Solutions, Chapters 1–4

1. Basic Notions

• **1.1.18** Since there are only finitely many possible "games" for any n, and each ends with one of the players winning the game, therefore one of the players must have a winning strategy. We show that this is always the first player. For a proof by contradiction, assume that the second player, Juliet has a winning strategy for some n. This includes that if Romeo starts with $d_1 = 1$, then Juliet can say $d_2 = r$ and continue the game so that she wins. But then Romeo can win starting with $d_1 = r$ and playing as Juliet did before (the number 1 could be the only difference to the previous game, but 1 cannot be chosen in any later step as it divides already $d_1 = r$). This contradiction proves that the first player has a winning strategy for every $n > 1$. — Observe that the proof yields only the fact that the first player can win, but gives no information about the concrete strategy. For numbers n having a complicated structure, it is not known, how Romeo should play (and even a computer cannot help him due to the extremely large number of possible games).

• **1.1.22 (f)** Since $1 + \sqrt{2}$ is a unit and the negative and every power of a unit (to an integer exponent) is a unit again, therefore the given numbers are units, indeed. We prove the converse by contradiction. Assume that there exists a unit ε not listed above. If necessary, we multiply it by -1 to get a unit $\delta > 0$. Then there exists an integer k satisfying $(1+\sqrt{2})^k < \delta < (1+\sqrt{2})^{k+1}$. Multiplying the inequality by the unit $(1+\sqrt{2})^{-k}$, we obtain a unit $u + v\sqrt{2}$ with $1 < u + v\sqrt{2} < 1 + \sqrt{2}$. Obviously, u and v cannot have the same sign (and none of them can be zero). We shall use $|u^2 - 2v^2| = 1$. If $u^2 - 2v^2 = -1$, then the unit $\varrho = v\sqrt{2} - u = 1/(u + v\sqrt{2})$ satisfies $0 < \varrho < 1$. On the other hand, $\varrho > 1$ for $v > 0$ and $u < 0$, and $\varrho < 0$ for $v < 0$ and $u > 0$, providing the contradiction. We get a contradiction similarly also in the case $u^2 - 2v^2 = 1$.

• **1.1.23 (a)** If e is the identity, then it is clearly a unit, as well. For the converse, let ε be a unit. Then $\varepsilon \mid \varepsilon$, so $\varepsilon = \varepsilon q$ for some q. We show that q is an identity. We have $\varepsilon c = \varepsilon q c$ for every c, i.e. $\varepsilon(c - qc) = 0$. There are no zero divisors, hence $c = qc$, so q is an identity, indeed.

• **1.3.11** Since $(a, b) \mid a$, therefore $c(a, b) \mid ca$, and similarly $c(a, b) \mid cb$. This means that $c(a, b)$ is a common divisor of ca and cb, hence $c(a, b)$ divides also

the special common divisor (ca, cb) of ca and cb. Thus $c(a,b)q = (ca, cb)$ for some integer q. We have to show that q is a unit.

Since $c(a,b)q = (ca,cb) \mid ca$, therefore $q(a,b) \mid a$, and similarly $q(a,b) \mid b$. This means that $q(a,b)$ is a common divisor of a and b, hence it divides also their special common divisor: $q(a,b) \mid (a,b)$. So $q \mid 1$, thus q is a unit, indeed.

• **1.3.13** Since $(n,k) \mid n$, thus $a^{(n,k)}-1 \mid a^n-1$, and similarly $a^{(n,k)}-1 \mid a^k-1$. This means that $a^{(n,k)}-1$ is a common divisor of a^n-1 and a^k-1.

Now we show the special property, i.e. any common divisor d of a^n-1 and a^k-1 divides also $a^{(n,k)}-1$. Obviously, u and v have opposite signs in the representation $(n,k) = nu+kv$, so we may assume $(n,k) = nr-ks$ where r and s are positive integers. Then

$$d \mid a^n-1 \mid a^{nr}-1 \qquad \text{and} \qquad d \mid a^k-1 \mid a^{ks}-1,$$

so

$$d \mid (a^{nr}-1)-(a^{ks}-1) = a^{nr}-a^{ks} = a^{ks}(a^{nr-ks}-1) = a^{ks}(a^{(n,k)}-1)\,.$$

Here d is coprime to the first factor a^{ks} of the last product as $d \mid a^{ks}-1$. Thus d must divide the second factor $a^{(n,k)}-1$.

• **1.4.5** We shall use that $c^k+(t+1-c)^k$ is divisible by $c+(t+1-c) = t+1$ for any c if k is odd.

Let first t be even. Then the grouping

$$\big(1^k+t^k\big)+\big(2^k+(t-1)^k\big)+\ldots+\big((t/2)^k+(1+(t/2))^k\big)$$

shows that the sum is divisible by $t+1$. Therefore, it can be a prime only if it equals $t+1$. However,

$$1^k+2^k+3^k+\ldots+t^k \ge 1+2+\ldots+t = t(t+1)/2 \ge t+1\,,$$

and equality holds only for $t=2$ and $k=1$. In this case, $1^1+2^1=3$ is a prime, indeed.

If t is odd, then the only change is that the sum has a middle term $\big((t+1)/2\big)^k$. So the sum is divisible by $(t+1)/2$ by the previous argument. As the sum is greater than $(t+1)/2$, it can never be a prime.

Thus the only solution is $t=2$, $k=1$.

We can solve the problem similarly also using the divisibility by t instead of $t+1$.

• **1.5.8** Let p be irreducible, and assume $p \mid ab$. We have to verify that at least one of $p \mid a$ and $p \mid b$ holds.

If $a = 0$, then $p \mid a$. If a is a unit, then $p \mid b$.

If a and b are different from zero and units, then factor them into the product of irreducible elements:

$$a = u_1 \dots u_k, \qquad b = v_1 \dots v_m.$$

Hence $ab = u_1 \dots u_k v_1 \dots v_m$.

The assumption $p \mid ab$ implies $ab = ps$ for some integer s. Write s as a product of irreducible elements: $s = w_1 \dots w_n$. Then $ab = pw_1 \dots w_n$.

By the Fundamental Theorem, the two decompositions of ab are essentially the same, so p must be an associate of some u_i or v_j. Accordingly, $p \mid a$ or $p \mid b$.

• **1.5.10** 2 and 3 suits, e.g. $2 = 1^3 + 1^3$ and $3^2 = 2^3 + 1^3$. We claim that no other primes meet the requirements.

Assume $x^3 + y^3 = p^\alpha$. Dividing the equation by $(x, y)^3$, we obtain a similar equation where the (new) x and y are coprime (and the new α may be smaller than the original was).

Factoring yields $(x + y)(x^2 - xy + y^2) = p^\alpha$. The Fundamental Theorem (and positivity) imply

$$\text{(S.1.1)} \quad x + y = p^\beta, \qquad x^2 - xy + y^2 = p^\gamma, \qquad \beta > 0, \quad \gamma \geq 0, \quad \beta + \gamma = \alpha.$$

Substituting (S.1.1) into the identity $(x+y)^2 - (x^2 - xy + y^2) = 3xy$, we obtain

$$\text{(S.1.2)} \qquad p^{2\beta} - p^\gamma = 3xy\,.$$

If $\gamma = 0$, then

$$1 = x^2 - xy + y^2 = (x - y)^2 + xy \geq xy \geq 1 \cdot 1 = 1$$

giving $x = y = 1$ and $p = 2$.

If $\gamma > 0$, then $p \mid 3xy$ by (S.1.2). If $p \mid x$, then $p \mid x + y (= p^\beta)$ implies $p \mid y$, which contradicts x and y being coprime. We get a contradiction similarly from $p \mid y$. Hence $p \mid 3$, i.e. only $p = 3$ is possible.

• **1.6.3 (a)** For a proof by contradiction, assume that $x(x + 1) = z^k$ holds for some integers $x > 0$, $z > 0$, and $k \geq 2$. Since $(x, x + 1) = 1$, therefore

$x = u^k$ and $x + 1 = v^k$ for some positive integers u and v by Exercise 1.6.2a. So $v^k - u^k = 1$. But this is impossible as

$$v^k - u^k \geq (u+1)^k - u^k > ku^{k-1} > 1.$$

• **(b)** We have to modify the previous argument slightly. The three factors are generally not pairwise coprime, but the middle one is coprime to the other two. Thus $(x-1)x(x+1) = z^k$ and $(x, x^2-1) = 1$ imply $x = u^k, x^2 - 1 = v^k$. Then $(u^2)^k - v^k = 1$ which is impossible.

• **(c)** First we show that the product of four consecutive positive integers cannot be a square, i.e.

$$(x-1)x(x+1)(x+2) = z^2 \tag{S.1.3}$$

is impossible (for $x \geq 2$). Put $x(x+1) = 2y$, then $(x-1)(x+2) = 2y - 2$, so (1) can be rewritten as $y(y-1) = (z/2)^2$. We saw in (a) that the product of two consecutive positive integers is never a square, so (S.1.3) cannot hold either.

Consider now $k \geq 3$, and for a proof by contradiction, assume that the product of four consecutive positive integers is a kth power. Observe that the odd one of the middle two numbers is always coprime to the other three. Then, as seen in (b), both this factor and the product of the other three are kth powers. This means either

$$(u^k - 1)(u^k + 1)(u^k + 2) = v^k \tag{S.1.4}$$

or

$$(u^k - 1)(u^k + 1)(u^k - 2) = v^k\,. \tag{S.1.5}$$

We prove, however, that for $k \geq 3$, the left-hand side in (S.1.4) and (S.1.5) fall between the kth powers of two consecutive integers, hence these cannot be kth powers themselves.

Consider first the left-hand side of (S.1.4): $u^{3k} + 2u^{2k} - u^k - 2$. We show

$$(u^3)^k < u^{3k} + 2u^{2k} - u^k - 2 < (u^3 + 1)^k\,.$$

The first inequality is obvious, and the second follows (for $k \geq 3$) since

$$(u^3+1)^k > u^{3k} + ku^{3(k-1)} > u^{3k} + 2u^{2k} > u^{3k} + 2u^{2k} - u^k - 2.$$

Consider now the left-hand side of (S.1.5): $u^{3k} - 2u^{2k} - u^k + 2$. We demonstrate

$$(u^3)^k > u^{3k} - 2u^{2k} - u^k + 2 > (u^3 - 1)^k \,.$$

The first inequality is obvious. The second is equivalent to $(u^3-1)(u^3-3) > 0$ for $k = 3$ which is true. For $k \geq 4$, rewrite the second inequality as

$$(u^3)^k - (u^3 - 1)^k > 2u^{2k} + u^k - 2.$$

We can verify this as follows:

$$\begin{aligned}(u^3)^k - (u^3 - 1)^k = u^{3(k-1)} + u^{3(k-2)}(u^3 - 1) + \ldots + (u^3 - 1)^{k-1} > \\ > u^{3k-3} + u^{3k-6} > u \cdot u^{2k} + u^k > 2u^{2k} + u^k - 2\,.\end{aligned}$$

• **1.6.4** Assume $2^{p-1} - 1 = n^2 p$. Since $p = 2$ is not a solution, so $p-1$ is even, and the equation is equivalent to

$$(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1) = n^2 p.$$

The two factors on the left-hand side are coprime, so the following two cases can occur: either

$$2^{(p-1)/2} - 1 = u^2 \qquad \text{and} \qquad 2^{(p-1)/2} + 1 = pv^2\,, \tag{S.1.6}$$

or

$$2^{(p-1)/2} - 1 = pu^2 \qquad \text{and} \qquad 2^{(p-1)/2} + 1 = v^2\,. \tag{S.1.7}$$

In Case (S.1.6), the left-hand side of the first equality gives a remainder 3 divided by 4 for $p > 3$, and so cannot be a square. Hence only $p = 3$ is possible which satisfies the requirements, indeed.

In Case (S.1.7), the equality assumes the form $2^{(p-1)/2} = (v-1)(v+1)$. This implies that both $v - 1$ and $v + 1$ must be powers of two. Since their difference is 2, only the pair 2 and 4 can occur, i.e. $v = 3$. This yields $p = 7$ which satisfies the requirements, indeed.

Hence all solutions are $p = 3$ and $p = 7$.

• **1.6.10** *First solution*: If $n = 1$, then $A(1) = B(1) = d(1) = 1$, so we have equality. For $n > 1$, let the standard form of n be $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ where $\alpha_i > 0$. The squarefree divisors are those where the exponent of every p_i is 0

or 1, thus $A(n) = 2^r$. In the square divisors, the exponent of every p_i is even, so $B(n) = (1 + \lfloor \alpha_1/2 \rfloor) \dots (1 + \lfloor \alpha_r/2 \rfloor)$.

To prove (a), consider the inequalities $2(1 + \lfloor \alpha_i/2 \rfloor) \geq \alpha_i + 1$ (we have $>$ for α_i even, and $=$ for α_i odd). Multiplying these inequalities for $i = 1, 2, \dots, r$, the left-hand side of the product is $A(n)B(n)$, and the right-hand side is $d(n)$. This shows that equality holds if and only if $2(1 + \lfloor \alpha_i/2 \rfloor) = \alpha_i + 1$ for every i, i.e. every α_i is odd.

• *Second solution*: Factoring out the largest square divisor from a number, the Fundamental Theorem implies that every positive integer has a unique decomposition into the product of a square and a squarefree number. Thus, also every divisor of n can uniquely be written as the product of a square divisor and a squarefree divisor of n. So $d(n) \leq A(n)B(n)$. We have equality if and only if all these products are divisors of n. If the exponent of a prime p_i is even in the standard form of n, i.e. $\alpha_i = 2m$, then the product $p_i^{2m} p_i$ is not a divisor of n. We can check similarly that if the exponent of every prime is odd in the standard form of n, then all such products divide n, indeed. Thus equality holds if and only if every prime occurs with an odd exponent in the standard form of n.

• **1.6.28** The game terminates for every initial position of the coins if and only if the number of monkeys is a power of two.

Replacing heads by -1 and tails by $+1$, we can rephrase the problem as follows. Let each of the numbers $x_1, x_2, \dots, x_n$ be 1 or -1, form the products $x_1x_2, x_2x_3, \dots, x_nx_1$, and iterate this procedure. We have to find all n for which the sequence of pure 1s will necessarily appear whatever the original numbers were.

We show first that the game does not terminate necessarily for an odd $n > 1$. In each step, the product of the new numbers is the square of the product of the previous numbers, hence it must equal $+1$. Therefore, the number of -1s must be even during the game (except perhaps for the initial position). So, if the starting n-tuple contained both a 1 and a -1, then just before the end of the game, every number has to be -1. But this would mean an odd number of -1s which is impossible. (Thus the game terminates for an odd n only if we start uniformly with 1s or -1s.)

Consider now $n = rt$ with an odd $t > 1$. If the starting position is periodic with a period of length t (and not all numbers are the same), then the argument given for the odd case shows that the game will not terminate.

Finally, we prove that the game ends if $n = 2^k$. Writing a few steps in detail, we can conjecture and then verify by induction on r or by Pascal's

triangle that the first term of our sequence after r steps is

$$x_1^{\binom{r}{0}} x_2^{\binom{r}{1}} \dots x_{r+1}^{\binom{r}{r}} \tag{S.1.8}$$

where we define x_i for $i > n$ by $x_1 = x_{n+1} = x_{2n+1} = \dots, x_2 = x_{n+2} = \dots$, etc. (this is true for every n, not just for the powers of two). Applying this for $r = n = 2^k$, we obtain that the exponents in (1) are 2 for x_1 and $\binom{2^k}{i-1}$ for the other x_i. These exponents are all even (see Exercise 1.6.27c2). So the product in (S.1.8) is a square, hence it equals $+1$. We get exactly the same way that all other terms of the sequence are $+1$ after the nth step. Thus the game terminates here at the latest.

• **1.6.29** *First solution*: Let $1 \le k \le n$. As $n! + k > k$, there must be a prime p that occurs with a higher exponent in the standard form of $n! + k$ than in the standard form of k. Let $p^\alpha \mid k$, $p^{\alpha+1} \nmid k$, , and $p^{\alpha+1} \mid n! + k$ (for some integer $\alpha \ge 0$). We claim that p does not divide the other numbers $n! + t$ $(t = 1, 2, \dots, n,\ t \ne k)$.

This is obvious for $p > n$, since then p can divide at most one of n consecutive integers. So it suffices to check $p \le n$. For a proof by contradiction assume $p \mid n! + t$ for some $1 \le t \le n$ and $t \ne k$. As $p \mid n!$, therefore $p \mid (n! + t) - n! = t$, and $kt \mid n!$ implies $p^{\alpha+1} \mid n!$. But this is a contradiction since $p^{\alpha+1} \mid n! + k$ and $p^{\alpha+1} \nmid k$.

• *Second solution*: We show first that each number $n! + k$ $(1 \le k \le n)$ has a prime divisor larger than $n/2$. Moreover, we claim that every prime divisor p of the second factor in $n! + k = k(n!/k + 1)$ is bigger than $n/2$. For a proof by contradiction, assume $p \le n/2$. The number $n!/k$ is the product of all numbers from 1 to n except k. If $p \le n/2$, then both p and $2p$ occur among the factors of $n!$, so at least one of them occurs also in $n!/k$ (this is p for $k = 2p$; it is $2p$ for $k = p$; and both remain for other values of k). So p divides both $n!/k$ and $n!/k + 1$ which is impossible.

Now we prove that any prime divisor $q > n/2$ of $n! + k$ meets the requirements. It suffices to show that q can divide at most one of the numbers $n! + j$ $(1 \le j \le n)$. For $q \ge n$ this is obvious, as we have only n consecutive integers. If $n/2 < q < n$, then q occurs in $n!$. So, if q divides $n! + j$, then it divides also $(n! + j) - n! = j$. But $2q > n \ge j > 0$, thus only $q = j$ is possible. This means that j is uniquely determined in this case, as well.

• **1.6.30** The maximum is 9.

We prove first that 9 pairwise coprime numbers can be attained. Let $p_1, p_2, \dots, p_{4991}$ be distinct primes and P be their product. Then the following

5000 numbers meet the requirements:

$$a_i = P/p_i, i = 1, 2, \ldots, 4991;\ b_j = p_j, j = 1, 2, \ldots, 8;\ \text{and } b_9 = p_9 \cdot p_{10} \cdot \ldots \cdot p_{4991}.$$

Here $b_1, b_2, \ldots, b_9$ are pairwise coprime. We show that the lcm of any ten numbers is P. Every a_i and b_j divides P, so the lcm cannot be bigger than P. On the other hand, the lcm of two or more a_i is P, and the lcm of all b_j is P, as well. Since any ten numbers either contain at least two a_i, or contain all b_j, their lcm cannot be less than P.

Now we show that we cannot have 10 pairwise coprime numbers. For a proof by contradiction, assume that the lcm of any ten of the distinct positive integers $c_1, c_2, \ldots, c_{5000}$ is the same C and (say) $c_1, c_2, \ldots, c_{10}$ are pairwise coprime. Then the lcm of $c_1, c_2, \ldots, c_{10}$ is $C = c_1 \cdot c_2 \cdot \ldots \cdot c_{10}$. Consider now c_{11}. According to the condition, the lcm of $c_2, c_3, \ldots, c_{10}, c_{11}$ is C, as well. This means that all prime divisors of c_{11} must occur also in one of $c_1, \ldots, c_{10}$, and c_{11} must contain the prime factors of c_1 with exactly the same exponents as c_1 (since these primes do not divide any of the numbers $c_2, \ldots, c_{10}$ coprime to c_1). Repeating the argument for all groups of ten numbers composed of c_{11} and nine elements from $c_1, c_2, \ldots, c_{10}$, we obtain that only $c_{11} = C$ is possible. The same applies also for c_{12}, which is a contradiction as the numbers have to be distinct.

• **1.6.34** I. We show first that $S(i)$ is a (positive) composite number for every $i \geq 2$. $S(i) \geq i \geq 2$ implies $S(i) \neq 1$. Further, $S(i)$ cannot be a prime, since a product of distinct positive integers with a prime maximal element cannot be a square as it is divisible only by the first power of this prime.

II. We prove now $S(i) \neq S(j)$ for $i < j$. For a proof by contradiction, assume $S(i) = S(j) = n$. Then both $b_1 b_2 \ldots b_r$ and $c_1 c_2 \ldots c_s$ are squares for some $i = b_1 < b_2 < \ldots < b_r = n$ and $j = c_1 < c_2 < \ldots < c_s = n$. We multiply the two products and delete both copies of the factors occurring twice (i.e. we divide $b_1 b_2 \ldots b_r c_1 c_2 \ldots c_s$ by the squares of the common factors of the original two products).

The new product is a square, its smallest element is i (due to $i < j$), and its maximal element is less than n (since we deleted the square of $n = b_r = c_s$). This, however, contradicts $S(i) = n$.

III. Finally, we verify that every composite n occurs among the values $S(i)$. Consider all sets of numbers $u_1 < u_2 < \ldots < u_k$ where $u_k = n$ and the product $u_1 u_2 \ldots u_k$ is a square. There always exists such a set: if n is a square, then $k = 1$, $u_1 = n$ suits, and if n is not a square, insert those primes that occur in the standard form of n with an odd exponent.

Let m be the maximal value among the smallest numbers u_1 of these sets. We claim that $S(m) = n$.

For a proof by contradiction, assume that $v_1 v_2 \dots v_q$ is a square for some numbers $m = v_1 < v_2 < \dots < v_q$ with $v_q < n$. Similarly to part II., we form the product of all u and v and delete both copies of the factors occurring twice. This product contains n, but m is missing. Hence this product is a square, its maximal factor is n, but its smallest factor is bigger than m. This, however, contradicts the maximality of m.

• **1.6.35 (a)** No.

•*First proof*: For a proof by contradiction, assume that the arithmetic progression $a+kd$, $k = 0, 1, 2, \dots$ satisfies the requirements. Let p be a prime that does not divide d. It is easy to show that the numbers $a + kd$, $k = 1, 2, \dots, p^2$, have distinct remainders at the division by p^2. This means that we obtain all possible residues, including also the remainder p. But a power cannot be of the form $mp^2 + p$, since it is divisible exactly by the first power of p.

• *Second proof*: An arithmetic progression with difference d has about N/d elements up to N. The number of powers up to N is, however, much less, it is not more than $N^{1/2} + N^{1/3} + N^{1/4} + \dots \le N^{1/2} + \log_2 N \cdot N^{1/3} < 2\sqrt{N}$ for N large enough. So, choosing a sufficiently big N, there are "too few" powers to make every element of the arithmetic progression a power.

• *Third proof*: We use Dirichlet's Theorem about the primes in arithmetic progressions: If $(A, D) = 1$, then the arithmetic progression $A + kD$ contains infinitely many primes (Theorem 5.3.1). Factoring out $m = (a, d)$ from $a+kd$, then $a + kd = m(A + kD)$ would be infinitely often of the form mp, but this cannot be a power for a prime p bigger than m.

• *Fourth proof*: If the first term of the arithmetic progression is $a = b^r$ where $r > 1$ is the maximal possible exponent (we may assume $a > 1$), then a simple calculation yields that the term $a + (a^2 d^{r-1})d$ cannot be a power.

• **(b)** Yes. We prove by induction. Assume that $a_1^{k_1}, \dots, a_n^{k_n}$ is an arithmetic progression with difference d, and let $s = a_n^{k_n} + d$ be its $n + 1$st term. Multiplying every term by $s^{k_1 k_2 \dots k_n}$, we obtain an arithmetic progression of $n + 1$ powers.

2. Congruences

• **2.2.4 (f)** There is a complete residue system modulo m purely of repunits if and only if m is of a power of three.

Assume first that m has a prime divisor $p \neq 3$ and still some repunits produce all possible remainders modulo m. Then also modulo p we get all remainders, i.e. there exists a complete residue system modulo p of repunits, as well.

Multiplying this complete residue system modulo p by 9 and adding 1, we obtain powers of 10. Due to $(9, p) = 1$, these form again a complete residue system modulo p. But this is impossible: for $p = 2$ or 5, all remainders are zero, and for other primes p, the zero remainder will certainly not occur.

This contradiction shows that if m is not a power of three, then there are no such repunits.

For the converse, consider $m = 3^k$. We show that the first m repunits are pairwise incongruent modulo m, so they form a complete residue system.

For a proof by contradiction, assume that the difference of the jth and ith repunits is a multiple of 3^k for some $1 \leq i < j \leq m$. Dividing this difference by 10^i, we obtain the $j - i$th repunit, and due to $(3^k, 10) = 1$, this is still a multiple of 3^k. We can prove by induction on r that the 3^rth repunit is the first one divisible by 3^r (see Exercise 1.3.12b). This implies the contradiction $3^k = m \leq j - i < m$.

Thus $m = 3^k$ meets the requirements, indeed.

• **(g)** There is a complete residue system modulo m purely of powers if and only if m is squarefree, i.e. m is the product of distinct primes.

If m is not squarefree, i.e. m is a multiple of p^2 for some prime p, then e.g. the remainder p can not be attained: p occurs with exponent 1 in the standard form of every element of this residue class, so none of these can be a power.

We start to verify the "if" part by showing that, to any prime p and integer c, we can find an $s > 0$ so that $c^{s+1} - c$ is divisible by p. If c is a multiple of p, then clearly every s suits. Otherwise, we apply that the powers of c can give only finitely many remainders when divided by p, thus p divides $c^t - c^r = c^{r-1}(c^{t-r+1} - c)$ for some $r < t$. But then $(p, c) = 1$ implies that p divides also $c^{t-r+1} - c$.

Let now m be $m = p_1 \dots p_r$, $p_i \neq p_j$. To every c, we shall generate a $T > 0$ such that c^{T+1} and c have the same remainder at the division by m, i.e. $c^{T+1} - c$ is a multiple of m. Consider the exponents s_i belonging to c and p_i in the previous paragraph; their product satisfies the requirement for T.

Finally, consider any complete residue system $c_1, \dots, c_m$ modulo m with $c_i > 1$. We saw above that, to every c_i, there is some $k_i > 1$ satisfying $c_i \equiv c_i^{k_i} \pmod{m}$. Then the powers $c_i^{k_i}$ form a complete residue system modulo m.

• **2.2.8 (a)** The squirrels can gather on one tree if and only if m is odd or is

a multiple of 4.

For m odd, the squirrel on the highest tree should remain there, its two neighbors should jump onto this tree in one step, the two second neighbors should jump here in two steps, etc.

If m is divisible by 4, then, after the above steps, one squirrel will remain on the tree opposite to the highest tree. She can arrive at the highest tree by an even number of jumps whereas another squirrel keeps jumping to and fro between the highest tree and one of its neighbors.

Finally, if m is even but not divisible by 4, then the squirrels cannot gather on one tree. If we count with how many jumps a squirrel can get on the designated tree (taking into consideration that the squirrel can jump in both directions in every minute) and add these numbers for all squirrels, then the total number of jumps is always odd. Thus the task cannot be done to meet the requirements.

• **(b)** Exactly the odd numbers m suit the conditions.

The arguments in (a) remain valid if m is not a multiple of 4.

If m is divisible by 4 (or is simply even), then we number the trees consecutively from 1 to m. In every minute and for each squirrel, we register the serial number of the tree where the squirrel actually sits, and add these m numbers (if there are k squirrels on a tree, then the serial number of this tree occurs k times in the sum). The remainder of this sum modulo m remains the same in every step. In the initial position, this is the remainder of $1 + 2 + \ldots + m = m(m+1)/2 = m \cdot (m/2) + m/2$, which is $m/2$ (we could have referred also to Exercise 2.2.7a). If every squirrel is on the same tree, then the remainder is 0, hence this situation cannot be achieved.

• **2.2.12 (a)** If $(a, m) = 1$, then ar_i form a reduced residue system, so they are pairwise incongruent modulo m.

We show that these numbers are pairwise incongruent also in the case $m = 4k + 2$ and $(a, m) = 2$. Assume $ar_i \equiv ar_j \pmod{m}$. By the cancelation rule of Theorem 2.1.3,

$$r_i \equiv r_j \pmod{\frac{m}{2}}. \tag{S.2.1}$$

Further, both r_i and r_j are odd due to $(r_i, m) = (r_j, m) = 1$. Thus

$$r_i \equiv r_j \pmod{2}. \tag{S.2.2}$$

Using $(m/2, 2) = 1$, congruences (S.2.1) and (S.2.2) imply $r_i \equiv r_j \pmod{m}$, i.e. $i = j$.

We give now two proofs that the numbers ar_i will not be pairwise incongruent modulo m in any other case.

First proof: We investigate the following two cases separately: (A) m and a share a prime divisor $p > 2$; (B) $2 \mid a$ and $4 \mid m$.

In Case (A),

$$a \cdot \Big(\frac{m}{p} + 1\Big) \equiv a \cdot 1 \equiv a \cdot \Big(\frac{2m}{p} + 1\Big) \pmod{m}. \tag{S.2.3}$$

If $(m/p + 1, m) = 1$, then for some $i \neq j$,

$$r_i \equiv 1 \not\equiv \frac{m}{p} + 1 \equiv r_j \pmod{m}, \quad \text{but} \quad ar_i \equiv ar_j \pmod{m}.$$

If $(2m/p + 1, m) = 1$, then we obtain similarly that the numbers ar_i are not pairwise incongruent modulo m.

Hence, to settle Case (A), it suffices to show that at least one of $m/p + 1$ and $2m/p + 1$ is coprime to m.

Let $(m/p + 1, m) = d$. Then $d \mid p(m/p + 1) - m = p$, so only $d = p$ or $d = 1$ is possible. We get similarly that $(2m/p + 1, m) = p$ or 1.

Both greatest common divisors, however, cannot equal p, since

$$2\Big(\frac{m}{p} + 1\Big) - \Big(\frac{2m}{p} + 1\Big) = 1$$

implies that $m/p + 1$ and $2m/p + 1$ are coprime.

Case (B) is similar, we use $(m/2 + 1, 2) = 1$ and (S.2.3).

Second proof: We shall use Euler's φ function.

Let p be an arbitrary prime divisor of m. There are $\varphi(m)$ numbers r_i, and these fall into (at most) $\varphi(m/p)$ residue classes modulo m/p. So, if $\varphi(m) > \varphi(m/p)$, then some r_i and r_j $(i \neq j)$ must have the same remainder at division by m/p implying $m \mid ar_i - ar_j$ for $p \mid a$. This means that if the numbers ar_i are pairwise incongruent mod m, then $\varphi(m) = \varphi(m/p)$ must hold for every common prime divisor p of a and m.

We can easily deduce from the formula for $\varphi(n)$ (see Theorem 2.3.1) that

$$\varphi(m) = p\varphi(m/p) \text{ if } p^2 \mid m; \quad \text{and} \quad \varphi(m) = (p-1)\varphi(m/p) \text{ if } (p, m/p) = 1\,.$$

Thus $\varphi(m) = \varphi(m/p)$ if and only if $p = 2$ and $(2, m/2) = 1$. This means that if ar_i are pairwise incongruent and a and m are not coprime, then m is necessarily even but not a multiple of 4 and $(a, m) = 2$.

• **(b)** There are $\varphi(m)$ pairwise incongruent numbers $r_i + b$, hence they form a reduced residue system if and only if each of them is coprime to m.

Let $p_1, \ldots, p_s$ be all distinct prime divisors of m. We show first that if $p_1 \cdot \ldots \cdot p_s \mid b$, then $(r_i + b, m) = 1$.

Since

$$p_j \mid b,\ p_j \nmid r_i \Longrightarrow p_j \nmid r_i + b$$

for every $1 \le j \le s$, i.e. $r_i + b$ and m have no common prime divisors, indeed.

We give two proofs that no other b suits, i.e. $(r_i + b, m) \neq 1$ for some i.

First proof: Assume that among the primes p_j, exactly $p_1, \ldots, p_k$ divide b. By the assumption, $k < s$. If no p_j divides b, then we handle it as $k = 0$.

Let $v = p_{k+1} \ldots p_s - b$. Then $(v, m) = 1$, as no p_j divides v, since each p_j divides exactly one of the two terms in the difference $p_{k+1} \ldots p_s - b$.

This implies that $r_i \equiv v \pmod{m}$ for some i. However, $r_i + b \equiv v + b = p_{k+1} \ldots p_s \pmod{m}$, so $r_i + b$ is not coprime to m.

Second proof: Assume that the numbers $a_i + b$ form a reduced residue system. Then $a_1 + b \equiv a_s$ for some s. This implies $a_1 + 2b \equiv a_s + b$. By the assumption, $(a_s + b, m) = 1$, hence also $(a_1 + 2b, m) = 1$ by Theorem 2.2.5. Continuing the procedure, we get by induction that $(a_1 + jb, m) = 1$ for every $j \ge 0$.

Let now p be a prime divisor of m that does not divide b. Then, by Theorem 2.2.4, $a_1, a_1 + b, a_1 + 2b, \ldots, a_1 + (p-1)b$ is a complete residue system mod p (we multiplied the complete residue system $0, 1, \ldots, p-1$ by b and added a_1). Thus some $a_1 + tb$ is divisible by p, which contradicts $(a_1 + tb, m) = 1$.

• **2.2.13** There exist such residue systems if and only if $(k, m) = 1$.

Sufficiency: Assume $(k, m) = 1$ and choose

$$a_i = 1 + ki, \quad i = 1, 2, \ldots, m, \qquad \text{and} \qquad b_j = 1 + mj, \quad j = 1, 2, \ldots, k\,.$$

These are complete residue systems modulo m and modulo k, resp., by Theorem 2.2.4.

We show that the mk products $a_i b_j$ form a complete residue system modulo mk, i.e. they are pairwise incongruent.

Assume

$$(1 + ki)(1 + mj) \equiv (1 + kr)(1 + ms) \pmod{mk}.$$

Performing the multiplications, subtracting 1 from both sides, and omitting the multiples of mk, we obtain

$$ki + mj \equiv kr + ms \pmod{mk}. \tag{S.2.4}$$

Considering (S.2.4) only modulo m, it reduces to $ki \equiv kr \pmod{m}$. Dividing by k coprime to the modulus m, we get $i \equiv r \pmod{m}$, i.e. $i = r$. We obtain $j = s$ similarly.

Necessity: Assuming $(m, k) \neq 1$, we have to demonstrate that the products $a_i b_j$, formed from the complete residue systems $a_1, \ldots, a_m$ (modulo m) and $b_1, \ldots, b_k$ (modulo k), cannot yield a complete residue system modulo mk.

Let p be a common prime divisor of m and k. Then there are m/p and k/p multiples of p among the elements a_i and b_j, resp.

The product $a_i b_j$ is divisible by p if and only if a_i or b_j is a multiple of p. Thus

$$m \cdot \frac{k}{p} + k \cdot \frac{m}{p} - \frac{m}{p} \cdot \frac{k}{p} = \frac{2mk}{p} - \frac{mk}{p^2} \tag{S.2.5}$$

products $a_i b_j$ are divisible by p. (The negative term stands for the number of products when both a_i and b_j are multiples of p since these products were counted twice in the previous sum.) In a complete residue system modulo mk, however, there are mk/p elements divisible by p, which is not equal to (S.2.5) by $p > 1$. Hence, the products $a_i b_j$ never form a complete residue system modulo mk.

• **2.2.14 (a)** *Necessity*: If $(a, b) = d > 1$, then every element of T is a multiple of d, thus e.g. the reduced residue classes are not represented by them.

Sufficiency: There are ab elements in T, so we need to verify the pairwise incongruence. If

$$i_1 b + j_1 a \equiv i_2 b + j_2 a \pmod{ab},$$

then this congruence holds also modulo a: $i_1 b \equiv i_2 b \pmod{a}$. Since $(a, b) = 1$, we can cancel by b yielding $i_1 \equiv i_2 \pmod{a}$, i.e. $i_1 = i_2$. We obtain $j_1 = j_2$ similarly.

• **(b)** The necessity and the pairwise incongruence for the sufficiency can be verified the same way as in (a). To complete the proof of sufficiency, we have to show that assuming $(a, b) = 1$, every element of R belongs to a reduced residue class and every reduced residue class is represented by some element of R. This means:

(A) The elements of R are coprime to ab; and

(B) If $(u, ab) = 1$, then R contains an element v satisfying $u \equiv v \pmod{ab}$.

To prove (A), consider an arbitrary prime divisor p of ab. We show that p does not divide $r_i b + s_j a$.

As p is a prime and $(a, b) = 1$, the following two cases are possible:

$$(\alpha)\ p \mid a \text{ and } p \nmid b, \qquad (\beta)\ p \nmid a \text{ and } p \mid b\,.$$

In Case (α), $p \nmid b$ and $p \nmid r_i$. As p is a prime, this implies $p \nmid r_i b$. But $p \mid s_j a$, thus $p \nmid r_i b + s_j a$, indeed. We can settle Case (β) similarly.

Finally, to verify (B), let $(u, ab) = 1$, and write u in the form

$$u = rb + sa. \tag{S.2.6}$$

This can be done as the Diophantine equation $u = bx + ay$ is solvable due to $(a, b) = 1$.

Clearly, $(r, a) \mid ab$, and (S.2.6) implies $(r, a) \mid u$. Since $(u, ab) = 1$, so $(r, a) = 1$. Therefore $r \equiv r_i \pmod{a}$ for some i. Similarly, $s \equiv s_j \pmod{b}$ for some j.

We show that the element $v = r_i b + s_j a$ of R is congruent to u modulo ab. Considering

$$v - u = (r_i b + s_j a) - (rb + sa) = (r_i - r)b + (s_j - s)a,$$

the last sum is clearly divisible by ab as $r_i - r$ in the first term is a multiple of a and $s_j - s$ in the second term is a multiple of b.

• **(c)** There are $\varphi(a)\varphi(b)$ elements in R on the one hand, and R is a reduced residue system modulo ab for $(a, b) = 1$, hence it has $\varphi(ab)$ elements on the other hand.

• **2.3.18** The integers $n \le 3$ clearly suit.

We show that $\varphi(n!) = k!$ is impossible for $n > 3$. This is obvious for $n = 4$, so we investigate $n \ge 5$.

Let $A(j)$ be the exponent of 2 in the standard form of j.

Since $k < n$, also

$$A(k!) \le A(n!)\,. \tag{S.2.7}$$

But $\varphi(n!)$ necessarily contains the factors $2^{A(n!)-1}$, $3-1$, and $5-1$, thus

$$A\big(\varphi(n!)\big) \ge (A(n!) - 1) + 1 + 2 > A(n!)\,. \tag{S.2.8}$$

(S.2.7) and (S.2.8) imply $A\big(\varphi(n!)\big) > A(k!)$, hence $\varphi(n!) = k!$ cannot hold.

• **2.3.19** A reduced residue system modulo m can form an arithmetic progression if and only if m is a prime, or the double of a prime, or a power of two.

Sufficiency: The following sets meet the requirements: $1, 3, \ldots, 2^k - 1$ for $m = 2^k$; $1, 2, \ldots, p-1$ for $m = p$; and $p+2, p+4, \ldots, 2p-1, 2p+1, \ldots, 3p-2$ for $m = 2p$ (where $p > 2$ is a prime).

Necessity: For a proof by contradiction, assume that m is not of the above form and the arithmetic progression

$$a, a+d, \ldots, a+(\varphi(m)-1)d \tag{S.2.9}$$

is still a reduced residue system modulo m.

Let p be an odd prime divisor of m.

If $p \mid d$, then every element in the above arithmetic progression is congruent to a modulo p. This cannot be true, however, for both of the elements representing the reduced residue classes $(1)_m$ and $(-1)_m$, as $1 \not\equiv -1 \pmod{p}$.

If $(p, d) = 1$, then $a, a+d, \ldots, a+(p-1)d$ is a complete residue system modulo p. Hence it contains also a multiple of p that is not coprime to m. Therefore, this number cannot occur in (S.2.9) which means that $p - 1 > \varphi(m) - 1$, so

$$p > \varphi(m)\,. \tag{S.2.10}$$

Write m in the form $m = tp$ where $t > 2$ according to the assumption on m. Then $\varphi(t) \geq 2$, and using Exercise 2.3.10a, we obtain

$$\varphi(m) = \varphi(tp) \geq \varphi(t)\varphi(p) \geq 2(p-1) > p\,,$$

which contradicts (S.2.10).

• **2.5.7** *First solution*: If $(a, m) = d$, then there are $f(b) = d$ solutions for the m/d numbers $b = d, 2d, \ldots, (m/d)d$; and there are no solutions for the other values of $1 \leq b \leq m$, so $f(b) = 0$ for these. Therefore the sum equals $\sum_{b=1}^{m} f(b) = (m/d)d = m$.

• *Second solution*: Each of the numbers $x = 1, 2, \ldots, m$ satisfies the congruence $ax \equiv b \pmod{m}$ for exactly one b. Hence $\sum_{b=1}^{m} f(b) = m$. This argument is valid also for any non-linear congruence $h(x) \equiv b \pmod{m}$ where h is an arbitrary polynomial of higher degree.

• **2.6.9** According to the hint, we investigate the congruence $x \equiv 39^{38^{37}} \pmod{1440}$, and using $1440 = 2^5 \cdot 3^2 \cdot 5$, we replace it by a system of congruences with moduli 2^5, 3^2, and 5.

Since $39 \equiv -1 \pmod{5}$ and 38^{37} is even, so $x \equiv 1 \pmod{5}$.

$3 \mid 39$ implies $x \equiv 0 \pmod{9}$.

Finally, $39 \equiv 7 \pmod{32}$ and $7^4 = 49^2 \equiv 17^2 \equiv 1 \pmod{32}$, further $4 \mid 38^{37}$, hence $x \equiv 1 \pmod{32}$.

Thus we have to solve the system

$$x \equiv 1 \pmod 5, \quad x \equiv 0 \pmod 9, \quad x \equiv 1 \pmod{32}.$$

Combining the first and last congruences, we get $x \equiv 1 \pmod{5 \cdot 32 = 160}$, i.e. $x = 160z + 1$. Substituting this into the second congruence, we have $160z + 1 \equiv 0 \pmod 9$ yielding $z \equiv 5 \pmod 9$ or $z = 9t + 5$. Hence

$$x = 160(9t + 5) + 1 = 1440t + 801, \quad \text{thus} \quad x \equiv 801 \pmod{1440}\,.$$

Thus the exact time is 13:21.

• **2.8.5 (c)** We prove the four statements indicated in the hint.

(i) We can prove similarly to (a) that the operations are well defined, the operational identities are valid, there exists a zero element, and every element has a negative.

(ii) Let $m = tk$ where $t > 1$ and $(t, k) = 1$ by the assumption. The arising residue classes are $(rk)_m$ for $0 \le r \le t - 1$. (Taking other values of r, we obtain the same residue classes just represented by different elements.)

The residue class $(sk)_m$ is an identity element if and only if

$$(sk)_m(rk)_m = (rk)_m, \text{ i.e. } srk^2 \equiv rk \pmod{tk},\ r = 0, 1 \ldots, t - 1. \tag{S.2.11}$$

If the congruence in (S.2.11) holds for $r = 1$, i.e.

$$sk^2 \equiv k \pmod{tk}, \tag{S.2.12}$$

then multiplying (S.2.12) by r, we obtain that (S.2.11) is true for every r. This means that also (S.2.12) is equivalent to $(sk)_m$ being an identity element.

Dividing (S.2.12) by k yields an equivalent congruence $sk \equiv 1 \pmod t$. This means that the linear congruence $xk \equiv 1 \pmod t$ is solvable. Since $(t, k) = 1$, this is true, indeed.

(iii) Now $m = tk$, $(t, k) = 1$, and t is a prime. Relying on (i) and (ii), we have to prove only that the residue class $(rk)_m$ has a multiplicative inverse for every $1 \le r \le t - 1$. Let $(sk)_m$ be the identity element, and we search the inverse of $(rk)_m$ in the form $(uk)_m$:

$$(rk)_m(uk)_m = (sk)_m, \qquad \text{i.e.} \qquad ruk^2 \equiv sk \pmod{tk}. \tag{S.2.13}$$

Dividing (S.2.13) by k, we get the equivalent congruence $ukr \equiv s \pmod{t}$. Thus we have to show that the linear congruence $xkr \equiv s \pmod{t}$ is solvable. Since $(t,k) = 1$, and t being a prime implies also $(t,r) = 1$, so $(t,kr) = 1$, i.e. the congruence is solvable, indeed.

Remark: Refining the above argument, we can prove that if $(t,k) = 1$ but t is composite, then we never get a field. Moreover, the following general proposition is true: If $(t,k) = 1$, then the ring R is "exactly the same" as the the ring of the residue classes modulo t (in a precise formulation, this means that the two rings are *isomorphic*, i.e. there is a bijection between them preserving the operations).

(iv) We use the previous notations. The residue class $(rk)_m \neq (0)_m$ is a zero divisor if and only if

$$(rk)_m(vk)_m = (0)_m, \qquad \text{i.e.} \qquad rvk^2 \equiv 0 \pmod{tk} \tag{S.2.14}$$

for some $(vk)_m \neq (0)_m$. Dividing (S.2.14) by k, we obtain the equivalent congruence $vkr \equiv 0 \pmod{t}$. We need to show that $xkr \equiv 0 \pmod{t}$ has a non-trivial solution $v \not\equiv 0 \pmod{t}$. Since there are $(t,kr) > 1$ solutions, this is true, indeed.

3. Congruences of Higher Degree

• **3.2.6** Assume $o_p(a) = o_p(-a) = k$. Then

$$1 \equiv a^k \equiv (-a)^k = (-1)^k a^k \equiv (-1)^k \pmod{p}\,, \tag{S.3.1}$$

so k is even, $k = 2t$. This implies $p \mid a^{2t} - 1 = (a^t - 1)(a^t + 1)$. Since p is a prime and $t < o_p(a)$, we obtain $p \mid a^t + 1$, i.e. $a^t \equiv -1 \pmod{p}$. Similarly, $(-a)^t \equiv -1 \pmod{p}$. An argument analogous to (S.3.1) yields that also t is even, thus $4 \mid o_p(a)$, indeed.

For the converse, consider $o_p(a) = 4s$. Then $(-a)^{4s} = a^{4s} \equiv 1 \pmod{p}$, so $r = o_p(-a) \mid 4s$. For a proof by contradiction, assume $r < 4s$. If r is even, then $1 \equiv (-a)^r = a^r \pmod{p}$ contradicts $o_p(a) = 4s$. If r is odd, then $r \mid s$ and $1 \equiv (-a)^{2r} = a^{2r} \pmod{p}$, a contradiction again.

Note that the converse holds also for composite moduli m, as we made no use of the modulus being a prime, but the other direction is false, e.g. $o_{21}(8) = o_{21}(-8) = 2$.

• **3.2.9** The assumption implies $(a,p) = 1$, so $o_p(a)$ makes sense. By Fermat's Little Theorem, $1 \equiv a^{2p-2} = a^{2p-10}a^8 \equiv -a^8 \pmod{p}$, thus $a^8 \equiv -1 \pmod{p}$.

Squaring yields $a^{16} \equiv 1 \pmod{p}$. Using the statement of part (i) in Theorem 3.2.2 (and $1 \not\equiv -1 \pmod{p}$ due to $p > 2$), we obtain $o_p(a) \mid 16$ and $o_p(a) \nmid 8$. Therefore $o_p(a) = 16$.

• **3.3.10** If $a \equiv b^r \pmod{p}$ and $b \equiv a^s \pmod{p}$, then $o_p(a)$ and $o_p(b)$ mutually divide each other by Exercise 3.2.4a, hence they are equal.

To prove the converse, let g be a primitive root and $a \equiv g^u \pmod{p}$, $b \equiv g^v \pmod{p}$. By Exercise 3.2.4c, $o_p(a) = (p-1)/(p-1,u)$ and $o_p(b) = (p-1)/(p-1,v)$. The equality of the orders implies $(p-1,u) = (p-1,v)$.

The roles of a and b are symmetric, so it suffices to guarantee an r satisfying $a \equiv b^r \pmod{p}$. We can rewrite this congruence into the form $g^u \equiv g^{vr} \pmod{p}$ which is equivalent to the linear congruence $u \equiv vr \pmod{p-1}$ (where r is the variable). As $(p-1,v) = (p-1,u) \mid u$, this linear congruence is solvable, indeed.

Another option to verify the existence of r is the following. Let $o_p(b) = k$. There are $\varphi(k)$ elements of order k by Exercise 3.3.9 (or by the second proof of Theorem 3.3.3). By Exercise 3.2.4b, there are $\varphi(k)$ elements of order k also among $b, b^2, \ldots, b^k$. Hence these elements contain all numbers of order k.

Remark: A similar argument proves the following more general result: $o_p(a) \mid o_p(b)$ if and only if $a \equiv b^r \pmod{p}$ for some positive integer r.

• **3.4.9** Assume first $\operatorname{ind}_g a = \operatorname{ind}_h b$. By Exercise 3.2.4c,

$$o_p(a) = \frac{p-1}{\big(\operatorname{ind}_g a\,,\, p-1\big)} = \frac{p-1}{\big(\operatorname{ind}_h b\,,\, p-1\big)} = o_p(b)\,.$$

To prove the converse, assume $o_p(a) = o_p(b)$, let g be an arbitrary primitive root mod p, and $\operatorname{ind}_g a = r$, $\operatorname{ind}_g b = s$. Using Exercise 3.2.4c again, we have $(r, p-1) = (s, p-1)$.

We want to find the primitive root h satisfying $\operatorname{ind}_h b = r$ in the form $h \equiv g^k \pmod{p}$. Here $(k, p-1) = 1$ by statement (i) of Theorem 3.3.4. The requirement can be rewritten as

$$g^s \equiv b \equiv h^r \equiv (g^k)^r = g^{kr} \pmod{p}$$

which is equivalent to

$$s \equiv kr \pmod{p-1}. \tag{S.3.2}$$

This is a linear congruence for k which is solvable as $(r, p-1) = (s, p-1) \mid s$.

We have to show the existence of a solution k coprime to $p-1$.

Denote $(r, p-1) = (s, p-1)$ by d. Dividing (S.3.2) by d, we obtain an equivalent congruence

$$\frac{s}{d} \equiv k \cdot \frac{r}{d} \quad \Big(\mathrm{mod}\,\frac{p-1}{d}\Big). \tag{S.3.3}$$

The left-hand side of (S.3.3) is coprime to the modulus since $(s/d, (p-1)/d) = 1$. Therefore also the right-hand side has this property, so $(k, (p-1)/d) = 1$.

If every prime divisor of $p-1$ occurs already in $(p-1)/d$, then $(k, p-1) = 1$, so we are done. Otherwise, let Q be the product of those prime divisors of $p-1$ that are coprime to $(p-1)/d$, and let k_0 be an arbitrary solution of (S.3.3). Then a solution k of the system

$$x \equiv k_0 \quad \Big(\mathrm{mod}\,\frac{p-1}{d}\Big), \qquad x \equiv 1 \pmod{Q}$$

meets all requirements: it satisfies (S.3.2) and is coprime to $p-1$.

• **3.5.12** *First proof*: If a is a 100th power residue, i.e. $p \nmid a$ and $a \equiv w^{100} \pmod p$ for some w, then $a \equiv (w^5)^{20} \equiv (w^2)^{50} \pmod p$, thus a is both a 20th and a 50th power residue, as well.

To prove the converse, assume that a is both a 20th and a 50th power residue, i.e. $p \nmid a$ and $u^{20} \equiv v^{50} \equiv a \pmod p$ for some u and v. This implies $u^{100} \equiv a^5 \pmod p$ and $v^{100} \equiv a^2 \pmod p$. Substituting these into $a \cdot (a^2)^2 = a^5$, we obtain $a(v^2)^{100} \equiv u^{100} \pmod p$. Multiplying both sides by $(v^{p-3})^{100}$ and applying Fermat's Little Theorem, we get $a \equiv (v^{p-3}u)^{100} \pmod p$. So a is a 100th power residue, indeed.

• *Second proof*: By the criterion about indices in Theorem 3.5.3, we have to show

$$(100, p-1) \mid \mathrm{ind}\, a \iff \begin{cases} (20, p-1) \mid \mathrm{ind}\, a \\ (50, p-1) \mid \mathrm{ind}\, a \end{cases}$$

The only if part is obvious, since both $(20, p-1)$ and $(50, p-1)$ divide $(100, p-1)$.

For the if part, we have to show that $(20, p-1) \mid \mathrm{ind}\, a$ and $(50, p-1) \mid \mathrm{ind}\, a$ imply $(100, p-1) \mid \mathrm{ind}\, a$. If $25 \nmid p-1$, then $(100, p-1) = (20, p-1)$, and if $4 \nmid p-1$, then $(100, p-1) = (50, p-1)$, so we are done. If both $25 \mid p-1$ and $4 \mid p-1$, then $(50, p-1) = 50 \mid \mathrm{ind}\, a$ and $(20, p-1) = 20 \mid \mathrm{ind}\, a$, thus $[50, 20] = 100 = (100, p-1) \mid \mathrm{ind}\, a$.

• We can create a third proof along similar lines using the criterion about powers of a in Theorem 3.5.3. We leave the details to the Reader.

• We formulated the generalization already at the hints: a is both a kth and an nth power residue if and only if it is a $[k,n]$th power residue.

Each of the three proofs above can be applied also for this general case. For the "more difficult" direction, we can use the representation $1 = b([k,n]/k) - c([k,n]/n)$ in the first proof instead of $1 = 1 \cdot 5 - 2 \cdot 2$ serving as a basis for $a \cdot (a^2)^2 = a^5$, and the relation $[(k, p-1), (n, p-1)] = ([k,n], p-1)$ (see Exercise 1.6.19b) in the second (and third) proof(s).

• **3.7.3 (b)** We show that for $k \geq 3$ and a odd, the congruence

$$x^2 \equiv a \pmod{2^k} \tag{S.3.4}$$

is solvable if and only if

$$a \equiv 1 \pmod{8}, \tag{S.3.5}$$

and there are 4 solutions (if it is solvable).

Since $c^2 \equiv 1 \pmod 8$ for any odd c, therefore (S.3.5) is necessary for the solvability of (S.3.4).

Next we prove that there are 4 solutions in the case of solvability. Assume that $x \equiv c \pmod{2^k}$ is a solution of (S.3.4) for some (fixed odd) a. Then d is a solution if and only if

$$2^k \mid d^2 - c^2 = (d-c)(d+c)\,. \tag{S.3.6}$$

As c and d are odd, both factors are even. Also, both cannot be divisible by 4, since that would imply $4 \mid (d-c) + (d+c) = 2d$ which contradicts d being odd.

Therefore (S.3.6) holds if and only if (exactly) one of $d-c$ and $d+c$ is a multiple of 2^{k-1}. This means $d \equiv \pm c \pmod{2^{k-1}}$, i.e. we obtain four (pairwise incongruent) solutions of (S.3.4) mod 2^k:

$$x \equiv c, \qquad x \equiv c + 2^{k-1}, \qquad x \equiv -c, \qquad x \equiv -c + 2^{k-1}\,.$$

Finally, we verify that (S.3.5) is not only a necessary but also a sufficient condition for the solvability of (S.3.4).

We can restrict ourselves to the values $1 \leq a < 2^k$ pairwise incongruent mod 2^k. Every element of a reduced residue system 2^k will be a solution of (S.3.4) exactly for one such a. For every such a there are 4 solutions, so the congruence will be solvable for $\varphi(2^k)/4 = 2^{k-3}$ values of a. Exactly that many a satisfy (S.3.5), hence (S.3.4) must be solvable for each of them.

4. Legendre and Jacobi Symbols

• **4.1.13 (a)** (The modulus of each congruence is 13.) The first step is to change the coefficient of the quadratic term into 1. To acieve this, we multiply the congruence by -4 (which is an equivalent step due to $(-4, 13) = 1$): $-12x^2 - 20x - 20 \equiv 0$, or $x^2 + 6x + 6 \equiv 0$. Now we form a complete square:

$$(x+3)^2 \equiv 3 \equiv 16 \iff x+3 \equiv \pm 4 \iff x \equiv 1 \text{ and } 6.$$

Instead of multiplying by -4, we can divide by 3 after converting all coefficients into multiples of 3: $3x^2 + 5x + 5 \equiv 3x^2 + 18x + 18 \equiv 0$, and thus $x^2 + 6x + 6 \equiv 0$.

Another option is to multiply the original congruence by $4 \cdot 3$ and then to transform it into a complete square:

$$36x^2 + 60x + 60 = (6x+5)^2 + 35 \equiv 0 \iff (6x+5)^2 \equiv 4 \iff 6x + 5 \equiv \pm 2\,.$$

Finally, we have to solve the linear congruences $6x \equiv -3$ and $6x \equiv -7$.

• **4.2.8** The polynomial $f = (x^2+1)(x^2-17)(x^2+17)$ given in the hint has clearly no rational roots.

To prove the solvability of the congruence $f(x) \equiv 0 \pmod{m}$ for every m, it suffices to prove it for every prime power p^k, by the Chinese Remainder Theorem.

The congruence $x^2 \equiv 17 \pmod{2^k}$ is solvable for every k as $17 \equiv 1 \pmod 8$, see the solution of Exercise 3.7.3b.

If $p > 2$ and $p \neq 17$, then

$$\left(\frac{-1}{p}\right)\left(\frac{17}{p}\right)\left(\frac{-17}{p}\right) = \left(\frac{-17}{p}\right)^2 = 1$$

guarantees that at least one of the factors in f has a solution mod p. Since p is odd, this implies that there exists a solution also mod p^k by Exercise 3.7.2 (or by Theorem 3.7.1).

Finally, for $p = 17$ the congruence $x^2 \equiv -1 \pmod{17}$ is solvable since $17 \equiv 1 \pmod 4$, and therefore there exists a solution mod 17^k, as well.

• **4.3.7 (b)** We show that exactly the squares have this property.

The squares suit, indeed: for $a = s^2$, we have

$$\left(\frac{a}{m}\right) = \left(\frac{s^2}{m}\right) = \left(\frac{s}{m}\right)^2 = 1\,.$$

To prove the converse, assume that a is not a square. Consider first when $a > 0$. Then some prime occurs with an odd exponent in the standard form of a.

If 2 is such a prime, i.e. $a = 2^i t$ where both i and t are odd, then let m be a (positive) solution of the system $x \equiv 5 \pmod 8$, $x \equiv 1 \pmod t$. Then

$$\left(\frac{a}{m}\right) = \left(\frac{2}{m}\right)^i \left(\frac{t}{m}\right) = (-1)\left(\frac{m}{t}\right) = (-1)\left(\frac{1}{t}\right) = -1\,.$$

If the exponent of some prime $p > 2$ is odd, i.e. $a = 2^i p^j v$ where $i \geq 0$, j is odd, and $(v, 2p) = 1$, then let m be a (positive) solution of the system $x \equiv 1 \pmod 8$, $x \equiv 1 \pmod v$, $x \equiv c \pmod p$ where c is a quadratic non-residue mod p. Then

$$\left(\frac{a}{m}\right) = \left(\frac{2}{m}\right)^i \left(\frac{v}{m}\right)\left(\frac{c}{p}\right)^j = 1 \cdot \left(\frac{m}{v}\right)(-1) = (-1)\left(\frac{1}{v}\right) = -1\,.$$

Finally, consider $a < 0$. If $|a|$ is not a square, then proceed as above. If $a = -s^2$, then any m coprime to a and of the form $4k + 3$ suits:

$$\left(\frac{-s^2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{s}{m}\right)^2 = -1\,.$$

Solutions, Chapters 5–6

5. Prime Numbers

• **5.1.5 (c)** For a proof by contradiction, assume that $p < n$ is the smallest prime satisfying $(p, d) = 1$. Then the first p elements of the arithmetic progression $a, a + d, \ldots, a + (p - 1)d$ consisting purely of primes form a complete residue system modulo p, thus one of them is divisible by p which has to be p itself, i.e. $p = a + jd$. If $j > 0$, then the minimality of p implies that the prime a divides d, hence a divides every element in the arithmetic progression, so they cannot be primes. Therefore, only $p = a$ is possible, but then the $p + 1$st element $a + pd = p(1 + d)$ is not a prime.

• **5.2.5** By Gauss's theorem, we have to determine which numbers of type $2^k - 1$ can be written as the product of distinct Fermat primes.

First, we show that k must be a power of two. Assume that k has an odd prime divisor q. Then also $2^q - 1 \mid 2^k - 1$ holds. Further, by Theorem 5.2.3, every prime divisor of $2^q - 1$ is of type $2rq + 1$ which cannot be a Fermat prime since q is odd. But this contradicts to the fact that every prime divisor of $2^k - 1$ is a Fermat prime.

Let $k = 2^{n+1}$. Then, by Exercise 5.2.1a, we have $2^k - 1 = F_0 F_1 \ldots F_n$. For $0 \le n \le 4$, this means that $2^k - 1$ is the product of distinct Fermat primes, so these five values of k satisfy the conditions. For $n \ge 5$, however, $2^k - 1$ is divisible by F_5, hence also by 641, which is not a Fermat prime.

Summarizing the results, a regular $2^k - 1$-gon is constructible if and only if $k = 2, 4, 8, 16$, or 32.

• **5.2.7** Assume first that $2p + 1 \mid M_p$, and let q be an arbitrary prime divisor of $2p + 1$. Then also $q \mid M_p$ holds, so $q = 2pk + 1$, by Theorem 5.2.3. Since $q \mid 2p + 1$, therefore only $q = 2p + 1$ is possible, i.e. $2p + 1$ is a prime. We have to show $p \equiv 3 \pmod 4$. Clearly $p \neq 2$. If $p \equiv 1 \pmod 4$, then $q = 2p + 1 \equiv 3 \pmod 8$, so $\left(\frac{2}{q}\right) = -1$ follows. But the condition $2p + 1 \mid M_p$ can be rewritten as $2^{(q-1)/2} \equiv 1 \pmod q$, or equivalently $\left(\frac{2}{q}\right) = 1$, which is a contradiction.

For the converse, let $q = 2p + 1$ be a prime and $p \equiv 3 \pmod 4$. Then $q \equiv 7 \pmod 8$, therefore $\left(\frac{2}{q}\right) = 1$, i.e. $2^{(q-1)/2} \equiv 1 \pmod q$ which means precisely the desired divisibility $2p + 1 \mid M_p$.

• **5.2.9** The even element of a pair can only be a power of two.

Consider first the case when $n+1=2^\alpha$ and $n=q^\beta$ (where q is an odd prime, α, $\beta \geq 1$). Then $2^\alpha = q^\beta + 1$.

If $\beta = 1$, then q is a Mersenne prime.

If β is even, then the residue mod 4 of the right-hand side is 2 which is impossible.

If $\beta > 1$ is odd, write the right-hand side as $(q+1)(q^{\beta-1} - q^{\beta-2} \pm \ldots + 1)$. The second factor is an odd number greater than 1, hence it cannot be a power of two, a contradiction.

Assume now $n = 2^\alpha$ and $n+1 = q^\beta$. Then $2^\alpha = q^\beta - 1$.

If $\beta = 1$, then q is a Fermat prime.

If β is even, write the right-hand side as $(q^{\beta/2}-1)(q^{\beta/2}+1)$. Here both factors have to be powers of two, and since their difference is two, only the product $2 \cdot 4$ is possible. Then $2^\alpha = 8, q^\beta = 9$.

If $\beta > 1$ is odd, factor the right-hand side as $(q-1)(q^{\beta-1} + q^{\beta-2} + \ldots + 1)$. The second factor is an odd number greater than 1, so it cannot be a power of two, which is a contradiction.

Thus the following pairs satisfy the requirements: $(8, 9)$; (M_p, M_p+1), where M_p is a Mersenne prime; and $(2^{2^n}, F_n)$, where F_n is a Fermat prime.

• **5.5.9 (a)** If $n = k^3$, then $(k+1)^3 = n + 3n^{2/3} + 3n^{1/3} + 1 > n + n^{2/3}$. By part (A) of Theorem 5.5.4 there is a prime between n and $n + n^{2/3}$ for n large enough, therefore the interval $\left(k^3, (k+1)^3\right)$ contains a prime, too.

• **(b)** We follow the ideas suggested in the hint. We construct a sequence of primes q_n satisfying

$$q_n = \lfloor \alpha^{3^n} \rfloor \tag{S.5.1}$$

for some α. Consider

$$c_n = \sqrt[3^n]{q_n} \qquad \text{and} \qquad d_n = \sqrt[3^n]{q_n + 1}\,.$$

This transforms (S.5.1) into

$$c_n \leq \alpha < d_n\,. \tag{S.5.2}$$

We shall choose the primes q_n so that $[c_n, d_n]$ should form nested intervals, i.e.

$$\sqrt[3^n]{q_n} < \sqrt[3^{n+1}]{q_{n+1}} < \sqrt[3^{n+1}]{q_{n+1}+1} < \sqrt[3^n]{q_n+1} \tag{S.5.3}$$

for every n. Raising (S.5.3) to the 3^{n+1}st power, we get condition

$$q_n^3 \le q_{n+1} < (q_n+1)^3 - 1. \tag{S.5.4}$$

Hence, let q_1 be a big prime, q_2 a prime between q_1^3 and $(q_1+1)^3$, and in general, if q_n was already selected, then let q_{n+1} be a prime satisfying (S.5.4). We can always find such a prime q_{n+1}, by part (a) (provided q_1 was sufficiently large).

Let α be a common point of the nested closed intervals $[c_n, d_n]$. We show that it meets the requirements.

By the construction of α, we have $c_n \le \alpha \le d_n$ for every n, and we need the slightly sharper inequality (S.5.2). We would run into a problem if $\alpha = d_n$ for some n. The numbers d_j, however, are *strictly* decreasing by (S.5.3) and (S.5.4), i.e. $\alpha \le d_{n+1} < d_n$, so $\alpha = d_n$ cannot occur.

• **(c)** In the proof of part (b) we could guarantee just the existence of α but could not exhibit its concrete value. In fact, the situation is even more weird: *first* we had to "construct" infinitely many suitable primes to guarantee an α which served *afterwards* to retrieve from the "formula" $\lfloor \alpha^{3^n} \rfloor$ the *same* primes that we needed to establish α.

• **5.6.1** We denote the sequences in parts (a), (b), ... by $A = \{a_1, a_2, \ldots\}$, $B = \{b_1, b_2, \ldots\}$, etc., and $A(n)$, $B(n)$, etc. should stand for the number of elements in them not exceeding n.

• **(a)** Clearly, $a_n = Ln$, thus

$$\sum_{n=1}^{\infty} \frac{1}{a_n} = \frac{1}{L} \sum_{n=1}^{\infty} \frac{1}{n} = \infty \qquad \text{and} \qquad A(n) = \left\lfloor \frac{n}{L} \right\rfloor \sim \frac{n}{L}\,.$$

• **(b)** The series consists of positive elements, hence we can rearrange the order of terms arbitrarily. We group them according to the bases of the powers (thus certain powers will be counted more times, e.g. $64 = 4^3 = 8^2$). Then

$$\sum_{n=1}^{\infty} \frac{1}{b_n} < \sum_{j=2}^{\infty} \sum_{k=2}^{\infty} \frac{1}{j^k} = \sum_{j=2}^{\infty} \frac{1}{j^2(1-\frac{1}{j})} = \sum_{j=2}^{\infty} \frac{1}{j(j-1)} = 1\,.$$

Turning to $B(n)$, we show that the squares dominate it, the number of higher powers is negligible compared to the number of squares.

For a fixed exponent $k > 1$, the number of kth powers greater than 1 and not greater than n is $\lfloor \sqrt[k]{n} \rfloor - 1$. So certain numbers (as e.g. 64) are taken into consideration for several values of k, further $2^k \le n$, i.e. $k \le \lfloor \log_2 n \rfloor$. Hence

$$\lfloor \sqrt{n} \rfloor \;-\; 1 \;\le\; B(n) \;\le\; \sqrt{n} \;+\; \sum_{k=3}^{\lfloor \log_2 n \rfloor} \sqrt[k]{n} \;\le\; \sqrt{n} \;+\; (\log_2 n)\, \sqrt[3]{n}\,.$$

Dividing by $\sqrt{n}$, we obtain $B(n) \sim \sqrt{n}$.

• **(c)** The squarefree integers contain also the primes, and the sum of reciprocals of the latter is divergent in itself.

• **(d)** Similarly to the third proof of Theorem 5.6.1, we get

$$\sum_{d_j \le n} \frac{1}{d_j} \;\le\; \prod_{p<L} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{\nu_p}} \right),$$

where

$$p^{\nu_p} \;\le\; n \;<\; p^{\nu_p+1}\,, \qquad \text{i.e.} \qquad \nu_p = \lfloor \log_p n \rfloor\,.$$

Summing up and estimating the geometric series from above, we have

$$\sum_{d_j \le n} \frac{1}{d_j} \;\le\; \prod_{p<L} \frac{1}{1 - \frac{1}{p}}\,.$$

The right-hand side is independent of n, therefore $\sum_{j=1}^{\infty} 1/d_j$ converges.

To estimate $D(n)$, let $p_1, \ldots, p_k$ be the primes less than L. Then the standard form of an element in D is

$$d = p_1^{\alpha_1} \ldots p_k^{\alpha_k}\,. \tag{S.5.5}$$

If $d \le n$, then clearly

$$p_i^{\alpha_i} \le n\,, \qquad \text{i.e.} \qquad 0 \le \alpha_i \le \frac{\log n}{\log p_i}$$

for every i in (S.5.5). This implies

$$D(n) \;\le\; \prod_{i=1}^{k} \Big(1 + \frac{\log n}{\log p_i} \Big) \;\le\; c(\log n)^k$$

with a suitable constant c.

To estimate $D(n)$ from below, observe that if

$$p_i^{\alpha_i} \;\le\; \sqrt[k]{n}\,, \qquad \text{i.e.} \qquad 0 \;\le\; \alpha_i \;\le\; \frac{\log n}{k \log p_i}$$

for every i in (S.5.5), then $d \le n$. This yields $D(n) > c'(\log n)^k$ for some constant $c' > 0$, similarly to the previous calculation.

To find an asymptotics, we use the logarithmic version of (S.5.5):

$$\log d = \alpha_1 \log p_1 + \ldots + \alpha_k \log p_k\,.$$

Then $D(n)$ is the number of k-tuples $(\alpha_1, \ldots, \alpha_k)$ where

(S.5.6) $\quad \alpha_1 \log p_1 + \ldots + \alpha_k \log p_k \le \log n$ and every $\alpha_i \ge 0$ is an integer.

We describe the proof first for $L = 6$, and then indicate how we can generalize the idea for any L.

If $L = 6$, then $k = 3$; these are the primes 2, 3, and 5. Then $D(n)$ is the number of non-negative integer solutions $(\alpha_1, \alpha_2, \alpha_3)$ of the inequality

$$\alpha_1 \log 2 + \alpha_2 \log 3 + \alpha_3 \log 5 \le \log n. \tag{S.5.7}$$

Equality $x_1 \log 2 + x_2 \log 3 + x_3 \log 5 = \log n$ can be interpreted as the equation of a plane in the space. Then

$$x_1 \log 2 + x_2 \log 3 + x_3 \log 5 \le \log n, \qquad x_i \ge 0$$

is satisfied by the points (x_1, x_2, x_3) of the trilateral pyramid G_n defined by the above plane and the positive half-lines of the coordinate axes.

The points (x_1, x_2, x_3) with integer coordinates form a lattice of unit cubes. This means that the number of solutions of (S.5.7) in non-negative integers is the number of lattice points in the pyramid G_n.

It is clear intuitively (and can be easily verified, cf. Exercise 7.5.9), that the number of lattice points in G_n is "approximately" the volume of G_n if n is large. To state it precisely, the number of lattice points and the volume of the pyramid are asymptotically equal as n tends to infinity.

The volume $V(G_n)$ of the pyramid G_n is one sixth of the product of the three pairwise perpendicular edges starting from the origin. Hence

$$D(n) \sim V(G_n) = \frac{(\log n)^3}{6 \cdot \log 2 \cdot \log 3 \cdot \log 5}\,.$$

We can proceed similarly for arbitrary L: by (S.5.6), we have to determine the number of lattice points in the "pyramid" (so-called simplex) in the k-dimensional space which is asymptotically equal to the volume of the pyramid. Thus

$$D(n) \sim V(G_n) = \frac{(\log n)^k}{k! \prod_{p<L} \log p}\,.$$

• **(e)** The primes greater than L occur among these numbers, so the sum of reciprocals is divergent.

To estimate $E(n)$, note that these are the integers coprime to every prime not exceeding L. Thus taking $M = \prod_{p\le L} p$, there are exactly $\varphi(M)$ such elements among any M consecutive integers. Hence,

$$\text{if} \quad tM \le n < (t+1)M, \quad \text{then} \quad t\varphi(M) \le E(n) \le (t+1)\varphi(M)\,.$$

These inequalities yield

$$\frac{t\varphi(M)}{(t+1)M} \le \frac{E(n)}{n} \le \frac{(t+1)\varphi(M)}{tM}\,.$$

Since $t = \lfloor n/M \rfloor$, therefore t tends to infinity, and both $t/(t+1)$ and $(t+1)/t$ tend to 1 when $n \to \infty$. This implies

$$\lim_{n\to\infty} \frac{E(n)}{n} = \frac{\varphi(M)}{M} = \prod_{p\le L}\Big(1-\frac{1}{p}\Big)\,, \qquad \text{i.e.} \qquad E(n) \sim n \prod_{p\le L}\Big(1-\frac{1}{p}\Big)\,.$$

• **(f)** We give two proofs for the convergence of the series $\sum_{j=1}^{\infty} 1/f_j$ composed of the reciprocals of squareful numbers. (Also a third proof can be obtained based on Exercise 5.6.7.)

First proof: Similarly to the third proof of Theorem 5.6.1, we get

$$\sum_{f_j\le n} \frac{1}{f_j} \le \prod_{p^2\le n} \Big(1 + \frac{1}{p^2} + \frac{1}{p^3} + \ldots + \frac{1}{p^{\nu_p}}\Big)\,,$$

where

$$p^{\nu_p} \le n < p^{\nu_p+1}\,, \qquad \text{i.e.} \qquad \nu_p = \lfloor \log_p n \rfloor\,.$$

In each factor, the first term 1 if followed by geometric series. Using the summation formula and estimating from above, we obtain

$$\sum_{f_j\le n} \frac{1}{f_j} \le \prod_{p\le\sqrt{n}} \Big(1 + \frac{1}{p^2(1-\frac{1}{p})}\Big) = \prod_{p\le\sqrt{n}} \Big(1 + \frac{1}{p(p-1)}\Big)\,. \tag{S.5.8}$$

Let p_k be the kth prime, then $p_k(p_k-1) > p_{k-1}^2$ for $k>1$. On the right-hand side of (S.5.8), we leave unaltered the first factor

$$1+\frac{1}{2\cdot 1}=\frac{3}{2}$$

corresponding to $p=p_1=2$, and apply the estimate

$$1+\frac{1}{p_k(p_k-1)} < 1+\frac{1}{p_{k-1}^2}$$

for the other factors corresponding to $p=p_k$ with $k>1$. This gives the following upper bound for the right-hand side of (S.5.8):

$$\prod_{p\le\sqrt{n}}\Big(1+\frac{1}{p(p-1)}\Big) \;<\; \frac{3}{2}\prod_{p\le\sqrt{n}}\Big(1+\frac{1}{p^2}\Big) \;<\; 2\sum_{j=1}^{\infty}\frac{1}{j^2}\,.$$

Second proof: We show first that every squareful number is the product of a square and a cube. Let the standard form of the squareful number f be

$$f=q_1^{\mu_1}\dots q_r^{\mu_r}\,,\qquad \mu_i\ge 2,\quad i=1,2,\dots,r\,.$$

The exponents μ_i can be written in the form $\mu_i=2\alpha_i+3\beta_i$ where $\alpha_i,\beta_i\ge 0$ (e.g. β_i is 0 or 1 according to μ_i being even or odd). Then

$$f=a^2b^3\,,\qquad \text{where}\qquad a=\prod_{i=1}^{r}q_i^{\alpha_i}\quad\text{and}\quad b=\prod_{i=1}^{r}q_i^{\beta_i}\,. \tag{S.5.9}$$

It follows from (S.5.9) that the sum of reciprocals of squareful numbers is less than the product of the sum of reciprocals of squares and the sum of reciprocals of the cubes, which verifies the convergence.

We shall use (S.5.9) to estimate $F(n)$. We saw that $\beta_i=0$ or 1 can be attained, i.e. b is squarefree. It is straightforward that the representation $f=a^2b^3$ is already unique in this case, i.e. every squareful number has a unique decomposition into the product of a cube of a squarefree number and a square. It is also clear that, except for the number 1, the products a^2b^3 are squareful, indeed.

Therefore, $F(n)$ is just one less than the number of such products a^2b^3 not greater than n. In these products b is squarefree, $b\le\sqrt[3]{n}$, and $1\le a\le\sqrt{n/b^3}$ for a fixed b. Therefore

$$F(n) \;=\; -1+{\sum_{b\le\sqrt[3]{n}}}'\left\lfloor\sqrt{\frac{n}{b^3}}\right\rfloor\,, \tag{S.5.10}$$

where $\sum'$ denotes that the sum is taken for the squarefree values of b.

Removing the floors on the right-hand side of (S.5.10), we get

$$\sqrt{n} \sum_{b \le \sqrt[3]{n}}{}' \frac{1}{b^{3/2}} \; + \; U(n),$$

where the error term $U(n)$ can be neglected compared to the other term as

$$|U(n)| \; \le \; 1 + \sum_{b \le \sqrt[3]{n}}{}' 1 \; \le \; 1 + \sqrt[3]{n}\,.$$

This implies

$$F(n) \sim c\sqrt{n}\,, \qquad \text{where} \qquad c = \sum_{b=1}^{\infty}{}' \frac{1}{b^{3/2}}\,.$$

• **5.6.6** We write the factors $(1 - 1/p^s)^{-1}$ as infinite geometric series and apply that the multiplication of two positive (or more generally, absolutely convergent) series "obeys the same rules as the multiplication of finite sums". Hence,

$$\prod_{p \le n} \frac{1}{1 - \frac{1}{p^s}} \; = \; \prod_{p \le n} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) \; = \; \sum_{j \in W_n} \frac{1}{j^s}\,,$$

where W_n is the set of integers having no prime factor greater than n. Clearly

$$\sum_{j=1}^{n} \frac{1}{j^s} \; \le \; \sum_{j \in W_n} \frac{1}{j^s} \; < \; \sum_{j=1}^{\infty} \frac{1}{j^s}\,. \tag{S.5.11}$$

Since the left-hand side of (S.5.11) tends to the right-hand side if $n \to \infty$, therefore

$$\lim_{n\to\infty} \prod_{p \le n} \frac{1}{1 - \frac{1}{p^s}} \; = \; \lim_{n\to\infty} \sum_{j \in W_n} \frac{1}{j^s} \; = \; \sum_{j=1}^{\infty} \frac{1}{j^s} \; = \; \zeta(s)\,.$$

• **5.7.4** By assumption, the composite number n satisfies

$$2^{n-1} \equiv 1 \pmod{n}. \tag{S.5.12}$$

We have to show that also 2^n-1 is composite which follows immediately of n being composite (see Exercise 1.4.4a), further that

$$2^{2^n-2} \equiv 1 \pmod{2^n-1}.$$

Since $2^n \equiv 1 \pmod{2^n-1}$, it is enough to check $n \mid 2^n-2$; this follows directly from (S.5.12).

• **5.7.17** Let the standard form of the odd integer $n>1$ be

$$n = q_1^{\alpha_1} \dots q_s^{\alpha_s}, \qquad \text{and} \qquad n-1 = 2^k r, \text{ where } r \text{ is odd.}$$

We have to verify that if

$$a^r,\ a^{2r},\ a^{4r},\ \dots,\ a^{2^{k-2}r} = a^{\frac{n-1}{4}},\ a^{2^{k-1}r} = a^{\frac{n-1}{2}}$$

is a good sequence, i.e. either -1 occurs among their mod n residues of least absolute value, or the residue of a^r is 1, then also

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}. \tag{S.5.13}$$

If $a^r \equiv 1 \pmod{n}$, then raising this congruence to exponent 2^{k-1}, we get $a^{(n-1)/2} \equiv 1 \pmod{n}$, and also

$$1 = \left(\frac{1}{n}\right) = \left(\frac{a^r}{n}\right) = \left(\frac{a}{n}\right)^r,$$

which implies $\left(\frac{a}{n}\right) = 1$ since r is odd. Thus (S.5.13) holds, indeed.

Assume now

$$a^{2^j r} \equiv -1 \pmod{n}, \quad \text{where} \quad 0 \le j \le k-2\,. \tag{S.5.14}$$

Then $j < k-1$ implies $a^{(n-1)/2} \equiv 1 \pmod{n}$. We have to show that $\left(\frac{a}{n}\right) = 1$ is true, as well.

Considering congruence (S.5.14) mod q_i and squaring it, we obtain

$$a^{2^j r} \equiv -1 \pmod{q_i} \qquad \text{and} \qquad a^{2^{j+1} r} \equiv 1 \pmod{q_i}\,.$$

This means that

$$o_{q_i}(a) \not\mid 2^j r \qquad \text{and} \qquad o_{q_i}(a) \mid 2^{j+1} r\,,$$

i.e.

$$o_{q_i}(a) = 2^{j+1} r_i\,, \quad \text{where} \quad r_i \mid r\,. \tag{S.5.15}$$

Since q_i is a prime, therefore (S.5.15) implies

$$a^{2^j r_i} \equiv -1 \pmod{q_i}, \tag{S.5.16}$$

further, $o_{q_i}(a) \mid q-1$ yields

$$q_i = 1 + 2^{j+1} r_i h_i \tag{S.5.17}$$

for some suitable h_i. Using (S.5.16) and (S.5.17), we infer

$$\left(\frac{a}{q_i}\right) \equiv a^{(q_i-1)/2} = a^{2^j r_i h_i} = \left(a^{2^j r_i}\right)^{h_i} \equiv (-1)^{h_i} \pmod{q_i}. \tag{S.5.18}$$

By (S.5.18),

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{s} \left(\frac{a}{q_i}\right)^{\alpha_i} = (-1)^{\sum_{i=1}^{s} \alpha_i h_i}\,,$$

i.e. $\left(\frac{a}{n}\right) = 1$ follows if $\sum_{i=1}^{s} \alpha_i h_i$ is even. As each r_i is odd, this is equivalent to $\sum_{i=1}^{s} \alpha_i r_i h_i$ being even.

By (S.5.17), we have

$$n = \prod_{i=1}^{s} q_i^{\alpha_i} = \prod_{i=1}^{s} (1 + 2^{j+1} r_i h_i)^{\alpha_i}\,. \tag{S.5.19}$$

Carrying out the multiplications on the right-hand side of (S.5.19), most terms will be divisible by 2^{j+2}:

$$n = 1 + 2^{j+1} \sum_{i=1}^{s} \alpha_i r_i h_i + 2^{j+2} C\,. \tag{S.5.20}$$

Since $n - 1 = 2^k r$, i.e. $n = 1 + 2^k r$, therefore (S.5.20) implies

$$2^k r = 2^{j+1} \sum_{i=1}^{s} \alpha_i r_i h_i + 2^{j+2} C\,,$$

and after cancelation by 2^{j+1}, we get

$$2^{k-j-1}r - 2C = \sum_{i=1}^{s} \alpha_i r_i h_i. \tag{S.5.21}$$

As $j < k-1$, the left-hand side of (S.5.21) is even, hence so is also $\sum_{i=1}^{s} \alpha_i r_i h_i$ on the right-hand side, indeed.

Finally, we can proceed similarly in the case

$$a^{2^{k-1}r} = a^{\frac{n-1}{2}} \equiv -1 \pmod{q_i}.$$

Then we have to show $\left(\frac{a}{n}\right) = -1$ which is equivalent to $\sum_{i=1}^{s} \alpha_i r_i h_i$ being odd. Then, due to $j = k-1$, the left-hand side of (S.5.21) is $r - 2C$, which is odd, as r is odd, indeed.

6. Arithmetic Functions

• **6.1.7 (a)** If we compute $f(ab)$ in two different ways using $ab = (a,b)[a,b]$ and complete additivity, we get just the desired equality

$$f(a) + f(b) = f((a,b)) + f([a,b]). \tag{S.6.1}$$

• **(b)** Let

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad \text{and} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \quad \text{where} \quad \alpha_i \geq 0,\ \beta_j \geq 0,$$

be the standard forms of a and b. Then

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}$$

and

$$[a,b] = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}.$$

By Theorem 6.1.7, we obtain

$$f(a) + f(b) = \sum_{i=1}^{r} \big(f(p_i^{\alpha_i}) + f(p_i^{\beta_i})\big) \tag{S.6.2}$$

and

$$f((a,b)) + f([a,b]) = \sum_{i=1}^{r} \big(f(p_i^{\min(\alpha_i,\beta_i)} + f(p_i^{\max(\alpha_i,\beta_i)}) \big) . \tag{S.6.3}$$

(These are valid also if some exponents are 0, as $f(1) = 0$.)

Considering any two real numbers, one of them is the maximum and the other is the minimum of them, thus the pairs α_i, β_i and $\min(\alpha_i, \beta_i), \max(\alpha_i, \beta_i)$ are the same for every i. Therefore (S.6.2) and (S.6.3) imply (S.6.1).

• **(c)** We show that condition (S.6.1) is satisfied exactly by the functions $f = g + c$, where g is additive and c is a constant.

We proved previously that (S.6.1) is true for additive functions, thus clearly, it holds also for the functions f in question.

For the converse, we assume that f satisfies (S.6.1) for any a, b, and we try to establish f in the form $f = g+c$, where g is additive and c is a constant.

From $g(1) = 0$ we obtain that only $c = f(1)$ is possible. Thus we have to show that the function $g(n) = f(n) - f(1)$ is additive. This requires

$$f(ab) - f(1) = \big(f(a) - f(1) \big) + \big(f(b) - f(1) \big) ,$$

i.e.

$$f(1) + f(ab) = f(a) + f(b) \tag{S.6.4}$$

for any coprime a and b. Since $(a, b) = 1$ implies $[a, b] = ab$, we can replace $f(1)$ and $f(ab)$ on the left-hand side of (S.6.4) by $f((a, b))$ and $f([a, b])$, resp. Thus (S.6.4) follows from (S.6.1).

• **(d)** We can verify similarly that a completely multiplicative function, moreover a constant multiple of any multiplicative function satisfies

$$f(a)f(b) = f((a, b))f([a, b]) \tag{S.6.5}$$

for every a, b, and there are no other solutions with $f(1) \neq 0$.

We investigate now the case $f(1) = 0$. Clearly, (S.6.5) holds for $f = 0$. Assume that (S.6.5) is true for some $f \neq 0$, and let K be the smallest positive integer for which $f(K) \neq 0$.

If $K \nmid n$, then consider

$$f(K)f(n) = f((K, n))f([K, n]). \tag{S.6.6}$$

Since $(K,n) < K$, we have $f((K,n)) = 0$, further $f(K) \neq 0$, thus (S.6.6) implies $f(n) = 0$.

Let $h(n) = f(Kn)$. Then also h satisfies (S.6.5) for any a, b, as

$$h(a)h(b) = f(Ka)f(Kb) = f((Ka,Kb))f([Ka,Kb]) = \\ = f(K(a,b))f(K[a,b]) = h((a,b))h([a,b]).$$

Further $h(1) = f(K) \neq 0$, thus h is a constant multiple of a multiplicative function.

We obtained

$$f(n) = \begin{cases} 0, & \text{if } K \nmid n; \\ cg\left(\frac{n}{K}\right), & \text{if } K \mid n, \end{cases} \tag{S.6.7}$$

where $g(n)$ is multiplicative, c is a constant, and K is a fixed positive integer.

We can easily check that (S.6.5) is true for all functions f in (S.6.7) with any a, b. Also, the cases $f(1) \neq 0$ and $f = 0$ are contained in (S.6.7) when $K = 1$ and $c = 0$ (or $g = 0$), resp. Herewith we have proved that (S.6.7) describes the general solution of (S.6.5).

• **6.1.9 (d)** Those additive functions play a crucial role here which assume 0 on every prime power apart from the powers of one or two primes.

Let p be an arbitrary prime. We say (for domestic use) that an additive function h has sole p if h can assume arbitrary values on the powers of p but assumes 0 on all other prime powers. To obtain $h(n)$ for a general integer n, we write $n = tp^\alpha$, where $(t,p) = 1$; then $h(n) = h(p^\alpha)$. (This is correct also for $\alpha = 0$, since $h(1) = 0$ follows from additivity.) Another characterization of these functions is that $(c,p) = 1$ implies $h(c) = 0$.

We define similarly the functions having sole (p,q), where p and q are distinct primes: then the additive function h can assume arbitrary values on the powers of p and q but is 0 on every other prime power. For a general integer n, we write $n = tp^\alpha q^\beta$, where $(t,pq) = 1$, then $h(n) = h(p^\alpha) + h(q^\beta)$. Another characterization of these functions is that $(c,pq) = 1$ implies $h(c) = 0$.

Turning to the solution of the problem, we note first that if one of the two additive functions is 0, then also their product is 0, thus the product is additive, as well.

Next we show that if f and g have the same sole p, then fg is additive.

We have to prove

$$(fg)(ab) = (fg)(a) + (fg)(b) \tag{S.6.8}$$

for every $(a,b)=1$. If none of a and b is a multiple of p, then both sides of (S.6.8) are 0.

If $a=tp^\alpha$, where $\alpha>0$, $(t,p)=1$, then $(a,b)=1$ implies $p\nmid b$, so

$$(fg)(b)=0\,,\quad (fg)(a)=(fg)(ab)=f(p^\alpha)g(p^\alpha)\,,$$

thus (S.6.8) holds, indeed.

We get further solutions if f and g have the same sole (p,q), and there exists a number c satisfying

$$g(p^\alpha)=cf(p^\alpha)\,,\qquad g(q^\beta)=-cf(q^\beta)\,,\qquad \alpha,\beta=1,2,3,\dots \tag{S.6.9}$$

We can verify (S.6.8) as before, if at least one of a and b is divisible neither by p, nor by q.

The remaining case is $a=tp^\alpha$, $b=sq^\beta$ (or vice versa), where $(ts,pq)=1$. Using (S.6.9), we obtain

$$\begin{aligned}(fg)(a)&=f(p^\alpha)g(p^\alpha)=c\big(f(p^\alpha)\big)^2\,,\\ (fg)(b)&=f(q^\beta)g(q^\beta)=-c\big(f(q^\beta)\big)^2\,,\\ (fg)(ab)&=\big(f(p^\alpha)+f(q^\beta)\big)\big(g(p^\alpha)+g(q^\beta)\big)=\\ &=\big(f(p^\alpha)+f(q^\beta)\big)\big(cf(p^\alpha)-cf(q^\beta)\big)\,,\end{aligned}$$

which verifies (S.6.8).

Summarizing the above, we found the following solutions sofar:

I. $f=0$ or $g=0$.

II. f and g are arbitrary functions with (a common) sole p.

III. f and g are functions with (a common) sole (p,q) satisfying also (S.6.9).

Now we show that there are no other solutions, i.e. if f,g, and fg are all additive, then the pair of functions f,g belongs to one of the above types.

Assume that f,g, and fg is additive. Then

$$f(a)g(a)+f(b)g(b)=f(ab)g(ab)=\big(f(a)+f(b)\big)\big(g(a)+g(b)\big)\,,$$

i.e.

$$f(a)g(b)+f(b)g(a)=0 \tag{S.6.10}$$

if $(a,b)=1$. We may assume $f\neq 0$ and $g\neq 0$. We shall examine the values of f and g at prime powers. We distinguish two cases:

(A) There exists a prime power p^α where $f(p^\alpha)\neq 0$ and $g(p^\alpha)=0$.

(B) $f(w) = 0 \iff g(w) = 0$ for every prime power w.

In Case (A) we apply (S.6.10) with $a = p^\alpha$ and $b = r^\gamma$, where r is a prime distinct from p. This yields $g(r^\gamma) = 0$, i.e. g has sole p. As $g \neq 0$, we have $g(p^\kappa) \neq 0$ for some κ. Applying (S.6.10) for $a = p^\kappa$ and $b = r^\gamma$, we get $f(r^\gamma) = 0$. Thus also f has sole p, i.e. our pair f, g is of type II.

Turning to Case (B), let p^α be a prime power where $f(p^\alpha) \neq 0$ and $g(p^\alpha) \neq 0$. If f has sole p, then condition (B) implies that the same holds also for g, thus we have again a pair f, g of type II.

So we may assume that there exists a prime power q^β for some prime $q \neq p$, where $f(q^\beta) \neq 0$ and $g(q^\beta) \neq 0$.

We show first that both f and g have sole (p, q), i.e. $f(r^\gamma) = g(r^\gamma) = 0$ for every prime r different from p and q, and for every γ.

For a proof by contradiction, assume $f(r^\gamma) \neq 0$ for some r^γ.

If $f(a)f(b) \neq 0$, we can rewrite (S.6.10) into

$$\frac{g(a)}{f(a)} = -\frac{g(b)}{f(b)}\,. \tag{S.6.11}$$

Applying (S.6.11) for all pairs taken from p^α, q^β, and r^γ, we get

$$\frac{g(p^\alpha)}{f(p^\alpha)} = -\frac{g(q^\beta)}{f(q^\beta)} = \frac{g(r^\gamma)}{f(r^\gamma)} = -\frac{g(p^\alpha)}{f(p^\alpha)}\,,$$

which contradicts $g(p^\alpha) \neq 0$.

Finally, to verify (S.6.9), apply (S.6.11) first for $a = p^\alpha$ and $b = q^\beta$, and let c be the common value of the two sides. Keeping now a unaltered, let $b = q^\nu$, where ν assumes all exponents with $f(q^\nu) \neq 0$, and similarly, fix $b = q^\beta$ and let $a = p^\mu$ for all μ satisfying $f(p^\mu) \neq 0$. Then we obtain just the relations (S.6.9) from (S.6.11).

This means that the pair f, g is of type III.

• **6.1.13 (a)** Let k be the number of (distinct) elements in the range of the additive function f. The integer 0 occurs in the range, as $f(1) = 0$, .

We show first that if $a_1, a_2, \ldots, a_k$ are k arbitrary, pairwise coprime integers, then we can select some of them (allowing also the selection of all numbers or just one of them) so that f is 0 on their product.

Consider the values

$$f(a_1),\ f(a_1a_2),\ \ldots,\ f(a_1a_2\ldots a_k)\,.$$

If these are all distinct, then 0 appears among them, and we are done. If two of them are equal, i.e. $f(a_1a_2\dots a_j) = f(a_1a_2\dots a_i)$ for some $1 \le i < j \le k$, then

$$\begin{aligned} 0 &= f(a_1a_2\dots a_j) - f(a_1a_2\dots a_i) = \\ &= \big(f(a_1) + f(a_2) + \dots + f(a_j)\big) - \big(f(a_1) + f(a_2) + \dots + f(a_i)\big) = \\ &= f(a_{i+1}) + \dots + f(a_j) = f(a_{i+1}\dots a_j)\,. \end{aligned}$$

Consider now an arbitrary b. Partition the primes greater than b into groups of size k. By our previous observation, for any r there exists a product c_r of some primes in the rth block for which $f(c_r) = 0$. Since $(b, c_r) = 1$, we have $f(bc_r) = f(b) + f(c_r) = f(b)$, thus the function assumes $f(b)$ at the infinitely many integers bc_r.

• **6.1.15** Clearly, $\varphi_2(1) = 1$. If p^α is a prime power, then $(j, p^\alpha) \ne 1 \iff p \mid j$, hence $(i, p^\alpha) \ne 1 \iff i = rp$, and $(i+1, p^\alpha) \ne 1 \iff i = rp - 1$. Thus we obtain $\varphi_2(p^\alpha)$ by subtracting the number of integers

$$p-1,\ p,\ 2p-1,\ 2p,\ \dots,\ p^\alpha - 1 = p^{\alpha-1}p - 1,\ p^\alpha = p^{\alpha-1}p$$

from the number of all integers $1, 2, \dots, p^\alpha$. Hence

$$\varphi_2(p^\alpha) = p^\alpha - 2p^{\alpha-1}\,. \tag{S.6.12}$$

We verify now that $\varphi_2(n)$ is multiplicative. Let $(a, b) = 1$, and

$$1 \le u_1 < u_2 < \dots < u_r \le a \qquad \text{and} \qquad 1 \le v_1 < v_2 < \dots < v_s \le b$$

be all integers (between 1 and a, or 1 and b, resp.) satisfying

$$(u_i, a) = (u_i + 1, a) = 1 \qquad \text{and} \qquad (v_j, b) = (v_j + 1, b) = 1, \text{ resp.}$$

Thus $r = \varphi_2(a)$ and $s = \varphi_2(b)$.

Consider the system of congruences

$$\begin{aligned} x &\equiv u_i \pmod a \\ x &\equiv v_j \pmod b. \end{aligned} \tag{S.6.13}$$

As $(a, b) = 1$, this system has a unique solution modulo ab for every $i = 1, \dots, \varphi_2(a)$ and $j = 1, \dots, \varphi_2(b)$. Let w_{ij} denote the solution satisfying condition $1 \le w_{ij} \le ab$. Thus we defined altogether $\varphi_2(a)\varphi_2(b)$ integers w_{ij}.

We show

$$(w_{ij}, ab) = (w_{ij} + 1, ab) = 1\,, \tag{S.6.14}$$

and no other integers have this property between 1 and ab. This means that there are $\varphi_2(ab)$ integers w_{ij}. Combining the two results, we get the desired multiplicativity.

To verify (S.6.14), we have to show that both w_{ij} and $w_{ij}+1$ are coprime both to a and b. Since $w_{ij} \equiv u_i \pmod{a}$, so

$$(w_{ij}, a) = (u_i, a) = 1 \qquad \text{and} \qquad (w_{ij} + 1, a) = (u_i + 1, a) = 1\,.$$

We get $(w_{ij}, b) = (w_{ij} + 1, b) = 1$ similarly.

Now assume that $1 \le c \le ab$ and $(c, ab) = (c + 1, ab) = 1$. We have to prove $c = w_{ij}$ for some i and j. Let c' and c'' be the least positive remainders of c upon division by a and b, resp. This means $c' = u_i$ and $c'' = v_j$ with some i and j.

Therefore c is a solution of the system of congruences (S.6.13), so $c = w_{ij}$. This completes the proof of multiplicativity of $\varphi_2(n)$.

Finally, let $n = \prod_{i=1}^{t} p_i^{\alpha_i}$ be the standard form of n. Then using multiplicativity and (S.6.12), we get

$$\varphi_2(n) = \prod_{i=1}^{t} \left(p_i^{\alpha_i} - 2p_i^{\alpha_i - 1}\right) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{2}{p}\right)\,.$$

• **6.2.7** *First solution*: We show $\sigma(n) \ne 2p$ if p is any prime of the form $6k-1$.

For a proof by contradiction, assume $\sigma(n) = 2p$ for some positive integer n of standard form $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$. Then

$$2p = \sigma(n) = \prod_{i=1}^{r} \sigma(q_i^{\alpha_i})\,.$$

Since 2 does not occur in the range of σ, therefore $r = 1$, i.e $n = q^\alpha$ for some prime q and

$$2p = 1 + q + q^2 + \ldots + q^\alpha\,. \tag{S.6.15}$$

The left-hand side of (S.6.15) is even, so $q > 2$ and α is odd. Then we can factor out $1 + q$ on the right-hand side of (S.6.15). Clearly, $1 + q \ne 1, 2, p$,

thus $1+q=2p$ (and $\alpha=1$). By the condition, $2p\equiv 1 \pmod 3$, so $3 \mid q$. This yields $q=3$, i.e. $p=2$, which is impossible.

We can prove similarly $\sigma(n)\neq 2p$ for any prime p of the form $5k-2$ greater than 3 or of the form $7k-3$ or $11k-5$, etc.

• *Second solution*: We show $\sigma(n)\neq 3^s$ for $s>1$.

We prove again by contradiction. As σ is multiplicative, $\sigma(q^\alpha)=3^t$ (with $1\leq t\leq s$) for any prime power q^α in the standard form of n, i.e.

$$3^t = 1+q+q^2+\ldots+q^\alpha\,. \tag{S.6.16}$$

Considering first the case $q=2$, we can rewrite (S.6.16) into

$$3^t = 2^{\alpha+1}-1. \tag{S.6.17}$$

If $\alpha=1$, then $t=1$ and we get a solution $q^\alpha=2$. If $\alpha>1$, then the left-hand side of (S.6.17) is 1 or 3 modulo 8, but the right-hand side is 7, a contradiction. Thus we may assume $q>2$ and $t>1$. Considering (S.6.16) modulo 2 and 3, we find that α is even, further $q\equiv 1 \pmod 3$ and $\alpha\equiv 2 \pmod 3$. Therefore $1+q+q^2$ is a factor of the right-hand side of (S.6.16), so it has to be a power of 3, as well. But this is impossible, since $1+q+q^2$ is not divisible even by 9 as we can check it substituting $q\equiv 1, 4$, and 7 (mod 9).

We obtained that 2 is the only prime power, and therefore the only integer n for which $\sigma(n)$ is a power of 3. This means that $\sigma(n)=3^s$ is impossible for $s>1$.

• *Third solution*: We show that "most" odd integers do not appear in the range of σ.

We fix a "big" N, and estimate, at most for how many integers x is $\sigma(x)$ an odd number less than $2N$. Then clearly $x<2N$ and x must be a square or the double of a square by Exercise 6.2.6a. There are $\lfloor\sqrt{2N-1}\rfloor$ squares and $\lfloor\sqrt{N-1}\rfloor$ doubles of squares less than $2N$. Hence there are less than $(\sqrt{2}+1)\sqrt{N}$ possible values for x, whereas there are N odd integers up to $2N$. This means that at least

$$N-(\sqrt{2}+1)\sqrt{N} \tag{S.6.18}$$

odd integers less than $2N$ are missing from the range of σ. (The function in (S.6.18) tends "very strongly" to infinity, since the second term is "negligible" compared to N.)

• *Fourth solution*: Again, we fix a "big" N and estimate, at most how many numbers x satisfy $\sigma(x) \le N$. Then clearly also $x \le N$, but the even numbers $s > 2N/3$ do not fit, since $\sigma(s) \ge s + s/2 > N$. There are

$$\left\lfloor \frac{N}{2} \right\rfloor - \left\lfloor \frac{N}{3} \right\rfloor > \frac{N}{6} - 1$$

even integers between $2N/3$ and N, thus there remain at most $5N/6 + 1$ possible values for x. This means that at least $N/6 - 1$ integers among $1, 2, \ldots, N$ are missing from the range of σ.

• *Fifth solution*: We apply a similar argument as in the fourth solution, but instead of using $\sigma(x) > N$ for many $x \le N$, we exhibit "many" pairs $x_i \ne x_j$ satisfying $\sigma(x_i) = \sigma(x_j)$. Such pairs are e.g. $6t$ and $11t$ for $(t, 66) = 1$, and their number up to N is approximately

$$N \frac{\varphi(66)}{66 \cdot 11} = 0.027\ldots N.$$

Since the values of σ coincide for the members of at least so many pairs $x \le N$, therefore at least that many integers must be out of the range.

• *Remark*: Even a much sharper statement holds: "most" integers are missing from the range of σ, i.e. the range is a "rare" subsequence of the natural numbers. The precise formulation is the following. Let $U(N)$ be the number of elements $y \le N$ in the range of σ. Then $\lim_{N\to\infty} U(N)/N = 0$. The proof requires results on the distribution of primes in arithmetic progressions, see Exercises 6.4.8 and 6.4.9.

• **6.2.8** Clearly, $n = 1$ meets the requirement. We show that there are no more solutions. For $n \ge 2$,

$$\frac{\sigma(n!)}{n!} = \prod_{p \le n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{\alpha_p}}\right) < \prod_{p \le n} \frac{p}{p-1} \le \prod_{2 \le v \le n} \frac{v}{v-1} = n\,.$$

Hence $n! < \sigma(n!) < n \cdot n! < (n+1)!$, i.e. $\sigma(n!) \ne k!$.

• **6.2.17 (b)** We show that $g(n)$ assumes only values 0 and ± 1.

If n is not squarefree, then every term in the sum is 0, so $g(n) = 0$.

If n is squarefree and is a multiple of every prime less than 100, then $g(n) = \mu(n) = \pm 1$.

Otherwise, let S be the product of all primes up to 100 which do not divide n. If $(n,k) \neq 1$ or k is not squarefree, then $\mu(nk) = 0$, so

$$g(n) = \sum_{k|S} \mu(nk) = \sum_{k|S} \mu(n)\mu(k) = \mu(n) \sum_{k|S} \mu(k) = 0$$

(we used Theorem 6.2.4 in the last step).

• **6.3.5 (a)** If $n = 2^{p-1}$, where $2^p - 1$ is a Mersenne prime, then $\sigma(n) = 2^p - 1$ and $\sigma(\sigma(n)) = 2^p = 2n$.

For the converse, assume that n is even and superperfect. Write $n = 2^k t$, where $k \geq 1$ and t is odd. We have to show that $2^{k+1} - 1$ is a prime and $t = 1$.

We get $\sigma(n) = (2^{k+1} - 1)\sigma(t)$, so $k \geq 1$ implies that $(2^{k+1} - 1)\sigma(t)$ and $\sigma(t)$ are two distinct divisors of $\sigma(n)$. Therefore

$$2^{k+1}t = 2n = \sigma(\sigma(n)) \geq (2^{k+1} - 1)\sigma(t) + \sigma(t) = 2^{k+1}\sigma(t)\,.$$

This is possible only if $\sigma(t) = t$, i.e. $t = 1$, and $\sigma(n)$ has only these two positive divisors, thus $\sigma(n) = 2^{k+1} - 1$ is a prime.

• **(b)** By Exercise 6.2.6a, an odd n is a square if and only if $\sigma(n)$ is odd. Thus it suffices to prove that $\sigma(n)$ is odd if n is an odd superperfect number.

To get a contradiction, assume that n is superperfect and $\sigma(n) = 2^v w$, where w is odd and $v \geq 1$. Then

$$2n = \sigma(\sigma(n)) = (2^{v+1} - 1)\sigma(w)\,.$$

This implies $\sigma(w) = 2z$ and $n = (2^{v+1} - 1)z$ with a suitable z. As $v \geq 1$, we obtain

$$\sigma(n) \geq (2^{v+1} - 1)z + z = 2^{v+1}z,$$

but, as $\sigma(w) = 2z$ implies $w \neq 1$, also

$$\sigma(n) = 2^v w < 2^v \sigma(w) = 2^{v+1}z,$$

a contradiction.

• **(c)** Assume that p^α is superperfect where p is an odd prime. Let $\prod_{j=1}^{s} q_j^{\beta_j}$ be the standard form of $\sigma(p^\alpha)$, i.e.

$$\sigma(p^\alpha) = 1 + p + \ldots + p^\alpha = \prod_{j=1}^{s} q_j^{\beta_j}\,. \tag{S.6.19}$$

Then

$$2p^\alpha = \sigma(\sigma(p^\alpha)) = \prod_{j=1}^{s} \left(1 + q_j + \ldots + q_j^{\beta_j}\right). \tag{S.6.20}$$

Exactly one is even among the factors on the right-hand side of (S.6.20), say the first one. This means

$$1 + q_1 + \ldots + q_1^{\beta_1} = \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} = 2p^{\gamma_1}, \tag{S.6.21a}$$

and

$$1 + q_j + \ldots + q_j^{\beta_j} = \frac{q_j^{\beta_j+1} - 1}{q_j - 1} = p^{\gamma_j}, \qquad j = 2, \ldots, s, \tag{S.6.21b}$$

where the exponents γ_j are suitable positive integers and their sum is α. (The steps of the proof will be correct also for $s = 1$.)

(S.6.21a) and (S.6.21b) imply

$$q_j^{\beta_j+1} \equiv 1 \pmod{p}, \qquad j = 1, 2, \ldots, s. \tag{S.6.22}$$

By (S.6.21a), β_1 is odd, so we can factor out $1+q_1$ from $1+q_1+\ldots+q_1^{\beta_1}$. Therefore also $1 + q_1 = 2p^\delta$, thus

$$q_1 \equiv -1 \pmod{p}. \tag{S.6.23}$$

By (S.6.21b), β_j is even for $j \geq 2$, so

$$K = (\beta_2 + 1) \ldots (\beta_s + 1) \text{ is odd.} \tag{S.6.24}$$

Multiplying (S.6.19) by $q_1 \ldots q_s$, we obtain

$$\prod_{j=1}^{s} q_j^{\beta_j+1} = q_1 q_2 \ldots q_s (1 + p + \ldots + p^\alpha). \tag{S.6.25}$$

Considering (S.6.25) modulo p and applying (S.6.22) and (S.6.23) we arrive at $1 \equiv -q_2 \ldots q_s \pmod{p}$, i.e.

$$q_2 \ldots q_s \equiv -1 \pmod{p}. \tag{S.6.26}$$

Now we raise (S.6.26) to the Kth power. Then

$$(q_2 \dots q_s)^K \equiv -1 \pmod{p}, \tag{S.6.27}$$

by (S.6.24). But $j \geq 2$ implies $\beta_j + 1 \mid K$ so (S.6.22) yields

$$(q_2 \dots q_s)^K \equiv 1 \pmod{p},$$

which contradicts (S.6.27) (as $p > 2$).

• **6.4.8 (b)** We follow the ideas sketched in the hint.

Let $\varepsilon > 0$ be arbitrary. We have to verify that if N is large enough, then at most εN integers among $1, 2, \dots, N$ occur in the range of φ.

Fix a positive integer r satisfying

$$2^r > \frac{2}{\varepsilon}.$$

We partition the range of $\varphi(n)$ into two subsets: H_1 contains those elements which are multiples of 2^r, and H_2 consists of the values not divisible by 2^r.

Clearly, there are

$$\left\lfloor \frac{N}{2^r} \right\rfloor < \frac{\varepsilon N}{2}$$

elements in H_1 not greater than N. Thus it is sufficient to show that also H_2 contains at most $\varepsilon N/2$ elements not greater than N for N large enough.

If $\omega(n) \geq r + 1$, then $2^r \mid \varphi(n)$, so $\varphi(n) \in H_1$ for every such integer n.

Thus we may restrict ourselves to integers n satisfying $\omega(n) \leq r$. In this case,

$$\frac{\varphi(n)}{n} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \tag{S.6.28}$$

is minimal if just the first r primes $p_1, \dots, p_r$ occur in the standard form of n. Therefore we can transform (S.6.28) into

$$\varphi(n) \geq nc, \tag{S.6.29}$$

where

$$c = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(S.6.29) implies

$$n \le \frac{\varphi(n)}{c} \le \frac{N}{c}$$

for $\varphi(n) \le N$, so the elements of H_2 not greater than N must be among the values

$$\varphi(1),\ \varphi(2),\ \ldots,\ \varphi(N'),$$

where $N' = \lfloor N/c \rfloor$. By part (a), if ha N' is large enough, then there are at most

$$\frac{c\varepsilon N'}{2} \le \frac{\varepsilon N}{2}$$

integers among $1, 2, \ldots, N'$ for which $\varphi(n)$ is not a multiple of 2^r, therefore at most $\varepsilon N/2$ values $\varphi(n)$ can occur in H_2, indeed.

• **6.6.12 (a)** Since $d(n) = (1*1)(n)$, the Dirichlet series of $d(n)$ is $D(s) = \zeta^2(s)$ by Theorem 6.6.4. So, for $s = 2$, we have

$$D(2) = \sum_{n=1}^{\infty} \frac{d(n)}{n^2} = \zeta^2(2) = \Big(\frac{\pi^2}{6}\Big)^2 .$$

• **(b)** Let $T(s)$ be the Dirichlet series of $d^2(n)$. Since $d^2(n)$ is multiplicative, we can apply Exercise 6.6.10a to deduce

$$T(s) = \sum_{n=1}^{\infty} \frac{d^2(n)}{n^s} = \prod_p \Big(\sum_{k=0}^{\infty} \frac{d^2(p^k)}{p^{ks}}\Big) = \prod_p \Big(\sum_{k=0}^{\infty} \frac{(k+1)^2}{p^{ks}}\Big) . \tag{S.6.30}$$

Let

$$H(x) = \sum_{k=0}^{\infty} (k+1)^2 x^k , \tag{S.6.31}$$

then (S.6.30) and (S.6.31) imply

$$T(s) = \prod_p H\big(\frac{1}{p^s}\big) . \tag{S.6.32}$$

We assume $s > 1$, and we investigate $H(x)$ in the region $0 < x < 1/2$, as $p \ge 2$. We get the infinite series $H(x)$ by differentiating the infinite geometric series

$$\sum_{j=0}^{\infty} x^j = \frac{1}{1-x}$$

by terms:

$$\sum_{j=1}^{\infty} jx^{j-1} = \frac{1}{(1-x)^2}\,,$$

multiplying the result by x:

$$\sum_{j=1}^{\infty} jx^{j} = \frac{x}{(1-x)^2}\,,$$

and differentiating again by terms:

$$\sum_{j=1}^{\infty} j^2x^{j-1} = \frac{1+x}{(1-x)^3}\,. \tag{S.6.33}$$

By the theorem about differentiating power series, the above steps were legal e.g. for $|x| \le 1/2$, thus the above equalities are valid.

Substitution $k = j-1$ shows that the left-hand side of (S.6.33) is just $H(x)$. Multiplying both the numerator and denominator of the fraction on the right-hand side by $1-x$, we get

$$H(x) = \frac{1-x^2}{(1-x)^4}\,. \tag{S.6.34}$$

Substituting (S.6.34) into (S.6.32) yields

$$T(s) = \prod_p \frac{1-\frac{1}{p^{2s}}}{\left(1-\frac{1}{p^s}\right)^4} = \frac{\zeta^4(s)}{\zeta(2s)}\,. \tag{S.6.35}$$

Applying (S.6.35) with $s=2$, we get

$$T(2) = \sum_{n=1}^{\infty} \frac{d^2(n)}{n^2} = \frac{\zeta^4(2)}{\zeta(4)} = \frac{\left(\frac{\pi^2}{6}\right)^4}{\frac{\pi^4}{90}} = \frac{5\pi^4}{72}\,.$$

• **6.7.4** We prove along the lines indicated in the hint.

We show first that if n is large enough, then $\sigma(i) \le 2n$ for more than the half of the integers i among $1, 2, \ldots, n$. Let t denote the number of values i for which this is false, then we have to verify $t < n/2$. Applying $\sigma(i) > 2n$ for

the t "bad" values and using the trivial estimate $\sigma(i) > 0$ for the others, we obtain

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) > 2tn\,. \tag{S.6.36}$$

On the other hand, by Theorem 6.7.3,

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) < n^2 \tag{S.6.37}$$

if N is large enough. (S.6.36) and (S.6.37) immediately imply $t < n/2$.

Let now k be arbitrary. By Exercise 6.4.9, the range of σ contains at most

$$\frac{2n}{4k}$$

integers $j \leq 2n$, if n is large enough. By the previous paragraph, $\sigma(i)$ is such a j for more than $n/2$ integers i, therefore σ must assume some value j at least at

$$\frac{n}{2} \;:\; \frac{2n}{4k} \;=\; k$$

places.

Solutions, Chapters 7–9

7. Diophantine Equations

• **7.1.4** Let M denote the year in question of the 20th century. We show first that at least one of A and B was born before 1900.

For a proof by contradiction, assume that they were born in $\overline{19uv}$ and $\overline{19xz}$ (clearly, none of them could be born in 2000, i.e. in the last year of the 20th century). By the condition,

$$M = 1900 + 10u + v + 1 + 9 + u + v = 1910 + 11u + 2v = 1910 + 11x + 2z.$$

We can rearrange it as $11(u-x) = 2(z-v)$, so we obtain $11 \mid z-v$. Since $|z-v| \le 9$, only $z - v = 0$ is possible. But then also $u = x$ which contradicts the different ages of A and B.

We get similarly that at least one of them was born after 1899: if the birth dates are $\overline{18uv}$ and $\overline{18xz}$, then

$$M = 1800 + 10u + v + 1 + 8 + u + v = 1809 + 11u + 2v = 1809 + 11x + 2z$$

leads to a contradiction exactly the same way.

This means that B was born in $\overline{19uv}$, and A was born in $\overline{18xz}$. Then

$$M = 1910+11u+2v = 1809+11x+2z, \qquad \text{i.e.} \qquad 101 = 11(x-u)+2(z-v).$$

Thus $x - u$ is odd, further $z - v \le 9$ implies

$$x - u \ge \frac{101 - 18}{11} > 7,$$

thus only $x - u = 9$ is possible. Hence

$$x = 9, \quad u = 0 \quad \text{and} \quad z = v + 1 \quad (v = 0, 1, \ldots, 8),$$

and these values satisfy the requirements, indeed (with suitable values M). Thus the difference in ages is

$$\overline{19uv} - \overline{18xz} = (1900 + v) - (1890 + v + 1) = 9 \text{ years}.$$

• **7.3.8** We show that there are no solutions apart from the trivial $x = y = s = t = 0$.

• *First proof*: For a proof by contradiction, assume the existence of a non-trivial rational solution. Multiplying by the least common multiple of the denominators, and if necessary, dividing by the greatest common divisor of the integers thus obtained, we get an integer solution satisfying $(x, y, s, t) = 1$.

We check the parity of the numbers. By the condition,

$$t^2 + s^2 + x^2 \equiv t^2 + (s + x)^2 = (y + t)^2 + x^2 \equiv y^2 + t^2 + x^2 \pmod 2,$$

so s and y have the same parity.

Considering now the system of equations modulo 4, we infer that also t, $s + x$, $y + t$, and x must have this parity.

All the six numbers cannot be odd, for if y and t are odd, then $y + t$ is even.

All the six numbers cannot be even either, since $(x, y, s, t) = 1$.

This contradiction completes the proof.

• *Second proof*: We prove again by contradiction. As in the previous proof, we may assume the existence of a non-trivial integer solution. Then the occurring sums of squares are greater than zero.

Consider the points $(0, 0)$, (s, y), and $(s+x, -t)$ in the lattice with integer coordinates. By the condition, these are vertices of an equilateral triangle.

Lattice points, however, cannot form an equilateral triangle, since the lattice rectangle containing it and the "corner triangles" have rational areas, but the area of the equilateral triangle is $\sqrt{3}/4$ times the square of the side length, and this square is an integer by the Pythagorean theorem.

• **7.3.10** Let s be the arithmetic mean of the 8 numbers. Then $2s = t$ where t is an odd integer, and the sum of cubes of the 8 numbers is

$$\left(s - \frac{7}{2}\right)^3 + \left(s - \frac{5}{2}\right)^3 + \left(s - \frac{3}{2}\right)^3 + \left(s - \frac{1}{2}\right)^3 + \left(s + \frac{1}{2}\right)^3 + \left(s + \frac{3}{2}\right)^3 + \left(s + \frac{5}{2}\right)^3 + \left(s + \frac{7}{2}\right)^3 = 8s^3 + 126s = t^3 + 63t\,.$$

Thus we are looking for solutions of $t^3 + 63t = v^3$ where v is an integer and t is an odd integer. If the pair (v, t) is a solution, then also the pair $(-v, -t)$ is a solution, hence it is sufficient to find the solutions with $t > 0$.

Clearly $v > t$, further, $(t + 5)^3 > t^3 + 63t = v^3$ implies $v < t + 5$. Also, v has to be even, therefore $v = t + 1$ or $v = t + 3$.

The first relation yields no solution, the second one gives $t = 1$ and $t = 3$. Accordingly, the integers v in question are 4, 6, -4, and -6. Indeed,

$4^3 = (-3)^3 + (-2)^3 + \ldots + 4^3$, $6^3 = (-2)^3 + (-1)^3 + \ldots + 5^3$, and multiplying these by -1 yields the other two representations.

• **7.3.13 (g)** Clearly, $x = \pm 1$, $y = 0$ satisfy the equation. We show that there are no other integer solutions.

For a proof by contradiction, we consider a solution where $x > 1$.

Writing the equation as $(x+1)(x-1) = 2y^4$, we see that $x+1$ and $x-1$ are even, so also $y = 2u$. Dividing both sides by 4, we get

$$\frac{x+1}{2} \cdot \frac{x-1}{2} = 8u^4\,. \tag{S.7.1}$$

The left-hand side of (S.7.1) is the product of two consecutive integers, therefore the factors are coprime. So one of them is a fourth power, and the other one is 8 times a fourth power. Their difference is 1, hence

$$w^4 - 8z^4 = 1 \qquad \text{or} \qquad w^4 - 8z^4 = -1.$$

The second case is impossible since a square cannot have a residue -1 modulo 8. In the first case, rearranging and factoring yields $(w^2+1)(w^2-1) = 8z^4$, i.e.

$$\frac{w^2+1}{2}(w^2-1) = (2z^2)^2\,. \tag{S.7.2}$$

We show that the two (positive) factors on the left-hand side of (S.7.2) are coprime. Let d denote their gcd. Since $(w^2+1)/2$ is odd, also d must be odd. Further,

$$d \mid 2\frac{w^2+1}{2} - (w^2-1) = 2,$$

thus $d = 1$, indeed.

This means that $(w^2+1)/2$ and w^2-1 are squares themselves. The difference of two positive squares, however, cannot be 1, so w^2-1 cannot a square, which is a contradiction.

• **(h)** We verify that all solutions are: $x = y$; $x = 2, y = 4$; and $x = 4$, $y = 2$.

Obviously, these are solutions, indeed. Thus we have to show that if $y > x$, then necessarily $x = 2$ and $y = 4$.

• *First proof*: Let $(x, y) = d$, then $x = da$, $y = db$, where $(a, b) = 1$. Substituting back into the equation and taking dth root, we get

$$(da)^b = (db)^a, \qquad \text{so, by } b > a, \qquad d^{b-a}a^b = b^a\,. \tag{S.7.3}$$

Therefore $a \mid b^a$, but $(a,b)=1$, so necessarily $a=1$. Then (S.7.3) means the equation

$$d^{b-1} = b\,.$$

Here $b > a = 1$, thus $d > 1$. Then $d^{b-1} \geq b$ for every $b > 1$, and equality holds only for $d = b = 2$. Thus we obtain the desired values

$$x = da = 2 \cdot 1 = 2 \qquad \text{and} \qquad y = db = 2 \cdot 2 = 4.$$

• *Second proof*: If $y > x > 1$, then an equivalent form of the equation is

$$\frac{x}{\log x} = \frac{y}{\log y}\,.$$

Since the (real) function $f(z) = z/\log z$ is strictly decreasing for $1 < z < e$ and is strictly increasing for $z > e$, it can assume the same value at two distinct integers only if the smaller integer is 2. Thus only $x = 2$ is possible. Then $y = 4$ satisfies the equation, and as f is strictly monotone for $z > e$, no other y can fit.

• **(i)** Clearly, $x = 5$, $y = 1$ satisfy the equation. We show that this is the only solution.

If the equation holds, then also

$$y^5 \equiv 2^x \pmod{31}. \tag{S.7.4}$$

We see from the original equation that $31 \nmid y$, therefore 2^x has to be a fifth power residue modulo 31, by (S.7.4). By Theorem 3.5.3,

$$(2^x)^{\frac{30}{(5,30)}} = 2^{6x} \equiv 1 \pmod{31}\,. \tag{S.7.5}$$

(S.7.5) implies

$$o_{31}(2) = 5 \mid 6x, \qquad \text{thus} \qquad 5 \mid x, \qquad \text{i.e.} \qquad x = 5u\,.$$

Substituting back into the original equation, we get

$$(2^u)^5 - y^5 = 31, \tag{S.7.6}$$

hence the difference of two (positive) fifth powers is 31. This happens only in the case $2^5 - 1^5$ which can be proved similarly as we handled the equation $a^3 - b^3 = 7$ during the solution of the example illustrating method II: either

we use that the difference of two fifth powers is bigger than 31 in every other case; or we prove via factoring the left-hand side of (S.7.6).

• **7.5.10** We factor the left-hand side of the equation: $(x+2i)(x-2i) = y^3$. Let $\delta = (x+2i, x-2i)$, then

$$\delta \mid (x+2i) - (x-2i) = 4i = (-i)(1+i)^4.$$

Therefore $\delta = (1+i)^r$, where $0 \le r \le 4$.

The properties of conjugation (see Exercise 7.4.2a) imply

$$(1+i)^s \mid x+2i \iff (1-i)^s \mid x-2i\,. \tag{S.7.7}$$

Since $1+i$ and $1-i$ are associates, we obtain from (S.7.7) that the exponents of $1+i$ in the standard forms of $x+2i$ and $x-2i$ are the same integer r. The product $(x+2i)(x-2i)$ is a cube (also among the Gaussian integers), therefore the exponent of the Gaussian prime $1+i$ in the standard form of this product is a multiple of 3. So $3 \mid 2r$, hence $r = 3t$ (i.e. $r = 0$ or 3).

By the above,

$$\frac{x+2i}{(1+i)^{3t}} \cdot \frac{x-2i}{(1-i)^{3t}} = \left(\frac{y}{2^t}\right)^3 \qquad \text{and} \qquad \left(\frac{x+2i}{(1+i)^{3t}}\,,\ \frac{x-2i}{(1-i)^{3t}}\right) = 1\,.$$

By the Fundamental Theorem of Arithmetic, each of $x+2i$ and $x-2i$ is an associate of a cube. Since every unit among the Gaussian integers is a cube, we obtain that $x+2i$ and $x-2i$ are cubes themselves.

Then

$$x+2i = (c+di)^3 = c^3 - 3cd^2 + (3c^2d - d^3)i\,. \tag{S.7.8}$$

Comparing the imaginary parts, we obtain $2 = d(3c^2 - d^2)$. Thus $d = \pm 1$ or ± 2, and substitution shows that only $d = 1$ and $d = -2$ yield an integer value for c which is $c = \pm 1$ in both cases.

Finally, we get $x = c^3 - 3cd^2$ from (S.7.8), so the solutions are $x = \pm 2$, $y = 2$; and $x = \pm 11$, $y = 5$.

• **7.5.11** We investigate the equation $\xi^2 + \psi^2 = \alpha$, where α is a given Gaussian integer, and ξ and ψ are the "unknown" Gaussian integers.

Factoring the left-hand side, we obtain $(\xi + \psi i)(\xi - \psi i) = \alpha$, i.e.

$$\xi + \psi i = \delta_1, \quad \xi - \psi i = \delta_2, \quad \text{where} \quad \delta_1\delta_2 = \alpha.$$

So

$$\xi = \frac{\delta_1 + \delta_2}{2}, \qquad \psi = \frac{\delta_1 - \delta_2}{2i}\,.$$

Since i is a unit, further $\delta_1 + \delta_2 = (\delta_1 - \delta_2) + 2\delta_2$, hence ξ and ψ are Gaussian integers if and only if

$$2 \mid \delta_1 - \delta_2\,. \tag{S.7.9}$$

Let $\alpha = a + bi$.

First we list the cases when (S.7.9) holds for some pair of divisors δ_1, δ_2 (so α has a representation as $\xi^2 + \psi^2$).

If a is odd and b is even, then $\delta_1 = \alpha, \delta_2 = 1$ satisfy (S.7.9): $2 \mid (a-1)+bi$.

If $4 \mid a$ and $4 \mid b$, then $\delta_1 = \alpha/2, \delta_2 = 2$ suit, as now each of δ_1 and δ_2 is a multiple of 2.

Let a and b even so that exactly one of them is a multiple of 4. Then the exponent of the Gaussian prime $1 + i$ is exactly 2 in the standard form of α, therefore

$$\alpha = (1+i)^2(c+di), \quad \text{where} \quad 1 + i \not\mid c + di, \quad \text{i.e.} \quad c \not\equiv d \pmod 2\,.$$

We can choose

$$\delta_1 = \frac{\alpha}{1+i} = (c+di)(1+i), \qquad \delta_2 = 1 + i,$$

since

$$\delta_1 - \delta_2 = (1+i)((c-1) + di)\,,$$

further

$$c - 1 \equiv d \pmod 2 \Longrightarrow 1 + i \mid c - 1 + di,$$

so $\delta_1 - \delta_2$ is divisible by $(-i)(1+i)^2 = 2$.

Now we show that α cannot be written as $\xi^2 + \psi^2$ in the other cases.

If $a \equiv b \equiv 2 \pmod 4$, then the Gaussian prime $1 + i$ occurs with exponent 3 in the standard form of α. Therefore exactly one element of any pair of divisors δ_1, δ_2 is divisible by $(-i)(1+i)^2 = 2$, so (S.7.9) cannot hold.

Finally, if b is odd, then $a + bi \neq (x_1 + x_2 i)^2 + (y_1 + y_2 i)^2$, since the imaginary part is even on the right-hand side, and odd on the left-hand side.

Thus we have proved that $\alpha = a + bi$ is *not* representable in the form $\xi^2 + \psi^2$ if and only if b is odd, or $a \equiv b \equiv 2 \pmod 4$.

• **7.5.17** We verify that n can be represented in the desired form if and only if $2n$ is the sum of three squares. Hence, by the Three Squares Theorem, we infer that those integers n are "bad" for which

$$2n = 4^{k+1}(8m+7), \qquad \text{i.e.} \qquad n = 4^k(16m+14)\,.$$

If n has a good representation, i.e. $n = 2x^2 + y^2 + z^2$, then

$$2n = (2x)^2 + (y+z)^2 + (y-z)^2\,.$$

Conversely, if $2n = a^2 + b^2 + c^2$, then we can assume that a is even, and b and c have the same parity, so

$$n = 2\Big(\frac{a}{2}\Big)^2 + \Big(\frac{b+c}{2}\Big)^2 + \Big(\frac{b-c}{2}\Big)^2\,.$$

• **7.5.5 (b)** We apply infinite descent. By solution we shall always mean a solution in positive integers. Assume that

$$x^4 + y^4 = z^2 \tag{S.7.10}$$

has a solution, and consider the solution $x_0,\ y_0,\ z_0$ where z_0 is minimal. We exhibit a solution $x_1,\ y_1,\ z_1$ with $z_1 < z_0$, which contradicts the minimality of z_0.

If $(x_0, y_0, z_0) = d > 1$, then also

$$\frac{x_0}{d}\,, \qquad \frac{y_0}{d}\,, \qquad \frac{z_0}{d^2}$$

satisfy (S.7.10), and $z_0/d^2 < z_0$ contradicts the minimality of z_0.

Therefore $x_0,\ y_0$, and z_0 are coprime, and the usual argument yields that they are pairwise coprime, as well.

So $x_0^2,\ y_0^2$, and z_0 form a primitive Pythagorean triple:

$$x_0^2 = 2mn \tag{S.7.11a}$$
$$y_0^2 = m^2 - n^2 \tag{S.7.11b}$$
$$z_0 = m^2 + n^2 \tag{S.7.11c}$$

where

$$m > n > 0, \qquad (m,n) = 1, \qquad \text{and} \qquad m \not\equiv n \pmod 2\,.$$

Considering (S.7.11b) modulo 4, we obtain that now m is odd and n is even; $n = 2n_1$. Substituting into (S.7.11a), we obtain

$$\left(\frac{x_0}{2}\right)^2 = mn_1, \qquad \text{where} \qquad (m, n_1) = 1.$$

Therefore

$$\text{(S.7.12)} \qquad m = u^2 \qquad \text{and} \qquad n_1 = v^2\,, \qquad \text{where} \qquad (u, v) = 1.$$

Substituting (S.7.12) into (S.7.11b), we get

$$y_0^2 = (u^2)^2 - (2v^2)^2\,,$$

i.e. y_0, $2v^2$, and u^2 is a primitive Pythagorean triple. Using the formula again,

$$\text{(S.7.13a)} \qquad 2v^2 = 2rs$$

$$\text{(S.7.13b)} \qquad u^2 = r^2 + s^2$$

where $(r, s) = 1$. Thus (S.7.13a) implies $r = t^2$, $s = w^2$, and so (S.7.13b) can be written as

$$u^2 = t^4 + w^4\,.$$

This means that $x_1 = t, y_1 = w$, $z_1 = u$ satisfy (S.7.10), and by (S.7.11c) and (S.7.12),

$$z_0 = m^2 + n^2 > m = u^2 \geq u = z_1,$$

which contradicts the minimality of z_0.

• **7.7.7** Let x be the base of the number system. We need the solutions of the Diophantine equation

$$\text{(S.7.14)} \qquad x^3 + x^2 + x + 1 = y^2$$

where $x \geq 2$. We prove that $x = 7$, $y = 20$ is the only solution. (We can easily see that for $x \leq 1$ we get integer solutions only for $x = 0$ and ± 1.)

Factoring the left-hand side of (S.7.14), we obtain

$$\text{(S.7.15)} \qquad (x + 1)(x^2 + 1) = y^2\,.$$

Let h be the gcd of the two factors on the left-hand side of (S.7.15), then

$$h \mid (x^2 + 1) - (x + 1)(x - 1) = 2, \qquad \text{thus} \qquad h = 1 \text{ or } 2.$$

If $h = 1$, then $x^2 + 1$ is a square (and so is also $x + 1$): $x^2 + 1 = z^2$. But this is impossible for $x \neq 0$.

If $h = 2$, then

$$x + 1 = 2u^2 \qquad \text{and} \qquad x^2 + 1 = 2v^2 \qquad (u > 1,\ v > 1). \tag{S.7.16}$$

Expressing $x = 2u^2 - 1$ from the first equation and substituting it into the second one, we get

$$(2u^2 - 1)^2 + 1 = 2v^2\,. \tag{S.7.17}$$

Rearranging (S.7.17) and dividing by 2 yields

$$(u^2)^2 + (u^2 - 1)^2 = v^2\,. \tag{S.7.18}$$

Since $u > 1$, $v > 0$, and $(u^2, u^2 - 1) = 1$, (S.7.18) implies that

$$u^2, \quad u^2 - 1, \quad \text{and} \qquad v$$

form a primitive Pythagorean triple. Thus

$$u^2 = m^2 - n^2 \tag{S.7.19a}$$

and

$$u^2 - 1 = 2mn, \tag{S.7.19b}$$

or with reverse roles,

$$u^2 = 2mn \tag{S.7.20a}$$

and

$$u^2 - 1 = m^2 - n^2 \tag{S.7.20b}$$

for some integers m and n satisfying the "usual" properties.

Consider first the case (S.7.19a)–(S.7.19b). Then u, n, and m form a primitive Pythagorean triple by (S.7.19a) and $(m, n) = 1$. Since u is odd [by (S.7.19a)], we have

$$u = r^2 - s^2, \qquad n = 2rs, \qquad \text{and} \qquad m = r^2 + s^2.$$

We infer

$$m - n = (r - s)^2. \tag{S.7.21}$$

Subtracting (S.7.19b) from (S.7.19a), we get

$$m^2 - n^2 - 2mn = 1, \qquad \text{i.e.} \qquad (m-n)^2 - 2n^2 = 1. \tag{S.7.22}$$

Using (S.7.21), we can rewrite (S.7.22) as

$$(r-s)^4 - 1 = 2n^2\,. \tag{S.7.23}$$

We can factor the left-hand side of (S.7.23):

$$\big((r-s)^2+1\big)\big((r-s)^2-1\big) = 2n^2\,. \tag{S.7.24}$$

The difference of the two factors on the left-hand side of (S.7.24) is 2, both factors are even, so their gcd is 2. The residue of an odd square modulo 4 is 1, thus the first factor is (even, but) not divisible by 4. Therefore

$$(r-s)^2 + 1 = 2t^2 \qquad \text{and} \qquad (r-s)^2 - 1 = w^2\,.$$

But the latter cannot hold as $w \neq 0$. Herewith we have proved the impossibility of the case (S.7.19a)–(S.7.19b).

Turning to the case (S.7.20a)–(S.7.20b), now u is even, so considering (S.7.20b) modulo 4, we see that m is even and n is odd. As $(m,n) = 1$, (S.7.20a) implies

$$m = 2a^2, \qquad n = b^2, \qquad \text{and so} \qquad u^2 = 4a^2b^2. \tag{S.7.25}$$

Substituting (S.7.25) into (S.7.20b), we get

$$4a^2b^2 - 1 = 4a^4 - b^4\,,$$

which can be rearranged as

$$(2a^2+b^2)^2 - 1 = 8a^4\,. \tag{S.7.26}$$

Factoring the left-hand side of (S.7.26), the two factors are even and their difference is 2, so their gcd is 2. This yields

$$2a^2 + b^2 + 1 = 2c^4 \qquad \text{and} \qquad 2a^2 + b^2 - 1 = 4d^4\,, \tag{S.7.27}$$

or

$$2a^2 + b^2 + 1 = 4d^4 \qquad \text{and} \qquad 2a^2 + b^2 - 1 = 2c^4\,. \tag{S.7.28}$$

Subtracting the two equations in (S.7.27) and dividing by 2, we get

$$c^4 - 2d^4 = 1\,.$$

By Exercise 7.3.13g, $d = 0$ follows, which is excluded now.

From (S.7.28), we obtain similarly

$$c^4 - 2d^4 = -1.$$

By Exercise 7.7.6, here $c = \pm 1$, $d = \pm 1$. Substituting these values into (S.7.28), we get $2a^2 + b^2 = 3$, so $a^2 = b^2 = 1$. Thus $u^2 = 4$ by (S.7.25), and finally $x = 7$ by (S.7.16).

• **7.7.10 (a)** Assume first that the Diophantine equation

$$x^2 + 3y^2 = n \tag{S.7.29}$$

is solvable, and let $x = a$, $y = b$ a solution. Then

$$\begin{aligned} n = a^2 + 3b^2 = a^2 + (bi\sqrt{3})^2 = N(a + bi\sqrt{3}) = N(a + b(1 + 2\omega)) = \\ = N(a + b + 2b\omega) = (a + b)^2 - (a + b)2b + (2b)^2\,, \end{aligned}$$

so $x = a + b$, $y = 2b$ is a solution of

$$x^2 - xy + y^2 = n. \tag{S.7.30}$$

Let now $x = c$, $y = d$ be a solution of (S.7.30). If

$$c = a + b \qquad \text{and} \qquad d = 2b \tag{S.7.31}$$

for some integers a, b, then reversing the previous argument we see that $x = a$, $y = b$ is a solution of (S.7.29). (S.7.31) holds if and only if d is even. As $n = x^2 - xy + y^2$ is symmetric in x and y, we are done also if c is even. Finally, if both c and d are odd, then

$$\begin{aligned} n = c^2 - cd + d^2 = N(c + d\omega) = N(c + d\omega^2) = \\ = N(c - d - d\omega) = (c - d)^2 - (c - d)(-d) + (-d)^2\,, \end{aligned}$$

so also $x = c - d$, $y = -d$ is a solution of (S.7.30), and here $c - d$ is even.

Of course, one can present the above arguments also via "tricky" transformations without referring to Eulerian integers.

• **7.7.11** We proceed similarly as in Exercise 7.5.10. We can factor the left-hand side of

$$x^2 + 243 = y^3 \tag{S.7.32}$$

among the Eulerian integers:

$$(x + 9i\sqrt{3})(x - 9i\sqrt{3}) = y^3\,. \tag{S.7.33}$$

Let

$$\alpha = x + 9i\sqrt{3} = x + 9 + 18\omega, \quad \text{then} \quad \overline{\alpha} = x - 9i\sqrt{3}\,.$$

We show that each of α and $\overline{\alpha}$ is an associate of a cube among the Eulerian integers.

Let $\delta = (\alpha, \overline{\alpha})$, then δ divides

$$\alpha - \overline{\alpha} = 18i\sqrt{3} = 2(i\sqrt{3})^5\,.$$

Considering (S.7.32) modulo 8, we find that x must be even, thus $2 \nmid x+9$, and so $2 \nmid \alpha = x + 9 + 18\omega$. Therefore the Eulerian prime 2 does not divide δ, thus

$$\delta = \pi^r, \qquad \text{where} \qquad \pi = i\sqrt{3} \qquad \text{and} \qquad 0 \le r \le 5.$$

Since

$$\pi^s \mid \alpha \iff \overline{\pi}^s \mid \overline{\alpha},$$

further, π and $\overline{\pi}$ are associates, so the exponents of π are the same r in the standard forms of α and $\overline{\alpha}$. By (S.7.33), the product $\alpha\overline{\alpha}$ is a cube, hence its standard form contains π with an exponent divisible by 3. Thus $3 \mid 2r$, so $r = 3t$ (i.e. $r = 0$ or 3). Therefore (some associate of) δ is a cube: $\delta = \tau^3$.

By the above,

$$\frac{\alpha}{\tau^3} \cdot \frac{\overline{\alpha}}{\tau^3} = \left(\frac{y}{\tau^2}\right)^3, \qquad \text{where} \qquad \left(\frac{\alpha}{\tau^3}\,,\, \frac{\overline{\alpha}}{\tau^3}\right) = 1.$$

According to the Fundamental Theorem of Arithmetic, $(x \pm 9i\sqrt{3})/\tau^3$ and thus $x \pm 9i\sqrt{3}$ are associates of cubes. (We cannot omit the unit factor, as not all units are cubes among the Eulerian integers.)

Then

$$\alpha = x + 9 + 18\omega = \varepsilon(c + d\omega)^3\,. \tag{S.7.34}$$

Since -1 is a cube, it is enough to investigate (S.7.34) for the cases $\varepsilon = 1$, ω, and ω^2.

If $\varepsilon = 1$, then $\omega^3 = 1$ and $\omega^2 = -1 - \omega$, so

$$(c + d\omega)^3 = c^3 + 3c^2 d\omega + 3cd^2\omega^2 + d^3\omega^3 = c^3 + d^3 - 3cd^2 + (3c^2 d - 3cd^2)\omega.$$

Comparing the "ω-free parts" and the coefficients of ω, resp., in (S.7.34), we get

$$x + 9 = c^3 + d^3 - 3cd^2 \tag{S.7.35a}$$

$$18 = 3c^2 d - 3cd^2. \tag{S.7.35b}$$

(S.7.35b) is equivalent to $cd(c-d) = 6$ the solutions of which are the following pairs (c, d):

$$(3,2); \qquad (3,1); \qquad (-1,2); \qquad (-1,-3); \qquad (-2,1); \qquad (-2,-3).$$

Substituting these into (S.7.35a), we get $x = \pm 10$, and then $y = 7$ by (S.7.32).

If $\varepsilon = \omega$, then we get similarly

$$18 = c^3 + d^3 - 3c^2 d \tag{S.7.36}$$

instead of (S.7.35b). We show that (S.7.36) has no solutions.

We look at (S.7.36) mod 3. By Fermat's Little Theorem, $a^3 \equiv a \pmod 3$ for every a, so

$$0 \equiv c^3 + d^3 \equiv c + d \pmod 3.$$

If $3 \mid c$, then $3 \mid d$, thus the right-hand side of (S.7.36) is a multiple of 27, but the left-hand side is not.

Otherwise $c = 3r + 1$ and $d = 3s - 1$, or vice versa, so

$$c^3 + d^3 = (3r+1)^3 + (3s-1)^3 = 27(r^3 + s^3 + r^2 - s^2) + 9(r+s)\,,$$

so rearranging (S.7.36) into

$$3c^2 d = c^3 + d^3 - 18,$$

the right-hand side is a multiple of 9, but the left-hand side is not.

Herewith we have proved that (S.7.36) has no solutions.

Finally, the case $\varepsilon = \omega^2$ leads to

$$18 = -c^3 - d^3 + 3cd^2$$

instead of (S.7.36), and we find the same way that it has no solutions.

Summarizing the results, we obtained that all solutions of the Diophantine equation $x^2 + 243 = y^3$ are $x = \pm 10$, $y = 7$.

8. Diophantine Approximation

• **8.1.8 (c)** We show that a real number ϱ can be written in the form $h(\alpha) = \{\alpha\}^2 - \{\alpha^2\}$ if and only if $-1 < \varrho < 1$.

Necessity follows from $0 \le \{c\} < 1$ for any c.

Concerning sufficiency, let $0 \le \vartheta < 1$, k a positive integer, and $\alpha = k + \vartheta$. Then

$$\{\alpha\}^2 = \vartheta^2 \qquad \text{and} \qquad \{\alpha^2\} = \{\vartheta^2 + 2k\vartheta\}. \tag{S.8.1}$$

If

$$0 \le \vartheta^2 + 2k\vartheta < 1, \qquad \text{i.e.} \qquad 0 \le \vartheta < -k + \sqrt{k^2+1}, \tag{S.8.2}$$

then, by (S.8.1),

$$h(\alpha) = \{\alpha\}^2 - \{\alpha^2\} = \vartheta^2 - \{\vartheta^2 + 2k\vartheta\} = \vartheta^2 - (\vartheta^2 + 2k\vartheta) = -2k\vartheta. \tag{S.8.3}$$

By (S.8.2), we have

$$0 \ge -2k\vartheta > -2k(-k + \sqrt{k^2+1}). \tag{S.8.4}$$

We see by (S.8.3) and (S.8.4) that $h(\alpha) = -2k\vartheta$ assumes all values in the interval

$$\big(-2k(-k + \sqrt{k^2+1})\,,\ 0\big].$$

Since

$$-2k(-k + \sqrt{k^2+1}) = \frac{-2k}{k + \sqrt{k^2+1}} = \frac{-2}{1 + \sqrt{1+k^{-2}}} \to -1, \quad \text{if} \quad k \to \infty,$$

the values $h(\alpha)$ cover the complete interval $(-1, 0]$.

If we replace condition (S.8.2) on ϑ by

$$2k \le \vartheta^2 + 2k\vartheta < 2k + 1, \qquad \text{i.e.} \quad -k + \sqrt{k^2+2k} \le \vartheta < 1$$

and repeat the above argument, then we get that every point in the interval $[0,1)$ appears in the range of $h(\alpha)$.

• **8.3.5** By formulas (8.3.8a), (8.3.8b), and (8.3.10) in Lemma 8.3.4,

$$r_n s_{n-2} - r_{n-2}s_n = (c_n r_{n-1} + r_{n-2})s_{n-2} - r_{n-2}(c_n s_{n-1} + s_{n-2}) = \\ = c_n(r_{n-1}s_{n-2} - r_{n-2}s_{n-1}) = (-1)^n c_n\,.$$

Dividing by $s_n s_{n-2}$, we get the statement of the exercise.

• **8.3.6** By the condition,

$$\alpha = C(c_0, c_1, \ldots, c_{M-k}, c_{M-k+1}, \ldots, c_M, c_{M-k+1}, \ldots, c_M, \ldots)\,.$$

Let

$$\beta = C(c_{M-k+1}, \ldots, c_M, c_{M-k+1}, \ldots, c_M, \ldots)\,.$$

Then

$$\alpha = C(c_0, c_1, \ldots, c_{M-k}, \beta) \qquad \text{and} \qquad \beta = C(c_{M-k+1}, \ldots, c_M, \beta)\,.$$

Condensing these multiple-decked fractions, we obtain

$$\alpha = \frac{u_1\beta + u_2}{u_3\beta + u_4} \qquad \text{and} \qquad \beta = \frac{u_5\beta + u_6}{u_7\beta + u_8}$$

with suitable integers u_i. We express β from the first equality with the help of α and substitute it into the second equality. This yields a quadratic equation with integer coefficients having α among its roots. (The continued fraction is infinite, so α is irrational, and cannot be a root of a linear equation with integer coefficients.)

• **8.4.1 (a)** Since $(1+\sqrt{2})^n + (1-\sqrt{2})^n$ is an integer and $\lim_{n\to\infty}(1-\sqrt{2})^n = 0$, the subsequences of $\{(1+\sqrt{2})^n\}$ for even and odd integers n, resp., tend to 1 and 0, resp. Thus the sequence cannot be dense in $[0,1]$.

• **(b)** The differences of two consecutive elements in the sequence tend to 0:

$$\sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1} + \sqrt{n}} \to 0 \quad \text{if} \quad n \to \infty\,.$$

Therefore, also the differences of the fractional parts of two consecutive elements tend to 0 except when the fractional part "jumps back" from nearly

1 to nearly 0. This implies that the fractional parts are everywhere dense in $[0,1]$.

• **(c)** Since

$$\{\sqrt{n^2+1}\} = \sqrt{n^2+1} - n = \frac{1}{\sqrt{n^2+1}+n} \to 0, \quad \text{if} \quad n \to \infty\,,$$

$\left\{\sqrt{n^2+1}\,\right\}$ cannot be dense in $[0,1]$.

• **(d)** Since

$$\sqrt{2n^2+1} - n\sqrt{2} \to 0, \quad \text{if} \quad n \to \infty\,,$$

and $\left\{n\sqrt{2}\,\right\}$ is everywhere dense in $[0,1]$ by Theorem 8.4.1, therefore also $\left\{\sqrt{2n^2+1}\,\right\}$ is everywhere dense in $[0,1]$.

• **(e)** The sine function is periodic, so the sequence assumes only finitely many (181) distinct values. Therefore the sequence of fractional parts cannot be dense in $[0,1]$.

• **(f)** As π, and so $1/(2\pi)$ are irrational, the angles n (measured in radian) are everywhere dense on the unit circle. The sine function is continuous, thus also the values $\sin n$ are everywhere dense in the range $[-1,1]$ of the sine function. Hence, the fractional parts are everywhere dense in $[0,1]$.

• **(g)** Since

$$\log_{10}(n+1) - \log_{10} n = \log_{10}\bigl(1+\frac{1}{n}\bigr) \to 0, \quad \text{if} \quad n \to \infty\,,$$

the sequence of fractional parts is everywhere dense in $[0,1]$, similar to the argument in part (b).

• **8.4.3** Assume that the points $P_n = (\{n\alpha_1\}, \{n\alpha_2\}, \ldots, \{n\alpha_k\})$ lie densely, i.e. we can find a P_n arbitrarily close to any point $(v_1, \ldots, v_k)$ of the k dimensional unit cube. In other words, to any $\varepsilon > 0$ there exists an n satisfying

$$|\{n\alpha_j\} - v_j| < \varepsilon, \qquad j = 1, 2, \ldots, k,$$

or equivalently,

$$|n\alpha_j - v_j - r_j| < \varepsilon, \qquad j = 1, 2, \ldots, k \tag{S.8.5}$$

with suitable integers r_j.

We have to show that $1, \alpha_1, \ldots, \alpha_k$ are linearly independent. For a proof by contradiction, assume

$$c_0 + c_1\alpha_1 + \ldots + c_k\alpha_k = 0 \tag{S.8.6}$$

for some rational numbers $c_0, \ldots, c_k$ not all zero. Multiplying (S.8.6) by the least common multiple of the denominators, we can achieve that the coefficients c_j in (S.8.6) should be integers.

The key step is that since the numbers $n\alpha_j - v_j - r_j$ are of "small" absolute value by (S.8.5), their linear combination by coefficients $c_1, \ldots, c_k$ extended with the term $0 = c_0(n \cdot 1 - n)$ has a small absolute value, too:

$$|c_0(n \cdot 1 - n) + \sum_{j=1}^{k} c_j(n\alpha_j - v_j - r_j)| < \varepsilon \sum_{j=1}^{k} |c_j| = \varepsilon'. \tag{S.8.7}$$

On the other hand, the left-hand side of (S.8.7) without the absolute value can be written as

$$n(c_0 + \sum_{j=1}^{k} c_j\alpha_j) - \sum_{j=1}^{k} c_j v_j - M \tag{S.8.8}$$

with some integer M. Combining (S.8.6), (S.8.7), and (S.8.8), we get

$$|\sum_{j=1}^{k} c_j v_j + M| < \varepsilon'.$$

Thus,

$$\{\sum_{j=1}^{k} c_j v_j\} < \varepsilon' \qquad \text{or} \qquad \{\sum_{j=1}^{k} c_j v_j\} > 1 - \varepsilon'.$$

This is clearly impossible for every $v_1, \ldots, v_k$, a contradiction.

9. Algebraic and Transcendental Numbers

• **9.2.8** By condition, $f \neq 0$, further, f has a root, so f cannot be a (non-zero) constant polynomial.

For a proof by contradiction, assume that f is irreducible over $\mathbf{Q}$. Then f is the minimal polynomial of its roots, i.e.

$$f = m_\alpha = m_\beta.$$

Since $g(\alpha) = 0$, we have $m_\alpha = f \mid g$. Then every root of f is a root of g, too, so $g(\beta) = 0$. This contradiction proves that f is reducible over $\mathbf{Q}$.

(The conditions give no information whether g is reducible or irreducible, both cases can occur.)

• **9.3.6** Assume that both r and $\cos\varphi$ are algebraic. Then $\sin\varphi = \pm\sqrt{1-\cos^2\varphi}$ and i are algebraic, too. We "assemble" α from r, $\cos\varphi$, $\sin\varphi$, and i using addition and multiplication, so α is algebraic, as well.

For the converse, assume that α is algebraic. By Theorem 9.3.3, both $r\cos\varphi$ and $r\sin\varphi$ are algebraic. Therefore $r = \sqrt{(r\cos\varphi)^2 + (r\sin\varphi)^2}$ is algebraic. So also $\cos\varphi = (r\cos\varphi)/r$ is algebraic.

• **9.4.1 (a)** (a1) Let $h = a/b$ with some integers $b > 0$ and a. As α is a Liouville number, to any n there exists a fraction r/s satisfying

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{2n}}\,. \tag{S.9.1}$$

As seen several times, the values s tend to infinity for $n \to \infty$, so we can assume $s > b$.

We can rewrite (S.9.1) as

$$\left|(h+\alpha) - \left(\frac{a}{b} + \frac{r}{s}\right)\right| < \frac{1}{s^{2n}}\,,$$

thus, using also $s > b$, we obtain

$$\left|(h+\alpha) - \frac{as+br}{bs}\right| < \frac{1}{s^{2n}} < \frac{1}{(bs)^n}\,.$$

This means that the fraction

$$\frac{R}{S} = \frac{as+br}{bs}$$

satisfies

$$\left|(h+\alpha) - \frac{R}{S}\right| < \frac{1}{S^n}\,,$$

so $h+\alpha$ is a Liouville number.

• (a2) We can handle $h\alpha$ similarly to $h+\alpha$ in (a1).

• (a3) We show that if r/s approximates α "well", then $(r/s)^k$ approximates α^k "almost so well". Consider the identity

$$\alpha^k - \Big(\frac{r}{s}\Big)^k = \Big(\alpha - \frac{r}{s}\Big)\Big(\alpha^{k-1} + \alpha^{k-2}\Big(\frac{r}{s}\Big) + \ldots + \Big(\frac{r}{s}\Big)^{k-1}\Big). \tag{S.9.2}$$

If r/s is close to α (in any sense), then the second factor on the right-hand side of (S.9.2) is close to $k\alpha^{k-1}$, so its absolute value is bounded by some constant c depending only on α and k. This implies that if

$$\Big|\alpha - \frac{r}{s}\Big| \;<\; \frac{1}{s^{kn}}\,, \tag{S.9.3}$$

then

$$\Big|\alpha^k - \frac{r^k}{s^k}\Big| \;<\; \frac{c}{(s^k)^n}\,. \tag{S.9.4}$$

As α is a Liouville number, we can achieve (S.9.3) and thus also (S.9.4) for an arbitrary n, i.e. α^k is a Liouville number, as well.

• (a4) We show that if r/s approximates α "well", then s/r approximates $1/\alpha$ "well". (If $r<0$, then we replace s/r by $(-s)/(-r)$.)

Using the form

$$|s\alpha - r| \;<\; \frac{1}{s^{2n-1}}$$

of inequality (S.9.1), we obtain

$$\Big|\frac{1}{\alpha} - \frac{s}{r}\Big| \;=\; \Big|\frac{r-s\alpha}{r\alpha}\Big| \;<\; \frac{1}{s^{2n-1}|r\alpha|} \tag{S.9.5}$$

(we may clearly assume $r\neq 0$). If $n\to\infty$, then the values s tend to infinity and the fractions r/s tend to α, so we may assume

$$\Big|\frac{r}{s}\Big| \;<\; |\alpha|+1 \;<\; s \qquad \text{and} \qquad s|\alpha| \geq 1. \tag{S.9.6}$$

Combining (S.9.5) and (S.9.6), we get

$$\Big|\frac{1}{\alpha} - \frac{s}{r}\Big| \;<\; \frac{1}{|r|^n}\,. \tag{S.9.7}$$

Since α is a Liouville number, we can achieve (S.9.1), and thus also (S.9.7) for an arbitrary n, i.e. $1/\alpha$ is a Liouville number, as well.

• **9.4.4** Assume that a complex number α is a multiple root of an irreducible polynomial f. Then α is a root of the derivative f' of f, too. Due to irreducibility, f is a minimal polynomial of α. Therefore $f'(\alpha) = 0$ implies $f \mid f'$. This is impossible, however, as ($f' \neq 0$ and) $\deg f' < \deg f$.

• **9.6.5 (a)** True. For a proof by contradiction, assume that all complex roots of f are algebraic integers, i.e.

$$f = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

where every α_j is an algebraic integer. Performing the multiplication, we obtain the coefficients of f from the numbers α_j via addition, subtraction, and multiplication. The algebraic integers form a ring, so every coefficient of f is an algebraic integer. The coefficients are rational numbers, too, so they must be integers, which contradicts the condition on f.

• **(b)** False. E.g.

$$f = (x^2 - 6)(x^2 - \frac{1}{2}) = x^4 - \frac{13}{2}x^2 + 3$$

is a polynomial with rational coefficients which are not all integers and the leading coefficient is 1. Still, f has the algebraic integers $\pm\sqrt{6}$ among its roots.

• **(c)** True. Since f is irreducible over $\mathbf{Q}$, it is a minimal polynomial of each of its roots. By Definition 9.6.1, none of the roots can be an algebraic integer.

• **(d)** True. Let α be the only not algebraic integer root of f. Since $f(\alpha) = 0$, we have $m_\alpha \mid f$, and so every root of m_α is a root of f, too. No root of m_α is an algebraic integer, further, m_α cannot have multiple roots (by Exercise 9.4.4), thus m_α must have degree 1. This means that α is rational, so f has a rational root, indeed.

Solutions, Chapters 10–12

10. Algebraic Number Fields

• **10.2.5 (a)** Let $\alpha = \sqrt{7} + 3i$ and $M = \mathbf{Q}(\alpha)$, then $\deg \alpha = \deg(M : \mathbf{Q})$.

Consider the chain of extensions

$$\mathbf{Q} \subseteq K \subseteq L, \qquad \text{where} \qquad K = \mathbf{Q}(\sqrt{7}) \qquad \text{and} \qquad L = K(i). \tag{S.10.1}$$

We prove $M = L$, and then compute $\deg(L : \mathbf{Q}) = \deg \alpha$.

By definition, $\sqrt{7} \in L$ and $3i \in L$, further, L is a field, so $\alpha = \sqrt{7}+3i \in L$, hence $M \subseteq L$.

To verify the other containment $L \subseteq M$, we have to demonstrate $\sqrt{7} \in M$ and $3i \in M$. Since

$$(\sqrt{7} - 3i)(\sqrt{7} + 3i) = 16, \qquad \text{i.e.} \qquad \overline{\alpha} = \frac{16}{\alpha}\,,$$

so $\overline{\alpha} \in M$, thus

$$\sqrt{7} = \operatorname{Re} \alpha = \frac{\alpha + \overline{\alpha}}{2} \in M \qquad \text{and} \qquad 3i = \frac{\alpha - \overline{\alpha}}{2} \in M.$$

To compute $\deg(L : \mathbf{Q})$, we show that both links have degree 2 in (S.10.1). Clearly, $\deg(K : \mathbf{Q}) = \deg \sqrt{7} = 2$. Since $L \neq K$ (because K has only real elements, whereas $i \in L$), therefore $\deg(L : K) \geq 2$. On the other hand, $\deg(L : K) = \deg_K i \leq \deg i = 2$, so $\deg(L : K) = 2$, indeed.

Applying the tower theorem, we obtain

$$\deg \alpha = \deg(L : \mathbf{Q}) = \deg(K : \mathbf{Q}) \cdot \deg(L : K) = 4.$$

• **10.2.7** Let V denote the set of real numbers in $\mathbf{Q}(\vartheta)$, i.e. $V = \mathbf{Q}(\vartheta) \cap \mathbf{R}$.

• **(a)** As $\vartheta = \sqrt[5]{3}(\cos 144^\circ + i \sin 144^\circ)$ is a root of the polynomial $x^5 - 3$ irreducible over $\mathbf{Q}$, the degree of $\mathbf{Q}(\vartheta)$ is 5.

Consider the chain $\mathbf{Q} \subseteq V \subseteq \mathbf{Q}(\vartheta)$. By the tower theorem,

$$5 = \deg(\mathbf{Q}(\vartheta) : \mathbf{Q}) = \deg(\mathbf{Q}(\vartheta) : V) \cdot \deg(V : \mathbf{Q}),$$

so $\deg(\mathbf{Q}(\vartheta) : V) = 1$ or 5. Since V consists purely of real numbers, but $\mathbf{Q}(\vartheta)$ contains non-real complex numbers, too, therefore $\mathbf{Q}(\vartheta) \neq V$. This

implies $\deg(\mathbf{Q}(\vartheta) : V) \neq 1$, i.e. only $\deg(\mathbf{Q}(\vartheta) : V) = 5$ is possible. Then $\deg(V : \mathbf{Q}) = 1$, so $V = \mathbf{Q}$.

• **(b)** We prove $V = \mathbf{Q}(\sqrt[3]{3})$.

As $\sqrt[3]{3}$ is a real number and

$$\sqrt[3]{3} = -\left(i\sqrt[6]{3}\right)^2 = -\vartheta^2 \in \mathbf{Q}(\vartheta),$$

therefore $\mathbf{Q}(\sqrt[3]{3}) \subseteq V$.

Consider now the chain

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{3}) \subseteq V \subseteq \mathbf{Q}(\vartheta). \tag{S.10.2}$$

Since $\vartheta = i\sqrt[6]{3}$ is a root of the polynomial x^6+3 irreducible over $\mathbf{Q}$, hence $\deg(\mathbf{Q}(\vartheta) : \mathbf{Q}) = 6$.

We get similarly $\deg(\mathbf{Q}(\sqrt[3]{3}) : \mathbf{Q}) = 3$.

Applying the tower theorem for the chain (S.10.2), we obtain

$$2 = \deg(\mathbf{Q}(\vartheta) : \mathbf{Q}(\sqrt[3]{3})) = \deg(\mathbf{Q}(\vartheta) : V) \cdot \deg(V : \mathbf{Q}(\sqrt[3]{3})).$$

Similarly to part (a), $\mathbf{Q}(\vartheta) \neq \mathbf{Q}(\sqrt[3]{3})$, so

$$\deg(V : \mathbf{Q}(\sqrt[3]{3})) = 1, \qquad \text{i.e.} \qquad V = \mathbf{Q}(\sqrt[3]{3}).$$

• **(c)** Since the two values of $\sqrt{i}$ are negatives of each other, we get the same extension for each value. We choose e.g.

$$\vartheta = \sqrt{i} = \frac{1+i}{\sqrt{2}}. \tag{S.10.3}$$

We prove $V = \mathbf{Q}(\sqrt{2})$.

First solution: Since

$$i = (\sqrt{i})^2 = \vartheta^2 \in \mathbf{Q}(\vartheta)\,,$$

(S.10.3) implies

$$\sqrt{2} \in \mathbf{Q}(\vartheta), \qquad \text{so} \qquad \mathbf{Q}(\sqrt{2}) \subseteq V.$$

Consider the chain

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq V \subseteq \mathbf{Q}(\vartheta).$$

Similar to the previous arguments, we obtain

$$\deg(\mathbf{Q}(\vartheta):\mathbf{Q})=4, \qquad \deg(\mathbf{Q}(\sqrt{2}):\mathbf{Q})=2, \qquad \text{and} \qquad V\neq\mathbf{Q}(\vartheta).$$

By the tower theorem,

$$\deg(V:\mathbf{Q}(\sqrt{2}))=1, \qquad \text{i.e.} \qquad V=\mathbf{Q}(\sqrt{2}).$$

Second solution: By Theorem 10.2.3, the elements of $\mathbf{Q}(\vartheta)$ have a unique representation

$$\text{(S.10.4)}\quad \alpha=a_0+a_1\sqrt{i}+a_2(\sqrt{i})^2+a_3(\sqrt{i})^3=a_0+a_1\frac{1+i}{\sqrt{2}}+a_2 i+a_3\frac{-1+i}{\sqrt{2}}$$

with rational numbers a_i.

Here α is a real number if and only if its imaginary part is 0, i.e.

$$\frac{a_1+a_3}{\sqrt{2}}+a_2=0.$$

Since $\sqrt{2}$ is irrational, this holds if and only if

$$a_3=-a_1 \qquad \text{and} \qquad a_2=0.$$

Substituting back into (S.10.4), we obtain that α is a real number if and only if

$$\alpha=a_0+a_1\sqrt{2}, \qquad \text{i.e.} \qquad \alpha\in\mathbf{Q}(\sqrt{2}).$$

Herewith we have proved $V=\mathbf{Q}(\sqrt{2})$.

Third solution: The statement follows also from Exercise 10.2.8.

• **10.2.8** Since $|\vartheta|=1$, we have $\overline{\vartheta}=1/\vartheta$, so

$$\text{(S.10.5)}\qquad \operatorname{Re}\vartheta=\frac{\vartheta+\overline{\vartheta}}{2}=\frac{1}{2}\big(\vartheta+\frac{1}{\vartheta}\big)\,.$$

This implies $\operatorname{Re}\vartheta\in\mathbf{Q}(\vartheta)$, thus $\mathbf{Q}(\operatorname{Re}\vartheta)\subseteq\mathbf{Q}(\vartheta)$. Obviously, $\mathbf{Q}(\operatorname{Re}\vartheta)\subseteq\mathbf{R}$, hence

$$\text{(S.10.6)}\qquad \mathbf{Q}(\operatorname{Re}\vartheta)\subseteq\mathbf{Q}(\vartheta)\cap\mathbf{R}.$$

For the opposite containment, let c be an arbitrary real element in $\mathbf{Q}(\vartheta)$, i.e. $c = g(\vartheta)/h(\vartheta)$ (where $g,\, h \in \mathbf{Q}[x]$, $h(\vartheta) \neq 0$). Then

$$h(\vartheta)c = g(\vartheta). \tag{S.10.7}$$

Conjugating (S.10.7) and using $c \in \mathbf{R}$,

$$h(\overline{\vartheta})c = g(\overline{\vartheta}). \tag{S.10.8}$$

We assume temporarily $h(\vartheta) + h(\overline{\vartheta}) \neq 0$. Adding (S.10.7) and (S.10.8) and expressing c, we obtain

$$c \;=\; \frac{g(\vartheta) + g(\overline{\vartheta})}{h(\vartheta) + h(\overline{\vartheta})} \;=\; \frac{g(\vartheta) + g(1/\vartheta)}{h(\vartheta) + h(1/\vartheta)}\,. \tag{S.10.9}$$

It can be easily shown by induction that $\vartheta^k + \vartheta^{-k}$ can be expressed as a polynomial of $\vartheta + (1/\vartheta) = 2\mathrm{Re}\,\vartheta$ with rational coefficients. So (S.10.9) implies $c \in \mathbf{Q}(\mathrm{Re}\,\vartheta)$. This proves

$$\mathbf{Q}(\vartheta) \cap \mathbf{R} \subseteq \mathbf{Q}(\mathrm{Re}\,\vartheta).$$

We still have to handle the case

$$h(\vartheta) + h(\overline{\vartheta}) = h(\vartheta) + h(1/\vartheta) = 0. \tag{S.10.10}$$

It follows that ϑ is an algebraic number. The next argument works for any algebraic number ϑ on the unit circle, independently of the validity of (S.10.10).

Relying on (S.10.6), consider the chain

$$\mathbf{Q}(\mathrm{Re}\,\vartheta) \subseteq \mathbf{Q}(\vartheta) \cap \mathbf{R} \subseteq \mathbf{Q}(\vartheta). \tag{S.10.11}$$

The statement is obvious for $\vartheta = \pm 1$, so we may assume that ϑ is not a real number. We show that in (S.10.11), both the entire chain and the second link have degree 2, so by the tower theorem the first link has degree 1 which proves that the two extensions coincide.

Since the first two fields of the chain (S.10.11) consist purely of real numbers, whereas the third field contains non-real numbers too, therefore both the second link and the entire chain must have at least degree 2. Hence, it suffices to prove that the entire chain has degree (at most) 2.

By condition $|\vartheta| = 1$, we have $\mathrm{Im}\,\vartheta = \pm\sqrt{1 - (\mathrm{Re}\,\vartheta)^2}$, so

$$\vartheta = \mathrm{Re}\,\vartheta + i\mathrm{Im}\,\vartheta = \mathrm{Re}\,\vartheta + \sqrt{(\mathrm{Re}\,\vartheta)^2 - 1}$$

has degree (exactly) 2 over $\mathbf{Q}(\operatorname{Re}\vartheta)$ (as $\operatorname{Im}\vartheta \neq 0$). So $\deg\big(\mathbf{Q}(\vartheta) : \mathbf{Q}(\operatorname{Re}\vartheta)\big) = 2$, indeed.

• **10.2.11** We show that there are no algebraic numbers of odd degree on the unit circle except ± 1.

• *First proof*: During the solution of Exercise 10.2.8 we proved that if ϑ is an algebraic number and $|\vartheta| = 1$, then

$$\mathbf{Q}(\operatorname{Re}\vartheta) \subseteq \mathbf{Q}(\vartheta),$$

and the degree of this extension is 2 for $\vartheta \neq \pm 1$.

This means that the second link in the chain

$$\mathbf{Q} \subseteq \mathbf{Q}(\operatorname{Re}\vartheta) \subseteq \mathbf{Q}(\vartheta)$$

has degree 2, so

$$\deg\vartheta = \deg(\mathbf{Q}(\vartheta) : \mathbf{Q}) \text{ is even}$$

by the tower theorem.

• *Second proof*: A complex number and its conjugate are roots with the same multiplicity of a polynomial with real coefficients. Thus, if $|\vartheta| = 1$, then also $1/\vartheta = \overline{\vartheta}$ is a root of the minimal polynomial of ϑ. As m_ϑ is irreducible, this implies

$$m_\vartheta = m_{1/\vartheta}. \tag{S.10.12}$$

We can easily deduce (see e.g. the hint to Exercise 9.1.2c) that if a minimal polynomial of ϑ is

$$m_\vartheta = a_0 + a_1 x + \ldots + a_n x^n \qquad (a_n \neq 0), \tag{S.10.13a}$$

then a minimal polynomial of $1/\vartheta$ is

$$m_{1/\vartheta} = a_n + a_{n-1} x + \ldots + a_0 x^n \qquad (a_0 \neq 0). \tag{S.10.13b}$$

Condition (S.10.12) implies that we get the polynomial in (S.10.13b) by multiplying the polynomial in (S.10.13a) by a rational constant c. Comparing the constant terms and leading coefficients, we obtain

$$a_n = c a_0 \qquad \text{and} \qquad a_0 = c a_n\,,$$

so $c = \pm 1$. Comparing now the other coefficients, either

$$a_j = a_{n-j}, \qquad j = 0, 1, \dots, n,$$

or

$$a_j = -a_{n-j}, \qquad j = 0, 1, \dots, n.$$

If $\deg \vartheta = n$ is odd, then in the first case,

$$m_\vartheta(-1) = \sum_{j=0}^{n} a_j(-1)^j = \sum_{j=0}^{(n-1)/2} a_j\big((-1)^j + (-1)^{n-j}\big) = 0,$$

and in the second case,

$$m_\vartheta(1) = \sum_{j=0}^{n} a_j = \sum_{j=0}^{(n-1)/2} \big(a_j + a_{n-j}\big) = 0.$$

This means that the rational number -1 or 1 is a root of m_ϑ. Since m_ϑ is irreducible over $\mathbf{Q}$, this can happen only if $\vartheta = -1$ or 1.

• **10.3.5** If t is a squarefree composite number, then it has a prime divisor $p > 2$.

Assume that the Fundamental Theorem still holds in $I(\sqrt{t})$. Then p is reducible in $I(\sqrt{t})$ by Theorem 10.3.8/(vii). Thus, $N(\alpha) = a^2 + |t|b^2 = p$ for some $\alpha = a + b\sqrt{t}$ where both a and b are integers or fractions with denominator 2. Hence, $u = 2a$ and $v = 2b$ are integers and

$$u^2 + |t|v^2 = 4p. \tag{S.10.14}$$

If $v = 0$, then $u^2 = 4p$, which is impossible.

Let $|t| = kp$. Since $k \geq 2$, the left-hand side of (S.10.14) is bigger than the right-hand side if $|v| \geq 2$.

Finally, if $|v| = 1$, then $u^2 = (4 - k)p$. This cannot hold for $k = 2, 3$, and $k \geq 5$, further $k \neq 4$ as t is squarefree.

Herewith we have shown that (S.10.14) is false which is a contradiction.

• **10.3.6** We follow the hint.

Let $t = -4k + 1$ and $\alpha_n = n + (1 + \sqrt{t})/2$. Then

(S.10.15)

$$N(\alpha_n) = N\Big(n + \frac{1 + \sqrt{t}}{2}\Big) = \Big(n + \frac{1 + \sqrt{t}}{2}\Big)\Big(n + \frac{1 - \sqrt{t}}{2}\Big) = n^2 + n + k\,.$$

We show that α_n is irreducible for $0 \le n \le k-2$. Assume that still $\alpha_n = \beta\gamma$ (for some n), where neither β, nor γ is a unit. Since α_n cannot be divisible by any integer different from ± 1,

$$\beta = b_0 + b_1\frac{1+\sqrt{t}}{2}, \quad \gamma = c_0 + c_1\frac{1+\sqrt{t}}{2}, \quad \text{where} \quad b_j, c_j \in \mathbf{Z} \quad \text{and} \quad b_1 c_1 \neq 0.$$

This implies

$$N(\beta) = b_0^2 + b_0 b_1 + b_1^2 k = \Big(b_0 + \frac{b_1}{2}\Big)^2 + b_1^2\Big(k - \frac{1}{4}\Big) \ge k,$$

and $N(\gamma) \ge k$ similarly. Then, however,

$$k^2 \le N(\beta)N(\gamma) = N(\alpha_n) < N(\alpha_{k-1}) = (k-1)^2 + (k-1) + k = k^2\,,$$

a contradiction.

Herewith we have proved that α_n is irreducible for $0 \le n \le k-2$. Then also $\overline{\alpha_n}$ is irreducible.

Assume now that $f(n)$ is not a prime number for some $0 \le n \le k-2$, i.e.

$$N(\alpha_n) = n^2 + n + k = rs, \qquad \text{where} \qquad r,\, s > 1. \tag{S.10.16}$$

Combining (S.10.15) and (S.10.16), we obtain

$$\Big(n + \frac{1+\sqrt{t}}{2}\Big)\Big(n + \frac{1-\sqrt{t}}{2}\Big) = rs. \tag{S.10.17}$$

The left-hand side of (S.10.17) is the product of two irreducible numbers. By the Fundamental Theorem, also the two non-unit factors on the right-hand side must be irreducible, moreover, they are associates of the factors on the left-hand side. But this is impossible since an integer $r \neq \pm 1$ cannot divide α_n or $\overline{\alpha_n}$.

• **10.3.9 (e)** Following the hint, we shall verify that if $p \equiv 1$ or $9 \pmod{20}$, then

$$p = a^2 + 5b^2 = (a + b\sqrt{-5})(a - b\sqrt{-5})$$

for some integers a and b. We give two different proofs. Both use that $\left(\frac{-5}{p}\right) = 1$ implies $p \mid c^2 + 5$ for some integer c.

• *First proof*: We proceed along the ideas seen at Theorem 8.2.4. Consider the points on the plane with coordinates $x = pu + cv$, $y = v$ where u and

v assume all integers independently. These points form a lattice where the fundamental parallelogram has area $\Delta = p$.

Every lattice point satisfies

$$x^2 + 5y^2 = (pu + cv)^2 + 5v^2 = p(pu^2 + 2cuv) + v^2(c^2 + 5) \equiv 0 \pmod{p},$$

i.e. $p \mid x^2 + 5y^2$.

We apply Minkowski's theorem for the closed ellipse $x^2 + 5y^2 \le 4\sqrt{5}p/\pi$ around the origin having area $4p = 4\Delta$. Thus, there is a lattice point (x, y) in the ellipse different from the origin satisfying

$$p \mid x^2 + 5y^2 \qquad \text{and} \qquad x^2 + 5y^2 \le \frac{4\sqrt{5}p}{\pi} < 3p,$$

so $x^2 + 5y^2 = p$ or $2p$.

But $x^2 + 5y^2 = 2p$ cannot hold since mod 5 the left-hand side is congruent to 0 or ± 1, and the right-hand side is congruent to ± 2 as $p \equiv \pm 1 \pmod 5$. Thus, necessarily $x^2 + 5y^2 = p$.

• *Second proof*: Let $p \mid c^2 + 5$. Then the congruence $cy \equiv x \pmod p$ has a solution x and y, where $0 < |x|, |y| < \sqrt{p}$. This follows from Thue's lemma in Exercise 7.5.21a with $k = 1$, $u = v = \lceil \sqrt{p} \rceil$, and $C = c$.

So

$$x^2 + 5y^2 \equiv c^2y^2 + 5y^2 = (c^2 + 5)y^2 \equiv 0 \pmod{p} \qquad \text{and} \qquad x^2 + 5y^2 < 6p\,.$$

We show $a^2 + 5b^2 = p$ for some integers a and b.

If $x^2 + 5y^2 = 5p$, then $5 \mid x$, i.e. $x = 5z$, and so $25z^2 + 5y^2 = 5p$ yields $5z^2 + y^2 = p$.

If $x^2 + 5y^2 = 4p$, then a check modulo 4 shows that both x and y are even, $x = 2a$, $y = 2b$, and so $4a^2 + 20b^2 = 4p$ yields $a^2 + 5b^2 = p$.

Equalities $x^2 + 5y^2 = 3p$ or $2p$ are impossible mod 5.

Finally, $x^2 + 5y^2 = p$ is just the desired claim.

• **10.5.6** We consider a general quadratic field $\mathbf{Q}(\sqrt{t})$ where $t \ne 1$ is a square-free integer. We prove that $\mathbf{Q}(\sqrt{t})$ possesses an integral basis with the desired property if and only if $t \equiv 1 \pmod 4$.

Sufficiency: If $t \equiv 1 \pmod 4$, then we can choose

$$\omega_1 = \frac{1 + \sqrt{t}}{2} \qquad \text{and} \qquad \omega_2 = \frac{1 - \sqrt{t}}{2}\,.$$

We have to show that

(i) every $\alpha \in \mathbf{Q}(\sqrt{t})$ has a unique representation

$$\alpha = c_1\omega_1 + c_2\omega_2 \tag{S.10.18}$$

with rational numbers c_j;

(ii) α is an algebraic integer if and only if both c_1 and c_2 are integers;

(iii) ω_1 and ω_2 share the same minimal polynomial.

(i) We know that α has a unique representation

$$\alpha = a + b\sqrt{t}, \tag{S.10.19}$$

where a and b are rational numbers. Comparing (S.10.18) and (S.10.19), we obtain

$$a + b\sqrt{t} = c_1\frac{1+\sqrt{t}}{2} + c_2\frac{1-\sqrt{t}}{2} = \frac{c_1+c_2}{2} + \frac{c_1-c_2}{2}\sqrt{t}\,.$$

Hence, (S.10.18) holds if and only if

$$a = \frac{c_1+c_2}{2} \qquad \text{and} \qquad b = \frac{c_1-c_2}{2}\,, \tag{S.10.20a}$$

i.e.

$$c_1 = a + b \qquad \text{and} \qquad c_2 = a - b. \tag{S.10.20b}$$

This proves the existence and uniqueness of suitable rational numbers c_1 and c_2.

(ii) By Theorem 10.3.2, α is an algebraic integer for $t \equiv 1 \pmod 4$ if and only if

$$a = \frac{u}{2}\,, \quad b = \frac{v}{2}\,, \quad \text{where} \quad u,\, v \in \mathbf{Z} \quad \text{and} \quad u \equiv v \pmod 2. \tag{S.10.21}$$

We have to show that (S.10.21) is equivalent to c_1 and c_2 being integers.

If a and b satisfy (S.10.21), then (S.10.20b) implies that

$$c_1 = \frac{u+v}{2} \qquad \text{and} \qquad c_2 = \frac{u-v}{2}$$

are integers.

Conversely, if c_1 and c_2 are integers, then $u = c_1 + c_2$ and $v = c_1 - c_2$ have the same parity, and so, by (S.10.20a), a and b satisfy (S.10.21).

(iii) The common minimal polynomial of the two numbers is

$$(x - \omega_1)(x - \omega_2) = x^2 - x + \frac{1 - t}{4}\,.$$

Necessity: Assume that $t \not\equiv 1 \pmod 4$, but still there exists an integral basis ω_1, ω_2 with the given property.

As ω_1 and ω_2 are conjugates over $\mathbf{Q}$, so

$$\omega_1 = r + s\sqrt{t} \qquad \text{and} \qquad \omega_2 = r - s\sqrt{t}, \qquad r,\, s \in \mathbf{Q}.$$

Since ω_1 and ω_2 are algebraic integers and $t \not\equiv 1 \pmod 4$, so (by Theorem 10.3.2) r and s are integers, further, $s \neq 0$, since ω_1 and ω_2 are linearly independent.

As 1 is an algebraic integer, so

$$1 = c_1\omega_1 + c_2\omega_2 = (c_1 + c_2)r + (c_1 - c_2)s\sqrt{t}$$

with suitable integers c_1 and c_2. This holds if and only if

$$(c_1 + c_2)r = 1 \qquad \text{and} \qquad (c_1 - c_2)s = 0.$$

As $s \neq 0$, we obtain $c_1 = c_2$, and so $1 = (c_1 + c_2)r = 2c_1 r$, which is impossible for integers c_1 and r.

11. Ideals

• **11.1.8 (a)** We show first that a1 and a3 are not fields as both contain zero divisors.

Let $I = (x^2 - 2)$. In the factor ring $\mathbf{R}[x]/I$, the product of two (non-zero) residue classes represented by polynomials $x + \sqrt{2}$ and $x - \sqrt{2}$ is the zero residue class:

$$\big[x + \sqrt{2} + I\,\big]\big[x - \sqrt{2} + I\,\big] = \big[x + \sqrt{2}\,\big]\big[x - \sqrt{2}\,\big] + I = x^2 - 2 + I = 0 + I\,.$$

This means that $x + \sqrt{2} + I$ and $x - \sqrt{2} + I$ are zero divisors in $\mathbf{R}[x]/I$, so $\mathbf{R}[x]/I$ cannot be a field.

The situation is similar in the factor ring $\mathbf{C}[x]/(x^2+1)$: here the product of (non-zero) residue classes represented $x+i$ and $x-i$ is zero.

Turning to a2, we prove that the factor ring $\mathbf{R}[x]/(x^2+1)$ is isomorphic to the complex field.

We adapt the arguments used in the Example after Theorem 11.1.6. Those polynomials (with real coefficients) fall into the same residue class modulo the principal ideal (x^2+1) which give the same remainder in the division algorithm by x^2+1. Thus, every residue class can be uniquely characterized by its "remainder", i.e. by a polynomial $a+bx$ (with real coefficients) of degree at most 1 (including the 0 polynomial representing the ideal itself).

We perform the operations in the factor ring with these remainders, e.g. multiplying two residue classes we multiply the remainders and take the remainder of the product upon division by x^2+1. Accordingly, the rules for addition and multiplication are

$$[a+bx]+[c+dx]=[a+c]+[b+d]x$$

and

$$\begin{aligned}[a+bx][c+dx] &= ac+[ad+bc]x+bdx^2 = \\ &= ac+[ad+bc]x-bd+bd[x^2+1]=[ac-bd]+[ad+bc]x.\end{aligned}$$

These are exactly the same rules as we add and multiply complex numbers (just replace letter x by letter i).

Herewith we have proved that the factor ring $\mathbf{R}[x]/(x^2+1)$ is a field isomorphic to $\mathbf{C}$.

• **(b)** We prove that the factor ring $R=F[x]/(g)$ is a field if and only if g is irreducible over F.

Necessity: Assume that g is not irreducible over F. Then $g=0$, or g is a unit, or g is reducible over F. We show that R is not a field in these cases.

If g is a unit, then $(g)=(1)=F[x]$, so R has just one element, and if $g=0$, then $(g)=(0)$, so R can be identified with $F[x]$. Hence R is not a field, obviously.

If g is reducible, i.e. $g=ht$ for some non-constant polynomials h and t, then the product of residue classes in R represented by polynomials h and t is residue class zero:

$$[h+(g)][t+(g)]=ht+(g)=g+(g)=0+(g)\,.$$

On the other hand, none of $h+(g)$ and $t+(g)$ is the zero residue class, as $g\nmid h$ and $g\nmid t$.

This means that if g is reducible, then R contains zero divisors, so it cannot be a field.

Sufficiency: We have to show that if g is irreducible over F, then the factor ring $R = F[x]/(g)$ is a field.

The ring R is commutative and the residue class $1 + (g)$ is an identity element (for multiplication). We have to show that every non-zero element has a multiplicative inverse.

We argue similarly as in part I. of the proof of Theorem 10.2.3.

Let $u + (g)$ be an arbitrary non-zero residue class, i.e. $g \nmid u$. A residue class $v + (g)$ is the inverse of $u + (g)$ if and only if

$$[u + (g)][v + (g)] = uv + (g) = 1 + (g)\,, \qquad \text{i.e.} \qquad g \mid 1 - uv.$$

This means

$$1 = uv + gw \tag{S.11.1}$$

for some polynomial $w \in F[x]$. In equation (S.11.1), u and g are given, and we want to find a suitable v and w. Thus, we reformulated the question of invertibility as the solvability of a "Diophantine" equation for polynomials.

As explained in the proof of Theorem 10.2.3, equation (1) is solvable (analogously to Theorem 1.3.6 about integers) if and only if the greatest common divisor of u and g divides 1, i.e. u and g are coprime. Since g is irreducible and $g \nmid u$, this holds, indeed.

• **(c)** To represent the residue classes modulo the ideal $I = (2, x^2 + x + 1)$, we take the remainders of polynomials upon division by both generators. (As $g = x^2 + x + 1$ has leading coefficient 1, we can apply the division algorithm for dividing any polynomial with integer coefficients by g.)

Accordingly, every residue class has a representative of degree at most 1 (including the 0 polynomial) and with coefficients 0 or 1. Thus, we have the four polynomials

$$0, \qquad 1, \qquad x, \qquad 1 + x.$$

We can easily check that no two of these fall into the same residue class (i.e. the ideal I contains no difference of two of them).

This means that the factor ring $R = \mathbf{Z}[x]/(2, x^2+x+1)$ has four elements which can be represented by the above four polynomials.

The ring R is commutative and the residue class $1 + I$ is an identity. The inverse of the identity is itself, and the other two non-zero elements are inverses of each other:

$$[x + I][1 + x + I] = x[1 + x] + I = 1 + [x^2 + x + 1 - 2] + I = 1 + I,$$

as $x^2 + x + 1 - 2 \in I$.

This proves that R is a field.

We sketched another possible proof in the hint to this exercise.

• **11.3.5** If R is a field, then $R[x]$ is a Euclidean ring (with a division algorithm with respect to the degree), so it is also a principal ideal domain by Theorem 11.3.5.

For the converse, assume that $R[x]$ is a principal ideal domain. We have to show that R is a field, i.e. every $a \neq 0$ has an inverse.

Consider in $R[x]$ the ideal $I = (a, x)$ generated by x and the non-zero constant polynomial a. By the condition, I is a principal ideal, i.e. $I = (g)$ for some polynomial $g \in R[x]$.

Since $x \in (a, x) = (g)$, therefore $g \mid x$. So $g = \varepsilon$ or $g = \varepsilon x$, where ε is a unit (i.e. a constant polynomial which has an inverse in $R[x]$, or equivalently, ε as an element in R has an inverse in R). Condition $g \mid a$ implies $g \neq \varepsilon x$, hence necessarily $g = \varepsilon$. Then $(g) = (1)$.

Since $(a, x) = (1)$, we have $1 = ah + xt$ with suitable polynomials h, $t \in R[x]$. It follows that the product of a and the constant term of h is 1, so a has an inverse, indeed.

• **11.3.9 (a)** By the hint to Exercise 11.1.10b, it follows that every ideal in R is finitely generated.

If $(a, b) = (d)$, then $(a, b, c) = (d, c)$. Thus, it suffices to prove that any ideal (a, b) generated by two elements is a principal ideal.

If one of the generators is 0, then the statement is obvious. So we may assume that none of a and b is 0.

The Fundamental Theorem of Arithmetic implies the existence of $d = \gcd\{a, b\}$. By Theorem 11.2.2/(iii), $(a, b) = (d)$ if and only if $d = \gcd\{a, b\}$ and $d = au + bv$ for some u, $v \in R$. Dividing by d, we obtain

$$1 = a_1 u + b_1 v, \qquad \gcd\{a_1, b_1\} = 1.$$

Hence, we have to show that 1 and $a_1 u$ fall into the same residue class modulo (b_1) for some u.

Pick an element in each of the finitely many residue classes mod (b_1) (i.e. form a complete residue system modulo b_1), let these be $r_1, \ldots, r_n$. We show that also $a_1 r_1, \ldots, a_1 r_n$ is a complete residue system modulo b_1.

If $a_1 r_i$ and $a_1 r_j$ fall into the same residue class modulo (b_1), then $a_1 r_i - a_1 r_j \in (b_1)$, so $b_1 \mid a_1(r_i - r_j)$. As a_1 and b_1 are coprime, the Fundamental of Arithmetic implies $b_1 \mid r_i - r_j$. Therefore, $r_i - r_j \in (b_1)$, so $i = j$.

Herewith we have proved that $a_1r_1, \dots, a_1r_n$ fall into disjoint residue classes, so they represent every class, indeed. In particular, also a_1r_i falls into the same class as 1 for some i, as claimed.

• **11.3.10** We have a division algorithm with respect to the norm in $I(\sqrt{t})$ for the given five values of t, as sketched in the hint to Exercise 10.3.4.

For the converse, assume that $I(\sqrt{t})$ is a Euclidean ring. We may obviously restrict ourselves to $t < -3$, then the only units are ± 1 in $I(\sqrt{t})$.

Let β be an element different from 0 and the units ± 1 for which $f(\beta)$ is minimal (apart from the values $f(0) = 0$ and $f(\pm 1)$).

The definition of β implies that applying the division algorithm for any $\xi \in I(\sqrt{t})$ and β, the remainder can be only 0 or ± 1. In other words, ξ, $\xi + 1$, or $\xi - 1$ is a multiple of β for any ξ.

In particular, for $\xi = 2$ we obtain $\beta \mid 2$, or $\beta \mid 3$, or $\beta \mid 1$. The last case cannot occur as $\beta \neq \pm 1$.

If $\beta \mid 2$, then $N(\beta) \mid N(2) = 4$, i.e. $N(\beta) = 2$ or $N(\beta) = 4$ [since $N(\beta) \neq 1$]. We show that necessarily $N(\beta) = 2$.

Condition $N(\beta) = 4$ (combined with $\beta \mid 2$) implies that β is an associate of 2. To exclude this possibility, it is enough to exhibit a single ξ such that 2 divides none of ξ, $\xi + 1$, and $\xi - 1$.

If $t \not\equiv 1 \pmod 4$, then $\xi = \sqrt{t}$, and if $t \equiv 1 \pmod 4$, then $\xi = (1 + \sqrt{t})/2$ clearly suits. (We used Theorem 10.3.2 about the representation of elements in $I(\sqrt{t})$.)

This proves that $\beta \mid 2$ implies $N(\beta) = 2$. We get similarly that $\beta \mid 3$ implies $N(\beta) = 3$.

Consider first $t \not\equiv 1 \pmod 4$. Then $\beta = c + d\sqrt{t}$, where c and d are integers. As $N(\beta)$ is not a square, $d \neq 0$, and so

$$3 \geq N(\beta) = c^2 + |t| \cdot d^2 \geq 0 + |t| \cdot 1 = |t|, \qquad \text{i.e.} \qquad t \geq -3,$$

which was excluded in the beginning.

If $t \equiv 1 \pmod 4$, then $\beta = c + d(1 + \sqrt{t})/2$, where c and d are integers. Again, $d \neq 0$, and so

$$3 \geq N(\beta) = \Big(c + \frac{d}{2}\Big)^2 + |t| \cdot \frac{d^2}{4} \geq \frac{1 + |t|}{4}, \qquad \text{i.e.} \qquad t \geq -11.$$

Combining this with $t < -3$ and $t \equiv 1 \pmod 4$, we get $t = -7$ or $t = -11$, as claimed.

• **11.4.8 (a)** We shall rely frequently on the two facts below:

(i) Divisibility and opposite containment are equivalent for ideals in $I(\sqrt{-5})$, so it suffices to find the ideals containing the given ideals.

(ii) Since $-5 \equiv 3 \pmod 4$, the elements of $I(\sqrt{-5})$ are of the form $u + v\sqrt{-5}$, where u and v are integers, by Theorem 10.3.2.

• (a1) We show first

$$a + b\sqrt{-5} \in (2,\, 1 + \sqrt{-5}) \iff a \equiv b \pmod 2. \tag{S.11.2}$$

(We avoid numbers as signs for formulas in this exercise to avoid possible confusion caused by the same notation, say, (2) for a principal ideal and a formula.)

If both a and b are even, then

$$a + b\sqrt{-5} = 2\Big[\frac{a}{2} + \frac{b}{2}\sqrt{-5}\Big] \in (2) \subseteq (2,\, 1 + \sqrt{-5})\,,$$

and if both a and b are odd, then

$$a + b\sqrt{-5} = 2\Big[\frac{a-1}{2} + \frac{b-1}{2}\sqrt{-5}\Big] + \big[1 + \sqrt{-5}\,\big] \in (2,\, 1 + \sqrt{-5})\,.$$

For the converse, assume $a + b\sqrt{-5} \in (2,\, 1 + \sqrt{-5})$, i.e.

$$a + b\sqrt{-5} = 2\alpha + \big[1 + \sqrt{-5}\,\big]\beta \tag{S.11.3}$$

with suitable elements $\alpha,\, \beta \in I(\sqrt{-5})$.

Multiplying (S.11.3) by $1 - \sqrt{-5}$, we obtain

$$\big[a + b\sqrt{-5}\,\big]\big[1 - \sqrt{-5}\,\big] = 2\big[1 - \sqrt{-5}\,\big]\alpha + 6\beta.$$

This implies

$$2 \,\Big|\, \big[a + b\sqrt{-5}\,\big]\big[1 - \sqrt{-5}\,\big] = [a + 5b] + [b - a]\sqrt{-5}.$$

Hence, both $a + 5b$ and $b - a$ are even, i.e. a and b have the same parity.

Herewith we have proved (S.11.2).

We turn now to the divisors of the ideal $I = (2,\, 1 + \sqrt{-5})$. Clearly, $I \mid I$ and $(1) \mid I$. We show that I has no more divisors (so I is an irreducible, and therefore also a prime ideal).

Assume $A \mid I$ for some ideal $A \neq I$. Then $I \subset A$ with a strict containment. We claim $A = (1)$, i.e. $1 \in A$.

Let $c + d\sqrt{-5} \in A \setminus I$. Then c and d are of opposite parity by $(*)$.

If c is odd and d is even, then again by $(*)$,

$$c - 1 + d\sqrt{-5} \in I \subset A,$$

and so

$$1 = \big[c + d\sqrt{-5}\,\big] - \big[c - 1 + d\sqrt{-5}\,\big] \in A.$$

If d is odd and c is even, then similarly

$$\sqrt{-5} = \big[c + d\sqrt{-5}\,\big] - \big[c + [d-1]\sqrt{-5}\big] \in A,$$

and so

$$1 = \big[\sqrt{-5}\,\big]\big[\sqrt{-5}\,\big] + 3 \cdot 2 \in A.$$

• (a2) Obviously, (1) and itself are divisors of (2). By $(*)$, $(2,\, 1 + \sqrt{-5})$ is a non-trivial divisor. We show that (2) has no other divisors.

Assume that $B \mid (2)$ for some ideal $B \neq (2)$. Then $(2) \subset B$ with a strict containment.

Let $u + v\sqrt{-5} \in B \setminus (2)$.

If u is odd and v is even, then $u - 1 + v\sqrt{-5} \in (2)$, and so

$$1 = \big[u + v\sqrt{-5}\,\big] - \big[u - 1 + v\sqrt{-5}\,\big] \in B, \qquad \text{thus} \qquad B = (1).$$

If u is even and v is odd, then we get similarly

$$\sqrt{-5} = \big[u + v\sqrt{-5}\big] - \big[u + [v-1]\sqrt{-5}\big] \in B,$$

which implies again

$$1 = \big[\sqrt{-5}\,\big]\big[\sqrt{-5}\,\big] + 3 \cdot 2 \in B, \qquad \text{i.e.} \qquad B = (1).$$

Finally, if both u and v are odd, then

$$1 + \sqrt{-5} = \big[u + v\sqrt{-5}\,\big] - 2\Big[\frac{u-1}{2} + \frac{v-1}{2}\sqrt{-5}\Big] \in B.$$

This means $(2,\, 1 + \sqrt{-5}) \subseteq B$, which implies $B = (2,\, 1 + \sqrt{-5})$ or $B = (1)$ by part (a1).

• (a3) We show that the principal ideal $(1+\sqrt{-5})$ has the following four (distinct) divisors:

$$(1), \qquad (1+\sqrt{-5}), \qquad (2,\, 1+\sqrt{-5}), \qquad \text{and} \qquad (3,\, 1+\sqrt{-5}).$$

These are divisors, indeed, as they contain $(1+\sqrt{-5})$.
$(2,\, 1+\sqrt{-5})$ is a non-trivial divisor since

$$1+\sqrt{-5} \not\mid 2 \Longrightarrow (2,\, 1+\sqrt{-5}) \neq (1+\sqrt{-5}),$$

and $(2,\, 1+\sqrt{-5}) \neq (1)$ by formula (S.11.2).

We get similarly that $(3,\, 1+\sqrt{-5})$ is a non-trivial divisor, here we can use

$$a+b\sqrt{-5} \in (3,\, 1+\sqrt{-5}) \iff a \equiv b \pmod 3 \tag{S.11.4}$$

which can be proved similarly as (S.11.2).

Finally, (e.g.) (S.11.2) and (S.11.4) imply

$$(2,\, 1+\sqrt{-5}) \neq (3,\, 1+\sqrt{-5}).$$

Now we verify that if an ideal C divides $(1+\sqrt{-5})$, then C is one of the four ideals above.

Assume $C \mid (1+\sqrt{-5})$ and $C \neq (1+\sqrt{-5})$, then $(1+\sqrt{-5}) \subset C$ with strict containment. Let

$$r+s\sqrt{-5} \in C \setminus (1+\sqrt{-5}). \tag{S.11.5}$$

Then

$$r-s = \big[r+s\sqrt{-5}\,\big] - s\big[1+\sqrt{-5}\,\big] \in C \tag{S.11.6}$$

on the one hand, and

$$6 = \big[1+\sqrt{-5}\,\big]\big[1-\sqrt{-5}\,\big] \in (1+\sqrt{-5}) \subset C \tag{S.11.7}$$

on the other hand.

Let d denote the greatest common divisors of 6 and $r-s$. Then $d = 6t + [r-s]w$ for suitable integers t and w, so (S.11.6) and (S.11.7) imply $d \in C$.

If $d = 1$, then $1 \in C$, so $C = (1)$.

If $d = 2$, then $2 \in C$, so $(2,\, 1+\sqrt{-5}) \subseteq C$. By (a1), we infer $C = (2,\, 1+\sqrt{-5})$ or $C = (1)$.

If $d = 3$, then $3 \in C$, so $(3,\, 1+\sqrt{-5}) \subseteq C$. Relying on (S.11.4), we can easily deduce $C = (3,\, 1+\sqrt{-5})$ or $C = (1)$ similar to (a1).

Finally we show $d \neq 6$. If $d = 6$, i.e. $6 \mid r - s$, then

$$r + s\sqrt{-5} = [r-s] + s\big[1+\sqrt{-5}\,\big] \in (1+\sqrt{-5}),$$

which contradicts (S.11.5).

• **11.4.9 (a)** False. E.g. 2 is irreducible in $I(\sqrt{-5})$, but (2) is not an irreducible ideal.

• **(b)** True. By the condition, α is not a unit or 0. Assume $\alpha = \beta\gamma$. Then $(\alpha) = (\beta)(\gamma)$, and as (α) is irreducible, $(\beta) = (1)$ or $(\gamma) = (1)$, i.e. β or γ is a unit.

• **(c)** and **(d)** Both are true. Since

$$(\alpha) \neq (0) \iff \alpha \neq 0 \qquad \text{and} \qquad (\alpha) \neq (1) \iff \alpha \text{ is not a unit},$$

we may assume that (α) is a non-trivial ideal.

Using the equivalence of divisibility and opposite containment,

$$\begin{aligned}(\alpha) \text{ is a prime ideal} &\iff \big[\,\beta\gamma \in (\alpha) \Longrightarrow \beta \in (\alpha) \text{ or } \gamma \in (\alpha)\,\big] \iff \\ &\iff \big[\,\alpha \mid \beta\gamma \Longrightarrow \alpha \mid \beta \text{ or } \alpha \mid \gamma\,\big] \iff \alpha \text{ is a prime element.}\end{aligned}$$

• **11.5.7 (c)** We prove that to a prime number $p > 0$ we can find an integer a such that $(p,\, a+\sqrt{-5})$ is a prime ideal if and only if $p = 2$, $p = 5$, or the remainder of p mod 20 is 1, 3, 7, or 9.

• We verify first that primes p in the list above have this property, indeed.

• If $p = 2$, then $a = 1$ suits: $I_2 = (2,\, 1+\sqrt{-5})$ is a prime ideal (see Exercise 11.4.8).

• If $p = 5$, then $a = 0$ works: $I_5 = (5,\, \sqrt{-5}) = (\sqrt{-5})$ is a prime ideal. By Exercise 11.4.9c–d, this is equivalent to $\sqrt{-5}$ being a prime element in $E(\sqrt{-5})$. Thus, we have to prove

$$\text{(S.11.8)}\quad \sqrt{-5}\,\big|\,\big[a+b\sqrt{-5}\,\big]\big[c+d\sqrt{-5}\,\big] \Rightarrow \sqrt{-5}\,\big|\,a+b\sqrt{-5} \text{ or } \sqrt{-5}\,\big|\,c+d\sqrt{-5}\,.$$

As $\sqrt{-5}$ divides itself, (S.11.8) is equivalent to

$$\text{(S.11.9)}\qquad \sqrt{-5}\,\big|\,ac \Longrightarrow \sqrt{-5}\,\big|\,a \quad \text{or} \quad \sqrt{-5}\,\big|\,c\,.$$

We easily see that an integer is divisible by $\sqrt{-5}$ if and only if it is divisible by 5, so we can rewrite (S.11.9) as

$$5 \mid ac \Longrightarrow 5 \mid a \quad \text{vagy} \quad 5 \mid c\,. \tag{S.11.10}$$

As 5 is a prime among the integers, (S.11.10), and so also (S.11.8) hold, indeed. (We could have used also Exercise 10.3.7b.)

• Let now p be a positive prime of the form $20k+1$, $20k+3$, $20k+7$, or $20k+9$. We obtain from the properties of the Legendre symbol that these are exactly the primes satisfying $\left(\frac{-5}{p}\right) = 1$. Hence, the congruence

$$x^2 \equiv -5 \pmod{p}$$

is solvable, i.e.

$$p \mid a^2 + 5 \tag{S.11.11}$$

for some integer a. We prove that $I_p = (p,\, a+\sqrt{-5})$ is irreducible, consequently it is a prime ideal. We have to verify $I_p \neq (1)$, $I_p \neq (0)$, and that I_p can be decomposed into the product of two ideals only trivially. This latter is equivalent (see (11.4.9) after Definition 11.4.6) to

$$I_p \subseteq A \subseteq I(\sqrt{-5}) \Longrightarrow A = I_p \quad \text{or} \quad A = I(\sqrt{-5}) \tag{S.11.12}$$

(for any ideal A).

Clearly, $I_p \neq (0)$.

If $I_p = (1)$, then

$$1 = \alpha p + \beta\big[a + \sqrt{-5}\,\big] \tag{S.11.13}$$

for some $\alpha,\ \beta \in I(\sqrt{-5})$. Multiplying equality (S.11.13) by $a - \sqrt{-5}$, we obtain

$$a - \sqrt{-5} = \alpha\big[a - \sqrt{-5}\,\big]p + \beta[a^2+5]\,. \tag{S.11.14}$$

By (S.11.11), the right-hand side of (S.11.14) is divisible p, so the same holds also for the left-hand side, i.e.

$$\frac{a}{p} - \frac{1}{p}\sqrt{-5} \in I(\sqrt{-5})\,,$$

which is clearly impossible. This proves $I_p \neq (1)$.

To verify implication (S.11.12), assume that an ideal A contains I_p, but they are not equal. We demonstrate $1 \in A$, i.e. $A = I(\sqrt{-5})$.

Pick any element

$$c + d\sqrt{-5} \in A \setminus I_p. \tag{S.11.15}$$

Then

$$\big[c + d\sqrt{-5}\,\big] - d\big[a + \sqrt{-5}\,\big] = c - da \in A. \tag{S.11.16}$$

If $p \mid c - da$, i.e. for some integer u,

$$c = da + up, \qquad \text{then} \qquad c + d\sqrt{-5} = d\big[a + \sqrt{-5}\,\big] + up \in I_p$$

contradicting (S.11.15).

This implies that $c - da$ is not divisible by p, so $c - da$ and p are coprime (among the integers). Thus,

$$1 = v[c - da] + wp \tag{S.11.17}$$

for some integers v and w. Since $p \in A$, and also $c - da \in A$ by (S.11.16), we get $1 \in A$ from (S.11.17), as claimed.

• Finally, we show that for the positive prime numbers p not listed, i.e. for the ones of the form $20k + 11$, $20k + 13$, $20k + 17$, and $20k + 19$, $(p,\, a + \sqrt{-5})$ is not a prime ideal for any integer a.

These prime numbers p satisfy $\left(\frac{-5}{p}\right) = -1$, and so they are primes also in $I(\sqrt{-5})$ by Theorem 10.3.7. Then (p) is a prime ideal by Exercise 11.4.9c.

Assume that $(p,\, a + \sqrt{-5})$ is still a prime ideal for some integer a. Since

$$(p) \subseteq (p,\, a + \sqrt{-5}), \qquad \text{and so} \qquad (p,\, a + \sqrt{-5}) \,\big|\, (p)\,,$$

further both $(p,\, a + \sqrt{-5})$ and (p) are prime ideals, only $(p,\, a + \sqrt{-5}) = (p)$ is possible. This implies $a + \sqrt{-5} \in (p)$, so

$$p \mid a + \sqrt{-5}, \qquad \text{i.e.} \qquad \frac{a}{p} + \frac{1}{p}\sqrt{-5} \in I(\sqrt{-5}),$$

which is false.

• **11.5.9** As a preliminary remark, we note that Theorem 11.5.1 remains valid if we replace algebraic integers everywhere by integers. This follows from the

fact that for integers u and v, the divisibility $u \mid v$ holds among algebraic integers if and only if it is true among integers. To see this, consider equality $uw = v$. If w is an integer, then it is an algebraic integer, too. Conversely, if w is an algebraic integer, then as (for $u \neq 0$) $w = v/u$ is rational, too, it must be an integer.

In the sequel we shall use this special case of Theorem 11.5.1 for integers.

• **(a)** Let

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m \qquad \text{and} \qquad g(x) = b_0 + b_1 x + \ldots + b_n x^n$$

be two primitive polynomials and

$$f(x)g(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$$

be their product. Assume that $f(x)g(x)$ is not a primitive polynomial, i.e.

$$p \mid c_k, \qquad k = 0, 1, \ldots, m+n$$

for some prime p. Then by (the special case of) Theorem 11.5.1,

$$p \mid a_i b_j, \qquad i = 0, 1, \ldots, m, \qquad j = 0, 1, \ldots, n.$$

Since f and g are primitive polynomials,

$$p \nmid a_i \qquad \text{and} \qquad p \nmid b_j$$

for some i and j. As p is a prime, this implies $p \nmid a_i b_j$ providing a contradiction.

• **(b)** Let r and s be the least common multiples of denominators in the coefficients of F and G, resp. Multiplying $H = FG$ by $t = rs$, we obtain

$$tH(x) = F_2(x)G_2(x), \qquad \text{where} \qquad F_2(x),\, G_2(x) \in \mathbf{Z}[x]\,. \tag{S.11.18}$$

If $t = 1$, then we are done. If $t > 1$, then let p be an arbitrary prime divisor of t. Then p divides every coefficient of $F_2(x)G_2(x)$.

If both $F_2(x)$ and $G_2(x)$ have a coefficient not divisible by p, then this contradicts Theorem 11.5.1 as seen in part (a). Hence p divides all coefficients of (say) $F_2(x)$, so $F_2(x) = pF_3(x)$.

Dividing (S.11.18) by p, we get

$$t_1 H(x) = F_3(x)G_2(x), \qquad F_3(x),\, G_2(x) \in \mathbf{Z}[x], \qquad t_1 = \frac{t}{p}\,.$$

If $t_1 = 1$, then we are done. Otherwise repeat the procedure till we get a required factorization of H.

• **11.6.3 (a)** Since k and h are coprime, $ku = 1 + hv$ for some positive integers u and v. Also,

$$A^k \sim B^k \Longrightarrow A^{ku} \sim B^{ku}\,,$$

i.e.

$$(\alpha)A^{ku} = (\beta)B^{ku} \tag{S.11.19}$$

for suitable non-zero principal ideals (α) and (β). Replace A^{ku} and B^{ku} in (S.11.19) by AA^{hv} and BB^{hv}, resp., and use that A^{hv} and B^{hv} are principal ideals, let $A^{hv} = (\gamma)$ and $B^{hv} = (\delta)$. This implies

$$(\alpha\gamma)A = (\beta\delta)B, \qquad \text{i.e.} \qquad A \sim B.$$

• **(b)** Applying part (a) for $B = (1)$, we get $A \sim (1)$, hence A is a principal ideal by Theorem 11.6.2/(iv).

• **11.6.4 (d)** We show that all integer solutions of $x^2 + 35 = y^3$ are $x = \pm 36$, $y = 11$.

We follow the proof of Theorem 11.6.5. We shall use that the number of ideal classes in $I(\sqrt{-35})$ is $h(\sqrt{-35}) = 2$ (see the table before Theorem 11.6.4). This implies that the Fundamental Theorem of Arithmetic is false in $I(\sqrt{-35})$.

We can factor the left-hand side of the equation in $I(\sqrt{-35})$:

$$\big[x + \sqrt{-35}\,\big]\big[x - \sqrt{-35}\,\big] = y^3\,. \tag{S.11.20}$$

As the Fundamental Theorem is false in $I(\sqrt{-35})$, we have to convert (S.11.20) into an equation for principal ideals:

$$(x + \sqrt{-35})(x - \sqrt{-35}) = (y)^3\,. \tag{S.11.21}$$

We show that the ideals $(x+\sqrt{-35})$ and $(x-\sqrt{-35})$ are coprime. Assume that there still exists a prime ideal P dividing both of them. Then P divides $(y)^3$, which implies $P \mid (y)$ as P is a prime ideal. By the containments corresponding to the divisibilities,

$$x + \sqrt{-35} \in P, \qquad x - \sqrt{-35} \in P, \qquad \text{and} \qquad y \in P.$$

Then also

$$\sqrt{-35}\big[[x-\sqrt{-35}\,]-[x+\sqrt{-35}\,]\big]=2\cdot 35=70\in P.$$

We show that y and 70 are coprime (among the integers).

If $7\mid y$, then the original equation implies $7\mid x$. However, the exponents of 7 in the standard forms of x^2+35 and y^3 are exactly 1 and at least 3, resp., which is impossible.

We get $5\nmid y$ similarly.

If $2\mid y$, then x is odd, and the remainders of the left-hand side and right-hand side modulo 8 are 4 and 0, resp., which is a contradiction again.

Herewith we have proved that y and 70 are coprime. Consequently, $1=yr+70s$ with suitable integers r and s. Since both 70 and y are in P, 1 is in P, as well, i.e. $P=(1)$, which contradicts P being a prime ideal.

Thus, the two (principal) ideals on the left-hand side of (S.11.21) are coprime, indeed. The Unique Factorization Theorem 11.5.8 for ideals yields that both ideals are cubes of suitable ideals, so

$$(x+\sqrt{-35})=A^3\,. \tag{S.11.22}$$

Since the number of ideal classes in $I(\sqrt{-35})$ is $h(\sqrt{-35})=2$, A^2 is a principal ideal, $A^2=(\gamma)$, by Theorem 11.6.4. Substituting it into (S.11.22), we get

$$(x+\sqrt{-35})=(\gamma)A.$$

By Exercise 11.4.3b, A is a principal ideal, $A=(\alpha)$. Then (S.11.22) can be written as

$$(x+\sqrt{-35})=(\alpha^3),\qquad \text{i.e.}\qquad x+\sqrt{-35}=\varepsilon\alpha^3, \tag{S.11.23}$$

where ε is a unit in $I(\sqrt{-35})$. The only units in $I(\sqrt{-35})$ are ±1, which are cubes themselves. Hence, (S.11.23) is equivalent to

$$x+\sqrt{-35}=\beta^3=\big[a+b\sqrt{-35}\,\big]^3\,, \tag{S.11.24}$$

where $-35\equiv 1 \pmod 4$ implies that either a and b are integers, or $a=u/2$ and $v=b/2$ for some odd integers u and v.

Cubing and comparing the imaginary parts, we obtain

$$1=3a^2b-35b^3=b[3a^2-35b^2]. \tag{S.11.25}$$

If a and b are integers, then $b = \pm 1$, but we do not get integer values for a.

If $a = u/2$ and $v = b/2$ with u and v odd, then multiplying (S.11.25) by 8, we have

$$8 = v[3u^2 - 35v^2].$$

As v is odd,

$$v = \pm 1 \qquad \text{and} \qquad 3u^2 - 35v^2 = 3u^2 - 35 = \pm 8.$$

This yields $u = \pm 3$ and $v = -1$. Substituting back into formula (S.11.24) and comparing the real parts, we get

$$x = \frac{u[u^2 - 105v^2]}{8} = \mp 36 \qquad \text{and} \qquad y = \sqrt[3]{x^2 + 35} = 11.$$

12. Combinatorial Number Theory

• **12.1.3** First we present a construction where the number of representations is $\lceil k/2 \rceil$. Let $k = 2j - 1$ or $2j$, then $\lceil k/2 \rceil = j$. Following the hint, take

$$q > j, \;\; a_1 = q + 1, a_2 = q + 2, \ldots, a_j = q + j, \text{ and } t = a_1 + a_2 + \ldots + a_j.$$

Now insert $a_{j+1} = a_1 + a_2$, then also

$$t = a_3 + a_4 + \ldots + a_j + a_{j+1}.$$

Similarly, if $a_{j+2} = a_3 + a_4$, then also

$$t = a_5 + a_6 + \ldots + a_{j+1} + a_{j+2}.$$

In general, put $a_{j+r} = a_{2r-1} + a_{2r}$ for $r \leq j - 1$ (and for $k = 2j$ let a_{2j} be an arbitrary number greater than a_{2j-1}). Then we have

$$t = a_{2r+1} + a_{2r+2} + \ldots + a_{j+r}.$$

We show $a_s < a_{s+1}$ for every s. For $s < j$ this follows from the definition of a_s, for $s = j$ we have $a_{j+1} = a_1 + a_2 = 2q + 3 > a_j = q + j$ (since $q > j$), and for $j < s \leq 2j - 2$ the two terms a_i in the sum a_{s+1} are bigger than the ones in the sum a_s.

The procedure guarantees that t is the sum of j, $j-1$, ... consecutive numbers a_i, till finally t is a one term sum, which means altogether j representations, as desired.

Now we show that no bigger number of representations is possible. Consider an arbitrary system $a_1, \ldots, a_k$ and a number t, and select the representation of t where the last (i.e. the biggest) term is the smallest, let this term be a_v.

If $v > j$, then at most $k-(v-1) \le k-j \le j$ representations are possible, since each representation must have a different last term.

If $v \le j$, then since the number of terms is different in every representation and it is at most v, therefore at most $v \le j$ representations are possible.

• **12.2.3** Consider a finite field F_2 of p^2 elements and its subfield F_1 of p elements. The multiplicative group of a finite field is cyclic, so F_2 has an element Δ such that every non-zero element in F_2 is a power of Δ.

Pick an arbitrary $\Theta \in F_2 \setminus F_1$, and let $\gamma_1, \ldots, \gamma_p$ be the elements of F_1. Write the elements $\Theta+\gamma_i$ as $\Theta+\gamma_i = \Delta^{a_i}$ defining thus p integers a_i between 1 and p^2-1.

We show that these meet the requirement, i.e. the sums a_i+a_j are pairwise incongruent modulo p^2-1.

Assume $a_i + a_j \equiv a_k + a_l \pmod{p^2-1}$. By the definition of integers a_i, this means $(\Theta+\gamma_i)(\Theta+\gamma_j) - (\Theta+\gamma_k)(\Theta+\gamma_l) = 0$. The left-hand side is a polynomial of Θ with coefficients from F_1 and of degree at most 1 as Θ^2 gets canceled. It cannot have degree 1 (or 0) since this would imply $\Theta \in F_1$, so it must be the zero polynomial (with all coefficients 0). Then, e.g. by the uniqueness of the root factors, $\{\gamma_i, \gamma_j\} = \{\gamma_k, \gamma_l\}$, and so the same holds for the numbers a_i, too, as claimed.

• **12.2.4** Following the hint, let g be a primitive root modulo p, and let a_i be the modulo $p(p-1)$ solution of the system of congruences $x \equiv i \pmod{p-1}$, $x \equiv g^i \pmod{p}$, $i = 1, 2, \ldots, p-1$. It suffices to verify that for any c, the congruence $c \equiv a_i + a_j \pmod{p(p-1)}$ can hold with at most one (unordered) pair $\{i, j\}$ (allowing also $i = j$). By the definition of a_i, this congruence is equivalent to the system of congruences $c \equiv i + j \pmod{p-1}$, $c \equiv g^i + g^j \pmod{p}$. The first congruence here can be written as $g^c \equiv g^i g^j \pmod{p}$. Hence we know both the sum and product of the numbers g^i and g^j modulo p. By Viète's formulas concerning roots and coefficients, the residue classes g^i and g^j are the uniquely determined solutions of the quadratic congruence $z^2 - cz + g^c \equiv 0 \pmod{p}$, as p is a prime. Therefore also i and j are unique.

• **12.3.6** Following the hint, let $|C| = |D| = n < p$, $C = \{c_1, \ldots, c_n\}$, $A_1 = \ldots = A_n = D$, and

$$G(x_1, \ldots, x_n) = \prod_{1 \le j < i \le n} (x_i - x_j)(x_i + c_i - x_j - c_j).$$

Then the degree of G is $n(n-1)$. Thus, if the coefficient of $\prod_{i=1}^n x_i^{n-1}$ is not zero, then by Exercise 12.3.5b,

$$G(d_1, \ldots, d_n) = \prod_{1 \le j < i \le n} (d_i - d_j)(d_i + c_i - d_j - c_j) \neq 0$$

for some $d_1, \ldots, d_n \in D$. Here necessarily $d_i \neq d_j$ for $i \neq j$, i.e. $d_1, \ldots, d_n$ are all elements of D. Further, $c_i + d_i \neq c_j + d_j$ for $i \neq j$, i.e. the map $c_i \longleftrightarrow d_i$ yields a suitable pairing between the elements of C and D.

Now we verify that the coefficient of $\prod_{i=1}^n x_i^{n-1}$ in G is not zero. We obtain the terms in G having degree $\deg G = n(n-1)$ from $\prod_{1 \le j < i \le n}(x_i - x_j)^2$ (all other terms have smaller degree). This part is just the square of the Vandermonde determinant

$$V(x_1, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix}.$$

Write $V(x_1, \ldots, x_n)$ according to the definition of determinants, and check the coefficient of $\prod_{i=1}^n x_i^{n-1}$ when multiplying V with itself. We obtain such a term if we multiply a term

$$(-1)^{I(j_1,\ldots,j_n)} x_1^{j_1} \ldots x_n^{j_n}$$

from the first determinant with the term

$$(-1)^{I(n-1-j_1,\ldots,n-1-j_n)} x_1^{n-1-j_1} \ldots x_n^{n-1-j_n}$$

from the second determinant, where $I()$ denotes the number of inversions in the corresponding permutation of the indices of columns numbered from 0 to $n-1$. Since the two permutations determining the sign are "complements" of each other, therefore

$$I(j_1, \ldots, j_n) + I(n-1-j, \ldots, n-1-j_n) = \binom{n}{2},$$

i.e. every such product is

$$(-1)^{\binom{n}{2}} x_1^{n-1} \dots x_n^{n-1}\,.$$

There are $n!$ such products, so the coefficient of $\prod_{i=1}^{n} x_i^{n-1}$ in G is $(-1)^{\binom{n}{2}} n!$, which is not zero, indeed, as $n < p$.

• **12.4.11 (b)** Assume that in the coloring defined in the hint, the integers $1 \le b < b+d < b+2d < \ldots < b+pd \le p(2^p-1)$ have the same color. Let $\Theta = \Delta^b, \Psi = \Delta^d$. By the monochromatic assumption, the "vectors" $\Theta, \Theta\Psi, \ldots, \Theta\Psi^p$ either all are in subspace W, or all are outside W.

If the arithmetic progression is red, then all these vectors are in a subspace of dimension $p-1$. Therefore, already the first p of them are linearly dependent, i.e. $\sum_{i=0}^{p-1} \gamma_i(\Theta\Psi^i) = 0$ holds non-trivially with suitable coefficients $\gamma_i \in \mathbf{Z}_2$. Dividing the equality by Θ, we obtain that Ψ is a root of a (non-zero) polynomial over $\mathbf{Z}_2$ having degree less than p. Since the degree of Ψ divides the degree p of F, the degree of Ψ must be 1, i.e. $\Psi \in \mathbf{Z}_2$. This is impossible, however, as $\Psi \ne 0$ and $d < 2^p - 1$ implies $\Psi \ne 1$.

If the arithmetic progression is blue, then we have to use the above argument for vectors $\Theta\Psi - \Theta, \Theta\Psi^2 - \Theta\Psi, \ldots, \Theta\Psi^p - \Theta\Psi^{p-1}$, and divide the suitable equality by $\Theta(\Psi - 1)$ instead of Θ (if $\Psi \ne 1$).

• **12.4.12** Following the hint, consider the positive integers up to n which have only digits less than $d/2$ in number system of base d and the sum of squares of digits is a fixed q. If three such integers form an arithmetic progression, then the same must hold for every digit since there is no overflow to the next digit due to the restriction on the digits. Therefore every digit of the second integer is the arithmetic mean of the corresponding digits of the other two integers. Using that the sum of squares of digits in each integer is q, a simple calculation yields that the three integers must be equal. (In other words: Considering the three integers as vectors where the coordinates are the digits, then one vector is the half of the sum of the other two, and each vector has the same Euclidean norm. This can happen only if the three vectors are equal.)

For a given d, the number of digits is $u \approx (\log n)/(\log d)$ and q can assume at most $ud^2/4$ values. Uniting our sets for all possible values of q, we obtain every integer having all digits less than $d/2$. This gives altogether about $n/2^u$ integers. Therefore there is a q for which the corresponding set contains at least $n/(2^{u-2}ud^2)$ integers. The maximum of this expression occurs when $\log d \approx \sqrt{\log n}$, and we obtain the value claimed in the exercise as a maximum.