v_2\rangle = 24$. Therefore $t = -24/9 \approx -2.667$, $\lfloor t \rceil = -3$, so the new v_2 is $(-2,8)^\mathsf{T} - 3(0,3)^\mathsf{T} = (-2,-1)^\mathsf{T}$.

Now $\|v_2\|^2 = 5$ so we swap v_1, v_2.

We have $\|v_1\|^2 = 5$, $\|v_2\|^2 = 9$, $\langle v_1, v_2\rangle = -3$. Therefore $t = 3/5 = 0.6$, $\lfloor t \rceil = 1$, so the new v_2 is $(0,3)^\mathsf{T} + (-2,-1)^\mathsf{T} = (-2,2)^\mathsf{T}$. Since $\|v_2\|^2 = 8$ we stop and the output is

$$\left(\begin{bmatrix}-2\\-1\end{bmatrix}, \begin{bmatrix}-2\\2\end{bmatrix}\right).$$

step	v_1	v_2	$\|v_1\|^2$	$\|v_2\|^2$	$\langle v_1, v_2\rangle$	$\lfloor t \rceil$
1	$\left[\begin{smallmatrix}-2\\8\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-2\\11\end{smallmatrix}\right]$	68	125	92	-1
2	$\left[\begin{smallmatrix}0\\3\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-2\\8\end{smallmatrix}\right]$	9	68	24	-3
3	$\left[\begin{smallmatrix}-2\\-1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0\\3\end{smallmatrix}\right]$	5	9	-3	1
4	$\left[\begin{smallmatrix}-2\\-1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-2\\2\end{smallmatrix}\right]$	5	8	2	0

(b) For a Lagrange–Gauss reduced basis, v_1 is a shortest nonzero vector of L. So a solution to SVP is $v_1 = \left[\begin{smallmatrix}-2\\-1\end{smallmatrix}\right]$, with $\|v_1\| = \sqrt{5}$.

Solution 99.52.

(a) We have $\|v_1\|^2 = 34$, $\|v_2\|^2 = 89$, $\langle v_1, v_2\rangle = 49$. Therefore $t = -49/34 \approx -1.441$, $\lfloor t \rceil = -1$, so the new v_2 is $(-5,-8)^\mathsf{T} - (-5,-3)^\mathsf{T} = (0,-5)^\mathsf{T}$.

Now $\|v_2\|^2 = 25$ so we swap v_1, v_2.

We have $\|v_1\|^2 = 25$, $\|v_2\|^2 = 34$, $\langle v_1, v_2\rangle = 15$. Therefore $t = -15/25 = -0.6$, $\lfloor t \rceil = -1$, so the new v_2 is $(-5,-3)^\mathsf{T} - (0,-5)^\mathsf{T} = (-5,2)^\mathsf{T}$. Since $\|v_2\|^2 = 29$ we stop and the output is

$$\left(\begin{bmatrix}0\\-5\end{bmatrix}, \begin{bmatrix}-5\\2\end{bmatrix}\right).$$

step	v_1	v_2	$\|v_1\|^2$	$\|v_2\|^2$	$\langle v_1, v_2\rangle$	$\lfloor t \rceil$
1	$\left[\begin{smallmatrix}-5\\-3\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-5\\-8\end{smallmatrix}\right]$	34	89	49	-1
2	$\left[\begin{smallmatrix}0\\-5\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-5\\-3\end{smallmatrix}\right]$	25	34	15	-1
3	$\left[\begin{smallmatrix}0\\-5\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-5\\2\end{smallmatrix}\right]$	25	29	-10	0

(b) For a Lagrange–Gauss reduced basis, v_1 is a shortest nonzero vector of L. So a solution to SVP is $v_1 = \left[\begin{smallmatrix}0\\-5\end{smallmatrix}\right]$, with $\|v_1\| = \sqrt{25}$.