Solution to selected exercises

Exercises of Chapter 1

A1.1. The basis of induction, that is, property 1 of (CI), is the same as for mathematical induction. Property 2 of (CI) is weaker than 2 of mathematical induction, so if (CI) is true, mathematical induction is true a fortiori.

A1.2. Assume by contradiction that there is a non-empty subset T of $\mathbb{N}$ that has no least element. Let A be the complement of T in $\mathbb{N}$. Then $0 \in A$, or else 0 would be the least element in T. Moreover, if $n \in A$, then $n+1 \in A$ as well, or else $n+1$ would be the least element in T. Then, by mathematical induction, $A = \mathbb{N}$, against the hypothesis that T is non-empty.

A1.3. Let A be a non-empty subset of $\mathbb{N}$ that satisfies the two properties of (CI), where we assume, for the sake of simplicity, $n_0 = 0$. Assume by contradiction that A is not equal to $\mathbb{N}$. Then the complement U of A is not empty, so it has a least element $m \in U$ by the well-ordering principle, with $m \neq 0$ because $0 \in A$. As m is the least element of U, for all k such that $0 \leq k < m$ we have $k \in A$, so from property 2 it follows that $m \in A$, yielding a contradiction.

A1.5. The correct answer is (d). It is necessary to define mathematically what we mean by a "small city", or else neither the basis of the induction nor the inductive step make sense.

A1.6. The correct answer is (c); indeed, the inductive step does not hold for $n = 49,999$.

A1.8. Recall that in the proof of Proposition 1.3.1 we have assumed $b > 0$. Assume further that $a \geq 0$. Consider the subset $S = \{\, n \mid (n+1)b > a \,\}$ of $\mathbb{N}$. Clearly S is not empty, because for instance $a \in S$. So, by the well-ordering principle, S has a least element, which will be called q. Then $(q+1)b > a$, because $q \in S$, and $qb \leq a$, or else we would have $q - 1 \in S$, contradicting the fact that q is the least element of S.

A1.9. Let A be the set of the ns for which we may compute a_n. Then A satisfies the two properties of mathematical induction, so for all $n > n_0$ we have $n \in A$, while $n \in A$ for $n = 1, 2, \ldots, n_0$ by hypothesis.

A1.12. The claim is true for $n = 1$. Suppose the number of elements of $\mathfrak{S}_{n-1}$ is $(n-1)!$. Define the mapping $f : \mathfrak{S}_n \to \mathfrak{S}_{n-1}$ that maps the permutation having symbol $(i_1, \ldots, i_n)$ to the permutation having the symbol obtained deleting n from $(i_1, \ldots, i_n)$. Prove that f is surjective and that the preimage of every element of $\mathfrak{S}_{n-1}$ consists of n elements of $\mathfrak{S}_n$. Deduce that the number of elements of $\mathfrak{S}_n$ is $n!$.

A1.13. The correct answer is (c). Indeed, a function between sets having the same (finite) size is injective if and only if it is bijective, and this happens if and only if it is surjective. So we prove by induction on n that there are $n!$ bijective functions from A to B. The basis of the induction, for $n = 1$, is trivial. Assume that A and B have $n+1$ elements. Fix an element $a \in A$. Then there are $n+1$ possible choices for the image of A under a function f. Now, if f is bijective, then $f : A \setminus \{a\} \to B \setminus \{f(a)\}$ is bijective too, and by the inductive hypothesis there are $n!$ such bijective functions. So there are $n! \cdot (n+1) = (n+1)!$ bijective functions from A to B.

A1.14. The reader might want to prove Formula (1.51) by induction on n. We give here a direct proof. Start with the identity

$$\frac{n+1}{k(n-k+1)} = \frac{1}{k} + \frac{1}{n-k+1}.$$

Multiplying both sides by $\dfrac{n!}{(k-1)!(n-k)!}$ we obtain

$$\frac{(n+1)!}{k!(n-k+1)!} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!},$$

that is, Formula (1.51), as wanted.

A1.15. The claim is true if $n = 1$. Notice next that the subsets of size m of I_n that include n are as many as the subsets of size $m-1$ of I_{n-1}, while the subsets of size m of I_n that do not include n are as many as the subsets of size m of I_{n-1}. Apply now the inductive hypothesis and Formula (1.51).

A1.19. The correct answer is (c). We have assumed $n \leq m$, else, if $n > m$ there would be no injective functions $A \hookrightarrow B$.

A1.20. The correct answer is (a), as may be proved by induction, or directly by noticing that for every element a of A there are m possible choices for its image.

A1.21. It suffices to remark that every ordered m–tuple of elements of A determines a mapping from I_m to A; apply then the previous exercise.

A1.22. The correct answer is (b). Indeed, given a subset Y of X, consider the function $f_Y : X \to I_2$, called *characteristic function of* Y, that takes the value 1 on all elements of Y and nowhere else. Prove that the mapping associating with $Y \in \mathcal{P}(X)$ its characteristic function is a bijection of $\mathcal{P}(X)$ in the set of mappings from X to I_n. Apply then Exercise A1.20.

A1.24. The formula for $s(n,h)$ is true for $n = 1$. As to $s(n,h)$ for $n > 1$, it is the sum of the number of monomials in which x_1 appears to the degree i, for all $i = 0, \ldots, h$, and this number is $s(n-1, h-i)$. Conclude by applying the inductive hypothesis and (1.52).

A1.26. In the hypotheses of the exercise we have

$$y_n + x_n = b_{k-1}y_{n-1} + \cdots + b_0 y_{n-k} + d_n + b_{k-1}x_{n-1} + \cdots + b_0 x_{n-k} = \\ = b_{k-1}(y_{n-1} + x_{n-1}) + \cdots + b_0(y_{n-k} + x_{n-k}) + d_n,$$

that is, $\{y_n + x_n\}$ is a solution of (1.4). Moreover, if z_n is another solution of (1.4), then

$$y_n - z_n = b_{k-1}y_{n-1} + \cdots + b_0 y_{n-k} + d_n + \\ - b_{k-1}z_{n-1} - \cdots - b_0 z_{n-k} - d_n = \\ = b_{k-1}(y_{n-1} - z_{n-1}) + \cdots + b_0(y_{n-k} - z_{n-k}),$$

that is, $\{y_n - z_n\}$ is a solution of (1.53).

A1.27. We have

$$a_1 = ba_0 + c, \qquad a_2 = ba_1 + c$$

which may be interpreted as a linear system in b and c. If $a_0 \neq a_1$, this system uniquely determines b and c and so the whole sequence starting from a_0. If $a_0 = a_1$, also $a_2 = a_1 = a_0$, else the system would not be compatible, which is not possible. Prove next by induction that the sequence $\{a_n\}$ is constant.

A1.28. The basis of the induction is obvious by the definition of A and of Fibonacci numbers f_n. Suppose Proposition 1.2.3 is true for $n-1$ and prove it for n. We have

$$A^n = A^{n-1} \cdot A = \quad \text{(by the inductive hypothesis)} \\ = \begin{pmatrix} f_{n-2} & f_{n-1} \\ f_{n-1} & f_n \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} f_{n-1} & f_{n-2} + f_{n-1} \\ f_n & f_{n-1} + f_n \end{pmatrix} = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix},$$

where the last equality follows from Definition (1.5) of Fibonacci sequence.

A1.30. Fix k and proceed by induction on n. For $n = 1$, Formula (1.54) becomes $f_{k+1} = f_k + f_{k-1}$, which is true. So, assume the truth of the formula for all $0 \leq m < n$ and prove it for n. By the inductive hypothesis we have

$$f_{n-1+k} = f_k f_n + f_{k-1} f_{n-1} \qquad \text{and} \qquad f_{n-2+k} = f_k f_{n-1} + f_{k-1} f_{n-2};$$

hence, summing, we get

$$f_{n+k} = f_{n-1+k} + f_{n-2+k} = f_k(f_n + f_{n-1}) + f_{k-1}(f_{n-1} + f_{n-2}) = \\ = f_k f_{n+1} + f_{k-1} f_n.$$

We want to prove now that f_{kn} is a multiple of f_n. Proceed by induction on k. For $k = 1$ this is obvious. Assume that f_{mn} is a multiple of f_n for all $m \leq k$ and prove it for $k+1$. The previous relation implies

$$f_{(k+1)n} = f_{kn+n} = f_{kn} f_{n+1} + f_{kn-1} f_n,$$

so, by the inductive hypothesis, both f_n and f_{kn} are multiples of f_n, so $f_{(k+1)n}$ is too.

A1.31. Proceed by induction on n, the result being trivial for $n = 1$. Assume the result to be true for every integer smaller than n and prove it for n. If n is a Fibonacci number, the result is true. If $f_k < n < f_{k+1}$, then $0 < n - f_k < f_{k+1} - f_k = f_{k-1}$. By

induction, $n-f_k$ is a sum of distinct Fibonacci numbers, $n-f_k = f_{k_1}+f_{k_2}+\cdots+f_{k_r}$. So, $n = f_k + f_{k_1} + f_{k_2} + \cdots + f_{k_r}$ is a sum of distinct Fibonacci numbers.

A1.33. For $n = 1$, Formula (1.55) is true. Define $\lambda = (1+\sqrt{5})/2$, assume Formula (1.55) to be true for all $m < n$ and prove it for n. We have $f_n = f_{n-1} + f_{n-2} \geq \lambda^{n-3} + \lambda^{n-4} = \lambda^{n-4}(\lambda+1) = \lambda^{n-4}\lambda^2 = \lambda^{n-2}$.

A1.34. The result is obtained by summing the following relations:

$$\begin{aligned} f_1 &= f_2, \\ f_3 &= f_4 - f_2, \\ f_5 &= f_6 - f_4, \\ &\vdots \\ f_{2n-1} &= f_{2n} - f_{2(n-1)}. \end{aligned}$$

A1.36. We know that there are q', r' such that $a = q'b + r'$, with $0 \leq r' < |b|$. If $r' \leq |b|/2$, set $q = q'$, $r = r'$. If not, set $q = q' + |b|/b$ and $r = r' - |b|$ and verify that $a = qb + r$. As we are assuming $r' > |b|/2$, we have $0 > r > |b|/2 - |b| = -|b|/2$. The task of verifying the uniqueness is left to the reader.

A1.37. Let $d = \mathrm{GCD}(b, c)$. Then $d \mid b$ and $d \mid c$, so $d \mid a$. But then d, which divides both a and b, must be invertible.

A1.38. Using Bézout's identity, verify that b divides 1 and is so invertible.

A1.39. The subset S is not empty (why?), so it has a least element d by the well-ordering principle.

A1.41. Let $(\bar{x}, \bar{y})$ be an integer solution of (1.18). Let (x_0, y_0) be a solution of $ax + by = 0$, that is, a pair such that $ax_0 + by_0 = 0$. Then $(\bar{x} + x_0, \bar{y} + y_0)$ is a solution of (1.18). Indeed,

$$a(\bar{x} + x_0) + b(\bar{y} + y_0) = a\bar{x} + b\bar{y} + ax_0 + by_0 = c + 0 = c.$$

Vice versa, let $(\bar{x}, \bar{y})$ and (x', y') be two solutions of (1.18). Then

$$a(\bar{x} - x') + b(\bar{y} - y') = a\bar{x} + b\bar{y} - ax' - by' = c - c = 0,$$

so (x', y') differs from $(\bar{x}, \bar{y})$ by a solution of the associate homogeneous equation $ax + by = 0$.

A1.42. Notice that q represents the largest integer such that $q \cdot 365$ is not greater than a, so q is the integer number 338. To determine r, it suffices to observe that $r = a - bq$, so

$$r = 123456 - 338 \cdot 365 = 86.$$

A1.44. If both d and d' are greatest common divisors of a and b, we have $d \mid d'$ and $d' \mid d$. So d and d' are associate. On the other hand, if $d = \mathrm{GCD}(a, b)$ and if d' is associate to d, then $d' \mid a$ and $d' \mid b$ and moreover $d' \mid d$, which implies that $d' = \mathrm{GCD}(a, b)$.

A1.46. Notice that $(x) = (y)$ if and only if $x \mid y$ and $y \mid x$.

A1.51. It suffices to prove that it has no zero-divisors. Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{j=0}^{m} b_j x^j$ be two *non-zero* polynomials (so they have at least one non-zero coefficient). Assume that $\partial p(x) = n$ and $\partial q(x) = m$; this means that $a_n \neq 0$ and $b_m \neq 0$. From the definition of product polynomial $p(x)q(x)$, it follows that the coefficient of x^{m+n} is $a_n b_m$, which is different from zero because a_n and b_m are different from zero and are elements of an integral domain, in which there are no zero-divisors. So $p(x)q(x)$ cannot be the zero polynomial.

A1.54. By the factor theorem, $g(x) = (f(c) - f(x))/(f(c) \cdot (x - c))$ is a polynomial, as $f(c) - f(x)$ is divisible by $x - c$. Verify that $g(x)$ has degree less than t and that $(x-c)\cdot g(x)-1$ is divisible by $f(x)$. This proves the existence. As for the uniqueness, notice that, if $h(x)$ is another polynomial of degree less than t such that $(x-c)\cdot h(x)$ is divisible by $f(x)$, then $(x - c) \cdot (g(x) - h(x))$ is divisible by $f(x)$ too. As $f(x)$ is relatively prime with $x - c$, $f(x)$ should divide $g(x) - h(x)$. The polynomials $g(x)$ and $h(x)$ having both degree less than t, the same holds for $g(x) - h(x)$, so the only possibility is $g(x) - h(x) = 0$. This proves the uniqueness.

A1.55. Proceed by induction on n. If $n = 0$, then $f(x)$ is a non-zero constant, which has no roots, so the thesis is trivial and the basis of induction is proved. Suppose then the thesis is true for every polynomial of degree less than n. Let $f(x)$ be a polynomial of degree n. If $f(x)$ has no roots, the thesis is trivial. If $f(x)$ has a root α, then by the factor theorem we have $f(x) = (x - \alpha)q(x)$, where $q(x)$ has degree $n - 1$. Moreover, the set of roots of $f(x)$ consists exactly of α and of the roots of $q(x)$, which by the inductive hypothesis are at most $n - 1$, so $f(x)$ has at most n roots.

A1.56. Proceed by induction on n. The basis of induction is obvious, because a linear polynomial has exactly a root. Let $n > 1$. If we denote by $\alpha_1 \in \mathbb{C}$ a root of $f(x)$ (which is sure to exist, by the Fundamental theorem of algebra) the factor theorem implies that

$$f(x) = (x - \alpha_1)q(x)$$

where $q(x)$ still has coefficients in $\mathbb{C}$ and $\partial q(x) = n - 1$. So, by the inductive hypothesis, $q(x)$ has exactly $n - 1$ roots $\alpha_2, \ldots, \alpha_n$ and by the factor theorem we have

$$q(x) = a(x - \alpha_2) \cdots (x - \alpha_n),$$

so $f(x)$ has exactly n solutions and

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

A1.57. Let $f(x) = \sum_{k=0}^{n} a_k x^k$. Then

$$0 = f(\alpha) = \sum_{k=0}^{n} a_k \alpha^k;$$

hence, by conjugating both sides, and observing that real numbers are self-conjugate,

$$0 = \bar{0} = \overline{f(\alpha)} = \overline{\sum_{k=0,n} a_k \alpha^k} = \sum_{k=0}^{n} a_k \bar{\alpha}^k = f(\bar{\alpha}),$$

that is, $\bar{\alpha}$ is also a root of $f(x)$.

A1.59. Keeping in mind the linearity of the derivative, it suffices to observe that Leibniz's law holds for monomials.

A1.64. Assume by contradiction that there is a $d > 1$ that divides f_n and f_{n+1}. Then it also divides $f_{n-1} = f_{n+1} - f_n$. Going backwards, we shall find that d divide $f_2 = 1$, which is impossible.

A1.65. Prove first that, if $m = nq + r$, then $\mathrm{GCD}(f_m, f_n) = \mathrm{GCD}(f_n, f_r)$. We have the following chain of equalities:

$$\mathrm{GCD}(f_m, f_n) = \mathrm{GCD}(f_{nq+r}, f_n) = \mathrm{GCD}(f_r f_{nq-1} + f_{r+1} f_{nq}, f_n),$$

where the last equality follows from (1.54). Now, f_{nq} is a multiple of f_n, so

$$\mathrm{GCD}(f_r f_{nq-1} + f_{r+1} f_{nq}, f_n) = \mathrm{GCD}(f_r f_{nq-1}, f_n).$$

If we prove that $\mathrm{GCD}(f_{nq-1}, f_n) = 1$, we may conclude that $\mathrm{GCD}(f_r f_{nq-1}, f_n) = \mathrm{GCD}(f_r, f_n)$, which was what had to be proved. Let $\mathrm{GCD}(f_{nq-1}, f_n) = d$: then $d \mid f_n$ (so, also, f_{qn}) and f_{qn-1}. As it divides two consecutive Fibonacci numbers, it must be $d = 1$.

Having this result, the fact that $\mathrm{GCD}(f_n, f_m) = f_d$, with $d = \mathrm{GCD}(n, m)$, is immediate. Indeed, applying the Euclidean algorithm starting with m and n, and denoting by r_t the last non-zero remainder (which is so $\mathrm{GCD}(m, n)$), we find

$$\mathrm{GCD}(f_m, f_n) = \mathrm{GCD}(f_{r_1}, f_n) = \ldots = \mathrm{GCD}(f_{r_{t-1}}, f_{r_t}) = f_{r_t},$$

the last equality holding because, as r_t divides r_{t-1}, then (by the above) f_{r_t} divides $f_{r_{t-1}}$.

A1.66. It has already been proved in Exercise A1.30 that, if $n \mid m$, then $f_n \mid f_m$. We have now to prove the converse, that is to say, $f_n \mid f_m$ implies that $n \mid m$. Let $f_n \mid f_m$. Then $\mathrm{GCD}(f_n, f_m) = f_n$. But, by Exercise A1.65, $\mathrm{GCD}(f_n, f_m) = f_d$, with $d = \mathrm{GCD}(n, m)$. So $d = n$, and if $\mathrm{GCD}(n, m) = n$, this means that $n \mid m$.

A1.67. The correct answer is (b). Indeed, for $n \geq 1$, we have the relation

$$\frac{f_{n+1}}{f_n} = 1 + \frac{f_{n-1}}{f_n},$$

so, setting $x = \lim_{n\to\infty} f_{n+1}/f_n$, we have

$$x = 1 + \frac{1}{x}.$$

A1.68. For $k = 0$, $r_n = 0 = f_0 = 0$, so the basis of induction is verified. Assume the inequality to be verified for every m such that $0 \leq m < k$ and prove it for k. From

$$r_{n-k} = r_{n-k+1} q_{n-k+2} + r_{n-k+2},$$

as the inductive hypothesis is $r_{n-k+1} \geq f_{k-1}$ and $r_{n-k+2} \geq f_{k-2}$, and as we have further $q_{n-k+2} \geq 1$, we get

$$r_{n-k} \geq f_{k-1} + f_{k-2} = f_k.$$

A1.69. If a and b ($a \geq b$) are two integers such that $D(a,b) \geq n$, this means that the last non-zero remainder is $\geq r_{n-1}$, so, using the result of the previous exercise, we have $r_{n-k} \geq f_k$. In particular, $b = r_0 \geq f_n$. So, if $b < f_n$, then certainly $D(a,b) < n$ must be true.

A1.74. If $\alpha = [a_0; a_1, \ldots, a_n, \ldots]$, with a_0 positive integer, we have $1/\alpha = [1; a_0, a_1, \ldots, a_n, \ldots]$.

A1.75. Proceed by induction, observing that $C_k = [a_0; a_1, \ldots, a_{k-1}, a_k + 1/a_{k+1}]$, so

$$C_k = \frac{\left(a_k + \dfrac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \dfrac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}}.$$

A1.76. From formula (1.43) we get

$$C_k - C_{k-2} = \frac{(-1)^k (q_k - q_{k-2})}{q_k q_{k-1} q_{k-2}}.$$

Hence, conclude by using (1.41).

A1.78. The first two claims follow from formula (1.44). The third one follows from formula (1.43).

A1.80. Let $\sqrt{n} \in \mathbb{Q}$, so $\sqrt{n} = p/q$, with p/q a reduced fraction. Then we have $p^2 = nq^2$. By applying Corollary 1.3.9 we see that $p \mid n$. Deduce that $q \mid p$. By applying Exercise A1.38 deduce that $q = \pm 1$ and consequently that n is a square.

A1.84. Keep in mind that $a/b = C_n$ and use formula (2.11).

A1.86. Prove that

$$|\alpha - C_{n+1}| + |\alpha - C_n| = |C_{n+1} - C_n| = \frac{1}{q_n q_{n+1}}$$

and conclude from here.

A1.89. We may write $\alpha = (a + \sqrt{b})/c$ with integers a, b, c, $b > 0$ and $c \neq 0$. So $\alpha = (a|c| + \sqrt{bc^2})/(c|c|)$. Set $p = a|c|, q = c|c|, d = bc^2$ and conclude.

B1.1. The correct answer is (d); indeed, $n < 2^n$ for all $n \in \mathbb{N}$. The basis of induction is true because $0 < 2^0 = 1$. Suppose $n < 2^n$ for a natural number n. Then $n + 1 < 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$, where the inequality $\leq$ follows from the fact that $1 \leq 2^n$ for all $n \in \mathbb{N}$.

B1.2. The correct answer is (a); indeed $S(n)$ may be obtained from $S(n-1)$ by adding to it the nth odd natural number, that is, $2n - 1$.

B1.3. The correct answer is (c). The basis of induction is obvious. Suppose the formula holds for $n-1$. From Exercise B1.2 we know that $S(n) = S(n-1) + 2n - 1$, so from the inductive hypothesis we find that $S(n) = (n-1)^2 + 2n - 1 = n^2$.

B1.6. The correct answer is (b), that is,

$$\sum_{k=0}^{n} (4k + 1) = (2n + 1)(n + 1). \tag{1}$$

For $n = 0$ formula (1) becomes $1 = 1$, so the basis of induction is true. Suppose (1) is true for n and prove it for $n + 1$:

$$\sum_{k=0}^{n+1}(4k+1) = 4(n+1) + 1 + \sum_{k=0}^{n}(4k+1) = \text{(by the induct. hyp.)}$$
$$= 4n + 5 + (2n+1)(n+1) = (2n+3)(n+2).$$

B1.7. The correct answer is (c), that is

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{2}$$

The basis of induction is obvious, because for $n = 1$ the equation (2) becomes $1 = 1$. Suppose (2) is true for n and prove it for $n + 1$:

$$\sum_{k=1}^{n+1} k^2 = (n+1)^2 + \sum_{k=1}^{n} k^2 = \text{(by the induct. hyp.)}$$
$$= (n+1)^2 + \frac{n(n+1)(2n+1)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}.$$

B1.8. The correct answer is (a). Verify it by induction.

B1.9. The correct answer is (c). The basis of induction is trivial. Assume (c) to be true for $n - 1$ and prove it for n:

$$\sum_{k=1}^{n}(2k)^3 = (2n)^3 + \sum_{k=1}^{n-1}(2k)^3 = (2n)^3 + 2(n-1)^2 n^2 =$$
$$= 2n^2[(n-1)^2 + 4n] = 2n^2(n+1)^2.$$

B1.10. The correct answer is (a). The basis of induction is trivial. Assume the result to be true for $n - 1$. Then $\sum_{k=0}^{n} 2 \cdot 3^k = 2 \cdot 3^n + (3^n - 1) = 3^{n+1} - 1$.

B1.11. The correct answer is (b).

B1.14. The correct answer is (a).

B1.15. The correct answer is (b).

B1.16. The correct answer is (c), because $(103/100)^{24}$ is about 2, so there will be about $2 \cdot 5 = 10$ billion people.

B1.17. Define $\lambda_1 = (-1 + i\sqrt{3})/2$ and $\lambda_2 = (-1 - i\sqrt{3})/2$. With the usual method the eigenvectors relative to λ_1, λ_2 and 1, respectively, are found:

$$\left(2\lambda_1, 1, \frac{\lambda_2}{3}\right), \qquad \left(2\lambda_2, 1, \frac{\lambda_1}{3}\right), \qquad (6, 3, 1).$$

Define next

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 2\lambda_1 & 2\lambda_2 & 6 \\ 1 & 1 & 3 \\ \lambda_2/3 & \lambda_1/3 & 1 \end{pmatrix}.$$

The inverse of C is

$$C^{-1} = \frac{1}{3}\begin{pmatrix} \lambda_2/2 & 1 & 3\lambda_1 \\ \lambda_1/2 & 1 & 3\lambda_2 \\ 1/6 & 1/3 & 1 \end{pmatrix}.$$

We have $A = C{\cdot}D{\cdot}C^{-1}$, so a closed formula is found by multiplying $A^n = C{\cdot}D^n{\cdot}C^{-1}$ for X_0.

B1.18. The correct answer is (a), as can be verified directly, without using the closed formula found in Exercise B1.17. Indeed, after one year there will be 120 newborn beetles and 60 one-year beetles (180 altogether). After two years there will be 60 one-year ones and 20 two-year ones (80 altogether), while after three years there will be 120 newborn ones and 20 two-year ones (140 altogether), exactly as in the starting year. So the same situation repeats every third year; hence the result follows.

B1.19. Two eigenvectors corresponding to 1 and 7/10, respectively, are $(2, 1)$ and $(-1, 1)$. Set

$$C = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}, \qquad \text{quindi} \quad C^{-1} = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}.$$

So we may compute

$$A^n = C \cdot \begin{pmatrix} 1 & 0 \\ 0 & (7/10)^n \end{pmatrix} \cdot C^{-1} = \frac{1}{3}\begin{pmatrix} 2+(7/10)^n & 2-2(7/10)^n \\ 1-(7/10)^n & 1+2(7/10)^n \end{pmatrix};$$

hance it is possible to compute X_n multiplying by X_0.

B1.20. The correct answer is (d), because there will be 5 million inhabitants, as may also be directly verified, without applying the formula found in Exercise B1.19.

B1.21. The correct answer is (c). Let $S(n)$ be the number sought. We have $S(1) = 2$. Moreover, given n lines in general position, forming $S(n)$ regions, one more line, in general position with respect to the other ones, intersects them in n points, so meets $n+1$ regions, dividing each into two parts. The number of regions, with those added after the $(n+1)$th line increases by $n+1$. So we have $S(n+1) - S(n) = n+1$. From here it is easy to conclude.

B1.22. The correct answer is (d). Reasoning as in the previous exercise, prove that the right answer is $n^2 - n + 2$.

B1.23. By induction on the number n of all lines. If $n = 1$, clearly two colours suffice. Suppose then we have proved that it is possible to colour with just two colours the regions formed by less than n lines, and prove it in the case in which the nth line, r, is added. Divide the regions into two groups, depending on which side of r they are on. Then it suffices to leave the colour of those on one side as it was, and to change the colour of those on the other side. We have to verify that this is a "good" colouring: indeed, if two bordering regions are on the same side with respect to r, they will have different colours (they had different colours before the appearance of r, and now, either they both keep their colours or the colours are changed in both, but in any case will be different). If the two regions are on different sides with respect to r, their colours are different because one of them has had its colour changed.

B1.24. The correct answer is (a), because every third month Mark gets a 1% interest, which so becomes 4,060401% yearly.

B1.28. The correct answer is (a). Indeed, the roots of the characteristic equation of the recurrence relation are 2 and -1. So the solution has the form $c_1 2^n + c_2(-1)^n$, where c_1 and c_2 are determined by the initial values $a_0 = 2 = c_1 + c_2$ and $a_1 = 7 = 2c_1 - c_2$.

B1.29. The correct answer is (a). Indeed, a solution is found to be of the form $-n - 7$.

B1.32. The correct answer is (a).

B1.33. The correct answer is (c).

B1.34. The correct answer is (a). Indeed, $491 = 2 \cdot 245 + 1$ and $245 = 245 \cdot 1 + 0$.

B1.35. The correct answer is (b), because the Euclidean algorithm ends after just two steps, as shown in the solution of Exercise B1.34.

B1.37. We have $34567 = 457 \cdot 76 - 165$, then $457 = (-165)(-3) - 38$, after which $-165 = (-38) \cdot 4 - 13$, then $-38 = (-13) \cdot 3 + 1$ and finally $-13 = 1 \cdot (-13) + 0$.

B1.38. The correct answer is (a).

B1.39. The correct answer is (c). Indeed $28762 = 18 \cdot 1515 + 1492$, then $1515 = 1492 + 23$, hence $1492 = 64 \cdot 23 + 20$, then $23 = 20 + 3$, $20 = 6 \cdot 3 + 2$, $3 = 2 + 1$ and finally $2 = 2 \cdot 1 + 0$.

B1.40. The correct answer is (c), as the solution of Exercise B1.39 shows.

B1.42. The correct answer is (b). There are integer solutions because $\mathrm{GCD}(92, 18) = 4$ and 4 divides 180. Using the Euclidean algorithm to find the GCD it is possible to find Bézout's identity

$$4 = 92 \cdot (-3) + 28 \cdot 10;$$

hence

$$180 = 45 \cdot 4 = 92 \cdot (-135) + 28 \cdot 450$$

so a solution is $(\bar{x}, \bar{y}) = (-135, 450)$. To find *all* solutions, consider the associate homogeneous equation:

$$0 = 92x + 28y = 4(23x + 7y).$$

It admits as its solutions the pairs $(x_0, y_0) = (-7t, 23t)$, with t ranging in $\mathbb{Z}$. So all the solutions of $92x + 28y = 180$ are the pairs

$$(x, y) = (-135 - 7t, 450 + 23t), \qquad \text{for all } t \in \mathbb{Z}.$$

B1.43. The correct answer is (a); indeed, there are no integer solutions because $\mathrm{GCD}(482, 20) = 2 \nmid 35$.

B1.47. The correct answer is (c), as the leading coefficient, that is to say, the coefficient of the highest degree term, is $-3 \neq 1$.

B1.48. The correct answer is (b).

B1.49. The correct answer is (d), because $-x-1$ is only *a* greatest common divisor, but *the* greatest common divisor of the two polynomials is $x+1$.

B1.51. The correct answer is (b).

B1.52. The correct answer is (d), because the greatest common divisor of these polynomials is $x+1$ (see Exercise B1.49), and if $h(x)$, $k(x)$ are the polynomials appearing in Bézout's identity, then $f(x) = 4h(x)$ and $g(x) = 4k(x)$.

B1.53. The correct answer is $-25x^4 - 8x^3 + 9x^2$, hence (d).

B1.55. The greatest common divisor is $1+i$.

B1.56. In base 10, the two factors of the multiplication are 29 and 13, while the result is 377, so the operation is correct.

B1.59. The correct answer is (a).

B1.60. The correct answer is (a).

B1.61. The correct answer is (c).

B1.62. The correct answer is (d), because the sum is 10110100, while the product is 1000100011011.

B1.63. The correct answer is (c).

B1.64. The correct answer is (b).

B1.65. The correct answer is (c).

B1.66. $40/99$.

B1.67. $2491/45$.

B1.68. $101/111$.

B1.69. $10001001/11000$.

B1.70. $40/66 = 10/15$.

B1.71. $10342/60 = 3521/30$.

B1.72. $2, \overline{3}$.

B1.73. $4, \overline{1254}$.

B1.74. $11, \overline{10}$.

B1.75. The correct answer is (d), because the continued fraction is $[1; 3, 1, 10, 2]$.

B1.76. The correct answer is (a).

B1.77. The correct answer is (d), because the continued fraction is $[1; 1, 1, 1, 13, 2, 2]$, which consists of 7 terms.

B1.81. The continued fraction of α may be written as follows:

$$\alpha = 4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{\alpha}}}.$$

Developing fractions, we get the equation

$$\alpha = \frac{19\alpha + 5}{4\alpha + 1}$$

which is equivalent to the second degree equation $4\alpha^2 - 18\alpha - 5 = 0$, so

$$\alpha = \frac{9 + \sqrt{101}}{4}.$$

B1.82. The correct answer is (d), because the continued fraction is $[5; \overline{5, 10}]$.

Exercises of Chapter 2

A2.1. By hypothesis we have $f(x) \leq k_1 g(x)$ for $x > c_1$ and $g(x) \leq k_2 h(x)$ for $x > c_2$. Then, having set $c_3 = \max\{c_1, c_2\}$, we find that

$$f(x) \leq k_1 g(x) \leq k_1 k_2 h(x) = k_3 h(x)$$

for $x > c_3$, where $k_3 = k_1 k_2$.

A2.5. For n even, we have that $f(n)/g(n) = 2n+1$ and so $\lim_{m\to\infty} f(2m)/g(2m) = \infty$. On the other hand, for n odd we have $f(n)/g(n) = 1/(2n+1)$, so $\lim_{m\to\infty} f(2m+1)/g(2m+1) = 0$. It can be found analogously that $\lim_{m\to\infty} g(2m)/f(2m) = 0$ and $\lim_{m\to\infty} g(2m+1)/f(2m+1) = \infty$. So we deduce that those limits do no exist.

A2.8. The correct answer is (c).

A2.9. The correct answer is (a). Indeed, by observing that all factors of $n!$ have length less than or equal to $L(n)$ and using the previous exercise, we conclude that

$$L(n!) \leq nL(n) \in \mathcal{O}(n \ln n) = \mathcal{O}(nk).$$

Notice that this estimate can be improved, as many factors of $n!$ have length less than the length of n.

A2.10. None of (a), (b), (c) is a reasonable estimate. Indeed, $\binom{n}{m}$ is the ratio of the two numbers $n(n-1)\cdots(n-m+1)$ and $m!$ having length $\mathcal{O}(mh)$ and $\mathcal{O}(mk)$, respectively. So the length of $\binom{n}{m}$ is $\mathcal{O}(mh - mk)$, so it is $\mathcal{O}(mh)$ as well.

A2.15. Let a/b be the number being considered. We may assume $a > b$. Developing a/b as a continued fraction is equivalent to searching $\mathrm{GCD}(a, b)$, which requires $\mathcal{O}(\log^3 a)$ bit operations.

A2.16. We have to verify the relation

$$p(x) = (x - \alpha)(p_n x^{n-1} + p_1(\alpha)x^{n-2} + \cdots + p_{n-2}(\alpha)x + p_{n-1}(\alpha)) + p(\alpha),$$

which can be easily done keeping in mind Table (2.14) and the meaning of its second row.

A2.18. Every $n \times n$ matrix has n^2 entries. We have to carry out n multiplications and n additions for each of them: so, in all, n^3 multiplications and n^3 additions are to be carried out. So the algorithm has complexity $\mathcal{O}(n^3(\log^2 m + \log n))$.

A2.20. See [13], Cap. 24, §1.

A2.21. Apply first Exercise A2.20 to reduce the matrices in row echelon form and notice that the determinant of the matrix is the product of the *pivot elements* (see [13], Cap. 8).

A2.22. Hint: use Gaussian algorithm to compute the inverse (see [13], pag. 146).

A2.23. The correct answer is (c). Indeed, to compute $n!$ we have to carry out successively n multiplications of two integers whose length can be estimated with that of n (which is k) and with that of $n!$ (which is nk).

A2.24. A reasonable estimate is $\mathcal{O}(m^2 \log^2 n)$. Keep in mind what was said in the solution to Exercise A2.10.

A2.25. A reasonable estimate is $\mathcal{O}(n^2 \log^2 m)$. Indeed, the length of m^n is $\mathcal{O}(n \log m)$ and to compute m^n it is necessary to carry out n multiplications of two integers whose length can be estimated with that of m (which is $\mathcal{O}(\log m)$) and with that of m^n (which is $\mathcal{O}(n \log m)$).

B2.1. The correct answer is (b). In fact, (a) is an estimate of the complexity of $f(n)$ too, but one which is worse than (b).

B2.2. The correct answer is (d); indeed, $\log n$ is negligible with respect to n

B2.7. The correct answer is (c).

B2.13. The correct answer is (b).

B2.14. The correct answer is (b).

B2.17. The correct answer is (c).

B2.19. The correct answer is (b).

B2.21. The correct answer is (c). Each squaring requires at most $\mathcal{O}(\log^2 n)$ bit operations, and it is necessary to carry out n of them, so obtaining the estimate $\mathcal{O}(n \log^2 n)$. The computation time of additions is negligible with respect to this one.

B2.22. The correct answer is (c).

B2.23. The correct answer is (c).

B2.24. The correct answer is (a); indeed, $1176 = 159 \cdot 7 + 63$, $159 = 63 \cdot 3 - 30$, $63 = -30 \cdot (-2) + 3$ and $-30 = 3 \cdot (-10) + 0$.

Exercises of Chapter 3

A3.1. For every integer a, $a - a = 0$ is a multiple of n for any n, so $a \equiv a \pmod{n}$, that is to say, congruence modulo n is a reflexive relation. We prove next that this relation is symmetric. If $a \equiv b \pmod{n}$, this means that $a - b = hn$, for some $h \in \mathbb{Z}$; hence follows that $b - a = -(a - b) = -(hn) = (-h)n$, which proves that $b \equiv a \pmod{n}$. Finally, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, this means that $a - b = hn$ and $b - c = kn$ with $h, k \in \mathbb{Z}$, so $a - c = (a - b) + (b - c) = hn + kn = (h + k)n$,

which implies that $a \equiv c \pmod{n}$. So we have proved that congruence relation is transitive too, for all n, so it is an equivalence relation.

A3.2. Let $A = \{a, b, c\}$ be a set consisting of three distinct elements. Consider the relation R on A defined as follows: $R = \{(a,a), (b,b), (c,c), (a,b), (b,a), (b,c), (c,b)\}$. Clearly, R is reflexive and symmetric, but is not transitive as $a\,R\,b$ and $b\,R\,c$, while it is not true that $a\,R\,c$, so R is an example of a). Consider now $R' = \{(a,a), (b,b), (c,c), (a,b)\}$ over the same A. Clearly, R' is reflexive and transitive but not symmetric, because $a\,R'\,b$ but it is not true that $b\,R'\,a$. Other examples of relations of type b) are order relations on sets with at least two distinct elements. Finally, consider the set B of the students in a same secondary school form, and let the relation R'' be defined on B as follows: $a\,R''\,b$ if and only if a and b got the same mark in the first maths test this year. The relation R'' is clearly symmetric and transitive, but is not necessarily reflexive, as some student might have been absent the day of the test. Clearly the relation R'' is an equivalence relation if we do not take it on the whole set B, but only on the subset of B consisting of the students who actually took the test.

A3.3. It is the relation *being a divisor of*, which we have denoted by $|$, that is, $a\,R\,b$ if and only if $a \mid b$. Clearly, $a = 1 \cdot a$ for all $a \in \mathbb{N}$, so $a \mid a$ and $|$ is a reflexive relation. Moreover, it is transitive, because if $a \mid b$ and $b \mid c$, then $b = ah$ and $c = bj$, so $c = a(jh)$, that is $a \mid c$. Suppose now $a \mid b$ and $b \mid a$ for two natural numbers a and b. Then there exist $h, k \in \mathbb{N}$ such that $a = bh$ and $b = ak$, so $a = a(hk)$ and, cancelling out a, we find $hk = 1$, which in $\mathbb{N}$ implies that $h = k = 1$, that is $a = b$ and $|$ is antisymmetric. So we have shown that $|$ is an order relation in $\mathbb{N}$. In $\mathbb{Z}$, on the other hand, we cannot conclude from $hk = 1$ that $h = k = 1$, because we might also have $h = k = -1$, so $|$ is not antisymmetric (nor an order relation) in $\mathbb{Z}$.

A3.11. If $ac = bc$ with $c \neq 0$, then $(a - b)c = 0$. In an integral domain (and in particular in $\mathbb{Z}$) there are no zero-divisors, so $a - b = 0$, that is $a = b$.

A3.14. The correct answer is (b). Indeed, a finite commutative ring with unity is a field if and only if it is an integral domain (see Exercise A1.48).

A3.15. The correct answer is (a).

A3.17. Consider the coefficients of the two polynomials as numbers in $\{0, \ldots, n\}$, so they have length bounded by the length of n. To sum the two polynomials we need at most $m + 1$ sums of such numbers and then reducing modulo n. But as the coefficients so obtained are bounded by $2n$, to reduce them modulo n it suffices to carry out at most one subtraction. From this it is possible to deduce the claim.

A3.18. Consider the coefficients of the two polynomials as numbers in $\{0, \ldots, n\}$, so they have length bounded by the length of n. By applying Proposition 2.5.9, verify that the product of the two polynomials has complexity $\mathcal{O}(m^2 \log^2 n)$. As the coefficients of the polynomial so obtained have to be reduced modulo n, from this it is possible to deduce the claim.

A3.19. It suffices to recall that a number is congruent modulo 11 to the sum of its decimal digits, taken with alternate signs, starting from the rightmost one. Then proceed as when casting out nines.

A3.24. If G is cyclic with generator x, there is a surjective homomorphism $n \in \mathbb{Z} \to x^n \in G$. If G is infinite, this is an isomorphism. If not, G is a quotient of $\mathbb{Z}$.

A3.25. If G is cyclic with generator x and if H is a non-trivial subgroup, let n be the smallest positive integer such that $x^n \in H$. Using the division algorithm, prove that x^n is a generator of H.

A3.27. Suppose m divides n. Then $n = mk$ for some integer k, so $x^n = (x^m)^k = 1^k = 1$. Vice versa, suppose $x^n = 1$. We may write $n = qm + r$, with $0 \leq r < m$. So $1 = x^n = (x^m)^q x^r = x^r$. Then, by definition of order we have $r = 0$, or else the order of x would be $r < m$. So $m \mid n$.

A3.28. The powers $x, x^2, \ldots, x^m$ are all different by definition of order. Apply now the same reasoning as in the previous exercise to show that every other power is equal to one of these.

A3.30. Let $\mathrm{GCD}(m, n) = 1$. For all $k \in Z$, there is an h such that $hm \equiv k \pmod{n}$. Then $(x^m)^h = x^k$, so x^m is a generator. Vice versa, if x^m is a generator, there is an integer h such that $(x^m)^h = x$. Then $hm \equiv 1 \pmod{n}$, which implies $\mathrm{GCD}(m, n) = 1$.

A3.32. Let $n = dm$. Then $\langle x^m \rangle$ has order d. Vice versa, if H is a subgroup of order d of G, we have $n = dm$ by Lagrange's theorem. We have seen that a generator of H is given by x^h with h the smallest positive integer such that $x^h \in H$ (see Exercise A3.25). As $(x^h)^d = 1$, we have a relation of the form $dh = nk$. Dividing by d we have $h = mk$. So $x^h = (x^m)^k \in \langle x^m \rangle$; hence, $H \subset \langle x^m \rangle$. As $\langle x^m \rangle$ has order d, we have $H = \langle x^m \rangle$ (and $k = 1$).

A3.33. Hint: the element x^h has order d if and only if it is a generator of the subgroup $\langle x^m \rangle$.

A3.34. Hint: the relation $y_1^m = y_2$ is equivalent to the congruence equation $mn_1 \equiv n_2 \pmod{n}$.

A3.36. Define in G the relation R_H as follows: xR_Hy if and only if $xy^{-1} \in H$. Verify that this is an equivalence relation. Verify that the equivalence class of an element x is the set denoted by Hx and called *right coset* of H, consisting of all the elements of the form tx with $t \in H$. Prove that Hx has the same number of elements as H. Conclude that the order of G is equal to the order of H times the order of the quotient set of G with respect to the relation R_H.

A3.37. We know that $\varphi(n)$ is the order of the finite group $U(\mathbb{Z}_n)$. Let m be the period of an element a of $U(\mathbb{Z}_n)$. Then m divides $\varphi(n)$, so $a^{\varphi(n)} = e$ (see Exercise A3.27).

A3.38. In the situation described, it suffices to divide m by $\varphi(n)$, that is, $m = q\varphi(n) + r$, so $a^m \equiv a^r \pmod{n}$, then compute $a^r \pmod{n}$.

B3.1. The correct answer is (c).

B3.2. The correct answer is (a).

B3.3. The correct answer is (c): the zero-divisors are classes [2], [3], [4].

B3.4. The correct answer is (a) as 19 is a prime number. The reader might want to verify explicitly the absence of zero-divisors.

B3.5. The correct answer is (b) as 27 is not a prime number. For instance, class [3] is a zero-divisor in $\mathbb{Z}_{27}$.

B3.6. We have $725843 \equiv 3 \pmod{10}$, so

$$(725843)^{594} \equiv 3^{594} \pmod{10}.$$

Moreover,

$$3^{594} = 3^{4\cdot 148+2} = (3^4)^{148} \cdot 3^2 \equiv 1^{148} \cdot 3^2 = 9 \pmod{10}.$$

So the last digit is 9.

B3.7. As $74 \equiv 2 \pmod 9$, then $74^{6h} \equiv 2^{6h} \pmod 9$. Moreover, $2^{6h} = (2^6)^h$ and $2^6 \equiv 1 \pmod 9$, so, for all $h \in \mathbb{N}$, we find that $74^{6h} \equiv 1^h \equiv 1 \pmod 9$ and the required congruence class is 1.

B3.8. We have $43816 \equiv 6 \pmod{10}$, and further $6^2 \equiv 6 \pmod{10}$. Then, $6^k \equiv 6 \pmod{10}$ for all $k > 0$; it follows that

$$43816^{20321} \equiv 6 \pmod{10}.$$

B3.9. We have $29345 \equiv 5 \pmod 6$. Moreover, $5^2 = 25 \equiv 1 \pmod 6$, so

$$29345^{362971} \equiv 5^{362971} = (5^2)^{181485} \cdot 5^1 \equiv 1 \cdot 5 \equiv 5 \pmod 6.$$

B3.10. We have $362971 \equiv 1 \pmod 6$, so $362971^{29345} \equiv 1 \pmod 6$.

B3.11. In class 1 modulo 9.

B3.16. The correct answer is (c).

B3.17. The correct answer is (a), as 4 is not relatively prime with 18.

B3.18. 39.

B3.23. As $9 \equiv 0 \pmod 3$, we have that 3 divides an integer n written in base 9 if and only if 3 divides the last digit of n.

B3.24. The correct answer is (a). Let us see why. First of all, $5 \bmod 4 = 1$, so the congruence given is equivalent to $3x \equiv 1 \pmod 4$. By Corollary 3.3.6, the congruence has exactly one solution modulo 4. Moreover, the solution is the inverse of 3 modulo 4, by the very definition of inverse. In order to find this inverse we may either proceed by trial and error, or with Bézout's identity, that is to say, computing the numbers α and β such that $3\alpha + 4\beta = 1 = \mathrm{GCD}(3, 4)$ using the Euclidean algorithm (see formula (1.14) on page 17 foll.). Indeed, from Bézout's identity it follows that α is the inverse of 3 modulo 4. In our case, we find $\alpha = -1 \equiv 3 \pmod 4$ and $\beta = 1$. So we conclude that the only solution modulo 4 of the congruence is 3.

B3.25. The correct answer is (b). Indeed, by Proposition 3.1.8 the congruence is found to be equivalent (by dividing all coefficients by 3) to $x \equiv 3 \equiv 1 \pmod 2$.

B3.26. The correct answer is (a). By Corollary 3.3.6 the congruence has exactly one solution modulo 9. We compute the inverse of 4 modulo 9, that is the solution of $4y \equiv 1 \pmod 9$. A way of finding y consists in computing Bézout's identity $4\alpha + 9\beta = 1$ using the Euclidean algorithm, finding $\alpha = 7$. Multiply both sides of the congruence by 7 we find the equivalent congruence $x \equiv 7 \cdot 7 \equiv 4 \pmod 9$. On the other hand, $4 \equiv -5 \pmod 9$.

B3.27. The correct answer is (c), by Proposition 3.3.4.

B3.28. The correct answer is (d).

B3.36. We have $190 \equiv 3 \pmod{17}$. So

$$190^{597} \equiv 3^{597} \pmod{17}.$$

As $\mathrm{GCD}(3, 17) = 1$, it follows that $3^{16} \equiv 1 \pmod{17}$ by Euler's Theorem, as $\varphi(17) = 16$ (verify this directly). So,

$$3^{597} = 3^{16 \cdot 37 + 5} = (3^{16})^{37} \cdot 3^5 \equiv 1^{37} \cdot 3^5 = 3^5 \equiv 5 \pmod{17}.$$

B3.38. As $\mathrm{GCD}(3, 7) = 1$ and $\varphi(7) = 6$, then Euler's Theorem says that $3^6 \equiv 1 \pmod{7}$, so $3^{13} = (3^6)^2 \cdot 3 \equiv 3 \pmod{7}$.

B3.39. The correct answer is (a).

B3.40. The correct answer is (c).

B3.41. The correct answer is (c).

B3.42. The correct answer is (c). Let us see why. By the Chinese remainder theorem 3.4.2, there exists exactly one solution modulo $5 \cdot 9 = 45$. The method for finding this solution is described in the proof of the theorem: with those notation we have $s = 2$, $r_1 = 5$, $r_2 = 9$, $c_1 = 3$ and $c_2 = 7$. So $R = 45$, $R_1 = 9$ and $R_2 = 5$. We have now to solve congruences $9x \equiv 3 \pmod{5}$ and $5x \equiv 7 \pmod{9}$. The only solution modulo 5 of the first one is $\bar{x}_1 = 2$, while the only solution modulo 9 of the second one is $\bar{x}_2 = 5$. So we may conclude that the solution of the congruence given is $\bar{x} = 9 \cdot 2 + 5 \cdot 5 = 43$.

B3.43. The correct answer is (d), because the system has solution $x \equiv 97 \pmod{120}$.

B3.48. It will happen on Saturday 31 March.

B3.49. There are 1786 books.

B3.53. The correct answer is (d), as may be verified by browsing any engagement diary, but we are sure the reader has applied instead the formula proved in the text, by substituting the values $g = 31$, $m = 10$ (as we are considering March as the first month of the year!), $s = 20$ and $y = 0$, because $2000 = 20 \cdot 100$, finding $x \equiv 31 + 25 - 40 + 5 = 21 \equiv 0 \pmod{7}$.

B3.54. The correct answer is (c); indeed, in this case we have $g = 28$, $m = 12$, $2003 = 20 \cdot 100 + 3$, that is, $s = 20$ and $y = 3$, because we consider February 2004 as the last month of year 2003, so $x \equiv 28 + 31 - 40 + 3 + 5 = 27 \equiv 6 \pmod{7}$.

Exercises of Chapter 4

A4.4. If $\sqrt{p} = a/b$, with a, b integers and relatively prime, then $b^2 p = a^2$. Now the irreducible factor p appears an odd number of times in the left-hand side and an even number of times in the right-hand side. This contradicts the Fundamental Theorem of Arithmetic.

A4.5. Notice that $\sum_{t=1}^{n} 1/t^s$ is the sum of the areas of n rectangles, each of width 1 and heights $1, 1/2^s, \ldots, 1/n^s$. We may assume these rectangles to be located in the cartesian plane with the bases along the x-axis, on the line segments having as endpoints the points of abscissas $1, 2, \ldots, n$ and with the heights having as endpoints $(1,1), (2,1/2^s), \ldots, (n,1/n^s)$. The graph of the function $y = 1/x^s$ is completely included in the union of these rectangles and the difference in the right-hand side of (4.2) is the area of the figure Σ between the graph and the union of the rectangles. This figure is the union of the figures $\Sigma_1, \ldots, \Sigma_n$ such that Σ_i, $i = 1, \ldots, n$, is the figure between the ith rectangle and the segment of the graph of $y = 1/x^s$ which lies above the ith interval $[i, i+1]$. For all $i = 2, \ldots, n$, translate Σ_i along the x-axis by a vector of length $i - 1$ with negative orientation. So we get a new figure Σ_i' included in the first rectangle R, which is a square of area 1. Notice that the area of Σ is equal to the area of the figure Σ', the union of $\Sigma_1, \Sigma_2', \ldots, \Sigma_n'$, which is strictly included in R.

A4.7. The prime numbers less than or equal to $\sqrt{n}$ are approximately $2\sqrt{n}/\log n$. For each of these numbers it is necessary to delete all its multiples that are less than n, so it is necessary to carry out a number of operations that may be estimated by $\log^2 n$.

A4.9. Recall that $\binom{p}{k} = p!/k!(p-k)!$, and p divides the numerator, but cannot divide the denominator, because it does not divide any of its factors.

A4.10. The binomial theorem yields

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p.$$

So we have to prove that the sum is divisible by p. But this is true, as in the sum we have both $k < p$ and $p - k < p$, so $\binom{p}{k}$ is an integer divisible by p, by Exercise A4.9.

A4.13. Let $n = pq$, where p and q are distinct primes. Then $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n + 1 - (p+q)$. Vice versa, if we know n and $\varphi(n)$, then p and q are the solutions of the second degree equation $x^2 - (n - \varphi(n) + 1)x + n$.

A4.16. Write out the factorisation of $n = p_1^{h_1} \cdots p_r^{h_r}$ di n. Then

$$\sum_{d|n} \mu(d) = \sum_{0 \le k_i \le 1, i=1,\ldots,r} \mu(p_1^{k_1} \cdots p_r^{k_r}) =$$

$$= 1 - r + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r = (1-1)^r = 0.$$

A4.17. It suffices to verify that $((f * g) * h)(n)$ and $(f * (g * h))(n)$ both coincide with $\sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)$.

A4.20. Let n, m relatively prime. We have

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \quad (f * g)(m) = \sum_{d'|m} f(d') g\left(\frac{m}{d'}\right)$$

so, by the multiplicativity of f and g,

$$((f*g)(n))((f*g)(m)) = \sum_{d|n,d'|m} f(d)f(d')g\left(\frac{n}{d}\right)g\left(\frac{m}{d'}\right) = \sum_{d|n,d'|m} f(dd')g\left(\frac{nm}{dd'}\right).$$

Hence the claim immediately follows.

A4.22. We have $\mu * E_f = \mu * (I * f) = (\mu * I) * f = \Pi * f = f$.

A4.24. Möbius inversion theorem says that $\phi = \mu * \iota$ because $E_\varphi = \iota$. So if $n = p_1^{h_1} \cdots p_r^{h_r}$, then

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{i,j=1}^{r} \frac{n}{p_i p_j} - \cdots$$

hence (4.4) may be imediately deduced.

A4.26. Apply Proposition 4.2.2. So it suffices to compute the functions ν and σ on prime numbers, for which it is trivial to compute the functions.

A4.30. Keeping in mind the proof of Proposition 4.2.3, prove that the obvious mapping $[x]_{nm} \in \mathbb{Z}_{nm} \to ([x]_n, [x]_m) \in \mathbb{Z}_n \times \mathbb{Z}_m$ induces a group isomorphism $U(\mathbb{Z}_{nm}) \to U(\mathbb{Z}_n) \times U(\mathbb{Z}_m)$. The claim immediately follows.

A4.31. The claims follow from easy properties of cyclic groups. For instance, for the second identity, notice that a and b generate in $U(\mathbb{Z}_p)$ cyclic groups of order $\mathrm{Gss}(p,a)$ and $\mathrm{Gss}(p,b)$, respectively. As $\mathrm{GCD}(\mathrm{Gss}(p,a), \mathrm{Gss}(p,b)) = 1$, these cyclic groups only intersect in 1, so their direct product is in $U(\mathbb{Z}_p)$ and is a cyclic group of order $\mathrm{Gss}(p,a) \cdot \mathrm{Gss}(p,b)$, which is generated by ab.

A4.36. We have $m' = m + hn$. Then $x^m - x^{m'} = x^m(1 - x^{hn})$. Notice that $h(x)$ divides $x^{hn} - 1$.

A4.37. In base a the number $a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1$ is written as $(1 \ldots 1)_a$, where n digits 1 appear. Multiplying by $a - 1$ we get the number $(a-1 \ldots a-1)_a$, where n digits $a - 1$ appear, and this is exactly $a^n - 1$. This proves part (i). Part (ii) is proved analogously.

A4.38. Proceed by induction.

A4.41. Assume M_p to be prime and $n = 2^{p-1} \cdot M_p$. Then, by Exercise A4.26, we have $\sigma(n) = 2^p \cdot M_p = 2n$. Vice versa, let $n = 2^s t$ be even and perfect, with t odd. Then, again by Exercise A4.26 and by the multiplicativity of σ, we have $2^{s+1}t = 2n = \sigma(n) = (2^{s+1} - 1)\sigma(t)$; hence follows that $2^{s+1} \mid \sigma(t)$, so we may write $\sigma(t) = 2^{s+1}q$ and so $\sigma(n) = (2^{s+1} - 1)\sigma(t) = 2^{s+1}(2^{s+1} - 1)q$. As $\sigma(n) = 2^{s+1}t$, we have $t = (2^{s+1} - 1)q$. Moreover, $\sigma(t) = 2^{s+1}q = t + q$, so $q = 1$ as $1, q, t$ divide t. Thus, $t = 2^{s+1} - 1$ and $\sigma(t) = t + 1$, so t is prime.

A4.48. If the claim were not true, there would be a decreasing sequence $\{h_n\}_{n\in\mathbb{N}}$ of positive integers such that $b = a^{h_n} b_n$ for all $n \in N$. Let I be the ideal generated by the elements of the sequence $\{b_n\}_{n\in\mathbb{N}}$. As A is Noetherian, I is finitely generated. Assume $I = (b_1, \ldots, b_n)$, so $b_{n+1} = a_1 b_1 + \cdots + a_n b_m$ and $b = a^{h_{n+1}} b_{n+1} = a^{h_{n+1}}(a_1 b_1 + \cdots + a_n b_n)$. Hence deduce that $b = b(a_1 a^{h_{n+1} - h_1} + \cdots + b(a_n a^{h_{n+1} - h_n})$, so $1 = a^{h_{n+1} - h_n}(a_1 a^{h_n - h_1} + \cdots + a_n)$. Thus, a would be invertible, yielding a contradiction.

A4.49. Verify for instance that it is closed under addition. If $a, b \in I$ there are positive integers n, m such that $a \in I_n$ and $b \in I_m$. If we assume $n \leq m$, then $a, b \in I_m$, so $a + b \in I_m \subseteq I$.

A4.50. To construct the sequence, proceed inductively. Choose $x_1 \in I$, any element of I. Having chosen next $x_1, \ldots, x_n$, notice that $I_n = (x_1, \ldots, x_n) \neq I$ as I is not finitely generated. So we may choose $x_{n+1} \in I - I_n$, and clearly $I_{n+1} \neq I_n$.

A4.52. Let n be the degree of $f(x)$ and let a be its leading coefficient. Notice that $\lim_{x \to +\infty} f(x)/x^n = a$. Hence deduce the claim.

A4.61. For all positive integers $m < n$ and for all pairs of polynomials of degree m and $n - m$ with coefficients bounded by N, we have to take their product and check whether it is equal to $f(x)$. Multiplying two of these polynomials has complexity $\mathcal{O}((m+1)(n-m+1)\log^2 N)$. Notice however that the pairs of such polynomials are $\mathcal{O}(N^n)$.

A4.62. First of all, to compute $\bar{f}(x)$ it is necessary to divide the $n+1$ coefficients by p and to take the remainder. This has complexity $\mathcal{O}((n+1)N \log p)$. Once $\bar{f}(x)$ has been found, for all positive integers $m < n$ and for all pairs of polynomials of degree m and $n - m$ in $\mathbb{Z}_p[x]$ we must take their product and check whether it is equal to $\bar{f}(x)$. Multiplying two of these polynomials and reducing the result modulo p has complexity $\mathcal{O}((m+1)(n-m+1)\log^3 p)$. Moreover, there are p^n such pairs of polynomials.

A4.63. Consider the coefficients of $p(x)$ as indeterminates and interpret (4.20) as a system of $M+1$ equations in $M+1$ unknowns. So it certainly has some solution. If there were two distinct solutions, we would find two distinct polynomials $p(x)$, $q(x)$ of degree $n \leq M$ verifying (4.20). Then the non-zero polynomial $p(x) - q(x)$ of degree $n \leq M$ would have the $M+1$ distinct roots $a_0, a_1, \ldots, a_M$, which is impossible (see Exercise A1.55).

A4.64. Notice that the determinant of the matrix of the system (4.20) is equal to $V(a_0, a_1, \ldots, a_M)$, so the uniqueness of the solution of (4.20) implies that it is not zero. Notice next that $V(x_1, \ldots, x_m)$, as a polynomial in $\mathbb{K}(x_1, \ldots, x_{m-1})[x_m]$, has the solutions $x_m = x_i$, $i = 1, \ldots, m-1$, so $V(x_1, \ldots, x_m)$ is divisible by $x_m - x_i$, $i = 1, \ldots, m-1$ in $\mathbb{K}(x_1, \ldots, x_{m-1})[x_m]$. The claim can be deduced using Gauss theorem.

A4.65. Proceed as in Exercise A4.63 considering the coefficients of $f(x)$ as indeterminates. The given conditions determine a system of $n+1$ equations in $n+1$ unknowns that always has a solution. It is unique, or else we would have a polynomial of degree n having h roots with multiplicities $m_1 + 1, \ldots, m_h + 1$, which is impossible.

B4.2. The correct answer is (a).

B4.4. The correct answer is (b).

B4.5. The correct answer is (d), because $1369 = 37^2$.

B4.11. The correct answer is (a).

B4.12. The correct answer is (b).

B4.14. The correct answer is (a), because the primes are 211, 223, 227, 229, 233, 239 and 241.

B4.19. $\mathrm{Gss}(8, a) = 2$.

B4.23. $\beta = 3, 6, 9$.

B4.24. $\beta = 2, 4, 5, 7, 8, 10$.

B4.25. $\beta = 23, 46, 92$.

B4.29. By Proposition 4.4.3, for every prime factor p of $2^{11} - 1 = 2047$, we have $p \equiv 1 \pmod{22}$. As $45 < \sqrt{2047} < 46$, we see that $p = 23$, and $2047 = 23 \cdot 89$.

B4.33. The number 2 is not prime in $\mathbb{Z}[i]$. Indeed, $2 = (1 + i)(1 - i)$, so 2 divides the product $(1 + i)(1 - i)$, but 2 does not divide $1 + i$ nor $1 - i$: assume 2 divides $1+i$, that is, $1+i = 2(a+bi)$, $a, b \in \mathbb{Z}$. Denoting by $N(a+ib) = a^2+b^2$ the complex norm of the number $a + ib$, we would have

$$N(1 + i) = 2 = N(2(a + ib)) = N(2)N(a + ib) = 4(a^2 + b^2);$$

now, the relation $2 = 4(a^2 + b^2)$ is a clearly impossible to be satisfied in $\mathbb{N}$. Analogously for $1 - i$. On the other hand, $2 + 3i$ is prime.

B4.35. For instance, 2, 5 and $2 \pm \sqrt{-6}$ are irreducible. Which of them are prime?

B4.36. The correct answer is (c), because $10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$.

B4.37. The correct answer is (d), because no one of the three polynomials is associate to the given polynomial; the primitive polynomials are $\pm(100x^3 + 36x^2 - 15x)$.

B4.40. The correct answer is (a). Let us see why. The polynomial $x^3 - 3x + 1$, as every third degree polynomial, is irreducible over $\mathbb{Q}$ if and only if it has no roots, because if it were reducible it would necessarily have a factorisation into a first degree polynomial and a second degree polynomial (or into three degree one polynomials); see page 190. But 1 and -1 are not roots of $x^3 - 3x + 1$, so by Proposition 4.5.37 this polynomial has no roots, so it is irreducible.

Let us see now what happens by considering the coefficients in $\mathbb{Z}_2$, $\mathbb{Z}_3$ or $\mathbb{Z}_{19}$. Over $\mathbb{Z}_2$ the polynomial becomes $x^3 + x + 1$, which is irreducible over $\mathbb{Z}_2$ because it has no roots, as may be verified by substituting $x = 0$ and $x = 1$ in the polynomial. As the polynomial is irreducible over $\mathbb{Z}_2$, it must be so a fortiori over $\mathbb{Q}$ (see page 190). It may be verified that the polynomial is reducible over $\mathbb{Z}_3$ and over $\mathbb{Z}_{19}$; indeed, over $\mathbb{Z}_3$ it becomes $x^3 + 1$ which admits -1 as a root, while 3 is a root over $\mathbb{Z}_{19}$.

B4.42. The correct answer is (a). Indeed, by substituting $x + 1$ for x, we find the polynomial $x^4 + 5x^3 + 10x^2 + 10x + 5$, which satisfies Eisenstein's criterion of irreducibility (Proposition 4.5.41 on page 188), so it is irreducible, and the given polynomial must be as well. We have argued exactly as in Example 4.5.42 on page 188 (with $p = 5$).

B4.47. The correct answer is (b), because $x^3 - 3x + 1 = x^3 + 1 = (x + 1)^3$ over $\mathbb{Z}_3$.

B4.52. The correct answer is (d); indeed, the polynomial in (d) verifies the required conditions, has degree two and may be computed using the Lagrange interpolation polynomial for this degree. Notice that there are infinitely many degree three polynomials that verify those conditions.

Exercises of Chapter 5

A5.3. Every field containing A and $b_1, \dots, b_n$ must also contain all rational expressions in $b_1, \dots, b_n$ with coefficients in A. Conclude by verifying that these expressions form a field.

A5.5. A basis of C as a vector space over A is also a basis of C as a vector space over B, so $[C : B]$ is finite. On the other hand, B is a vector subspace of C as a vector space over A, so $[B : A]$ is finite, because $[C : A]$ is finite.

A5.6. To prove that the given elements are linearly independent, suppose we have a relation of the form $\sum_{i,j} \alpha_{ij} a_i b_j = 0$, with $\alpha_{ij} \in A$. Then we have $\sum_{j=1}^{m} (\sum_{i=1}^{n} \alpha_{ij} a_i) b_j = 0$. By the linear independence of $\{b_1, \dots, b_m\}$ over B we have $\sum_{i=1}^{n} \alpha_{ij} a_i = 0$ for all $j = 1, \dots, m$. By the linear independence of $\{a_1, \dots, a_n\}$ over A we have $\alpha_{ij} = 0$ for all $i = 1, \dots, n, j = 1, \dots, m$.

To prove that this is a system of generators, notice that for all $c \in C$ we have $c = \sum_{j=1}^{m} \beta_j b_j$, with $\beta_j \in B$ for all $j = 1, \dots, m$. Use now the fact that $\{a_1, \dots, a_n\}$ is a basis of B as a vector space over A to express every β_j as a combination of $\{a_1, \dots, a_n\}$ with coefficients in A and conclude.

A5.8. Let $f_b(x) = f_1(x) \cdot f_2(x)$ with $f_1(x), f_2(x) \in A[x]$ be monic polynomials of positive degree. We have $f_1(b) \cdot f_2(b) = f_b(b) = 0$ so either $f_1(b) = 0$ or $f_2(b) = 0$; thus, either $f_1(x) \in I_b$ or $f_2(x) \in I_b$. Hence $f_b(x)$ divides either $f_1(x)$ or $f_2(x)$, leading to a contradiction. The fact that I_b is prime may be proved analogously.

A5.10. If A is a field and I is a non-zero ideal of A, there is a non-zero element $a \in I$. Then $1 = a^{-1} \cdot a \in I$, so $I = A$ (see Exercise A5.9). Vice versa, let $a \neq 0$ be an element of A. Then (a) is a non-zero ideal, so $(a) = A$. Hence, $1 \in (a)$, so there is a b such that $ab = 1$. This proves that every non-zero element of A has an inverse, so A is a field.

A5.11. B is an integral domain (see Exercise A5.8 and Exercise A3.12). Let I be an ideal of B. Let J be the preimage of I under the natural mapping $A[x] \to B$. Verify that J is an ideal and observe that $f(x) \in J$. Let $g(x)$ be the monic generator of J. Then $g(x)$ divides $f(x)$. Conclude that either $g(x) = f(x)$ or $g(x) = 1$, so $J = I$ or $J = A[x]$; hence either $I = (0)$ or $I = B$. Conclude by applying Exercise A5.10.

A5.13. Hint: use Lemma 5.1.8 and proceed by induction.

A5.14. Let $c \in C$. As $B \subset C$ is algebraic, there are $b_0, \dots, b_n \in B$ not all zero such that $b_0 + b_1 c + \cdots + b_n c^n = 0$. Then c is algebraic over $A(b_0, \dots, b_n)$, so $[A(b_0, \dots, b_n, c) : A(b_0, \dots, b_n)]$ is finite. As $A \subset B$ is algebraic, $[A(b_0, \dots, b_n) : A]$ is also finite, so by the multiplicativity of degrees $[A(b_0, \dots, b_n, c) : A]$ is finite. Conclude by applying Exercise A5.13.

A5.15. Let a, b be elements of B that are algebraic over A. Then $[A(a, b) : A]$ is finite. As $a \pm b$, ab, and a^{-1}, if $a \neq 0$, are in $A(a, b)$, this implies that they are algebraic over A. Hence we deduce that C is a field. If $c \in B$ is algebraic over C, it is algebraic over A as well, so $c \in C$.

A5.16. Prove first that $A[x]$ is countable. Using this fact, prove that the set $X \subset B \times A[x]$ of pairs $(\alpha, f(x))$ such that $f(\alpha) = 0$ is countable. Conclude by observing that the projection of X on B has as its image the algebraic closure of A in B.

A5.19. Observe that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. Then carry out the product.

A5.22. Apply the previous exercise.

A5.23. If $n = mh$ and if $\xi^m = 1$ then $\xi^n = (\xi^m)^h = 1$. Vice versa, let $R_m \subseteq R_n$. If either $\mathbb{K}$ has characteristic 0 or p is relatively prime with n and m, then R_n has order n and R_m has order m and we conclude by applying Lagrange's theorem (see Exercise A3.36).

A5.24. Suppose it has order $d < n$. Then $d = q_1^{\mu_1} \cdots q_h^{\mu_h}$ with $\mu_1, \ldots, \mu_h$ non-negative integers and $\mu_i \leq m_i$, $i = 1, \ldots, h$, where for at least one i the inequality holds. Set $d_i = q_i^{\mu_i}$ and $e_i = d/d_i, i = 1, \ldots, h$. We have $\xi^d = \prod_{i=1}^h (\xi_i^{d_i})^{e_i}$. At least one of the elements $\xi_i^{d_i}$ is not 1: assume this happens exactly for the indices $i = 1, \ldots, k$. So, $\xi^d = \prod_{i=1}^k (\xi_i^{d_i})^{e_i}$. Notice that $\xi_i^{d_i}$ has order $\delta_i = n_i/d_i = q_i^{m_i - \mu_i}$ and $\delta_i \nmid e_i$, for $i = 1, \ldots, k$. So, for all $i = 1, \ldots, k$ we have $\xi_i^d = (\xi_i^{d_i})^{e_i} \neq 1$. In conclusion, notice that $\xi_1^d \xi_2^d \neq 1$ as $R_{n_1} \cap R_{n_2} = (1)$. Analogously, $\xi_1^d \xi_2^d \xi_3^d \neq 1$ as $R_{n_1 n_2} \cap R_{n_3} = (1)$, and so on.

A5.29. The roots of $x^{p^f} - x$ are 0, plus those of the polynomial $x^{p^f - 1} - 1$. As $\mathbb{F}^*$ has order $p^f - 1$, every non-zero element $a \in \mathbb{F}$ satisfies $a^{p^f - 1} = 1$, so is a root of $x^{p^f - 1} - 1$.

A5.31. Mimic the proof of Proposition 5.1.37.

A5.32. Mimic the proof of Corollary 5.1.38.

A5.33. Keeping in mind Exercise A5.32 and Möbius inversion theorem (see Exercise A4.22), one can find the formula $n_{d,q} = (1/d) \sum_{h|d} \mu(h) q^{d/h}$; hence $n_{d,q} > (1/d)(q^d - q^{d/2} - q^{d/3} - \cdots) > (1/d)(q^d - \sum_{i=0}^{[d/2]} q^i)$. From here, the claim immediately follows.

A5.34. Every automorphism of $\mathbb{F}$ fixes $\mathbb{F}'$. So we have an obvious restriction homomorphism $r : \mathrm{Aut}(\mathbb{F}) \to \mathrm{Aut}(\mathbb{F}')$. Recall that $\mathrm{Aut}(\mathbb{F})$ [$\mathrm{Aut}(\mathbb{F}')$, respectively] is cyclic of order f [f', resp.] generated by $\phi_{\mathbb{F}}$ [$\phi_{\mathbb{F}}$, resp.]. As obviousy $r(\phi_{\mathbb{F}}) = \phi_{\mathbb{F}'}$, the homomorphism r is surjective. Its kernel, which is the group we are looking for, has order f/f' and is generated by $(\phi_{\mathbb{F}})^{f'}$.

A5.35. We have $\mathbb{F}_{p^d} = \mathbb{Z}_p[x]/(f(x)) = \mathbb{Z}_p(\alpha) \subset \mathbb{F}$. Conclude keeping in mind Theorem 5.1.35.

A5.36. Every element $g(x) \in \mathbb{K}[x]$ is congruent modulo $(f(x))$, to the remainder of its division by $f(x)$.

A5.38. Keep in mind Exercise A2.20 and Proposition 5.1.44.

A5.39. Keep in mind Exercise A2.21 and Proposition 5.1.44.

A5.40. Keep in mind Exercise A2.22 and Proposition 5.1.44.

A5.41. In each division, d^2 multiplications are carried out, each having complexity $\mathcal{O}(\log^3 q)$. Moreover, at most d division have to be performed. For more information, see Section 2.5.3.

A5.42. Use the method of completing the square discussed on page 234.

A5.48. Use Exercise A5.47 and Corollary 5.1.31.

A5.49. Notice that $\xi^4 = -1$, so $\xi^5 = -\xi, \xi^7 = -\xi^3$, then $G = 2(\xi - \xi^3)$. Hence, $G^2 = 4(\xi^2 - 2\xi^4 + \xi^6) = 8$. So we have $G^{p-1} = (G^2)^{(p-1)/2} = 8^{(p-1)/2}$. Using Proposition 5.2.22, we get $G^p = (8/p)G = (2/p)G$.

A5.50. We have $G^p = (\sum_{i=0}^7 \epsilon(i)\xi^i)^p = \sum_{i=0}^7 \epsilon(i)\xi^{pi} = \sum_{i=0}^7 \epsilon(pi)\xi^i$. Keep in mind Exercise A5.58, we have $\epsilon(p)\epsilon(pi) = \epsilon(p^2 i) = \epsilon(p^2)\epsilon(i) = \epsilon(i)$. Hence, $\epsilon(p)G^p = \sum_{i=0}^7 \epsilon(p)\epsilon(pi)\xi^i = \sum_{i=0}^7 \epsilon(i)\xi^i = G$. Finally, notice that $G \neq 0$, as $G^2 = 8 \neq 0$.

A5.52. With the same idea as Exercise A5.50, we have $G^p = \sum_{i=0}^{q-1} (\frac{i}{q})^p \xi^{ip} = \sum_{i=0}^{q-1} (\frac{i}{q})\xi^{ip}$. Now notice that $(\frac{i}{q}) = (\frac{i}{q})(\frac{p^2}{q}) = (\frac{p^2 i}{q}) = (\frac{pi}{q})(\frac{p}{q})$. So $G^p = \sum_{i=0}^{q-1} (\frac{i}{q})\xi^{ip} = \sum_{i=0}^{q-1} (\frac{pi}{q})(\frac{p}{q})\xi^{ip} = (\frac{p}{q})(\sum_{i=0}^{q-1} (\frac{pi}{q})\xi^{ip}) = (\frac{p}{q})(\sum_{i=0}^{q-1} (\frac{i}{q})\xi^i) = (\frac{p}{q})G$.

A5.53. Using Proposition 5.2.22, we have

$$G^2 = G \cdot G = \left(\sum_{i=1}^{q-1} \left(\frac{i}{q}\right)\xi^i\right)\left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)\xi^j\right) = \left(\sum_{i=1}^{q-1} \left(\frac{i}{q}\right)\xi^i\right)\left(\sum_{j=1}^{q-1} \left(\frac{-j}{q}\right)\xi^{-j}\right) =$$
$$= \left(\frac{-1}{q}\right)\sum_{i=1}^{q-1}\sum_{j=1}^{q-1} \left(\frac{ij}{q}\right)\xi^{i-j} = (-1)^{(q-1)/2}\sum_{i=1}^{q-1}\sum_{j=1}^{q-1} \left(\frac{ij}{q}\right)\xi^{i-j}.$$

Notice that we may consider the indices i, j as non-zero elements of $\mathbb{Z}_q$. For every index i in the external sum, perform in $\mathbb{Z}_q^*$ the variable change $j = ik$. This may be done, as when k ranges in $\mathbb{Z}_q^*$, also j ranges in $\mathbb{Z}_q^*$. So we have $G^2 = (-1)^{(q-1)/2}\sum_{i=1}^{q-1}\sum_{k=1}^{q-1}(i^2 k/q)\xi^{i(1-k)} = (-1)^{(q-1)/2}\sum_{i=1}^{q-1}\sum_{k=1}^{q-1}(k/q)\xi^{i(1-k)}$. Keeping in mind Exercise A5.46, we get

$$G^2 = (-1)^{(q-1)/2}\sum_{i=0}^{q-1}\sum_{k=0}^{q-1} \left(\frac{k}{q}\right)\xi^{i(1-k)} = (-1)^{(q-1)/2}\sum_{k=0}^{q-1} \left(\frac{k}{q}\right)\left(\sum_{i=0}^{q-1} \xi^{i(1-k)}\right).$$

For every $k \neq 1$ the internal sum equals zero: indeed, ξ is a primitive qth root of unity, and being q prime, every power ξ^h with $q \nmid h$ is too, so for the values $i = 0, \ldots, q-1$, the powers $\xi^{i(1-k)}$ span the whole set R_q (see Exercise A5.22). In conclusion, we have $G^2 = (-1)^{(q-1)/2}\sum_{i=0}^{q-1} \xi^0 = (-1)^{(q-1)/2} q$.

A5.54. We have $G^p = (G^2)^{(p-1)/2} G = ((-1)^{(q-1)/2} q)^{(p-1)/2} G$. Conclude keeping in mind Proposition 5.2.22 and Exercise A5.52.

A5.57. The claim is trivial if $\alpha = 1$. Proceed next by induction on α.

A5.58. Hint: notice that

$$\epsilon(n) = \begin{cases} 1 & \text{if} \quad n \equiv \pm 1 \pmod 8, \\ -1 & \text{if} \quad n \equiv \pm 3 \pmod 8, \end{cases}$$

and examine separately the different cases for n, m modulo 8.

B5.2. The correct answer is (a).

B5.3. The correct answer is (a), because $64 = 2^6$ and $\mathbb{F}_{64}$ may be constructed, for instance, as a quotient of $\mathbb{Z}_2[x]$ with respect to an irreducible polynomial of degree 6.

B5.4. The correct answer is (d), because $323 = 17 \cdot 19$ is not a prime number, but this is not sufficient to rule out the existence of a field of order 323. It is necessary to remark that 323 is neither a prime nor a prime power.

B5.8. The correct answer is (a).

B5.13. The correct answer is (c), as $16 = 2^4$.

B5.20. The correct answer is (c).

B5.21. The correct answer is (d), as $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ over $\mathbb{Z}_2$. Let us see how to get this factorisation.

First of all, we check whether $x^4 + x^2 + 1$ has roots in $\mathbb{Z}_2$, but we do not find any. Verify next if the polynomial splits into two degree two polynomials. We may assume that there is a factorisation of the form: $x^4 + x^2 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ where a and b are unknowns. In general, we should have written $x^4 + x^2 + 1 = (cx^2 + ax + d)(ex^2 + bx + f)$ where c, d, e and f are further unknowns. But a factor of a monic polynomial with coefficients in a field may always be chosen to be monic, so we may assume $c = 1$. Then also $e = 1$, as in the right-hand side the highest degree term is cex^4. Moreover, the constant term must be $1 = df$, which in $\mathbb{Z}_2$ is possible only if $d = f = 1$. Back to the factorisation of $x^4 + x^2 + 1$, by carrying out the product in the right-hand side we get $x^4 + (a+b)x^3 + (1+ab+1)x^2 + (a+b)x + 1$, so $0 = a + b$ and $1 = ab$. Both equations are satisfied only if $a = b = 1$. So we get the factorisation given at the beginning.

Another possible way of finding this factorisation consists in noticing that the degree two factors, if they exist, have to be irreducible, otherwise they would have a degree one factor which would also be a factor of the original polynomial. There are only four degree two polynomial over $\mathbb{Z}_2$: x^2, x^2+1, x^2+x, x^2+x+1. The first three of them are reducible, because they have a root equal to 0, 1 and 0, respectively. So $x^2 + x + 1$ is the only degree two irreducible polynomial over $\mathbb{Z}_2$. If we divide our polynomial by x^2+x+1, we find a zero remainder and a quotient equal to x^2+x+1, so we get again the above factorisation.

B5.22. The correct answer is (a).

B5.25. The correct answer is (d). First of all, notice that $x^{27} - x$ has linear factors, because it has roots 0, 1 and -1 $(= 2)$. Next, dividing by $x(x-1)(x+1)$, we find that the quotient is

$$x^{24} + x^{22} + x^{20} + x^{18} + x^{16} + x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1,$$

and we must try to factor this. Verify that it has no linear factors, because 0, 1 and -1 are not roots of this polynomial. Then we have to look for its factors among the monic, irreducible polynomials of degree two or greater. We may verify that there are three monic, irreducible polynomials of degree two over $\mathbb{Z}_3$, but they do not divide our polynomial. So we look at the monic, irreducible polynomials of degree three. After some calculations, we find the following polynomials:

$$\begin{array}{llll} x^3 + 2x + 1, & x^3 + 2x + 2, & x^3 + x^2 + 2, & x^3 + x^2 + x + 2, \\ x^3 + x^2 + 2x + 1, & x^3 + 2x^2 + 1, & x^3 + 2x^2 + x + 1, & x^3 + 2x^2 + 2x + 2 \end{array}$$

and they are exactly all the factors of the degree 24 polynomial (so also of $x^{27} - x$), as may be verified by carrying out the divisions. So we have found 11 factors: three linear ones and eight of degree three.

B5.27. The correct answer is (a).

B5.28. The correct answer is (a), as only $\mathbb{Z}_5$ is a subfield of $\mathbb{F}_{125}$.

B5.43. The correct answer is (a).

B5.44. The correct answer is (d), as the solutions are $x = -1$, $x = -3$, $x = 4$ and $x = 6$ modulo 14.

B5.49. The correct answer is (a), as 13 divides 65.

B5.50. The correct answer is (d), as Legendre symbol is defined only if the denominator is a prime number.

B5.51. The correct answer is (c).

B5.54. The correct answer is (b). Let us see why. First of all, $973 = 7{\cdot}139$, so $(\frac{1003}{973})$ is equal, by definition of Jacobi symbol, to the product of the Legendre symbols $(\frac{1003}{7})$ e $(\frac{1003}{139})$. Now, $1003 \bmod 7 = 2$, so $(\frac{1003}{7}) = (\frac{2}{7}) = 1$, where the last equality follows from Proposition 5.2.27. On the other hand, $1003 \bmod 139 = 30$, so $(\frac{1003}{139}) = (\frac{30}{139})$. By part (4) of Proposition 5.2.22, we have $(\frac{30}{139}) = (\frac{2}{139})(\frac{3}{139})(\frac{5}{139})$. Proposition 5.2.27 tells us also that $(\frac{2}{139}) = -1$, while the law of quadratic reciprocity (Theorem 5.2.28) implies that $(\frac{3}{139}) = -(\frac{139}{3})$ and $(\frac{5}{139}) = (\frac{139}{5})$. Finally, $139 \bmod 3 = 1$ and $139 \bmod 5 = -1$, so $(\frac{139}{3}) = (\frac{1}{3}) = 1$ and $(\frac{139}{5}) = (\frac{-1}{5}) = 1$. So we may conclude that $(\frac{1003}{973}) = (-1)(-1) = 1$.

Exercises of Chapter 6

A6.1. As n is not a prime, it is clear that neither is m (see Section 4.4.1). As n is a pseudoprime in base 2, we have $m - 1 = 2^n - 2 = kn$ for some integer k. So $2^{m-1} - 1 = 2^{kn} - 1 \equiv 0 \pmod{m}$.

A6.3. As n is a pseudoprime in bases a_1 and a_2, then $a_1^{n-1} \equiv 1 \pmod{n}$ and $a_2^{n-1} \equiv 1 \pmod{n}$, so $(a_1 a_2)^{n-1} = a_1^{n-1} a_2^{n-1} \equiv 1 \pmod{n}$. Moreover, $(a_2^{-1})^{n-1} \equiv a_2^{1-n} \equiv 1^{-1} \equiv 1 \pmod{n}$.

A6.8. As for Exercise A6.1, we have that m is not prime. We have $2^{n-1} - 1 = nk$ and k is odd. So $m - 1 = 2^n - 2 = 2kn$ with kn odd. Moreover, $2^{(m-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \pmod{m}$. Indeed, $2^n = m + 1 \equiv 1 \pmod{m}$.

A6.10. Write $n = 2^s t + 1$ with odd t. From the hypotheses, it follows that $b^{2^{s-1}t} \equiv -1 \pmod{n}$.

A6.12. It suffices to observe that for all positive integers k we have $5^k \not\equiv -1 \pmod{4}$.

A6.15. Use the properties of cyclic groups (see Exercises A3.23–A3.35).

A6.16. We have to compute the product of all elements of the group $U(\mathbb{Z}_n)$. As two reciprocal elements cancel out in the product, the result is $\prod_{x \in G} x$, where G is the subgroup of the elements of order 2 of $U(\mathbb{Z}_n)$. Consider G as an additive group, so the above product becomes the sum of the elements. The group G is a $\mathbb{Z}_2$-vector space as well. If it has dimension 1, then G has order 2; this corresponds exactly to

the cases $n = 2, 4, p^h, 2p^h$, and the sum of its elements is of course 1. If the dimension of G is greater than 1, we see that the sum of its elememts is 0. Indeed, we may interpret G as $\mathbb{Z}_2^d$, $d > 1$. Put the 2^d elements of $\mathbb{Z}_2^d$ in a $2^d \times d$ matrix. Every column has 2^{d-1} entries equal to 0 and as many equal to 1. Summing the elements of $\mathbb{Z}_2^d$ columnwise, it is clear that the sum of the entries in each column is 0.

A6.19. We are working in $U(\mathbb{Z}_{2^l})$. So we may write $x = (-1)^s 5^t, m \equiv (-1)^\sigma 5^\tau \pmod{2^l}$ (see Remark 6.2.10). Then the equation to be solved is translated into the system consisting of the two equations

$$sh \equiv \sigma \pmod 2, \quad th \equiv \tau \pmod{2^{l-2}}$$

in s and t. If h is odd, then this system admits a unique solution. If h is even, the first equation admits solutions, and exactly two of them, if and only if σ is even, that is, $m \equiv 1 \pmod 4$. If h is even, the second equation admits solutions, and exactly d of them, if and only if $d \mid \tau$ that is, if and only if $\tau = dk$, that is $m = 5^{dk}$, so $m^{2^{l-2}/d} \pmod 5^{2^{l-2}} \equiv 1 \pmod{2^l}$.

A6.21. Assume, for instance, n to be odd. Let $n = p_1^{l_1} \cdots p_s^{l_s}$ be its factorisation. Then $U(\mathbb{Z}_n)$ is the direct product of $U(\mathbb{Z}_{p_i^{l_i}})$, $i = 1, \ldots, s$. Let r_i be a generator of $U(\mathbb{Z}_{p_i^{l_i}})$, $i = 1, \ldots, s$. Then for every integer m that is relatively prime with n the class of m in $U(\mathbb{Z}_n)$ may be written uniquely as $r_1^{d_1} \cdots r_s^{d_s}$ with $0 \le d_i \le p_i^{l_i - 1}(p_i - 1)$, $i = 1, \ldots, s$. The vector $(d_1, \ldots, d_s)$ is called *index system* of m with respect to $(r_1, \ldots, r_s)$.

A6.22. Proceed by induction.

A6.25. If $n = m^k$, then $k \le \log_2 n$. For all k find an estimate for the kth root of n and then compute a kth power. The latter computation has complexity $\mathcal{O}(\log^3 n)$, while for the first estimate the complexity is $\mathcal{O}^\sim(\log^2 n)$.

A6.26. Proceed as in § 3.3.1.

A6.28. A pair (x, f) is found by assigning arbitrarily $x_1 = f(x)$, in k ways, $x_2 = f(x_1)$ arbitrarily in $X \setminus \{x_1\}$, in $k - 1$ ways, $\ldots$, $x_m = f(x_{m-1})$ arbitrarily in $X \setminus \{x_1, \ldots, x_{m-1}\}$, in $k - m$ ways, and the remaining values of f arbitrarily without restrictions.

B6.4. The correct answer is (c).

B6.20. For instance, 5.

B6.23. The answer is $2, 5, 25, 121$.

B6.24. The group $U(\mathbb{Z}_{15})$ is the product of a cyclic group of order 2 and of a cyclic group of order 4.

B6.25. The group $U(\mathbb{Z}_{16})$ is the product of a cyclic group of order 2 and of a cyclic group of order 4.

B6.26. The group $U(\mathbb{Z}_{17})$ is cyclic of order 16.

B6.27. The group $U(\mathbb{Z}_{18})$ is cyclic of order 6.

B6.28. $|U(15)| = |U(16)| = 8$, $|U(17)| = 16$, $|U(18)| = 6$.

B6.35. The correct answer is (a).

B6.36. The factorisation is found to be $906113 = 13 \cdot 47 \cdot 1483$.

Exercises of Chapter 7

A7.10. The solution is trivial if n is even. Let n be odd. Then $\varphi(n) = (p-1)(q-1) = n+1-(p+q)$. So we know the sum of p and q, that is $p+q = n+1-\varphi(n) = 2b$, which is even, and their product $n = pq$. Thus, p and q are equal to $b \pm \sqrt{b^2 - n}$. Now there is a simple algorithm, having complexity $\mathcal{O}(\log^3 n)$, which computes $\lfloor \sqrt{n} \rfloor$. Indeed, if n has $k+1$ binary digits, a first approximation m_1 of $\lfloor \sqrt{n} \rfloor$ is given by 1 followed by $\lfloor k/2 \rfloor$ zeros. If m_1 is not the correct value, change its second digit from left, a 0, into a 1, obtaining a value m_2. If it is too large, put the second digit back to 0 and repeat the above with the third digit, obtaining m_3. If on the other hand m_2 is too small, change its second digit into a 1 obtaining a different m_3, and so on.

A7.11. By the Chinese remainder theorem, it suffices to prove that $a^{de} \equiv a \pmod{p}$ for all a and for all prime $p \mid n$. This is obvious if $p \mid a$, else it follows from Fermat's little theorem.

A7.16. If $g(x)y - f(x)$ were reducible, we would have $g(x)y - f(x) = a(x,y) \cdot b(x,y)$ where the two polynomials $a(x,y), b(x,y)$ have positive degree and at least one of them does not depend on y. Let $a(x,y) = a(x)$ be such a polynomial. Then $a(x)$ is a common factor of $f(x)$ and of $g(x)$, which is impossible.

A7.17. Hint: study the case in which the conic curve contains the point $O = (0,1)$ first; define the projection of the conic on the x-axis, associating with each point $P \neq O$ of the conic the intersection of the line through P and O with the x-axis.

A7.27. Here is the proof in the case $p \neq q$. We have already shown in the text that the line through p and q has equation $y - y_1 = (y_2 - y_1)(x - x_1)/(x_2 - x_1)$, so the ordinate y_r of the point r collinear with p and q is

$$y_r = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1),$$

where x_3 is the abscissa of r; hence follows the formula for y_3, because $p + q$ is the symmetric point of r with respect to the x-axis. On the other hand, the fact that r lies on the elliptic curve says that (x_3, y_r) is a solution of the following system:

$$\begin{cases} y = y_1 + \dfrac{y_2 - y_1}{x_2 - x_1}(x - x_1), \\ y^2 = x^3 + ax + b. \end{cases}$$

Squaring the first equation, we find that the right-hand side of the second equation is equal to the square of the right-hand side of the first equation, so we find a third degree equation in x, equivalent to

$$x^3 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 x^2 + (\text{terms of degree 1 and 0 in } x) = 0,$$

whose solutions are x_1, x_2 and x_3. So the left-hand side of the last equation is a polynomial equal to

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (\cdots)x - x_1x_2x_3;$$

hence follows that

$$x_1 + x_2 + x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2,$$

giving the formula for x_3.

A7.34. By Exercise A7.32, x and z are odd. Set $r = (z + x)/2$, $s = (z - x)/2$. Using Exercise A7.31, prove that $\mathrm{GCD}(r, s) = 1$. As $y^2 = 4rs$, deduce that rs is a square and, by Exercise A7.33, that there exist two integers n, m such that $r = m^2, s = n^2$. Deduce (7.31).

B7.1. The correct answer is (d).

B7.5. The correct answer is (d).

B7.7. The correct answer is (d).

B7.9. The correct answer is (c).

B7.11. The correct answer is (a).

B7.14. The correct answer is (a).

B7.15. The correct answer is (c).

B7.16. The correct answer is (b).

B7.20. Consider the plaintext of the message sent to Edgar Allan Poe (see page 325). By applying Vigenère enciphering using as key word *UNITED STATES*, for instance using the program of Exercise C7.3, the following ciphertext is found:

GE IEIASGDXV, ZIJ QL MW LAAM XZY ZMLWHFZEK EJLVDXW KWKE TX LBR ATQH LBMX AANU BAI VSMUKHSS PWN VLWKAGH GNUMK WDLNRWEQ JNXXVV OAEG EUWBZWMQY MO MLW XNBX MW AL PNFDCFPXH WZKEX HSSF XKIYAHUL? MK NUM YEXDM WBXZ SBC HV WZX PHWLGNAMIUK?

It is straightforward to check that in the ciphertext given by Poe there are exactly 16 transcription errors: the third letter should be `I` rather than `J`, the fifth letter (a `I`) was omitted. The reader might want to check the remaining errors.

B7.23. The correct answer is (d).

B7.24. The correct answer is (d), as the plaintext is `take a day out`.

B7.26. The correct answer is (a).

B7.27. The correct answer is (d).

B7.28. The correct answer is (d), as the inverse matrix exists and is $\begin{pmatrix} 12 & 1 \\ 7 & -11 \end{pmatrix}$.

B7.30. The correct answer is (a).

B7.31. The correct answer is (d).

B7.33. The correct answer is (b).

B7.35. The correct answer is (d), because the image of f is $\{1, 4\}$, so f is not surjective. It follows that f is not injective either, because the domain and the codomain have the same (finite) size: when this happens, the function is bijective if

and only if it is surjective, and this happens if and only if it is injective. Or, more simply, f is not injective because $f(1) = 4 = f(3)$.

B7.38. We have $2^{70} = 2^{50+20} = 2^{50}2^{20} = (-\bar{1})(-\bar{6}) = \bar{6} = \bar{2}\cdot\bar{3}$, so $2^{69} = \bar{3}$; therefore $\overline{69}$ is the required discrete logarithm.

B7.39. The correct answer is (d).

B7.40. The correct answer is (b).

B7.41. The correct answer is (b), because the only solution is $34 = 20 + 13 + 1$.

B7.43. The correct answer is (a).

B7.45. The correct answer is (a).

B7.47. The correct answer is (a).

B7.49. The correct answer is (d).

B7.51. The correct answer is (c), because 7927 is a prime number.

B7.53. The correct answer is (a).

B7.55. The correct answer is (a).

B7.60. The correct answer is (b).

B7.61. The correct answer is $p + q = (3, -2\sqrt{6})$, so (d).

B7.64. The correct answer is (a).

B7.67. The correct answer is (c). A way of solving this exercise is by trial and error. In the affine plane with coordinates in $\mathbb{F}_7$ there are $7 \cdot 7 = 49$ points. In particular, fixing an abscissa (which is a number modulo 7), there are exactly 7 points having that abscissa (and different ordinates). We shall see if any of these poins lies on the elliptic curve, and how many (at most two).

Consider first $x = 0$. Then, of the 7 points having abscissa 0, only $(0, 0)$ belongs to the elliptic curve, because by substituting $x = 0$ in the curve equation we find $y^2 = 0$ that has 0 as its only solution. Consider now $x = 1$. Substituting it in the curve equation we find $y^2 = 0$, so among the points with abscissa 1 only $(1, 0)$ belongs to the curve. For $x = 2$, we find $y^2 = 6$, which has no solutions, so there are no points having abscissa 2 on the elliptic curve. Analogously, by substituting $x = 3$ we find $y^2 = 3$, which admits no solutions either. For $x = 4$, on the other hand, we find $y^2 = 4$, which admits two solutions: $y = 2$ e $y = 5$, so $(4, 2)$ and $(4, 5)$ are points of the elliptic curve (the only ones with abscissa 4). For $x = 5$, we have $y^2 = 1$, which has two solutions: $y = 1$ and $y = 6$, that is $(5, 1)$ and $(5, 6)$ are points of the elliptic curve. Finally, for $x = 6$ we find $y^2 = 0$, that is, $(6, 0)$ is a further point of the elliptic curve. And this is all: in the affine plane we have found 7 points, so the curve has 8 points, including the point at infinity.

B7.68. The correct answer is (d). Proceed as in example 7.9.18.

Exercises of Chapter 8

A8.1. This a variation of the classic *binomial probability distribution* (see [29], p. 63). Fix a value of i, $0 \leq i \leq n$. The probability of $n-i$ errors occurring in $n-i$ fixed positions of a binary string of length n is $p^{n-i}(1-p)^i$. So the probability of $n-i$ occurring in any given string of length n is $\binom{n}{i}p^{n-i}(1-p)^i$ (see Exercise A1.15). If we have more 0's than 1's and decode as HEADS the incoming string, the probability of having made a mistake is that of at least $\lfloor n/2 \rfloor$ errors having occurred, and the formula follows from the above. Notice that $1 = (p+(1-p))^n = \sum_{i=0}^{n}\binom{n}{i}p^{n-i}(1-p)^i$. Hence follows that $0 < P_n < 1$. Finally, we have (see Exercise A1.23)

$$P_n < [p(1-p)]^{n/2} \sum_{0 \leq i < [n/2]} \binom{n}{i} < 2^{n-1}[p(1-p)]^{n/2}.$$

Notice that $(2p-1)^2 > 0$, that is, $4p^2 - 4p + 1 > 0$, so $p(1-p) < 1/4$ and from this it immediately follows that P_n tends to zero when n tends to infinity.

A8.2. Using the theorems about linear systems over a field, prove that there is exactly one solution of the system (8.3) when the values of x_1, x_2, x_3, x_4 are assigned arbitrarily.

A8.4. The triangle inequality is the only property whose truth it is interesting to verify. Notice that, if x and x' differ in the ith coordinate, then in that coordinate either x differs from x'' or x' differs from x''.

A8.5. A code detects k errors if and only if, by modifying a codeword in $h \leq k$ coordinates, we never get another codeword. This happens if and only if two codeword always have distance at least $k+1$. This proves (i). A code corrects k errors if and only if by modifying a codeword in $h \leq k$ coordinates, the n-tuple we get has distance greater than k from every other codeword. This happens if and only if two codewords always have distance at least $2k+1$. This proves (ii).

A8.6. See the solution of Exercise A8.1.

A8.8. Let i be a positive integer smaller than n. The elements of $\mathbb{F}_q^n$ having Hamming distance exactly i from $x = (x_1, \ldots, x_n)$ are those differing from x in exactly i coordinates. They can be obtained as follows: choose in $\binom{n}{i}$ ways the coordinates $x_{h_1}, \ldots, x_{h_i}$, with $1 \leq h_1 < \cdots < h_i$, of x to be modified and, for each $j = 1, \ldots, i$, modify the coordinate of x in position h_j in $q-1$ ways, as many as the elements of $\mathbb{F}_q$ different from x_{h_j}.

A8.11. By the properties of the binomials (see Exercise A1.14), we have $2^d = \sum_{i=1}^{d}\binom{n}{i} = 2 \cdot \sum_{i=1}^{k}\binom{n}{i}$.

A8.13. If Singleton bound is better than Hamming one, we have $\sum_{i=1}^{k}\binom{n}{i} < 2^{d-1}$, where $k = (d-2)/2$. By proceeding as in the previous solution, verify that this relation is equivalent to $\sum_{i=0}^{k}\binom{d}{i} + 1/2\binom{d}{k+1} > \sum_{i=0}^{k}\binom{n}{i}$. Notice that $n \geq d$ and that the previous inequality holds for $n = d$. Prove instead that it does not hold for $n = d+1$, and deduce that it does not hold for $n \geq d+1$. Indeed, for $n = d+1$, by using Equation (1.51), the inequality may be written as $1/2\binom{d}{k+1} > \sum_{i=0}^{k}[\binom{d+1}{i} -$

$\binom{d}{i}] = \sum_{i=1}^{k} \binom{d}{i-1}$ and notice that for $d \geq 12$ we have $2\binom{d}{k-1} > \binom{d}{k+1}$. Directly verify cases $d = 8, 10$.

A8.16. Suppose $\mathbf{x}$ different from zero and notice that the degree two polynomial $f(t) = (t\mathbf{x} + \mathbf{y}) \times (t\mathbf{x} + \mathbf{y})$ only assumes positive or zero values. So its discriminant is non-positive.

A8.17. If the sequence $\{x_n\}_{n\in\mathbb{N}}$ is bounded from above, its least upper bound is also an upper bound for the sequence $\{b_n\}_{n\in\mathbb{N}}$, so $\xi = \limsup_{n\to\infty} x_n$ is finite.

A8.20. Set $n! = n^n e^{-n} a(n)$. It suffices to prove that $a(n)$ is $\mathcal{O}(n)$. Notice that $a(n+1)/a(n) = e(1+1/n)^{-n}$ and that we have the inequality $(1+1/n)^{n+1/2} > e$. The latter follows from the well-known formula

$$\log \frac{1+x}{1-x} = \log(1+x) - \log(1-x) = 2\left(x + \frac{x^3}{3} + \frac{x^5}{5} + \cdots\right) > 2x,$$

which holds for $0 < x < 1$, setting $x = 1/(2n+1)$. Then we have $a(n+1)/a(n) < (1+1/n)^{1/2}$, that is, the function $b(n) = a(n)/\sqrt{n}$ is positive and decreasing, so it tends to a finite, positive limit. Hence follows the claims.

A8.21. Set $r = [\delta n]$. The last term in the sum that appears in (8.6) is the largest one. So we have

$$\binom{n}{r}(q-1)^r \leq V_q(n,r) \leq (1+r)\binom{n}{r}(q-1)^r.$$

Take the logarithm in base q and divide by n. Applying Stirling formula we get

$$\frac{1}{n}\log_q \binom{n}{r}(q-1)^r = \delta\log_q(q-1) + \log_q n - \delta\log_q r - (1-\delta)\log_q(n-r) + \mathcal{O}(1),$$

so

$$\frac{1}{n}\log_q \binom{n}{r}(q-1)^r = H_q(\delta) + \mathcal{O}(1).$$

Hence follows the claim.

A8.22. By the Gilbert–Varshamov bound, we have

$$\alpha(\delta) = \limsup_{n\to\infty} \frac{\log_q A_q(n, n\delta)}{n} \geq \lim_{n\to\infty}\left(1 - \frac{\log_q V_q(n,n\delta)}{n}\right).$$

The claim follows from Lemma 8.4.7.

A8.23. We have $(q-1)/q \leq \delta$ if and only if $dq - nq + n > 0$. In this case the Plotkin bound implies $A_q(n,d) \leq qd/(qd - n(q-1))$. Then

$$0 \leq \alpha(\delta) = \limsup_{n\to\infty} \frac{\log_q A_q(n,n\delta)}{n} \leq \limsup_{n\to\infty}\left(\frac{\log_q(n\delta q)}{n} - \frac{\log_q(n\delta q - nq + n)}{n}\right) = 0.$$

Suppose now $0 \leq \delta \leq (q-1)/q$, which implies that $dq - nq + n \leq 0$. Set $m = [q(d-1)/(q-1)]$ and notice that $m < n$. Let C be a code of type $(n, M, d)_q$. Considering the mapping $p : C \to \mathbb{F}_q^{n-m}$ which, to each $x \in C$, associates the vector in $\mathbb{F}_q^{n-m}$ consisting of its last $n-m$ coordinates, notice that there is a subset C' of

C of size $M' \geq q^{m-n}M$ such that all elements of C' have the same image in p. We may consider C' as a code of type $(m, M', d)_q$. We may apply the Plotkin bound, which yields $q^{m-n}M \leq M' \leq qd/(qd - mq + m) \leq d$. So we have $q^{m-n}A_q(n,d) \leq d$, hence, by taking $d = n\delta$ and $n \gg 0$ we obtain the claim.

A8.26. The rows of a generating matrix $\mathbf{X}$ are linearly independent. So there is a non-zero minor of order k. Up to renaming the coordinates, we may assume that this minor is determined by the first k columns. Let $\mathbf{A}$ be the submatrix of $\mathbf{X}$ determined by the first k columns. The matrix $\mathbf{A^{-1}} \cdot \mathbf{X}$ is in standard form and is again a generating matrix for the same code, obtained with a basis change.

A8.29. It is sufficient to verify that $\mathbf{X} \cdot \mathbf{H}^t = \mathbf{0}$, where $\mathbf{0}$ is here the $k \times (n-k)$ zero matrix.

A8.33. The mapping $\mathbf{x} \in C \to \mathbf{e} + \mathbf{x} \in \mathbf{e} + C$ is a bijection between the words of C and the elements of the coset $\mathbf{e} + C$. Show, further, that every element of $\mathbb{F}_n^q$ lies in exactly one coset.

A8.40. Consider the two binary codes

$$\begin{aligned} C = \{&(1,0,1,1,1,0,1,1,1,0),(1,0,1,1,0,1,1,1,0,1),(0,1,1,1,0,1,0,1,0,1),\\ &(1,1,0,1,1,0,1,1,0,1),(0,0,0,0,1,1,1,1,0,0)\},\\ C' = \{&(1,1,1,1,1,0,0,1,1,0),(1,0,0,0,0,0,0,0,0,0),(0,1,1,0,0,0,0,0,0,0),\\ &(0,1,1,1,1,1,1,0,0,0),(1,1,1,1,0,1,0,0,0,1)\}. \end{aligned}$$

Verify that $\mathbf{D}(C) = \mathbf{D}(C')$. To prove that C and C' are not equivalent, show that there is a coordinate such that all the elements of C have the same symbol on that coordinate, while for no coordinate the same happens in C'.

A8.45. Hint: prove that the ring of classes modulo $x^n - 1$ admits as a representative system the set of polynomials $\{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},\ a_i \in \mathbb{F}_q,\ 0 \leq i < n\}$.

A8.46. Let $x^n - 1 = a(x) \cdot b(x)$. A polynomial $c(x)$ in $\mathbb{F}_q[x]/(x^n - 1)$ is in C if and only if it is divisible by $a(x)$ in $\mathbb{F}_q[x]$, so if and only if its product by $b(x)$ is zero modulo $x^n - 1$.

B8.1. The correct answer is (b). Let us see why. The vector $(0,1,1,1,1,1,1)$ is a word of the Hamming code if and only if it satisfies the system of three linear equations (8.3) on page 410, where the calculations are carried out in $\mathbb{Z}_2$. As the given vector does not satisfy any of the three equations of the system, this means that it is not a word of the Hamming code. Moreover, by the reasoning on page 410, it follows that the error is in the first position, so the correct word is $(1,1,1,1,1,1,1)$. To check that the calculations are correct, it is useful to verify that $(1,1,1,1,1,1,1)$ is actually a word of the Hamming code, that is, it satisfies the system (8.3). If this happens, as in our case, we may be sure that no mistake has been made.

B8.2. The correct answer is (a); indeed the vector satisfies all three equations of the system (8.3).

B8.3. The correct answer is (d), because the vector satisfies the first two equations of the system (8.3), but not the third one, so the error is in the seventh position, by what has been argued on page 410. To double-check this, notice that the correct

vector $(0,1,0,0,0,1,1)$ verifies the system (8.3), that is to say, it is a word of the Hamming code.

B8.4. The correct answer is (c); indeed Hamming distance is by definition the number of different coordinates, which in this case are the second, third, fifth and sixth ones.

B8.6. The correct answer is (c). Indeed, a subset of a vector space is a vector subspace if: (1) it is closed under addition, (2) it is closed under the product by scalars. When we consider binary codes, the scalars are only 0 and 1, so condition (2) is automatically verified. We have only to check condition (1). Notice now that $(0,0,1)+(0,1,0)=(0,1,1)$; hence follows that all other possible sums, that is, $(0,0,1)+(0,1,1)=(0,1,0)$ and $(0,1,0)+(0,1,1)=(0,0,1)$, always give elements belonging to the subset, so it is a vector subspace. Finally, the relation we have found among the elements of the subspace says that the dimension is 2, because $(0,1,0)$ and $(0,0,1)$ clearly are linearly independent vectors.

B8.11. The correct answer is (b); indeed, $(1,1,2,0)=(1,0,1,1)+(0,1,1,2)$, so there are no more than two linearly independent generators (recall that the dimension of a vector space is equal to the greatest number of linearly independent generators).

B8.12. The correct answer is (d). Let us see why. To compute the minimum distance of the code, write all codewords and compute their weight, that is, the number of non-zero coordinates. By Proposition 8.5.3, the minimum distance is equal to the minimum weight of the non-zero words. In our case, we find that the minimum distance is $d=3$. On the other hand, we know that $n=4$ and that $k=2$ by Exercise B8.11, so $d=3=n-k+1$, that is to say, the code is maximum-distance separable, according to Definition 8.5.2 on page 420. Finally, $d=3$ implies that the code detects two errors and corrects one, by Theorem 8.3.4 on page 412.

B8.18. The correct answer is (d). Theorem 8.5.9 on page 424, indeed, says that the minimum distance of the linear code is equal to the minimum number of linearly independent columns of the parity check matrix. So, examine the columns of the matrix given in the exercise. Considering all possible combinations, we see that there are no three columns whose sum is zero (thus being linearly dependent), while there are four columns, for instance, the third, fourth, seventh and eighth one, whose sum is zero (so they are linearly dependent). So we may conclude that the minimum distance of the linear code is four.

Exercises of Chapter 9

A9.1. Notice that every key is an ordered r-tuple of elements of the alphabet (see Exercise A1.21).

A9.5. Start as in the solution of Exercise A8.16.

A9.6. Again, start as in the solution of Exercise A8.16.

A9.10. The claim is trivial if the vector space has dimension 1. Moreover, one implication is trivial. Finally, assume that $AB=BA$. Deduce that A and B have a common eigenvector v. So the subspace $\langle v\rangle$ is invariant under A and B. But then

the orthogonal subspace $\langle v\rangle^{\perp}$ is also invariant under A and B. Then proceed by induction.

A9.11. Every observable of the form

$$\frac{1}{2}\begin{pmatrix} \lambda_1+\lambda_2 & \lambda_1-\lambda_2 \\ \lambda_1-\lambda_2 & \lambda_1+\lambda_2 \end{pmatrix}$$

with $\lambda_1 \neq \lambda_2$.

B9.1. The solution is *HQRC*.

B9.2. The solution is *QMIA*.

B9.6. The answer is NO.

B9.7. We have

$$[B, A] = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}.$$

References

1. Adleman, L.M., Rivest, R.L., Shamir, A.: *A method for obtaining digital signatures and public–key cryptosystems*. Communications of the ACM, **21**, 120–126 (1978)
2. Agrawal, M., Kayal, N., Saxena, N.: *PRIMES in P*. Ann. of Math., **160**, n. 2, 781–793 (2004)
3. Alford, W.R., Granville A., Pomerance, C.: *There are infinitely many Carmichael numbers*. Ann. of Math., **139**, n. 3, 703–722 (1994)
4. Artin, M.: *Algebra*. Prentice Hall, Englewood Cliffs, NJ, USA (1991)
5. Baldi, P.: *Introduzione alla probabilità con elementi di statistica*. McGraw-Hill, Milano (2003)
6. Baylis, J.: *Error–correcting codes*. Chapman and Hall Math., Londra (1998)
7. Bennet, C.H., Brassard, G.: *Quantum cryptography: public key distribution and coin tossing*. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, 175–179 (1984)
8. Bennet, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: *Experimental quantum cryptography*. J. Cryptology, **5**, 3–28 (1992)
9. Bennet, C.H., Brassard, G., Ekert, A.: *Quantum cryptography*. Scientific American October 1992, 50–57 (1992)
10. Boyer, C.B.: *A History of Mathematics*. Wiley, New York (1968).
11. Burton, D.M.: *Elementary number theory*. Allyn and Bacon, Inc., Boston, Mass.-Londra (1980)
12. Canuto, C., Tabacco, A.: *Analisi Matematica 1*. Unitext, Springer-Verlag, Milano (2003)
13. Ciliberto, C.: *Algebra lineare*. Bollati Boringhieri, Torino (1994)
14. Coppersmith, D.: *Fast evaluation of logarithms in fields of characteristic two*. IEEE Transactions on Information Theory IT, **30**, 587–594 (1984)
15. Curzio, M.: *Lezioni di algebra*. Liguori, Napoli (1970)
16. Davenport, H.: *The higher arithmetic. An introduction to the theory of numbers*. Cambridge University Press, Cambridge (1999)
17. Deutsch, D.: *The fabric of Reality*. Allen Lane, Londra (1977)
18. Deutsch, D., Ekert, A.: *Quantum Computation*. Physics World, **11**, n. 3, 33–56 (1998)
19. Diffie, W., Hellman, M.E.: *New directions in cryptography*. IEEE Transactions on Information Theory IT, **22**, 644–654 (1976)

20. Dirac, P.A.M.: *The principles of quantum mechanics*. Oxford University Press, New York (1958)
21. Doxiadis, A.: *Uncle Petros and Goldbach's Conjecture*. Bloombsbury Publ., New York and London (2000)
22. Ebbinghaus, H.D., et al.: *Numbers*. Springer-Verlag, Berlin Heidelberg New York (1991)
23. Garey, M.R., Johnson, D.S.: *Computers and intractability. A guide to the theory of $\mathcal{NP}$–completeness*. W. H. Freeman & C., San Francisco, Calif. (1979)
24. Grimaldi, R.: *Discrete and Combinatorial Mathematics*. Addison–Wesley, 5th ed., Reading, Mass. (1988)
25. Hardy, G. H.: *A Mathematician's Apology*. Cambridge University Press (1940)
26. Hardy, G.H., Wright, E.M.: *An introduction to the theory of numbers*. Oxford Science Publ., 5th ed., New York (1979)
27. Herstein, I.N.: *Topics in Algebra*. Wiley, New York (1975)
28. Hodges, A.: *A. Turing: the Enigma of Intelligence*. Unwin Paperbacks, Londra (1983)
29. Isaac, R.: *The pleasures of probability*. Springer-Verlag, Berlin Heidelberg New York (1995)
30. Koblitz, N.: *A course in number theory and cryptography*. Springer-Verlag, Berlin Heidelberg New York (1994)
31. Kraitchick, M.: *Recherches sur la théorie des nombres*. Gauthiers-Villars, Parigi (1929)
32. Lang, S.: *Algebra*. Addison Wesley, New York (1978)
33. Lenstra, A., Jr., Lenstra, H.W., Jr. (ed.): *The development of the number field sieve*. Springer-Verlag, Berlin Heidelberg New York (1993)
34. Lenstra, H.W., Jr.: *Primality testing*. In: Studiezweek Getaltheorie en Computers, 1–5 September 1980, Stichting Mathematisch Centrum, Amsterdam (1982)
35. Lenstra, H.W., Jr.: *Factoring integers with elliptic curves*. Ann. of Math., **126**, n. 2, 649–673 (1987)
36. van Lint, J.H.: *Introduction to coding theory*. II ed., Springer-Verlag, Berlin Heidelberg New York (1992)
37. van Lint, J.H., van der Geer, G.: *Introduction to coding theory and algebraic geometry*. DMV Seminar 12, Birkhäuser, Basel (1988)
38. Lomonaco, S.J.: *A talk on quantum cryptography or how Alice outwits Eve*. Proc. Sympos. Appl. Math. 58, American Math. Soc., Providence, R.I., 237–264 (2002)
39. McEliece, R.J.: *The theory of information and coding*. Encyclopedia of Math. and its Appl., vol. 3. Addison–Wesley, Reading, Mass. (1977)
40. McEliece, R.J., Ash, R.B., Ash, C.: *Introduction To Discrete Mathematics*. McGraw-Hill, New York, (1989)
41. MacWilliams, F.J., Sloane, N.J.A.: *The theory of error–correcting codes*. North Holland, Amsterdam (1977)
42. Menezes, A., Okamoto, T., Vanstone, S.A.: *Reducing elliptic curves logarithms to logarithms in a finite field*. IEEE Transactions on Information Theory IT, **39**, 1639–1646 (1993)
43. Monk, J. D.: *Introduction to set theory*, McGraw-Hill, New York (1969)
44. Odlyzko, A.M.: *Discrete logarithms in finite fields and their cryptographic significance*. Advances in Cryptology, Proc. Eurocrypt, **84**, 224–314 (1985)
45. Piacentini Cattaneo, G.M.: *Algebra, un approccio algoritmico*. Decibel Zanichelli, Bologna (1996)

46. Pomerance, C., Selfridge, J.L., Wagstaff, S.S.: *The pseudoprimes to* $25 \cdot 10^9$. Math. Comp., **35**, 1003–1026 (1980)
47. Quarteroni, A., Saleri, F.: *Introduzione al calcolo scientifico*. Unitext, Springer-Verlag, Milano (2004)
48. Ribenboim, P.: *The new book of prime numbers records*. Springer-Verlag, Berlin Heidelberg New York (1996)
49. Rosen, K.H.: *Elementary number theory*. Addison–Wesley, Reading, Mass. (1988)
50. Schoof, R.: *Elliptic curves over finite fields and the computation of square roots mod p*. Math. Comp., **44**, 483–494 (1985)
51. Sernesi, E.: *Geometria I*. Bollati Boringhieri, Torino (1989); published in English as Sernesi, E., Montaldi J.: *Linear Algebra: A Geometric Approach*. Kluwer Academic Publishers Group (1992)
52. Shamir, A.: *A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem*. Proc. 23rd annual symposium on the foundation of computer science (Chicago, Ill., 1982), IEEE, New York, 145–152 (1982)
53. Shannon, C.E.: *Communication theory of secrecy systems*. Bell Systems Technical Journal, **28**, 656–715 (1949)
54. Shor, P.W.: *Polynomial–time algorithms for prime factorization and discrete logarithm on a quantum computer*. SIAM J. Computing, **26**, 14–84 (1997)
55. Siegel, C.L.: *Topics in complex function theory, Vol. I*. Wiley, New York (1969)
56. Silverman, J.H.: *The arithmetic of elliptic curves*. Springer-Verlag, Berlin Heidelberg New York (1985)
57. Singh, S.: *Fermat's Last Theorem*. Anchor Books, New York (1998)
58. Singh, S.: *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books, New York (2000)
59. Tenenbaum, G., Mendès France, M.: *The prime numbers and their distribution*. Student Math. Library, vol. 6, American Mathematical Society (2000)
60. Tsfaman, M.A., Vladut, S.G., Zink, T.: *On Goppa codes which are better than the Varshamov–Gilbert bound*. Math. Nachr., **109**, 21–28 (1982)
61. Weil, A.: *Number Theory. An approach through history from Hammurabi to Legendre*. Birkhäuser, Boston (1983)
62. Wiesner, S.: *Conjugate coding*. SIGACT News, **15**, n. 1, 78–88 (1983; original manuscript, around 1970)
63. Wiles, A.: *Modular elliptic curves and Fermat's Last Theorem*. Ann. of Math., **142**, 443–551 (1995)

Index