Appendix
Hints and Answers to Exercises

A.1 Chapter 1

1. By assumption we have $a = bq + r$ with $q \leqslant r < b$ so that $q(b+1) \leqslant a < b(q+1)$. Now if $a = q_1(b+1) + r_1$ with $0 \leqslant r_1 < b+1$, we deduce that

$$q(b+1) \leqslant q_1(b+1) + r_1 < b(q+1)$$

and hence

$$q - \frac{r_1}{b+1} \leqslant q_1 < \frac{b}{b+1}(q+1) + \frac{r_1}{b+1}$$

implying $q - 1 < q_1 < q + 1$ and therefore $q_1 = q$.

2. If $1 \leqslant q < a$, let b_q be the quotient of the Euclidean division of a by q. We have

$$b \in \mathcal{S}_q \iff \left[\frac{a}{b}\right] = q \iff \frac{a}{b} - 1 < q \leqslant \frac{a}{b} \iff \frac{a}{q+1} < b \leqslant \frac{a}{q}$$

and since $b \in \mathbb{N}$, this is equivalent to $b_{q+1} < b \leqslant b_q$. Hence we have

$$\sum_{q=1}^{a} |\mathcal{S}_q| = \sum_{q=1}^{a-1} |\mathcal{S}_q| + 1 = \sum_{q=1}^{a-1} (b_q - b_{q+1}) + 1 = b_1 - b_a + 1 = a - 1 + 1 = a.$$

3. For (i), the Euclidean division of n by m gives $n = qm + r$ with $0 \leqslant r \leqslant m-1$ so that

$$\frac{n+1}{m} - 1 = q + \frac{r+1}{m} - 1 \leqslant q + \frac{m-1+1}{m} - 1 = q = \left[\frac{n}{m}\right].$$

O. Bordellès, *Arithmetic Tales*, Universitext,
DOI 10.1007/978-1-4471-4096-2, © Springer-Verlag London 2012

For (ii), the proof is similar except that we use $m \nmid n \Longrightarrow 1 \leqslant r \leqslant m-1$. The identity (iii) is obvious if $m \mid n$. Otherwise, we have by (i) and (ii)

$$0 \leqslant \left[\frac{n}{m}\right] - \left[\frac{n-1}{m}\right] \leqslant 1 - \frac{1}{m} < 1$$

and we conclude the proof by noticing that the difference above is an integer.

4. The first identity follows from Theorem 1.14 (i) and letting $x \longrightarrow \infty$. The second identity follows from

$$\sum_{n>x} f(n)g(n) = \sum_{n=1}^{\infty} f(n)g(n) - \sum_{n\leqslant x} f(n)g(n).$$

5. Using Theorem 1.14 (i) we get for all integers $N > M$

$$\sum_{n=1}^{N} \frac{a_n}{n} = \frac{1}{N}\sum_{n=1}^{N} a_n + \int_1^M \frac{1}{t^2}\Big(\sum_{n\leqslant t} a_n\Big)\,\mathrm{d}t + \int_M^N \frac{1}{t^2}\Big(\sum_{n\leqslant t} a_n\Big)\,\mathrm{d}t.$$

By assumption, the first term on the right-hand side tends to 0 as $N \longrightarrow \infty$ and the second integral converges by Rule 1.20 since $|\sum_{n\leqslant t} a_n| \leqslant M$. Hence we obtain

$$\begin{aligned}\left|\sum_{n=1}^{\infty} \frac{a_n}{n}\right| &\leqslant \int_1^M \frac{1}{t^2}\left|\sum_{n\leqslant t} a_n\right|\mathrm{d}t + \int_M^{\infty} \frac{1}{t^2}\left|\sum_{n\leqslant t} a_n\right|\mathrm{d}t \\ &\leqslant \int_1^M \frac{\mathrm{d}t}{t} + M\int_M^{\infty} \frac{\mathrm{d}t}{t^2} = \log M + 1\end{aligned}$$

as asserted.

6. One may assume that $N \geqslant 2$. By Abel's summation as stated in Remark 1.15, we get

$$\begin{aligned}&\sum_{k=1}^{n-1} \frac{k}{N}(a_{k+1}-a_k) + \sum_{k=n}^{N-1} \frac{k-N}{N}(a_{k+1}-a_k) \\ &\quad= \sum_{k=1}^{N-1} \frac{k}{N}(a_{k+1}-a_k) - \sum_{k=n}^{N-1}(a_{k+1}-a_k) \\ &\quad= \frac{1}{N}\left\{(N-1)\sum_{k=1}^{N-1}(a_{k+1}-a_k) - \sum_{k=1}^{N-2}\sum_{j=1}^{k}(a_{j+1}-a_j)\right\} - a_N + a_n \\ &\quad= \left(1-\frac{1}{N}\right)(a_N - a_1) - \frac{1}{N}\sum_{k=1}^{N-2}(a_{k+1}-a_1) - a_N + a_n\end{aligned}$$

$$= a_n - \frac{a_1 + a_N}{N} - \frac{1}{N}\sum_{k=2}^{N-1} a_k = a_n - \frac{1}{N}\sum_{k=1}^{N} a_k$$

so that

$$a_n = \frac{1}{N}\sum_{k=1}^{N} a_k + \sum_{k=1}^{N} \Delta_N(n,k)(a_{k+1} - a_k)$$

where

$$\Delta_N(n,k) = \frac{1}{N} \times \begin{cases} k, & \text{if } 1 \leqslant k \leqslant n-1, \\ k-N, & \text{if } n \leqslant k \leqslant N \end{cases}$$

and the result follows from the trivial estimate $|\Delta_N(n,k)| \leqslant 1$.

7. This is an immediate consequence of Theorem 1.14 (ii) using

$$\sum_{p \leqslant x} f(p) = \sum_{p \leqslant x} \left(\frac{f(p)}{\log p} \times \log p \right).$$

8.

(a) By integration by parts

$$\mathrm{Li}(x) = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{\mathrm{d}t}{(\log t)^2}$$

as required.

(b) Using Exercise 7 with $f(x) = 1$ and the previous question, we get

$$\begin{aligned} \pi(x) &= \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t(\log t)^2}\,\mathrm{d}t \\ &= \frac{x}{\log x} + \int_2^x \frac{\mathrm{d}t}{(\log t)^2} + \frac{\theta(x) - x}{\log x} + \int_2^x \frac{\theta(t) - t}{t(\log t)^2}\,\mathrm{d}t \\ &= \mathrm{Li}(x) + \frac{2}{\log 2} + \frac{\theta(x) - x}{\log x} + \int_2^x \frac{\theta(t) - t}{t(\log t)^2}\,\mathrm{d}t \end{aligned}$$

and hence

$$\left|\pi(x) - \mathrm{Li}(x)\right| \leqslant \frac{2}{\log 2} + \frac{R(x)}{\log x} + \int_2^x \frac{R(t)}{t(\log t)^2}\,\mathrm{d}t$$

with

$$\int_2^x \frac{R(t)}{t(\log t)^2}\,\mathrm{d}t = \left(\int_2^{\sqrt{x}} + \int_{\sqrt{x}}^x \right) \frac{R(t)}{t(\log t)^2}\,\mathrm{d}t$$

$$
\begin{aligned}
&< \frac{\sqrt{x}}{(\log 2)^2} + R(x) \int_{\sqrt{x}}^{x} \frac{\mathrm{d}t}{t(\log t)^2} \\
&= \frac{\sqrt{x}}{(\log 2)^2} + \frac{R(x)}{\log x} \\
&\leqslant \frac{R(x)}{\log x} \left(1 + \frac{1}{(\log 2)^2} \right)
\end{aligned}
$$

and therefore

$$
\left| \pi(x) - \mathrm{Li}(x) \right| < \frac{R(x)}{\log x} \left(2 + \frac{1}{(\log 2)^2} \right) + \frac{2}{\log 2} < \frac{5R(x)}{\log x}.
$$

A.2 Chapter 2

1.

(a) If $d = (a, b)$, then d divides $2a$ and $2b$, so that d divides $2(a, b) = 2$.

(b) If $d = (a, b)$, then d divides $a(a + b) - ab = a^2$ and $b(a + b) - ab = b^2$, so that d divides $(a^2, b^2) = 1$.

(c) If $b = ka$ for some integer k, then $b^n = k^n a^n$ and thus $a^n \mid b^n$. Conversely, assume that $a^n \mid b^n$ and set $d = (a, b)$ and write $a = da'$ and $b = db'$ so that $(a', b') = 1$. We have $a'^n \mid b'^n$ and since $(a'^n, b'^n) = (a', b')^n = 1$, we infer that $a'^n = 1$ and then $a' = 1$. Thus $a = d$ and therefore $b = ab'$, so that $a \mid b$.

(d) Set $d = (a, b)$ and $D = (ax + by, az + bt)$ with $|xt - yz| = 1$. We have clearly $d \mid D$. Conversely, assuming $ax + by \geqslant 0$ and $az + bt \geqslant 0$, we have

$$
\left.
\begin{aligned}
D \mid ax + by \\
D \mid az + bt
\end{aligned}
\right\}
\quad \Longrightarrow \quad
D \mid \big\{ X(ax + by) + Y(az + bt) \big\}
$$

for all $(X, Y) \in \mathbb{Z}^2$. Taking $X = t$ and $Y = -y$ we obtain $D \mid \pm a$ and taking $X = z$ and $Y = -x$ gives $D \mid \pm b$, and hence $D \mid d$.

2.

(a) We have $|\mathcal{S}^2| = ([\sqrt{p}] + 1)^2 > p = |\{0, \ldots, p - 1\}|$ so that f is not injective by the Dirichlet pigeon-hole principle.

(b) We have $f(u_1, v_1) = f(u_2, v_2) \Longleftrightarrow au_1 - v_1 \equiv au_2 - v_2 \pmod{p} \Longleftrightarrow au \equiv v \pmod{p}$.

Furthermore, $|u| = |u_1 - u_2| \leqslant [\sqrt{p}] < \sqrt{p}$ and similarly $|v| < \sqrt{p}$.

If $u = 0$, then we have $v \equiv 0 \pmod{p}$ and hence $v = 0$ since $|v| < \sqrt{p}$. This is impossible in view of the condition $(u_1, v_1) \neq (u_2, v_2)$.

If $v = 0$, then we have $au \equiv 0 \pmod{p}$ and since $p \nmid a$ and p is prime, then we get $u = 0$ by Lemma 3.4, which is also impossible.

3. Let us first notice that $q_k \geqslant 1$ for all $1 \leqslant k < n$ and $q_n \geqslant 2$.

(a) The identity is true when $k = 0$ and $k = 1$. Assume it is true for some $1 \leqslant k \leqslant n$. Then

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k \\ &= s_{k-1}a + t_{k-1}b - q_k(s_k a + t_k b) \\ &= a(s_{k-1} - q_k s_k) + b(t_{k-1} - q_k t_k) \\ &= s_{k+1}a + t_{k+1}b \end{aligned}$$

proving the asserted result by induction.

(b) We show the identity $\operatorname{sgn}(s_k) = (-1)^k$ by induction, where we set $\operatorname{sgn}(0) = \pm 1$ by convention. The identity is true when $k = 0$ and $k = 1$. Assume it is true for some $1 \leqslant k \leqslant n$. Then $\operatorname{sgn}(s_{k+1}) = \operatorname{sgn}(-q_k s_k + s_{k-1})$ and by induction hypothesis we have

$$\operatorname{sgn}(-q_k s_k) = -\operatorname{sgn}(s_k) = (-1)^{k+1} = \operatorname{sgn}(s_{k-1})$$

and hence $\operatorname{sgn}(s_{k+1}) = (-1)^{k+1}$ as required. Similarly, we have $\operatorname{sgn}(t_k) = (-1)^{k+1}$. We conclude the proof using $x = \operatorname{sgn}(x)|x|$.

For all $k \in \{1, \ldots, n\}$, we then have

$$s_{k+1} = -q_k s_k + s_{k-1} \iff (-1)^{k+1}|s_{k+1}| = (-1)^{k+1} q_k |s_k| + (-1)^{k-1}|s_{k-1}|$$

and simplifying by $(-1)^{k+1}$ gives the desired result. The proof is analogous for the identity

$$|t_{k+1}| = q_k |t_k| + |t_{k-1}|.$$

(c) Define the sequence (u_k) by $u_k = |t_k| r_{k-1} + |t_{k-1}| r_k$ for all $k \in \{1, \ldots, n+1\}$. Using the previous questions, we get

$$\begin{aligned} u_{k+1} &= |t_{k+1}| r_k + |t_k| r_{k+1} \\ &= \big(q_k |t_k| + |t_{k-1}|\big) r_k + |t_k|(r_{k-1} - r_k q_k) \\ &= |t_k| r_{k-1} + |t_{k-1}| r_k = u_k \end{aligned}$$

and hence $u_k = u_1 = |t_1| r_0 + |t_0| r_1 = a$ for all $k \in \{1, \ldots, n+1\}$, as asserted.

4.

(a) By induction.

(b) Set $d = (u_n, u_{n-1})$ so that d divides $u_{n-1}^2 - u_n = 2$, and since u_n and u_{n-1} are odd, we get $d = 1$.

(c) By induction, the result being clearly true when $n = 3$ since

$$u_3 - 2 = u_2^2 - 4 = (u_2 + 2)(u_2 - 2) = u_1^2(u_2 - 2).$$

Assume it is true with n replaced by $n-1$. We have

$$\begin{aligned} u_n - 2 &= u_{n-1}^2 - 4 \\ &= (u_{n-1}+2)(u_{n-1}-2) \\ &= u_{n-2}^2(u_{n-1}-2) \end{aligned}$$

and using induction hypothesis we get

$$u_n - 2 = u_{n-2}^2 u_{n-3}^2 \cdots u_1^2(u_2 - 2)$$

concluding the proof.

(d) For all $r \in \{2, \ldots, n-1\}$, define $d_r = (u_n, u_{n-r})$. We have $d_r \mid u_n$ and $d_r \mid u_{n-r}$ so that d_r divides

$$u_n - u_{n-r}^2 u_{n-2}^2 \cdots u_{n-r+1}^2 u_{n-r-1}^2 \cdots u_1^2(u_2 - 2) = 2$$

and we conclude the proof by using the fact that both u_n and u_{n-r} are odd.

5.

▹ The first equation is equivalent to $19x + 14y = 3$ and has solutions

$$(9 + 14k, -12 - 19k) \quad \text{with } k \in \mathbb{Z}$$

by Proposition 2.15.

▹ Let $(x, y) \in \mathbb{N}^2$ be a solution of the second equation and set $d = (x, y)$ and $x = dx'$ and $y = dy'$ so that $(x', y') = 1$. The equation is equivalent to $5d(x' + y')^2 = 147x'y'$ and hence $(x' + y')^2$ divides $147x'y'$. By Exercise 1(b), we have $((x' + y')^2, x'y') = 1$ and Theorem 2.12 implies that

$$\left(x' + y'\right)^2 \mid 147 = 3 \times 7^2$$

and therefore $x' + y' \mid 7$. Since $x' + y' > 1$, we get $x' + y' = 7$, implying that $5d = 3x'y'$ and hence $5 \mid x'y'$ by Theorem 2.12 since $(3, 5) = 1$. This implies that $(x', y') \in \{(2, 5), (5, 2)\}$ and then $d = 6$, and

$$(x, y) \in \big\{(12, 30), (30, 12)\big\}.$$

Conversely, one can check that these pairs are solutions of the equation.

▹ The system is equivalent to

$$\begin{cases} x \equiv 2 \pmod 5, \\ x \equiv 6 \pmod 7 \end{cases}$$

and by Theorem 2.27, we infer that the solution of this system is $x \equiv 27 \pmod{35}$.

6.

(a) Write $a = da'$ and $b = db'$ and thus $(a', b') = 1$. The line (OA) has equation $y = (b'/a')x$ so that a point $N\langle x, y\rangle$ is an integer point of the segment $]OA]$ if and only if $x, y \geqslant 1$, $x \leqslant a$ and $a'y = b'x$. Then $a' \mid b'x$ and Theorem 2.12 implies that $a' \mid x$. Hence the number of integer points lying on the segment $]OA]$ is equal to the number of non-zero multiples of a' which are $\leqslant a$, and this number is in turn equal to $[a/a'] = d$ by Proposition 1.11 (v).

(b) The result follows at once using Pick's formula applied to the triangle OAB with $\text{area}(OAB) = ab/2$ and $\mathcal{N}_{\partial\mathcal{P}} = a + b + d$ by the previous question.

7. The answer is "no" as can be seen with the solution $(x, y, z) = (2, 2, 2)$.

8.

(a) We have $n \equiv k \pmod 4$ with $k \in \{0, \pm 1, 2\}$ which implies that $n^2 \equiv k^2 \pmod 8$ with $k^2 \in \{0, 1, 4\}$. We infer that the sum of three squares can only be congruent to $0, 1, 2, 4, 5, 6$ modulo 8.

(b) Similarly, we have $n \equiv k \pmod 3$ with $k \in \{0, \pm 1\}$ so that $n^3 \equiv k^3 \pmod 9$ with $k^3 \in \{0, \pm 1\}$. Thus the sum of three cubes can only be congruent to $0, 1, 2, 3, 6, 7, 8$ modulo 9.

(c) Let $(x, y, z) \in \mathbb{N}^3$ be a solution. We have $x^3 + y^3 + z^3 = 2005^2 \equiv 4 \pmod 9$ contradicting the previous question. Thus the equation has no solution in $\mathbb{N}^3$.

9.

▷ First method. We use $641 = 2^4 + 5^4 = 5 \times 2^7 + 1$ giving

$$\begin{aligned} 2^{32} &= 2^4 \times 2^{28} = \left(641 - 5^4\right) \times 2^{28} \\ &= 641 \times 2^{28} - \left(5 \times 2^7\right)^4 \\ &= 641 \times 2^{28} - (641 - 1)^4 \\ &= 641 \times \left(2^{28} - 641^3 + 4 \times 641^2 - 6 \times 641 + 4\right) - 1 \end{aligned}$$

and then

$$2^{32} + 1 = 641 \times 6\,700\,417.$$

▷ Second method. We use $2^{32} + 1 = 16 \times 2^{28} + 1 = (1 + 3 \times 5) \times (2^7)^4 + 1$ and notice that $3 = 128 - 125 = 2^7 - 5^3$ so that

$$\begin{aligned} 2^{32} + 1 &= \left\{1 + 5 \times \left(2^7 - 5^3\right)\right\} \times \left(2^7\right)^4 + 1 \\ &= \left(1 + 5 \times 2^7 - 5^4\right) \times \left(2^7\right)^4 + 1 \\ &= \left(1 + 5 \times 2^7\right) \times 2^{28} + 1 - \left(5 \times 2^7\right)^4 \\ &= \left(1 + 5 \times 2^7\right) \times 2^{28} + \left\{1 - \left(5 \times 2^7\right)^2\right\}\left\{1 + \left(5 \times 2^7\right)^2\right\} \end{aligned}$$

$$
\begin{aligned}
&= \big(1+5\times 2^7\big)\times 2^{28} + \big(1+5\times 2^7\big)\big(1-5\times 2^7\big)\big(1+\big(5\times 2^7\big)^2\big)\\
&= \big(1+5\times 2^7\big)\times \big\{2^{28} + \big(1-5\times 2^7\big)\big(1+\big(5\times 2^7\big)^2\big)\big\}\\
&= 641\times 6\,700\,417.
\end{aligned}
$$

Remark Euler was the first to obtain this result, disproving the old conjecture stating that the *Fermat numbers* $F_n = 2^{2^n}+1$ are all primes. Euler proved that $641 \mid F_5$ although F_n was already known to be prime for $n \in \{0,\dots,4\}$. Currently, it is known that F_n is composite for $n \in \{5,\dots,19\}$. The largest known prime Fermat number is $F_4 = 65\,537$ and the largest known composite Fermat number is $F_{23\,471}$. The Fermat number whose complete prime factorization is known are F_5, F_6, F_7, F_8, F_9 and F_{11}. The smallest Fermat number for which no prime factor is known is F_{14}. Finally, the following questions are still open:

1. Do there exist infinitely many prime Fermat numbers?
2. Do there exist infinitely many composite Fermat numbers?
3. Is every Fermat number squarefree?

10. Let us first show that $x > y$. Indeed, if $x = y$, then $a = b$ which is impossible by assumption. If $x < y$, then we have

$$0 < by^2 - ax^2 = x - y < 0$$

giving a contradiction.

(a) Let us notice that

$$ax^2 + x = by^2 + y \quad\Longleftrightarrow\quad x - y = by^2 - ax^2$$

and hence

$$
\begin{aligned}
(x-y)\big\{1+b(x+y)\big\} &= x - y + b\big(x^2-y^2\big) = by^2 - ax^2 + bx^2 - by^2\\
&= (b-a)x^2 = (mx)^2.
\end{aligned}
$$

The second identity is similar.

(b) Define $d = (x, y)$ and $D = (b-a, x-y)$.

▹ Set $x - y = DA$ and $m^2 = DB$ with $(A, B) = 1$. By the previous question, we have

$$A\big(1+b(x+y)\big) = Bx^2 \quad\text{and}\quad A\big(1+a(x+y)\big) = By^2$$

so that $A \mid (Bx^2, By^2) = Bd^2$. Since $(A, B) = 1$, Theorem 2.12 implies that $A \mid d^2$.

▹ On the other hand, since $d^2 \mid x^2$ and $x^2 \mid A(1+b(x+y))$, we deduce that

$$d^2 \mid A\big(1+b(x+y)\big).$$

Suppose that $(d^2, 1 + b(x + y)) > 1$ and let p be a prime factor of this gcd. Hence p divides x, y and $1 + b(x + y)$, so that p must divide $1 + b(x + y) - b(x + y) = 1$ which is impossible. Hence $(d^2, 1 + b(x + y)) = 1$ and using Theorem 2.12 we get $d^2 \mid A$.

▷ We thus have $d^2 = A$ and then

$$x - y = DA = Dd^2 = (b - a, x - y) \times (x, y)^2$$

as required.

(c) $x - y$ is not always a square as can be seen by taking $(a, b, x, y) = (109, 334, 7, 4)$ or $(a, b, x, y) = (3, 199, 8, 1)$.

▷ Suppose that $b = a + 1$. Hence $(b - a, x - y) = 1$ and then $x - y = (x, y)^2$.

▷ Now suppose that there exist integers $m \geqslant 1$ and $n \geqslant 2$ such that $a = m^2(n - 1)$ and $b = m^2 n$. Then

$$x - y = by^2 - ax^2 = m^2\big(ny^2 - (n - 1)x^2\big)$$

and then $m^2 = b - a$ divides $x - y$ so that $(b - a, x - y) = b - a = m^2$ and hence $x - y = (md)^2$.

11.

(a) Since $(a, b) = 1$, there exist $U, V \in \mathbb{Z}$ such that $aU + bV = 1$ by Corollary 2.6. Since $a, b \in \mathbb{N}$, we have $UV \leqslant 0$, and without loss of generality, one may assume that $U \leqslant 0$ and $V \geqslant 0$. Setting $u = -U$ and $v = V$, we get two non-negative integers u, v such that $-au + bv = 1$.

By Proposition 2.15, the solutions of the equation $ax + by = n$ are given by the pairs

$$(-un + bk, vn - ak) \quad \text{with } k \in \mathbb{Z}$$

and the non-negative solutions are obtained by solving the inequalities $-un + bk \geqslant 0$ and $vn - ak \geqslant 0$ implying

$$\frac{un}{b} \leqslant k \leqslant \frac{vn}{a}.$$

Hence $\mathcal{D}_2(n)$ is equal to the number of integers in the interval $[un/b, vn/a]$ so that

$$\mathcal{D}_2(n) = \left[\frac{vn}{a} - \frac{un}{b}\right] + r$$

and we conclude the proof with

$$\frac{vn}{a} - \frac{un}{b} = \frac{n(-au + bv)}{ab} = \frac{n}{ab}.$$

(b) Using Theorem 2.31 we get

$$r=0 \iff \left[\frac{n}{ab}\right]=\frac{n}{ab}-1+\frac{aa'+bb'}{ab} \iff \left\{\frac{n}{ab}\right\}=1-\frac{aa'+bb'}{ab}$$

which is equivalent to

$$0\leqslant 1-\frac{aa'+bb'}{ab}<1$$

giving the asserted result. The case $r=1$ is similar.

12.

(a) The first identity is trivial if $a=1$. If $a\geqslant 2$, it follows from the logarithmic derivative of (2.9) and taking $x=1$. For the second identity, we have

$$\prod_{\substack{j=1\\ j\neq k}}^{a}\frac{1}{e_a(k)-e_a(j)}=e_a\big(-k(a-1)\big)\prod_{\substack{j=1\\ j\neq k}}^{a}\frac{1}{1-e_a(j-k)}$$

$$=e_a(k)\prod_{h=1}^{a-1}\frac{1}{1-e_a(h)}=\frac{e_a(k)}{a}$$

where we used (2.9) with $x=1$.

(b) By (2.8), we infer that $F(z)=z^{n+1}f(z)$ is the generating function of $\mathcal{D}_2(n)$. Therefore

$$f(z)=\frac{1}{z^{n+1}}\sum_{k=0}^{\infty}\mathcal{D}_2(k)z^k=\frac{\mathcal{D}_2(n)}{z}+\sum_{\substack{k=0\\ k\neq n}}^{\infty}\mathcal{D}_2(k)z^{k-n-1}$$

so that

$$\operatorname*{Res}_{z=0} f(z)=\mathcal{D}_2(n).$$

The non-zero poles of f are respectively 1 (order 2), $e_a(k)$ (order 1) for all $1\leqslant k\leqslant a-1$ and $e_b(k)$ (order 1) for all $1\leqslant k\leqslant b-1$. Since

$$z^a-1=\prod_{j=1}^{a}\big(z-e_a(j)\big)\quad\text{and}\quad z^b-1=\prod_{j=1}^{b}\big(z-e_b(j)\big)$$

we get

$$\operatorname*{Res}_{z=1} f(z)=G'(1)$$

where

$$G(z)=(z-1)^2f(z)=z^{-n-1}\prod_{k=1}^{a-1}\big(z-e_a(k)\big)^{-1}\prod_{k=1}^{b-1}\big(z-e_b(k)\big)^{-1}$$

so that

$$\frac{G'}{G}(z) = -\frac{n+1}{z} - \sum_{k=1}^{a-1} \frac{1}{z - e_a(k)} - \sum_{k=1}^{b-1} \frac{1}{z - e_b(k)}.$$

Now (2.9) with $x = 1$ implies that $G(1) = (ab)^{-1}$ and then we get using the previous question

$$\begin{aligned}\operatorname*{Res}_{z=1} f(z) &= \frac{1}{ab}\left\{-n-1-\sum_{k=1}^{a-1}\frac{1}{1-e_a(k)} - \sum_{k=1}^{b-1}\frac{1}{1-e_b(k)}\right\}\\ &= \frac{1}{ab}\left\{-n-1-\frac{a-1}{2}-\frac{b-1}{2}\right\}\\ &= -\frac{a+b+2n}{2ab}.\end{aligned}$$

Finally, for all $k \in \{1, \dots, a-1\}$, we have using the previous question

$$\begin{aligned}\operatorname*{Res}_{z=e_a(k)} f(z) &= \frac{1}{e_a(kb)-1} \times \frac{1}{e_a(k(n+1))} \times \prod_{\substack{j=1\\ j\neq k}}^{a} \frac{1}{e_a(k) - e_a(j)}\\ &= \frac{1}{a\, e_a(kn)(e_a(kb)-1)}\end{aligned}$$

and similarly

$$\operatorname*{Res}_{z=e_b(k)} f(z) = \frac{1}{b\, e_b(kn)(e_b(ka)-1)}$$

for all $k \in \{1, \dots, b-1\}$.

(c) Since $\lim_{|z|\to\infty} z f(z) = 0$, Jordan's (first) lemma implies that

$$\lim_{R\to\infty} \frac{1}{2\pi i} \int_{|z|=R} f(z)\, \mathrm{d}z = 0$$

and Cauchy's residue theorem then gives

$$\mathcal{D}_2(n) = \frac{a+b+2n}{2ab} + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{e_a(kn)(1-e_a(kb))} + \frac{1}{b}\sum_{k=1}^{b-1} \frac{1}{e_b(kn)(1-e_b(ka))} \tag{A.1}$$

which is similar to (2.4).

(d) If $b = 1$, then the equation is $ax + y = n$ so that $n/a \geqslant x$ and then

$$\mathcal{D}_2(n) = \left|\left[0, \frac{n}{a}\right] \cap \mathbb{Z}\right| = \left[\frac{n}{a}\right] + 1 = \frac{n}{a} - \left\{\frac{n}{a}\right\} + 1.$$

Replacing in (A.1) gives

$$\frac{n}{a} - \left\{\frac{n}{a}\right\} + 1 = \frac{a+1+2n}{2a} + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{e_a(kn)(1-e_a(k))}$$

so that

$$\frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{e_a(kn)(1-e_a(k))} = \frac{a-1}{2a} - \left\{\frac{n}{a}\right\}.$$

(e) By above we get

$$\frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{e_a(kn)(1-e_a(kb))} = \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{e_a(k\overline{b}n)(1-e_a(k))} = \frac{a-1}{2a} - \left\{\frac{n\overline{b}}{a}\right\}$$

and similarly

$$\frac{1}{b}\sum_{k=1}^{b-1} \frac{1}{e_b(kn)(1-e_b(ka))} = \frac{b-1}{2b} - \left\{\frac{n\overline{a}}{b}\right\}$$

and therefore

$$\begin{aligned}\mathcal{D}_2(n) &= \frac{a+b+2n}{2ab} + \frac{a-1}{2a} - \left\{\frac{n\overline{b}}{a}\right\} + \frac{b-1}{2b} - \left\{\frac{n\overline{a}}{b}\right\} \\ &= \frac{n}{ab} + 1 - \left\{\frac{n\overline{b}}{a}\right\} - \left\{\frac{n\overline{a}}{b}\right\}.\end{aligned}$$

A.3 Chapter 3

1. Let $A = 3^{4^5} + 4^{5^6}$. Using Sophie Germain's identity

$$m^4 + 4n^4 = \left(m^2 + 2mn + 2n^2\right)\left(m^2 - 2mn + 2n^2\right)$$

with $m = 3^{4^4}$ and $n = 4^{3906}$, we get $A = BC$ with $B > 1$ and $C > 1$, implying that A is composite.

2. The inequality may be numerically checked for all $n \in \{33, \ldots, 65\}$ so that we suppose that $n \geqslant 66$. Among the integers $\{2, \ldots, n\}$, we remove the $[n/2] - 1$ even integers $\neq 2$ and the $[n/3] - 1$ integers $\neq 3$ multiples of 3. However, the $[n/6]$

integers multiples of 6 have been removed twice, and removing the numbers 25, 35, 55 and 65, we get

$$\pi(n) \leqslant n - \left(\left[\frac{n}{2}\right] - 1\right) - \left(\left[\frac{n}{3}\right] - 1\right) + \left[\frac{n}{6}\right] - 4$$

and the inequalities $x - 1 < [x] \leqslant x$ imply the asserted result.

3. This sequence has $6k - 5$ integers. Furthermore, if $n \geqslant 6$ is even, then $n^2 + 2$ is also even and then is composite. Similarly, if $n \equiv \pm 1 \pmod 6$, then $n^2 + 2 \equiv 3 \pmod 6$ and $n^2 + 2$ is odd and composite. We infer that the number of primes in the sequence is

$$\leqslant 6k - 5 - (3k - 2) - 2(k - 1) = k - 1 < k.$$

4.

(a) Let $N \geqslant 2$ be an integer. Using Theorem 1.14 (ii) and a weak version of Corollary 3.50, we get

$$\sum_{p \leqslant N} \frac{1}{p \log p} = \frac{1}{\log N} \sum_{p \leqslant N} \frac{1}{p} + \int_2^N \frac{1}{t(\log t)^2} \left(\sum_{p \leqslant t} \frac{1}{p}\right) \mathrm{d}t$$

$$= \frac{\log\log N + O(1)}{\log N} + \int_2^N \frac{\log\log t + O(1)}{t(\log t)^2}\, \mathrm{d}t = O(1)$$

implying the asserted result.

(b) The sum is clearly convergent. By Exercise 7 in Chap. 1 and Corollary 3.98, we have[1]

$$\sum_p \frac{\log p}{p^2} = \left(\sum_{p \leqslant 100} + \sum_{p > 100}\right) \frac{\log p}{p^2}$$

$$= \sum_{p \leqslant 100} \frac{\log p}{p^2} - \frac{\theta(100)}{10^4} + 2\int_{100}^\infty \frac{\theta(t)}{t^3}\, \mathrm{d}t$$

$$< 0.484 - 0.0075 + 2.000\,162 \int_{100}^\infty \frac{\mathrm{d}t}{t^2} < \frac{1}{2}$$

as required.

[1] Exercise 7 in Chap. 1 is used in the following form. If $f \in C^1[2, +\infty[$ such that $f(x)\theta(x)/\log x \longrightarrow 0$ as $x \longrightarrow \infty$, then

$$\sum_{p > x} f(p) = -\frac{f(x)\theta(x)}{\log x} - \int_x^\infty \theta(t) \frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{f(t)}{\log t}\right) \mathrm{d}t.$$

5. By Theorem 3.37 we get

$$v_p\big\{(pa)!\big\} = \sum_{k=1}^{\infty}\left[\frac{a}{p^{k-1}}\right] = a + v_p(a!)$$

so that

$$\begin{aligned} v_p\left\{\binom{pa}{pb}\right\} &= v_p\big\{(pa)!\big\} - v_p\big\{(pb)!\big\} - v_p\big\{\big(p(a-b)\big)!\big\} \\ &= v_p(a!) - v_p(b!) - v_p\big((a-b)!\big) = v_p\left\{\binom{a}{b}\right\} \end{aligned}$$

as required.

6. If (x, y) is a solution, set $d = (x, y)$ and write $x = dx'$ and $y = dy'$ so that $(x', y') = 1$. The equation is equivalent to $dx'y' = p(x' + y')$ and hence $x'y'$ divides $p(x' + y')$. Since $(x' + y', x'y') = 1$ by Exercise 1 in Chap. 2, we infer that $x'y' \mid p$ by Theorem 2.12, and thus

$$x'y' = 1 \quad \text{or} \quad x'y' = p$$

and hence $(x', y') \in \{(1, 1), (1, p), (p, 1)\}$. This implies that $d = 2p$ if $(x', y') = (1, 1)$ and $d = p + 1$ otherwise, so that we get

$$(x, y) \in \big\{(2p, 2p),\ \big(p + 1, p(p + 1)\big),\ \big(p(p + 1), p + 1\big)\big\}.$$

Conversely, one easily checks that these pairs are solutions.

7. 2 and 3 are not solutions, but 5 is a solution. Suppose now that $p \geqslant 7$ is prime. We then have $(p - 1)(p + 1) = 2^3 \times q$ with $q \geqslant 7$ prime. This implies that either q divides $p - 1$ or q divides $p + 1$ by Lemma 3.4.

▹ If $p - 1 = hq$ for some $h \in \mathbb{N}$ then $8 = h(hq + 2)$, so that $h \mid 8$. We then get

h	1	2	4	8
q	6	1	0	$\notin \mathbb{N}$

and since q is prime, we see that this case does not provide any solution.

▹ Similarly, if $p + 1 = kq$ then $8 = k(kq - 2)$, so that $k \mid 8$. We then get

k	1	2	4	8
q	10	3	1	$\notin \mathbb{N}$

and since q is prime, $q = 3$ is the only admissible value, giving $p = 5$.

8. Let (x, y, z) be a solution. Note that

$$\begin{aligned} x+y+z+xy+yz+zx+xyz+1 &= (x+y+xy+1)+z(x+y+xy+1) \\ &= (x+y+xy+1)(z+1) \\ &= (x+1)(y+1)(z+1) \end{aligned}$$

so that the equation is equivalent to $(x+1)(y+1)(z+1) = 2010 = 2 \times 3 \times 5 \times 67$. Furthermore, since $x < y < z$, this implies that $(x+1)^3 < 2010$ so that $x \leqslant 11$. We deduce that $x \in \{2, 4, 5, 9\}$ and we obtain the triples

$$(2, 4, 133),\ (2, 9, 66) \text{ and } (4, 5, 66).$$

Conversely, one easily checks that these triples are solutions.

9. Observe first that $2 \nmid a$ and $5 \nmid a$ since $(a, 10) = 1$.

(a) Since a is odd, we have $a^8 \equiv 1 \pmod 2$. Furthermore, since $5 \nmid a$, Fermat's little theorem implies that $a^4 \equiv 1 \pmod 5$ and hence $a^8 \equiv 1 \pmod 5$. Finally, since $(2, 5) = 1$, one may apply Proposition 2.13 (vi) which gives $a^8 \equiv 1 \pmod{10}$.

The congruence $a^{8\times 10^k} \equiv 1 \pmod{10^{k+1}}$ can be proved by induction as in Exercise 10.

Taking $k = 8$ and multiplying by a gives $a^{800\,000\,001} \equiv a \pmod{10^9}$.

(b) Since $(123\,456\,789, 10) = 1$, we get by the previous question

$$123\,456\,789^{800\,000\,001} \equiv 123\,456\,789 \pmod{10^9}$$

so that if $x = 123\,456\,789^{266\,666\,667}$, then $x^3 \equiv 123\,456\,789 \pmod{10^9}$ as required.

10. We prove the congruence by induction, the case $k = 0$ being clear using Fermat's little theorem. Assume that the result is true for some $k \geqslant 0$. By Lemma 1.6, we have

$$a^{p^{k+2}} - a^{p^{k+1}} = \left(a^{p^{k+1}} - a^{p^k}\right) \sum_{j=1}^{p} a^{j \times p^k (p-1)}.$$

By induction hypothesis, we have $a^{p^{k+1}} - a^{p^k} \equiv 0 \pmod{p^{k+1}}$ and since $a^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem, we infer that

$$\sum_{j=1}^{p} a^{j \times p^k (p-1)} \equiv p \equiv 0 \pmod p$$

so that $p \times p^{k+1} = p^{k+2}$ divides $a^{p^{k+2}} - a^{p^{k+1}}$, completing the proof.

11.

(a) If $n \equiv 1 \pmod p$, then $0 \equiv n^2 + n + 1 \equiv 3 \pmod p$ which is impossible since $p \geqslant 5$.

If $n^2 \equiv 1 \pmod p$, then $n \equiv \pm 1 \pmod p$ by Lemma 3.4. Since $n \not\equiv 1 \pmod p$, we obtain $n \equiv -1 \pmod p$ and then $0 \equiv n^2 + n + 1 \equiv 1 \pmod p$ giving a contradiction again.

Since $n^3 - 1 = (n-1)(n^2 + n + 1)$, we deduce that $n^3 \equiv 1 \pmod p$ and hence $\operatorname{ord}_p(n) = 3$.

We infer that $3 \mid (p-1)$ by (3.4). If $p = 1 + 3k$ for some even integer k, then $p \equiv 1 \pmod 6$. If $p = 1 + 3(1 + 2h) = 2(2 + 3h)$ for some $h \in \mathbb{N}$, then p is composite, giving a contradiction. Hence $p \equiv 1 \pmod 6$.

(b) Assume that the set of primes of the form $p \equiv 1 \pmod 6$ is finite and write all these primes as

$$p_1 = 7 < p_2 < \cdots < p_m.$$

Set $M = (p_1 \cdots p_m)^2 + p_1 \cdots p_m + 1$ supposed to be composite without loss of generality. Using the previous question, the prime factors of M are all congruent to 1 modulo 6 and then there exists an index $i \in \{1, \ldots, m\}$ such that $p_i \mid M$, giving a contradiction since we also have $p_i \mid (M-1)$.

12. Let $p \leqslant n$ be a prime number and set $N = [\log n / \log p]$. By Theorem 3.37 and the inequalities $x - 1 < [x] \leqslant x$, we get

$$n \sum_{k=1}^{N} \frac{1}{p^k} - N < v_p(n!) \leqslant n \sum_{k=1}^{N} \frac{1}{p^k}$$

so that

$$\frac{n}{p-1}\left(1 - \frac{1}{p^N}\right) - N < v_p(n!) \leqslant \frac{n}{p-1}\left(1 - \frac{1}{p^N}\right)$$

and using $\log n / \log p - 1 < N \leqslant \log n / \log p$ gives

$$\frac{n}{p-1}\left(1 - \frac{p}{n}\right) - \frac{\log n}{\log p} < v_p(n!) \leqslant \frac{n}{p-1}\left(1 - \frac{1}{n}\right)$$

implying the asserted inequalities. This also may be written in the form

$$\frac{1}{(p-1)\log n} \leqslant \frac{\frac{n}{p-1} - v_p(n!)}{\log n} < \frac{1}{\log p} + \frac{p}{(p-1)\log n}$$

and since $p \geqslant 2$, we get

$$0 < \frac{\frac{n}{p-1} - v_p(n!)}{\log n} < \frac{1}{\log 2} + \frac{2}{\log n} = O(1)$$

as required.

Remark Used with $p = 5$, this asymptotic formula shows that, if n is sufficiently large, the decimal expansion of $n!$ ends up with approximately $n/4$ zeros.

13. Since a square is congruent to 0 or 1 modulo 4, we see that $a^2 - b^2$ cannot be congruent to 2 modulo 4. Conversely, let $n \not\equiv 2 \pmod 4$. Then either n is odd or it is a multiple of 4. If n is odd, then

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$$

is a difference of two squares. If $4 \mid n$, then

$$n = \left(\frac{n}{4} + 1\right)^2 - \left(\frac{n}{4} - 1\right)^2$$

is also a difference of two squares. Finally, if $n \geqslant 4$, then $n! \equiv 0 \pmod 4$ and hence $n!$ can be expressed as a difference of two squares in this case. For instance, we have $13! = 78\,912^2 - 288^2 = 112\,296^2 - 79\,896^2$. Furthermore, $2! \equiv 2 \pmod 4$ and $3! \equiv 2 \pmod 4$ so that neither $2!$ nor $3!$ can be expressed as a difference of two squares.

14. The proof is the same as in Proposition 7.28. Suppose that P is not irreducible over $\mathbb{Z}$. Then $P = QR$ for some $Q, R \in \mathbb{Z}[X]$ such that $Q, R \neq \pm 1$. Set $d = \deg Q$ and $\delta = \deg R$ so that $n = d + \delta$. Since $Q \neq \pm 1$, each polynomial $Q \pm 1$ has at most d roots. Therefore, there are at most d integers m such that $Q(m) = 1$ and at most d integers m such that $Q(m) = -1$, so that there are at most $2d$ integers m such that $Q(m) = \pm 1$. Similarly, there are at most 2δ integers m such that $R(m) = \pm 1$. Now if $|P(m)| = |Q(m)| \times |R(m)|$ is prime, then either $Q(m) = \pm 1$ or $R(m) = \pm 1$. We infer that there are at most $2d + 2\delta = 2n$ integers m such that $|P(m)|$ is prime, as required.

The polynomials P_1 and P_2 are both irreducible over $\mathbb{Z}$ by applying this criterion respectively with $m \in \{2, 3, 4, 5, 6, 9, 11, 12, 15\}$ and $m \in \{3, 5, 8, 9, 12, 14, 15, 17, 21\}$.

15. Since $(7, 15) = 1$, the sequence $7 - 15k$ contains infinitely many primes by Theorem 3.63. Now $7 - 15k + 2 = 3(3 + 5k)$ and $7 - 15k - 2 = 5(1 + 3k)$ and hence these two numbers are composite. We deduce that the primes contained in the sequence $7 - 15k$ cannot lie in a pair of twin primes.

16. The sequence (d_j) of the positive divisors of n is strictly increasing so that $d_j \geqslant j$ for all j. Note also that $d_j d_{k+1-j} = n$ for all $j \in \{1, \ldots, k\}$ so that

$$d_j = \frac{n}{d_{k+1-j}} \leqslant \frac{n}{k+1-j}$$

and hence

$$\begin{aligned}\sum_{j=2}^{k} d_{j-1}d_j &\leqslant \sum_{j=2}^{k} \frac{n^2}{(k+2-j)(k+1-j)} \\ &= n^2 \sum_{j=2}^{k} \left(\frac{1}{k+1-j} - \frac{1}{k+2-j} \right) \\ &= n^2 \left(1 - \frac{1}{k} \right) < n^2.\end{aligned}$$

17.

(a) Since $P(a/b) = 0$ we get

$$c_n \left(\frac{a}{b} \right)^n + c_{n-1} \left(\frac{a}{b} \right)^{n-1} + \cdots + c_1 \left(\frac{a}{b} \right) + c_0 = 0$$

so that

$$c_n a^n + c_{n-1} a^{n-1} b + \cdots + c_1 a b^{n-1} + c_0 b^n = 0. \tag{A.2}$$

This may be written as $c_0 b^n = ha$ with

$$h = -c_n a^{n-1} - c_{n-1} a^{n-2} b - \cdots - c_1 b^{n-1} \in \mathbb{Z}$$

so that $a \mid c_0 b^n$ and since $(a, b) = 1$, Theorem 2.12 implies that $a \mid c_0$.

Similarly, (A.2) may be written as $c_n a^n = kb$ with

$$k = -c_{n-1} a^{n-1} - \cdots - c_1 a b^{n-2} - c_0 b^{n-1} \in \mathbb{Z}$$

and we conclude as above.

(b) By the previous question, if a/b is a root of a monic polynomial, then $b = \pm 1$.

(c) The roots of $X^2 - p$ are $\pm\sqrt{p}$. By above, these roots are either integer or irrational, and since p is prime, we have $\sqrt{p} \notin \mathbb{Z}$.

18.

Part A.

(a) This follows easily from the fact that a square is congruent to 0 or 1 modulo 4 and that p is odd.

(b) Using Theorem 3.19, we have

$$\begin{aligned}-1 \equiv (p-1)! &\equiv 1 \times 2 \times \cdots \times \frac{p-1}{2} \times \frac{p+1}{2} \times \cdots \times (p-1) \\ &\equiv 1 \times 2 \times \cdots \times \frac{p-1}{2} \times \left(-\frac{p-1}{2} \right) \times \cdots (-2) \times (-1)\end{aligned}$$

$$\equiv (-1)^{(p-1)/2}\left\{\left(\frac{p-1}{2}\right)!\right\}^2$$

$$\equiv \left\{\left(\frac{p-1}{2}\right)!\right\}^2 \equiv x^2 \pmod{p}.$$

(c) Using Thue's lemma, there exist two integers u, v such that

$$\begin{cases} xu \equiv v \pmod{p}, \\ 1 \leqslant |u| < \sqrt{p}, \\ 1 \leqslant |v| < \sqrt{p}. \end{cases}$$

Hence

$$u^2 + v^2 \equiv u^2 + x^2u^2 \equiv u^2\big(x^2+1\big) \equiv 0 \pmod{p}$$

so that $p \mid (u^2+v^2)$, and we also have

$$2 \leqslant u^2 + v^2 < 2p$$

implying that $p = u^2 + v^2$.

Remark We have then proved that, if $p \equiv 1 \pmod 4$, then -1 is quadratic residue modulo p. This is also true for $p = 2$ since $-1 \equiv 1^2 \pmod 2$. By Example 3.35, the converse is also true so that we may state the following result.

-1 *is quadratic residue modulo* p *if and only if either* $p = 2$ *or* $p \equiv 1 \pmod 4$.

Part B.

(a) The sequence (r_n) of the remainders is a strictly decreasing sequence of non-negative integers and since $p > \sqrt{p} > 1$, we infer that there exists an index k such that $r_{k-1} > \sqrt{p} > r_k$.

(b) By Exercise 3 in Chap. 2, we have $p = |t_k| r_{k-1} + |t_{k-1}| r_k$ and hence

$$p \geqslant |t_k| r_{k-1} > |t_k| \sqrt{p}$$

so that $|t_k| < \sqrt{p}$. Since $r_k = s_k p + t_k x$, we get $r_k \equiv t_k x \pmod p$ and hence the pair (t_k, r_k) satisfies the conditions of Thue's lemma.

(c) 9733 is prime and satisfies $9733 \equiv 1 \pmod 4$. By above, we have $9733 = r_k^2 + t_k^2$ where the (r_n) are the successive remainders in the Euclidean division of 9733 by $x = 7024$, and the index k is given by $r_{k-1} > \sqrt{9733} \approx 98.7 > r_k$. Using Exercise 3 in Chap. 2, we get

k	1	2	3	4	5	6
r_k	7024	2709	1606	1103	503	97
q_k	1	2	1	1	2	5
t_k	1	−1	3	−4	7	−18

so that $9733 = r_6^2 + t_6^2 = 97^2 + 18^2$.

19. Using Lemma 3.42 and Theorem 3.49, we get

$$\begin{aligned}\prod_p p^{[n/p]} &= \prod_{p\leqslant n} p^{[n/p]} = \exp\biggl\{\sum_{p\leqslant n}\biggl[\frac{n}{p}\biggr]\log p\biggr\}\\ &= \exp\biggl\{n\sum_{p\leqslant n}\frac{\log p}{p} + O\bigl(\theta(n)\bigr)\biggr\}\\ &= \exp\bigl\{n\log n + O(n)\bigr\}.\end{aligned}$$

20. Let $\sigma > 1$. We have

$$\begin{aligned}N^{\sigma-1}\sum_{n=N}^{\infty}\frac{1}{n^\sigma} &= N^{\sigma-1}\sum_{j=1}^{\infty}\sum_{n=jN}^{(j+1)N-1}\frac{1}{n^\sigma}\\ &= \frac{1}{N}\sum_{j=1}^{\infty}\sum_{n=jN}^{(j+1)N-1}\biggl(\frac{N}{n}\biggr)^\sigma\\ &\leqslant \frac{1}{N}\sum_{j=1}^{\infty}\biggl(\frac{N}{jN}\biggr)^\sigma\sum_{n=jN}^{(j+1)N-1}1 = \zeta(\sigma).\end{aligned}$$

The second inequality is similar.

21.

(a) Set $d = (m,n)$ and $d^* = (m,n)^*$. Since $d^* \mid m$ and $d^* \mid n$, we have $d^* \mid d$. Now set

$$\begin{aligned}m &= dm' = d^*m'',\\ n &= dn' = d^*n''\end{aligned}$$

with $(m',n') = (d^*,m'') = (d^*,n'') = 1$. Thus $m'n'' = m''n'$ and then $m' \mid n'm''$ hence $m' \mid m''$ using Theorem 2.12. Write $m'' = m_1m'$. Since $(d^*,m'') = 1$, we have $(d^*,m_1) = 1$. Thus, we have $dm' = d^*m'' = d^*m_1m'$, and then $d = d^*m_1$ with $(d^*,m_1) = 1$, showing that d^* is a unitary divisor of d.

(b) Follows at once from the fact that the unitary divisors of p^e are 1 and p^e.

(c) If either $f_i = 0$ or $f_i = e_i$ then $\min(f_i, e_i - f_i) = 0$ and then

$$(d, n/d) = p_1^{\min(f_1,e_1-f_1)}\cdots p_r^{\min(f_r,e_r-f_r)} = 1$$

so that d is a unitary divisor of n. Conversely, if d is a unitary divisor of n, then $(d,n/d) = 1$ so that $\min(f_i, e_i - f_i) = 0$ for all $i = 1,\dots,r$ which implies that either $f_i = 0$ or $f_i = e_i$.

Let $n = p_1^{e_1}\cdots p_r^{e_r}$. By above, there are exactly two possible choices for the valuation of a prime p_i. Thus, the number of unitary divisors of n is equal to $2^{\omega(n)}$.

Example

n	Unitary divisors
$6615 = 2^4 \times 3^3 \times 7$	$1, 5, 27, 49, 135, 245, 1323, 6615$
$3024 = 3^3 \times 5 \times 7^2$	$1, 7, 16, 27, 112, 189, 432, 3024$

(d) Let $n = p_1^{e_1} \cdots p_r^{e_r}$ and $m = p_1^{f_1} \cdots p_r^{f_r}$, $d^* = (m, n)^*$ and set $\delta = p_1^{g_1} \cdots p_r^{g_r}$ where g_i are given in the exercise. By the previous question, δ is a unitary common divisor of m and n, and then $\delta \leqslant d^*$. Conversely, we have by above $d^* = p_1^{h_1} \cdots p_r^{h_r}$ where either $h_i = 0$ or $h_i = \min(e_i, f_i)$, and then $d^* \leqslant \delta$.

Example $(6615, 3024)^* = 2^0 \times 3^3 \times 5^0 \times 7^0 = 27$.

A.4 Chapter 4

1.

(a) To each divisor d of n corresponds a unique divisor d' such that $dd' = n$. Hence either d or d' must be $\leqslant \sqrt{n}$ so that

$$\tau(n) \leqslant 2 \sum_{\substack{d|n \\ d \leqslant \sqrt{n}}} 1 \leqslant 2\sqrt{n}.$$

(b) By Example 4.8, we have $\sigma = \mathbf{1} \star \mathrm{Id}$ and hence

$$\sigma(n) = (\mathbf{1} \star \mathrm{Id})(n) = \sum_{d|n} \frac{n}{d}.$$

Now let $t \in [1, n]$ be a parameter at our disposal and write

$$\sum_{d|n} \frac{1}{d} = \sum_{\substack{d|n \\ d \leqslant t}} \frac{1}{d} + \sum_{\substack{d|n \\ d > t}} \frac{1}{d} \leqslant \sum_{d \leqslant t} \frac{1}{d} + \frac{\tau(n)}{t}.$$

Now using the previous question we get

$$\sum_{d|n} \frac{1}{d} \leqslant \log t + 1 + \frac{2\sqrt{n}}{t}$$

and choosing $t = 2\sqrt{n}$ implies the asserted result.

(c) Since n is composite, it has a prime factor q such that $q \leqslant \sqrt{n}$ by Proposition 3.1 and hence

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \leqslant n\left(1 - \frac{1}{q}\right) \leqslant n\left(1 - \frac{1}{\sqrt{n}}\right)$$

as required.

2. The following ideas are due to Pólya (see [HW38] for instance). Fix a small real number $\varepsilon > 0$. By assumption, the product

$$\prod_{\substack{p^\alpha \\ |f(p^\alpha)| \geqslant 1}} f\left(p^\alpha\right)$$

is finite and set M its value. Furthermore, except for finitely many integers, each integer n has at least a prime power p^A such that

$$\left|f\left(p^A\right)\right| < \frac{\varepsilon}{|M|}.$$

Thus

$$\begin{aligned} |f(n)| &= \left|f\left(p_1^{\alpha_1} \cdots p^A \cdots\right)\right| \\ &= \left|f\left(p_1^{\alpha_1}\right)\right| \left|f\left(p_2^{\alpha_2}\right)\right| \cdots \left|f\left(p^A\right)\right| \cdots \\ &< |M| \times \frac{\varepsilon}{|M|} = \varepsilon. \end{aligned}$$

This implies the asserted result since ε may be as small as we want. We apply now this result to the positive multiplicative function

$$f(n) = \frac{\tau(n)}{n^\varepsilon}.$$

In view of the inequality

$$\frac{\alpha+1}{p^{\varepsilon\alpha}} \leqslant \frac{2(1+\log p^\alpha)}{p^{\varepsilon\alpha}} \underset{p^\alpha \to \infty}{\longrightarrow} 0$$

we get

$$\lim_{p^\alpha \to \infty} f\left(p^\alpha\right) = \lim_{p^\alpha \to \infty} \frac{\alpha+1}{p^{\varepsilon\alpha}} = 0$$

and hence $\tau(n) = O(n^\varepsilon)$.

3. The method is similar for the four identities, this is why we only give the details for the first one.

We have to show that $\tau^3 \star \mathbf{1} = (\tau \star \mathbf{1})^2$. As in Example 4.11, we need to verify this identity only for prime powers. Using the well-known identity

$$\sum_{j=0}^{N} j^3 = \left(\sum_{j=0}^{N} j\right)^2$$

we get

$$\big(\tau^3 \star \mathbf{1}\big)\big(p^\alpha\big) = \sum_{j=0}^{\alpha} (j+1)^3 = \left(\sum_{j=0}^{\alpha} (j+1)\right)^2 = (\tau \star \mathbf{1})^2\big(p^\alpha\big).$$

4.

(a) We make use of the convolution identity $\Lambda_j = \log^j \star \mu$ and, by the Möbius inversion formula, we also have $\log^j = \Lambda_j \star \mathbf{1}$ so that

$$\begin{aligned}\Lambda_k(n) &= \sum_{d|n} \mu(d) \log^k(n/d) = \sum_{d|n} \mu(d) \log^{k-1}(n/d) \log(n/d) \\ &= \log n \sum_{d|n} \mu(d) \log^{k-1}(n/d) - \sum_{d|n} \mu(d) \log d \log^{k-1}(n/d) \\ &= \Lambda_{k-1}(n) \log n - \big(\log^{k-1} \star \mu \log\big)(n)\end{aligned}$$

and the identity $\mu \star \mathbf{1} = e_1$ together with the use of Lemma 4.9 implies that

$$\log^{k-1} \star \mu \log = \big(\log^{k-1} \star \mu\big) \star (\mathbf{1} \star \mu \log) = -(\Lambda_{k-1} \star \Lambda)$$

giving the asserted identity.

(b) We proceed as in Theorem 4.10. Since $(m, n) = 1$ and using Newton's formula, we get

$$\begin{aligned}\Lambda_k(mn) &= \sum_{a|m} \sum_{b|n} \mu(ab) \log^k\left(\frac{mn}{ab}\right) \\ &= \sum_{a|m} \mu(a) \sum_{b|n} \mu(b) \big(\log(m/a) + \log(n/b)\big)^k \\ &= \sum_{a|m} \mu(a) \sum_{b|n} \mu(b) \sum_{j=0}^{k} \binom{k}{j} \log^j(m/a) \log^{k-j}(n/b) \\ &= \sum_{j=0}^{k} \binom{k}{j} \left(\sum_{a|m} \mu(a) \log^j(m/a)\right) \left(\sum_{b|n} \mu(b) \log^{k-j}(n/b)\right) \\ &= \sum_{j=0}^{k} \binom{k}{j} \Lambda_j(m) \Lambda_{k-j}(n).\end{aligned}$$

5. Define the multiplicative function f by $f(1) = 1$ and, for all prime powers

$$f\big(p^\alpha\big) = -\frac{\binom{2\alpha}{\alpha}}{4^\alpha(2\alpha - 1)}.$$

Then $f \star f$ is multiplicative by Theorem 4.10 and hence $(f \star f)(1) = 1 = \mu(1)$. Furthermore, for all primes p, we have

$$(f \star f)(p) = 2p = -\frac{2}{4} \times \binom{2}{1} = -1 = \mu(p)$$

and for all prime powers p^α such that $\alpha \geqslant 2$, we have

$$\begin{aligned}(f \star f)\big(p^\alpha\big) &= \sum_{j=0}^{\alpha} f\big(p^j\big) f\big(p^{\alpha-j}\big) \\ &= \sum_{j=0}^{\alpha} \left(-\frac{\binom{2j}{j}}{4^j(2j-1)}\right)\left(-\frac{\binom{2\alpha-2j}{\alpha-j}}{4^{\alpha-j}(2\alpha-2j-1)}\right) \\ &= 4^{-\alpha} \sum_{j=0}^{\alpha} \frac{\binom{2j}{j}\binom{2\alpha-2j}{\alpha-j}}{(2j-1)(2\alpha-2j-1)} = 0 = \mu\big(p^\alpha\big)\end{aligned}$$

where we used [Gou72, identity 3.93], which concludes the proof.

6. We proceed as in Theorem 4.10 or in Exercise 4 above.

$$\begin{aligned}(f \star g)(mn) &= \sum_{a|m} \sum_{b|n} f(ab) g\left(\frac{mn}{ab}\right) \\ &= \sum_{a|m} \sum_{b|n} \big(f(a) + f(b)\big) g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a) g\left(\frac{m}{a}\right) \sum_{b|n} g\left(\frac{n}{b}\right) + \sum_{a|m} g\left(\frac{m}{a}\right) \sum_{b|n} f(b) g\left(\frac{n}{b}\right) \\ &= (f \star g)(m)(g \star \mathbf{1})(n) + (g \star \mathbf{1})(m)(f \star g)(n)\end{aligned}$$

as required. We apply this identity with $g = \mu$ and f any additive function. First, $(f \star \mu)(1) = f(1) = 0$. If $n = p_1^{\alpha_1} p_2^{\alpha_2}$, we get using (4.6)

$$(f \star \mu)(n) = (f \star \mu)\big(p_1^{\alpha_1}\big) e_1\big(p_2^{\alpha_2}\big) + (f \star \mu)\big(p_2^{\alpha_2}\big) e_1\big(p_1^{\alpha_1}\big) = 0$$

and by induction this result is still true for all $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $r \geqslant 2$. Note that if $f(p^\alpha) \neq f(p^{\alpha-1})$, then $(f \star \mu)(p^\alpha) \neq 0$ by Example 4.11.

7.

(a) One may assume that $n \geqslant 2$ is expressed in the form $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $\alpha_j \geqslant 1$. Then $n^n = p_1^{n\alpha_1} \cdots p_r^{n\alpha_r}$ and hence

$$\varphi(n)\sigma\left(n^n\right) = n\prod_{j=1}^{r}\left(1-\frac{1}{p_j}\right)\prod_{j=1}^{r}\left(\frac{p_j^{n\alpha_j+1}-1}{p_j-1}\right)$$
$$= n\prod_{j=1}^{r} p^{n\alpha_j}\left(1-\frac{1}{p_j^{n\alpha_j+1}}\right)$$
$$= n^{n+1}\prod_{j=1}^{r}\left(1-\frac{1}{p_j^{n\alpha_j+1}}\right)$$

which implies the asserted upper bound by noticing that the product is $\leqslant 1$. For the lower bound, we use $\alpha_j \geqslant 1$ which provides

$$\varphi(n)\sigma\left(n^n\right) \geqslant n^{n+1}\prod_{j=1}^{r}\left(1-\frac{1}{p_j^{n+1}}\right) \geqslant n^{n+1}\prod_{p}\left(1-\frac{1}{p^{n+1}}\right) = \frac{n^{n+1}}{\zeta(n+1)}$$

as asserted.

(b) By the previous question, we first have $f(n) \geqslant 0$ and

$$f(n) \leqslant \frac{n}{\varphi(n)} - \frac{n^{n+1}}{n^n\varphi(n)\zeta(n+1)} = \frac{n(\zeta(n+1)-1)}{\varphi(n)\zeta(n+1)}.$$

Now by Exercise 20 in Chap. 3, we get

$$\zeta(n+1)-1 = \sum_{k=2}^{\infty}\frac{1}{k^{n+1}} \leqslant \frac{\zeta(n+1)}{2^n}$$

and the estimate

$$\frac{n}{\varphi(n)} < e^{\gamma}\log\log n + \frac{2.51}{\log\log n}$$

valid for all $n \geqslant 3$ and which may be found in [Rn62], implies that

$$0 \leqslant f(n) < 2^{-n}\left(e^{\gamma}\log\log n + \frac{2.51}{\log\log n}\right)$$

for all $n \geqslant 3$, and hence the series $\sum_{n\geqslant 1} f(n)$ converges. Using PARI/GP we obtain

$$\sum_{n=1}^{\infty}\left(\frac{n}{\varphi(n)} - \frac{\sigma(n^n)}{n^n}\right) \approx 0.298\,603\ldots$$

8. This is [HT88, Lemma 61.1].

9.

1. (a) Let m be the smallest period of x. The Euclidean division of n by m gives $n = mq + r$ with $0 \leqslant r < m$ and then

$$x = F^n(x) = F^{mq+r}(x) = F^r\big(\big(F^m\big)^q(x)\big) = F^r(x).$$

If $r \geqslant 1$, then $r \geqslant m$ since m is the smallest positive integer k such that $F^k(x) = x$, contradicting the inequality $0 \leqslant r < m$. Hence $r = 0$ and thus $m \mid n$.

(b) It is sufficient to show that

$$\mathrm{Per}_n(F) = \bigcup_{d|n} \mathrm{Per}_d^*(F). \tag{A.3}$$

Note first that, since each point of E has at most a smallest period, the union is disjoint. Furthermore, if $d \mid n$ and $F^d(x) = x$ for some $x \in E$, then $F^n(x) = (F^d)^{n/d}(x) = x$ so that

$$\bigcup_{d|n} \mathrm{Per}_d^*(F) \subseteq \mathrm{Per}_n(F).$$

Conversely, if $F^n(x) = x$ for some $x \in E$, then using the previous question we infer that x has a smallest period d dividing n and therefore

$$\mathrm{Per}_n(F) \subseteq \bigcup_{d|n} \mathrm{Per}_d^*(F).$$

The proof of (A.3) is thus complete and implies at once the first identity. The second one follows by using the Möbius inversion formula.

(c) Let x have smallest period n. By definition of $\mathcal{O}_x$, we have

$$\big\{x, F(x), F^2(x), \ldots, F^{n-1}(x)\big\} \subseteq \mathcal{O}_x.$$

Conversely, let $F^k(x) \in \mathcal{O}_x$ for some $k \in \mathbb{Z}_{\geqslant 0}$. The Euclidean division of k by n gives $k = nq + r$ with $0 \leqslant r < n$. Thus we have

$$F^k(x) = F^r\big(\big(F^n\big)^q(x)\big) = F^r(x) \in \big\{x, F(x), F^2(x), \ldots, F^{n-1}(x)\big\}$$

and then

$$\mathcal{O}_x = \big\{x, F(x), F^2(x), \ldots, F^{n-1}(x)\big\}.$$

Finally, suppose there exist two integers $0 \leqslant i < j < n$ such that $F^i(x) = F^j(x)$. Then we have

$$x = F^n(x) = F^{n-i}\big(F^i(x)\big) = F^{n-i}\big(F^j(x)\big) = F^{j-i}\big(F^n(x)\big)$$

and hence $F^{j-i}(x) = x$, so that $j - i$ is a period of x, so $j - i \geqslant n$, contradicting the inequalities $0 \leqslant i < j < n$. We infer that the elements of $\{x, F(x), F^2(x), \ldots, F^{n-1}(x)\}$ are pairwise distinct and thus

$$|\mathcal{O}_x| = \left|\left\{x, F(x), F^2(x), \ldots, F^{n-1}(x)\right\}\right| = n.$$

(d) Let x have smallest period n. By the previous question, it suffices to show that $F^k(x)$ has smallest period n for some $k \in \{0, \ldots, n-1\}$.

Since n is a period for x, we have $F^n(F^k(x)) = F^k(F^n(x)) = F^k(x)$ and thus n is a period for $F^k(x)$. Assume that $m \leqslant n$ is the smallest period of $F^k(x)$. Then $F^m(F^k(x)) = F^k(x)$ and

$$F^{n-k}\left\{F^m\left(F^k(x)\right)\right\} = F^{n-k}\left(F^k(x)\right)$$

and then $F^m(F^n(x)) = F^n(x) = x$ so that m is a period for x. This implies that $m \geqslant n$ and thus $m = n$, as required.

(e) We will only prove the symmetry, leaving the reflexivity and the transitivity to the reader.

Let $x \in \mathcal{O}_y$. By above, there exists an integer $0 \leqslant r < n$ such that $x = F^r(y)$ and hence

$$y = F^n(y) = F^{n-r}\left(F^r(y)\right) = F^{n-r}(x)$$

showing that $y \in \mathcal{O}_x$. Therefore the relation $\sim$ is symmetric.

The equivalence class of x is the set $\{y \in \mathrm{Per}_n^*(F) : y \in \mathcal{O}_x\} = \mathcal{O}_x$ since $\mathcal{O}_x \subseteq \mathrm{Per}_n^*(F)$. Since $|\mathcal{O}_x| = n$, we deduce that, if $\mathrm{Per}_n^*(F)$ is a finite set, then d divides $|\mathrm{Per}_n^*(F)|$.

(f) Let $u = (u_n)$ be a realizable sequence. By definition, there exist a set E and a map $F : E \longrightarrow E$ such that $u_n = |\mathrm{Per}_n^*(F)|$. By the previous questions, we have

$$\sum_{d|n} \left|\mathrm{Per}_d^*(F)\right| \mu(n/d) \equiv 0 \pmod{n}. \tag{A.4}$$

2. We apply (A.4) to the sequences (i) and (ii). For Fermat's little theorem for integer matrices, we first restrict ourselves to matrices with non-negative integer entries since each matrix has such a representative modulo p. The use of (A.4) with $n = p$ gives the desired result.
3. (a) Let $P = X^3 - X - 1$. Since A is the companion matrix of P, A is diagonalizable in $\mathcal{M}_3(\mathbb{C})$ and P is the minimal polynomial of A. Note that P is also the characteristic polynomial of the sequence (u_n). Thus, if λ_1, λ_2 and $\overline{\lambda_2}$ are the eigenvalues of A, then there exist three constants $a, b, c \in \mathbb{C}$ such that, for all $n \in \mathbb{Z}_{\geqslant 0}$, we have

$$u_n = a\lambda_1^n + b\lambda_2^n + c\overline{\lambda_2}^n.$$

The initial values of the sequence, together with the easy identities

$$\mathrm{Tr}(A) = 0 = \lambda_1 + \lambda_2 + \overline{\lambda_2} \quad \text{and} \quad \mathrm{Tr}\big(A^2\big) = 2 = \lambda_1^2 + \lambda_2^2 + \overline{\lambda_2}^2$$

provide the following Vandermonde system of equations

$$\begin{cases} a' + b' + c' = 0, \\ a'\lambda_1 + b'\lambda_2 + c'\overline{\lambda_2} = 0, \\ a'\lambda_1^2 + b'\lambda_2^2 + c'\overline{\lambda_2}^2 = 0 \end{cases}$$

where $a' = a-1$, $b' = b-1$ and $c' = c-1$. Since the eigenvalues are distinct, this system has the unique solution $(a', b', c') = (0, 0, 0)$ and thus $a = b = c = 1$. We deduce that, for all $n \in \mathbb{Z}_+$, we have

$$u_n = \lambda_1^n + \lambda_2^n + \overline{\lambda_2}^n = \mathrm{Tr}\big(A^n\big).$$

(b) By Fermat's little theorem for integer matrices, we get for all primes p

$$u_p = \mathrm{Tr}\big(A^p\big) \equiv \mathrm{Tr}(A) \equiv 0 \pmod{p}.$$

Remark The converse is untrue: Adam and Shanks [AS82] discovered that, if $n = 521^2$, then $n \mid u_n$.

10. By the convolution identity $\varphi = \mu \star \mathrm{Id}$ and Proposition 4.17, we get

$$\begin{aligned} \sum_{n \leqslant x} \varphi(n) &= \sum_{d \leqslant x} \mu(d) \sum_{k \leqslant x/d} k = \frac{1}{2} \sum_{d \leqslant x} \mu(d) \left[\frac{x}{d}\right] \left(\left[\frac{x}{d}\right] + 1\right) \\ &= \frac{1}{2} \sum_{d \leqslant x} \mu(d) \left\{\frac{x^2}{d^2} + O\left(\frac{x}{d}\right)\right\} \\ &= \frac{x^2}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - \frac{x^2}{2} \sum_{d > x} \frac{\mu(d)}{d^2} + O\left(x \sum_{d \leqslant x} \frac{1}{d}\right) \\ &= \frac{x^2}{2\zeta(2)} + O(x) + O(x \log x) = \frac{x^2}{2\zeta(2)} + O(x \log x) \end{aligned}$$

where we used the bound of Exercise 20 in Chap. 3.

11. We have

$$\sum_{i=1}^{n} f\big((i, n)\big) = \sum_{d \mid n} f(d) \sum_{\substack{k \leqslant n/d \\ (k, n/d) = 1}} 1 = \sum_{d \mid n} f(d) \varphi\left(\frac{n}{d}\right) = (f \star \varphi)(n).$$

12.

(a) By partial summation, we obtain

$$\begin{aligned}\sum_{n\leqslant z} n\tau(n) &= z\sum_{n\leqslant z}\tau(n) - \int_1^z \Big(\sum_{n\leqslant t}\tau(n)\Big)\,\mathrm{d}t\\ &= z\big\{z(\log z + 2\gamma - 1) + O\big(z^{\theta+\varepsilon}\big)\big\}\\ &\quad - \int_1^z \big\{t(\log t + 2\gamma - 1) + O\big(t^{\theta+\varepsilon}\big)\big\}\,\mathrm{d}t\\ &= \frac{z^2\log z}{2} + z^2\Big(\gamma - \frac{1}{4}\Big) + O\big(z^{1+\theta+\varepsilon}\big)\end{aligned}$$

as asserted.

(b) Exercise 11 with $f = \mathrm{Id}$ implies that $S = \varphi \star \mathrm{Id}$ and (4.7) gives

$$S = \mu\star\mathrm{Id}\star\mathrm{Id} = \mu\star\mathrm{Id}\times(\mathbf{1}\star\mathbf{1}) = \mu\star(\mathrm{Id}\times\tau)$$

where we used the complete multiplicativity of the function Id.

(c) By above and Proposition 4.17, we have

$$\begin{aligned}\sum_{n\leqslant x} S(n) &= \sum_{d\leqslant x}\mu(d)\sum_{k\leqslant x/d} k\tau(k)\\ &= \sum_{d\leqslant x}\mu(d)\Big\{\frac{x^2}{d^2}\Big(\frac{1}{2}\log\frac{x}{d} + \gamma - \frac{1}{4}\Big) + O\Big(\Big(\frac{x}{d}\Big)^{1+\theta+\varepsilon}\Big)\Big\}\\ &= x^2\Big\{\Big(\frac{\log x}{2} + \gamma - \frac{1}{4}\Big)\sum_{d\leqslant x}\frac{\mu(d)}{d^2} - \sum_{d\leqslant x}\frac{\mu(d)\log d}{2d^2}\Big\}\\ &\quad + O\Big(x^{1+\theta+\varepsilon}\sum_{d\leqslant x}\frac{1}{d^{1+\theta+\varepsilon}}\Big).\end{aligned}$$

Now using Exercise 20 in Chap. 3 we get as usual

$$\sum_{d\leqslant x}\frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + O\Big(\sum_{d>x}\frac{1}{d^2}\Big) = \frac{1}{\zeta(2)} + O\Big(\frac{1}{x}\Big)$$

and the use of Theorem 4.41 implies that

$$\sum_{d\leqslant x}\frac{\mu(d)\log d}{d^2} = \sum_{d=1}^{\infty}\frac{\mu(d)\log d}{d^2} + O\Big(\frac{\log x}{x}\Big) = \frac{\zeta'(2)}{\zeta(2)^2} + O\Big(\frac{\log x}{x}\Big)$$

so that

$$\sum_{n\leqslant x} S(n) = \frac{x^2}{\zeta(2)}\left(\frac{\log x}{2} + \gamma - \frac{1}{4}\right) - \frac{x^2\zeta'(2)}{2\zeta(2)^2} + O\big(x^{1+\theta+\varepsilon}\big)$$
$$= \frac{x^2}{2\zeta(2)}\left(\log x + 2\gamma - \frac{1}{2} - \frac{\zeta'(2)}{\zeta(2)}\right) + O\big(x^{1+\theta+\varepsilon}\big).$$

The best value for θ to date is given by Huxley in Theorem 6.40. We get for all $\varepsilon > 0$

$$\sum_{n\leqslant x} S(n) = \frac{x^2}{2\zeta(2)}\left(\log x + 2\gamma - \frac{1}{2} - \frac{\zeta'(2)}{\zeta(2)}\right) + O\big(x^{547/416+\varepsilon}\big).$$

13.

(a) Using $\tau_{k+1} = \tau_k \star \mathbf{1}$, we get with Proposition 4.17

$$S_{k+1}(x) = \sum_{n\leqslant x} (\tau_k \star \mathbf{1})(n) = \sum_{d\leqslant x} \tau_k(d)\left[\frac{x}{d}\right] \tag{A.5}$$

and the inequalities $x - 1 < [x] \leqslant x$ then give

$$x\sum_{d\leqslant x}\frac{\tau_k(d)}{d} - S_k(x) < S_{k+1}(x) \leqslant x\sum_{d\leqslant x}\frac{\tau_k(d)}{d}$$

and using Theorem 1.14 we get

$$\sum_{d\leqslant x}\frac{\tau_k(d)}{d} = \frac{S_k(x)}{x} + \int_1^x \frac{S_k(t)}{t^2}\,\mathrm{d}t \tag{A.6}$$

which concludes the proof.

(b) The inequalities are true for $k = 1$. Assume they are true for some positive integer k. By the previous question and the induction hypothesis, we have

$$S_{k+1}(x) \leqslant x\sum_{j=0}^{k-1}\binom{k-1}{j}\frac{(\log x)^j}{j!} + x\int_1^x \frac{1}{t}\left(\sum_{j=0}^{k-1}\binom{k-1}{j}\frac{(\log t)^j}{j!}\right)\mathrm{d}t$$
$$= x\sum_{j=0}^{k-1}\binom{k-1}{j}\frac{1}{j!}\left\{(\log x)^j + \int_1^x \frac{(\log t)^j}{t}\,\mathrm{d}t\right\}$$
$$= x\sum_{j=0}^{k-1}\binom{k-1}{j}\frac{1}{j!}\left\{(\log x)^j + \frac{(\log x)^{j+1}}{j+1}\right\}$$

$$= x\left(1 + \frac{(\log x)^k}{k!}\right) + x\sum_{j=1}^{k-1}\left\{\binom{k-1}{j} + \binom{k-1}{j-1}\right\}\frac{(\log x)^j}{j!}$$

$$= x\left(1 + \frac{(\log x)^k}{k!}\right) + x\sum_{j=1}^{k-1}\binom{k}{j}\frac{(\log x)^j}{j!} = x\sum_{j=0}^{k}\binom{k}{j}\frac{(\log x)^j}{j!}$$

and

$$S_{k+1}(x) > x\sum_{j=0}^{k-1}\frac{(-1)^{k+j+1}}{j!}\int_1^x \frac{(\log t)^j}{t}\,\mathrm{d}t + (-1)^k x\int_1^x \frac{\mathrm{d}t}{t^2}$$

$$= x\sum_{j=0}^{k-1}(-1)^{k+j+1}\frac{(\log x)^{j+1}}{(j+1)!} + (-1)^k(x-1)$$

$$= x\sum_{j=1}^{k}(-1)^{k+j+2}\frac{(\log x)^j}{j!} + (-1)^{k+2}x + (-1)^{k+1}$$

$$= x\sum_{j=0}^{k}(-1)^{k+j+2}\frac{(\log x)^j}{j!} + (-1)^{k+1}$$

completing the proof.

(c) The result follows from the upper bound of the previous question and the inequality

$$\frac{1}{j!} = \frac{1}{(k-1)!}\times\prod_{i=0}^{k-j-2}(i+j+1) \leqslant \frac{(k-j-2+j+1)^{k-j-1}}{(k-1)!} = \frac{(k-1)^{k-j-1}}{(k-1)!}$$

so that

$$S_k(x) \leqslant \frac{x}{(k-1)!}\sum_{j=0}^{k-1}\binom{k-1}{j}(\log x)^j(k-1)^{k-1-j} = \frac{x(\log x + k - 1)^{k-1}}{(k-1)!}$$

by Newton's formula.

Remark One may proceed slightly differently by using the arithmetic-geometric mean inequality which implies that, for all $k \geqslant 3$ and $0 \leqslant j \leqslant k-3$, we have

$$\prod_{i=0}^{k-j-2}(i+j+1) = (k-1)\prod_{i=0}^{k-j-3}(i+j+1)$$

$$\leqslant (k-1)\left(\frac{1}{k-j-2}\sum_{i=0}^{k-j-3}(i+j+1)\right)^{k-j-2}$$

$$= (k-1)\left(\frac{k+j-1}{2}\right)^{k-j-2} \leqslant (k-1)(k-2)^{k-j-2}$$
$$= \frac{k-1}{k-2}(k-2)^{k-j-1}$$

since $k \geqslant 3$, and this inequality remains clearly true if $j \in \{k-2, k-1\}$, so that for all $k \geqslant 3$, we get

$$S_k(x) \leqslant \frac{x(\log x + k - 2)^{k-1}}{(k-2)(k-2)!}.$$

It was proved in [Bor06] that the denominator may be replaced by $(k-1)!$.

(d) The identity is true for $k = 2$ by Corollary 4.20. Suppose it is true for some integer $k \geqslant 2$. By (A.5), (A.6) and induction hypothesis, we get

$$\begin{aligned} S_{k+1}(x) &= x \sum_{d \leqslant x} \frac{\tau_k(d)}{d} + O\big(S_k(x)\big) \\ &= x \int_1^x \frac{S_k(t)}{t^2}\,\mathrm{d}t + O\big(x(\log x)^{k-1}\big) \\ &= x \int_1^x \left\{ \frac{(\log t)^{k-1}}{(k-1)!} + O\big((\log t)^{k-2}\big) \right\} \frac{\mathrm{d}t}{t} + O\big(x(\log x)^{k-1}\big) \\ &= \frac{x(\log x)^k}{k!} + O\big(x(\log x)^{k-1}\big) \end{aligned}$$

completing the proof.

(e) Define

$$S_k^\star(x) = \sum_{n \leqslant x} \tau_k^\star(n)$$

and we prove the inequality by induction on k, the case $k = 1$ being clearly true via

$$S_1^\star(x) = [x] - 1 < x.$$

Assume the inequality is true for some $k \in \mathbb{N}$. By induction hypothesis we have

$$S_{k+1}^\star(x) = \sum_{2 \leqslant n \leqslant x2^{-k}} S_k^\star\left(\frac{x}{n}\right) \leqslant \frac{x}{(k-1)!} \sum_{2 \leqslant n \leqslant x2^{-k}} \frac{1}{n}\left(\log \frac{x}{n}\right)^{k-1}.$$

Now when $x < 2^{k+1}$, we have $S_{k+1}^\star(x) = 0$ and otherwise

$$S_{k+1}^\star(x) \leqslant \frac{x}{(k-1)!} \int_1^{x2^{-k}} \left(\log \frac{x}{t}\right)^{k-1} \frac{\mathrm{d}t}{t} = \frac{x(\log x)^k}{k!} - \frac{x(k \log 2)^k}{k!} < \frac{x(\log x)^k}{k!}$$

as required.

14. Using Corollary 3.7 (v) we obtain

$$\sum_{n\leqslant x} s_2(n) = \sum_{\substack{a^2b^3\leqslant x\\ \mu_2(b)=1}} 1 = \sum_{b\leqslant x^{1/3}} \mu_2(b) \sum_{a\leqslant (x/b^3)^{1/2}} 1$$

$$\leqslant x^{1/2} \sum_{b\leqslant x^{1/3}} \frac{\mu_2(b)}{b^{3/2}} \leqslant \frac{\zeta(3/2)\, x^{1/2}}{\zeta(3)} < 3x^{1/2}$$

where we used Lemma 3.58 in the last inequality.

The second estimate follows from partial summation in the form of Exercise 4 in Chap. 1. Indeed, using this and the above estimate, we get

$$\sum_{n>x} \frac{s_2(n)}{n} = -\frac{1}{x} \sum_{n\leqslant x} s_2(n) + \int_x^\infty \Big(\sum_{n\leqslant t} s_2(n)\Big) \frac{\mathrm{d}t}{t^2} < 3\int_x^\infty \frac{\mathrm{d}t}{t^{3/2}} = \frac{6}{x^{1/2}}$$

as asserted.

15. Define $g = f \star \mu$. Then g is multiplicative by Theorem 4.10, $|g(p)| = |f(p) - 1| \leqslant p^{-1}$ and, for all prime powers p^α with $\alpha \geqslant 2$, we have $|g(p^\alpha)| \leqslant 1$, so that $|g(n)| \leqslant 1$ for all $n \in \mathbb{N}$. Let $x \geqslant 2$ be a large real number. We have

$$\sum_{p\leqslant x} \sum_{\alpha=1}^\infty \frac{|g(p^\alpha)|}{p^\alpha} = \sum_{p\leqslant x} \frac{|f(p)-1|}{p} + \sum_{p\leqslant x} \sum_{\alpha=2}^\infty \frac{|g(p^\alpha)|}{p^\alpha}$$

$$\leqslant \sum_{p\leqslant x} \frac{1}{p^2} + \sum_{p\leqslant x} \sum_{\alpha=2}^\infty \frac{1}{p^\alpha}$$

$$\leqslant 3 \sum_{p\leqslant x} \frac{1}{p^2} < \frac{3}{2}$$

by (4.20), so that the series $\sum_{d\geqslant 1} g(d)/d$ converges absolutely by Theorem 4.47 and we have

$$1 + \sum_{\alpha=1}^\infty \frac{g(p^\alpha)}{p^\alpha} = 1 + \sum_{\alpha=1}^\infty \frac{f(p^\alpha) - f(p^{\alpha-1})}{p^\alpha} = \Big(1 - \frac{1}{p}\Big)\Big(1 + \sum_{\alpha=1}^\infty \frac{f(p^\alpha)}{p^\alpha}\Big).$$

Using Theorem 4.13 and Proposition 4.17, we get

$$\sum_{n\leqslant x} f(n) = \sum_{n\leqslant x} (g \star \mathbf{1})(n) = \sum_{d\leqslant x} g(d) \Big[\frac{x}{d}\Big]$$

$$= x \sum_{d\leqslant x} \frac{g(d)}{d} + O\Big(\sum_{d\leqslant x} |g(d)|\Big)$$

$$= x\sum_{d=1}^{\infty}\frac{g(d)}{d} + O\Big(\sum_{d\leqslant x}\big|g(d)\big| + x\sum_{d>x}\frac{|g(d)|}{d}\Big)$$

and by partial summation in the form of Exercise 4 in Chap. 1, we obtain

$$\sum_{d>x}\frac{|g(d)|}{d} = -\frac{1}{x}\sum_{d\leqslant x}\big|g(d)\big| + \int_x^{\infty}\Big(\sum_{d\leqslant t}\big|g(d)\big|\Big)\frac{\mathrm{d}t}{t^2}$$

and

$$\sum_{d=1}^{\infty}\frac{g(d)}{d} = \prod_p\Big(1+\sum_{\alpha=1}^{\infty}\frac{g(p^\alpha)}{p^\alpha}\Big) = \prod_p\Big(1-\frac{1}{p}\Big)\Big(1+\sum_{\alpha=1}^{\infty}\frac{f(p^\alpha)}{p^\alpha}\Big)$$

so that

$$\sum_{n\leqslant x} f(n) = x\prod_p\Big(1-\frac{1}{p}\Big)\Big(1+\sum_{\alpha=1}^{\infty}\frac{f(p^\alpha)}{p^\alpha}\Big) + R(x)$$

with

$$\big|R(x)\big| \ll \sum_{d\leqslant x}\big|g(d)\big| + x\int_x^{\infty}\Big(\sum_{d\leqslant t}\big|g(d)\big|\Big)\frac{\mathrm{d}t}{t^2}.$$

It remains to estimate the sum $\sum_{d\leqslant x}|g(d)|$. To do this we use the unique decomposition of each positive integer d in the form $d=ab$ with $\mu_2(a)=s_2(b)=1$ and $(a,b)=1$. Also note that, for all squarefree numbers a, we have $|g(a)|\leqslant a^{-1}$. Using Exercise 14, we obtain

$$\begin{aligned}\sum_{d\leqslant x}\big|g(d)\big| &= \sum_{a\leqslant x}\mu_2(a)\big|g(a)\big|\sum_{b\leqslant x/a}s_2(b)\big|g(b)\big|\\ &\leqslant \sum_{a\leqslant x}\frac{\mu_2(a)}{a}\sum_{b\leqslant x/a}s_2(b)\\ &< 3x^{1/2}\sum_{a\leqslant x}\frac{\mu_2(a)}{a^{3/2}} \leqslant \frac{3\zeta(3/2)x^{1/2}}{\zeta(3)}.\end{aligned}$$

Hence

$$\big|R(x)\big| \ll x^{1/2} + x\int_x^{\infty}\frac{\mathrm{d}t}{t^{3/2}} \ll x^{1/2}$$

completing the proof.

16. This is a direct application of Exercise 15 since $\beta(p)=1$ and $\beta\star\mu = s_2$.

17. Again a direct application of Exercise 15 with $f(n) = \varphi(n)\gamma_2(n)/n^2$ since, for all prime powers p^α, we have

$$f(p) = 1 - \frac{1}{p} \quad \text{and} \quad (f \star \mu)\big(p^\alpha\big) = \begin{cases} -1/p, & \text{if } \alpha = 1, \\ -p^{-\alpha}(p-1)^2, & \text{if } \alpha \geqslant 2. \end{cases}$$

18.

(a) Let $g(n) = \mu(n)/\tau(n)$ and $G = g \star \mathbf{1}$. By Theorem 4.10, G is multiplicative and, for all prime powers p^α, we have

$$G\big(p^\alpha\big) = 1 + \sum_{j=1}^{\alpha} g\big(p^j\big) = 1 - \frac{1}{\tau(p)} = \frac{1}{2}$$

so that, for all $n \in \mathbb{N}$, we get

$$G(n) = 2^{-\omega(n)}$$

and hence using Proposition 4.17 we obtain

$$\begin{aligned} \sum_{n \leqslant x} G(n) &= \sum_{n \leqslant x} (g \star \mathbf{1})(n) = \sum_{d \leqslant x} g(d) \left[\frac{x}{d}\right] \\ &= x \sum_{d \leqslant x} \frac{g(d)}{d} - \sum_{d \leqslant x} g(d) \left\{\frac{x}{d}\right\} \\ &= x F(x) - \sum_{d \leqslant x} g(d) \left\{\frac{x}{d}\right\} \end{aligned}$$

as required.

(b) Using the inequalities $0 \leqslant \{x\} < 1$ we get

$$\left| \sum_{n \leqslant x} \frac{\mu(n)}{\tau(n)} \left\{\frac{x}{n}\right\} \right| < \sum_{n \leqslant x} \frac{\mu^2(n)}{\tau(n)} = \sum_{n \leqslant x} \frac{\mu^2(n)}{2^{\omega(n)}} \leqslant \sum_{n \leqslant x} \frac{1}{2^{\omega(n)}}$$

so that

$$\sum_{n \leqslant x} \frac{1}{2^{\omega(n)}} + \sum_{n \leqslant x} \frac{\mu(n)}{\tau(n)} \left\{\frac{x}{n}\right\} > 0.$$

Furthermore, we also have

$$F(x) = \big|F(x)\big| \leqslant \frac{1}{x}\left(\sum_{n \leqslant x} \frac{1}{2^{\omega(n)}} + \left| \sum_{n \leqslant x} \frac{\mu(n)}{\tau(n)} \left\{\frac{x}{n}\right\} \right| \right) < \frac{2}{x} \sum_{n \leqslant x} \frac{1}{2^{\omega(n)}}.$$

The function $2^{-\omega}$ satisfies the Wirsing conditions (4.21) with $\lambda_1 = 1/2$ and $\lambda_2 = 1$ so that we may apply Theorem 4.22 with $(a, b) = (\log 2, 3/2)$ by Lemma 4.23. This gives

$$\sum_{n\leqslant x} \frac{1}{2^{\omega(n)}} \leqslant e^{3/2}\left(\frac{5}{2}+\log 2\right)\frac{x}{\log ex}\exp\left(\frac{1}{2}\sum_{p\leqslant x}\frac{1}{p}\right).$$

By Corollary 3.99, we have

$$\sum_{p\leqslant x}\frac{1}{p} < \log\log x + \frac{1}{2}$$

as soon as $x \geqslant 8$ implying that

$$\sum_{n\leqslant x}\frac{1}{2^{\omega(n)}} < \frac{19x}{(\log x)^{1/2}}$$

and hence we finally get for all $x \geqslant 8$

$$0 < F(x) < 38\,(\log x)^{-1/2}.$$

19.

(a) We have $f(p^\alpha) = t^\alpha - t^{\alpha-1}$ and using Theorem 4.13 and Proposition 4.17, we get

$$\begin{aligned}\sum_{n\leqslant x} t^{\Omega(n)} &= \sum_{n\leqslant x}(f\star\mathbf{1})(n) = \sum_{d\leqslant x} f(d)\left[\frac{x}{d}\right]\\ &\leqslant x\sum_{d\leqslant x}\frac{f(d)}{d} \leqslant x\prod_{p\leqslant x}\left(1+\sum_{\alpha=1}^{\infty}\frac{t^\alpha - t^{\alpha-1}}{p^\alpha}\right)\\ &= x\prod_{p\leqslant x}\left(1+\frac{t-1}{p-t}\right).\end{aligned}$$

We treat the cases $p = 2$ and $p \geqslant 3$ separately which gives

$$\begin{aligned}\sum_{n\leqslant x} t^{\Omega(n)} &\leqslant \frac{x}{2-t}\prod_{3\leqslant p\leqslant x}\left(1+\frac{t-1}{p-t}\right)\\ &\leqslant \frac{x}{2-t}\prod_{3\leqslant p\leqslant x}\left(1+\frac{1}{p-2}\right)\\ &\leqslant \frac{x}{2-t}\exp\left(\sum_{3\leqslant p\leqslant x}\frac{1}{p-2}\right) \ll \frac{x\log x}{2-t}\end{aligned}$$

as required.

(b) We have

$$N_k(x) = \sum_{\substack{n \leqslant x \\ \Omega(n)=k}} t^{-\Omega(n)} t^{\Omega(n)} \leqslant t^{-k} \sum_{n \leqslant x} t^{\Omega(n)} \ll \frac{t^{-k} x \log x}{2-t}$$

and the choice of

$$t = \frac{2k}{k+1}$$

gives the asserted estimate.

20.

1. (a) Since n is squarefree, a positive integer d is a divisor of n if and only if either d divides n/p or $d \mid n$ is a multiple of p, so that

$$\sum_{d|n} f(d) = \sum_{d|(n/p)} f(d) + \sum_{\substack{d|n \\ p|d}} f(d) = \sum_{d|(n/p)} f(d) + \sum_{k|(n/p)} f(kp).$$

Since f is multiplicative and $k \mid (n/p)$ implies that $(k, p) = 1$, we infer that

$$\sum_{d|n} f(d) = \sum_{d|(n/p)} f(d) + f(p) \sum_{k|(n/p)} f(k) = \big(1 + f(p)\big) \sum_{k|(n/p)} f(k)$$

giving (4.49).

(b) First note that $f(d) \geqslant 0$ for all divisors d of n necessarily squarefree. Thus, using (4.49), we get

$$\begin{aligned}
\sum_{d|n} f(d) \log d &= \sum_{d|n} f(d) \sum_{p|d} \log p = \sum_{p|n} \log p \sum_{k|(n/p)} f(kp) \\
&= \sum_{p|n} f(p) \log p \sum_{k|(n/p)} f(k) \\
&= \sum_{p|n} \left(\frac{f(p) \log p}{1 + f(p)} \sum_{d|n} f(d) \right) \\
&= \left(\sum_{d|n} f(d) \right) \left(\sum_{p|n} \frac{f(p) \log p}{1 + f(p)} \right)
\end{aligned}$$

as required. Now the function $t \longmapsto t/(1+t)$ is increasing on $[0, \lambda]$ and since $f(d) \geqslant 0$ for all divisors d of n, we deduce that

$$\sum_{d|n} f(d) \log d \leqslant \frac{\lambda}{1+\lambda} \left(\sum_{d|n} f(d) \right) \left(\sum_{p|n} \log p \right) = \frac{\lambda \log n}{1+\lambda} \left(\sum_{d|n} f(d) \right).$$

2. First note that $\log(n^{1/a}/d) \leqslant \log(n^{1/a})$ and since $f(d) \geqslant 0$, we get

$$\sum_{\substack{d|n \\ d\leqslant n^{1/a}}} f(d)\,\frac{\log(n^{1/a}/d)}{\log(n^{1/a})} \leqslant \sum_{\substack{d|n \\ d\leqslant n^{1/a}}} f(d).$$

Note also that, if $d > n^{1/a}$, then $\log(n^{1/a}/d) < 0$ and hence

$$\sum_{d|n} f(d)\,\frac{\log(n^{1/a}/d)}{\log(n^{1/a})} \leqslant \sum_{\substack{d|n \\ d\leqslant n^{1/a}}} f(d)\,\frac{\log(n^{1/a}/d)}{\log(n^{1/a})}.$$

We infer that

$$\sum_{\substack{d|n \\ d\leqslant n^{1/a}}} f(d) \geqslant \sum_{d|n} f(d)\,\frac{\log(n^{1/a}/d)}{\log(n^{1/a})} = \sum_{d|n} f(d) - \frac{a}{\log n}\sum_{d|n} f(d)\log d$$

and using (4.50) gives

$$\sum_{\substack{d|n \\ d\leqslant n^{1/a}}} f(d) \geqslant \sum_{d|n} f(d)\left(1 - \frac{\lambda a}{1+\lambda}\right)$$

implying the desired estimate since $\lambda < (a-1)^{-1}$.

21. Let $S_n = (s_{ij})$ and $T_n = (t_{ij})$ be the matrices defined by

$$s_{ij} = \begin{cases} 1, & \text{if } i \mid j, \\ 0, & \text{otherwise} \end{cases} \quad \text{and} \quad t_{ij} = \begin{cases} M(n/i), & \text{if } j = 1, \\ 1, & \text{if } i = j \geqslant 2, \\ 0, & \text{otherwise.} \end{cases}$$

We will prove the following result.

Lemma *We have* $R_n = S_n T_n$. *In particular we have* $\det R_n = M(n)$.

Proof Set $S_n T_n = (x_{ij})$. If $j = 1$ we have

$$x_{i1} = \sum_{k=1}^{n} s_{ik}t_{k1} = \sum_{\substack{k\leqslant n \\ i|k}} M\left(\frac{n}{k}\right) = \sum_{d\leqslant n/i} M\left(\frac{n/i}{d}\right) = 1 = r_{i1}$$

by (4.15). If $j \geqslant 2$, then $t_{1j} = 0$ and thus

$$x_{ij} = \sum_{k=2}^{n} s_{ik}t_{kj} = s_{ij} = \begin{cases} 1, & \text{if } i \mid j, \\ 0, & \text{otherwise} \end{cases} = r_{ij}$$

which is the desired result. The second assertion follows at once from

$$\det R_n = \det S_n \det T_n = \det T_n = M(n).$$

The proof is complete. □

22.

1. We may suppose $n > 1$. Let p^α be a prime power. Using Bernoulli's inequality, we get

$$\big(t^\omega \star \mathbf{1}\big)\big(p^\alpha\big) = 1 + \alpha t \leqslant (1+t)^\alpha = (1+t)^{\Omega(p^\alpha)}$$

   implying the first inequality by multiplicativity.
2. Write $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and, for each $j \in \{1, \dots, k\}$, let d_j be a divisor of n with $\omega(d_j) = j \leqslant k$. The number of such divisors is at most equal to the number of integers which are the products of j prime powers from the list

$$p_1, p_1^2, \dots, p_1^{\alpha_1}, p_2, p_2^2, \dots, p_2^{\alpha_2}, \dots, p_r, p_r^2, \dots, p_r^{\alpha_r}.$$

   Since this list contains $\Omega(n)$ elements, we infer that the number of divisors d_j is at most $\binom{\Omega(n)}{j}$ and hence

$$\sum_{\substack{d|n \\ \omega(d)\leqslant k}} t^{\omega(d)} \leqslant 1 + \sum_{j=1}^{k} \binom{\Omega(n)}{j} t^j = \sum_{j=0}^{k} \binom{\Omega(n)}{j} t^j$$

   as asserted. It is easy to see that this inequality generalizes the previous one and, with a little more work, one can prove that

$$\sum_{\substack{d|n \\ \omega(d)\leqslant k}} t^{\omega(d)} = \sum_{j=0}^{k} t^j \sum_{1\leqslant i_1 < i_2 < \cdots < i_j \leqslant \omega(n)} \alpha_{i_1} \cdots \alpha_{i_j}.$$

23. This exercise follows readily from the convolution identities

$$\tau = \mathbf{1} \star \mathbf{1} \quad \text{and} \quad \mathbf{1} \star \Lambda = \log$$

since then

$$\tau \star \mu \star \Lambda = \mathbf{1} \star \mathbf{1} \star \mu \star \Lambda = \mathbf{1} \star \Lambda = \log$$

and

$$\sum_{n\leqslant N} (\tau \star \mu \star \Lambda)(n) = \sum_{n\leqslant N} \log n = \log(N!).$$

A.5 Chapter 5

1. We have $0 \leqslant \|x\| \leqslant 1/2$, and the function ψ is odd and 1-periodic, implying that the function $\|\cdot\|$ is even and 1-periodic. For the first inequality, it suffices to suppose that $|x|, |y| \leqslant \frac{1}{2}$ giving in this case

$$|\|x\| - \|y\|| = ||x| - |y|| \leqslant |x - y|.$$

The second inequality may be proved similarly, noticing that for all $x \in \mathbb{R}$, there exists a unique $\theta_x \in]-\frac{1}{2}, \frac{1}{2}]$ such that $x = \lfloor x \rceil + \theta_x$, so that by periodicity we get $\|x + y\| = \|\theta_x + \theta_y\|$ showing that we may suppose that $|x|, |y| \leqslant \frac{1}{2}$, and we also may restrict ourselves to $0 \leqslant x, y \leqslant \frac{1}{2}$ since the function $\|\cdot\|$ is even. In this case, we finally have

$$\|x + y\| = \begin{cases} x + y = \|x\| + \|y\|, & \text{if } 0 \leqslant x + y \leqslant \frac{1}{2}, \\ 1 - (x + y) \leqslant x + y = \|x\| + \|y\|, & \text{if } \frac{1}{2} \leqslant x + y \leqslant 1 \end{cases}$$

as required.

2. The functions $x \longmapsto |\sin(\pi x)|$ and $x \longmapsto \|x\|$ are both even and 1-periodic, so that it suffices to prove the asserted inequality for all $x \in [0, \frac{1}{2}]$. In this interval, the inequality takes the shape

$$2x \leqslant \sin(\pi x) \leqslant \pi x$$

which is well-known. For instance, if f is the function $x \longmapsto \sin(\pi x) - 2x$, then $f''(x) = -\pi^2 \sin(\pi x) \leqslant 0$ for all $x \in [0, \frac{1}{2}]$, so that f is concave on this interval and therefore

$$f(x) \geqslant \min\big(f(0), f(1/2)\big) = 0$$

as required.

3.

(a) If $N < x^{1/5}$, one may take $T = \mathcal{S}(f, N, \delta)$ since then $x^{-1/6}N^{5/6} < 1$. Now suppose that $N \geqslant x^{1/5}$ and let $a, b \in \mathbb{N}$ and n, $n + a$ and $n + a + b$ be three consecutive elements of $\mathcal{S}(f, N, \delta)$ such that

$$1 \leqslant a, b \leqslant 2^{2/3}x^{-1/6}N^{5/6}.$$

As in Lemma 5.32, we will show that there are only two possibilities for the choice of b. The result will then follow by taking each 4th element of $\mathcal{S}(f, N, \delta)$.

There exist non-zero integers m_i and real numbers δ_i such that

$$\begin{aligned} f(n) &= m_1 + \delta_1, \\ f(n + a) &= m_2 + \delta_2, \\ f(n + a + b) &= m_3 + \delta_3 \end{aligned}$$

with $|\delta_i| < \delta$ for $i \in \{1,2,3\}$. In fact, each integer m_i is positive since, for all $u \in [N, 2N]$, we have $f(u) \geqslant \sqrt{x}/\sqrt{2N} \geqslant 1/\sqrt{2}$ and $\delta \leqslant c_0 N^{-1}$. Using the given polynomials P and Q, we get

$$\begin{aligned} f(n)P(n,a) - f(n+a)Q(n,a) &= \left(\frac{x}{n}\right)^{1/2}(4n+a) - \left(\frac{x}{n+a}\right)^{1/2}(4n+3a) \\ &= \left(\frac{x}{n}\right)^{1/2}\frac{(n+a)^{1/2}(4n+a) - n^{1/2}(4n+3a)}{(n+a)^{1/2}} \\ &= \frac{x^{1/2}a^3}{n^{1/2}(n+a)^{1/2}D(n,a)} \end{aligned}$$

where

$$D(n,a) = (n+a)^{1/2}(4n+a) + n^{1/2}(4n+3a) \geqslant 8N^{3/2}$$

so that

$$0 < f(n)P(n,a) - f(n+a)Q(n,a) \leqslant \frac{x^{1/2}a^3}{8N^{5/2}} < \frac{1}{2}.$$

On the other hand, we have

$$f(n)P(n,a) - f(n+a)Q(n,a) = m_1P(n,a) - m_2Q(n,a) + \varepsilon$$

with

$$|\varepsilon| \leqslant 7\delta(n+a) \leqslant 14N\delta < \frac{1}{2}.$$

Hence by Lemma 5.31, we obtain

$$m_1P(n,a) - m_2Q(n,a) = 0. \tag{A.7}$$

Similarly we have

$$\begin{aligned} m_2P(n+a,b) - m_3Q(n+a,b) &= 0, \\ m_1P(n,a+b) - m_3Q(n,a+b) &= 0 \end{aligned}$$

and eliminating m_3 we obtain

$$m_2P(n+a,b)Q(n,a+b) - m_1P(n,a+b)Q(n+a,b) = 0$$

implying that

$$3b^2(m_1 - m_2) + \kappa_1 b + 2\kappa_2 = 0 \tag{A.8}$$

where

$$\begin{aligned} \kappa_1 &= a(7m_1 - 15m_2) - 16n(m_1 - m_2), \\ \kappa_2 &= a^2(m_1 - 3m_2) - an(-20m_1 + 28m_2) - 16n^2(m_1 - m_2). \end{aligned}$$

If $m_1 = m_2$, then by (A.7) we have $P(n,a) = Q(n,a)$ and then $4n + a = 4n + 3a$, so that $a = 0$ which is impossible since $a \geqslant 1$. Therefore $m_1 \neq m_2$ and (A.8) is a quadratic equation in b, concluding the proof.

(b) Hence we deduce that

$$\mathcal{R}\left(\sqrt{\frac{x}{n}}, N, \delta\right) \ll |T| + 1 \ll \frac{N}{x^{-1/6}N^{5/6}} + 1 \ll (Nx)^{1/6}.$$

4. We follow the proof of Corollary 5.35 from which we borrow the notation. If $16 \leqslant y \leqslant x^{1/5}$, then obviously

$$\left| \sum_{x < n \leqslant x+y} \mu_2(n) - \frac{y}{\zeta(2)} \right| < 3y \leqslant 3\, x^{1/15} y^{2/3}.$$

Suppose that $x^{1/5} < y < x^{1/2}/4$. We may write

$$\sum_{2\sqrt{y} < n \leqslant \sqrt{x}} \left(\left[\frac{x+y}{n^2} \right] - \left[\frac{x}{n^2} \right] \right) = \left(\sum_{2\sqrt{y} < n \leqslant c_0^{-1} y} + \sum_{c_0^{-1} y < n \leqslant \sqrt{x}} \right) \left(\left[\frac{x+y}{n^2} \right] - \left[\frac{x}{n^2} \right] \right)$$
$$= \Sigma_1 + \Sigma_2$$

where c_0 is the constant appearing in (5.33). We use Theorem 5.23 (i) with $k = 4$ for Σ_1 and Theorem 5.30 for Σ_2 which gives

$$\Sigma_1 \ll \left(x^{1/10} y^{2/5} + y^{2/3} + (xy)^{1/7} \right) \log x \ll x^{1/15} y^{2/3} \log x$$

and

$$\Sigma_2 \ll \max_{c_0^{-1} y < n \leqslant \sqrt{x}} \left(x^{1/5} + x^{1/15} y N^{-1/3} \right) \log x \ll \left(x^{1/5} + x^{1/15} y^{2/3} \right) \log x$$
$$\ll x^{1/15} y^{2/3} \log x$$

since $y > x^{1/5}$. This completes the proof since clearly $y^{1/2} \leqslant x^{1/15} y^{2/3}$.

5. The proof is exactly the same as that of Corollary 5.35 except that Theorem 5.30 is replaced by Theorem 5.36 and Theorem 5.23 (i) is used with $k = 2r$ instead of $k = 4$. We omit the details.

6.

(a) Let $L < T \leqslant (x+y)^{1/3}$ be any parameter at our disposal. We have

$$\sum_{L < b \leqslant (x+y)^{1/3}} \left(\left[\sqrt{\frac{x+y}{b^3}} \right] - \left[\sqrt{\frac{x}{b^3}} \right] \right)$$

$$
\begin{aligned}
&= \Big(\sum_{L<b\leqslant T} + \sum_{T<b\leqslant (x+y)^{1/3}}\Big)\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big)\\
&= \sum_{L<b\leqslant T}\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big) + \sum_{T<b\leqslant (x+y)^{1/3}}\ \sum_{x<a^2b^3\leqslant x+y} 1\\
&= \sum_{L<b\leqslant T}\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big) + \sum_{a\leqslant \sqrt{\frac{x+y}{T^3}}}\ \sum_{(\frac{x}{a^2})^{1/3}<b\leqslant (\frac{x+y}{a^2})^{1/3}} 1\\
&= \sum_{L<b\leqslant T}\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big) + \sum_{a\leqslant \sqrt{\frac{x+y}{T^3}}}\Big(\Big[\Big(\frac{x+y}{a^2}\Big)^{1/3}\Big] - \Big[\Big(\frac{x}{a^2}\Big)^{1/3}\Big]\Big)\\
&= \sum_{L<b\leqslant T}\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big)\\
&\quad + \Big(\sum_{a\leqslant L} + \sum_{L<a\leqslant \sqrt{\frac{x+y}{T^3}}}\Big)\Big(\Big[\Big(\frac{x+y}{a^2}\Big)^{1/3}\Big] - \Big[\Big(\frac{x}{a^2}\Big)^{1/3}\Big]\Big)\\
&\ll \sum_{L<b\leqslant T}\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big) + \sum_{a\leqslant L}\Big(\frac{y}{(ax)^{2/3}} + 1\Big)\\
&\quad + \sum_{L<a\leqslant \sqrt{\frac{x+y}{T^3}}}\Big(\Big[\Big(\frac{x+y}{a^2}\Big)^{1/3}\Big] - \Big[\Big(\frac{x}{a^2}\Big)^{1/3}\Big]\Big)\\
&\ll \sum_{L<b\leqslant T}\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big) + yx^{-2/3}L^{1/3} + L\\
&\quad + \sum_{L<a\leqslant \sqrt{\frac{2x}{T^3}}}\Big(\Big[\Big(\frac{x+y}{a^2}\Big)^{1/3}\Big] - \Big[\Big(\frac{x}{a^2}\Big)^{1/3}\Big]\Big).
\end{aligned}
$$

Using (5.45), we get $yx^{-2/3}L^{1/3} < L$ and, for all $A, B > L$, we infer

$$
\begin{aligned}
\frac{y}{\sqrt{xB^3}} < \frac{y}{\sqrt{xL^3}} &= x^{1/4}y^{-1/2}(\log x)^{3/4} \leqslant \frac{1}{4},\\
\frac{y}{(Ax)^{2/3}} < \frac{y}{(xL)^{2/3}} &= \big(x^{-1}y\log x\big)^{1/3} \leqslant \frac{1}{4}
\end{aligned}
$$

as soon as $x \geqslant 3$. Now the choice of $T = (2x)^{1/5}$ and the usual splitting argument provide the final result.

(b) Using Corollary 3.7 (v) and the previous question, we have

$$\sum_{x<n\leqslant x+y} s_2(n) = \sum_{b\leqslant (x+y)^{1/3}} \mu_2(b) \sum_{\sqrt{\frac{x}{b^3}}<a\leqslant\sqrt{\frac{x+y}{b^3}}} 1$$

$$= \Big(\sum_{b\leqslant L} + \sum_{L<b\leqslant (x+y)^{1/3}}\Big)\mu_2(b)\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big)$$

$$= \sum_{b\leqslant L} \mu_2(b)\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big) + O\big\{(R_1+R_2)\log x + L\big\}$$

and since

$$\sqrt{\frac{x+y}{b^3}} - \sqrt{\frac{x}{b^3}} = \frac{y}{2\sqrt{xb^3}} + O\Big(\frac{y^2}{(bx)^{3/2}}\Big)$$

we infer that

$$\sum_{b\leqslant L} \mu_2(b)\Big(\Big[\sqrt{\frac{x+y}{b^3}}\Big] - \Big[\sqrt{\frac{x}{b^3}}\Big]\Big)$$

$$= \frac{y}{2x^{1/2}} \sum_{b\leqslant L} \frac{\mu_2(b)}{b^{3/2}} + O\Big(\frac{y^2}{x^{3/2}} + L\Big)$$

$$= \frac{y}{2x^{1/2}} \sum_{b=1}^{\infty} \frac{\mu_2(b)}{b^{3/2}} + O\Big(L + \frac{y}{x^{1/2}} \sum_{b>L} \frac{1}{b^{3/2}}\Big)$$

$$= \frac{\zeta(3/2)}{2\zeta(3)} \frac{y}{x^{1/2}} + O\big(L + \big(y^2x^{-1}\log x\big)^{1/4}\big)$$

$$= \frac{\zeta(3/2)}{2\zeta(3)} \frac{y}{x^{1/2}} + O(L)$$

where we used (5.45) which implies that L dominates all the other terms.

(c) To bound R_2, we split the sum into two subsums estimating trivially in the interval $]L, x^{2/15}]$ and using Theorem 5.22 in the interval $]x^{2/15}, (2x)^{1/5}]$ giving

$$\mathcal{R}\Big(\Big(\frac{x}{a^2}\Big)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\Big) \ll (Ax)^{1/9} + y\big(Ax^{-2}\big)^{1/3} + \big(x^{-1}y^3A^{-4}\big)^{1/6} + Ayx^{-1}$$

so that

$$\max_{x^{2/15}<A\leqslant(2x)^{1/5}} \mathcal{R}\Big(\Big(\frac{x}{a^2}\Big)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\Big) \ll x^{2/15} + yx^{-3/5} + y^{1/2}x^{-23/90}.$$

Now (5.45) gives

$$R_2 \ll x^{2/15} + \frac{L}{\log x}.$$

We treat R_1 by using Theorem 5.23 (i) with $k = 3$ giving

$$\mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll \big(B^3x\big)^{1/12} + \big(yB^{-1}\big)^{1/4} + y(Bx)^{-1/2} + B\big(yx^{-1}\big)^{1/2}$$

so that

$$\max_{L<B\leqslant(2x)^{1/5}} \mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll x^{2/15} + y^{1/2}x^{-1/4}(\log x)^{1/4} + y^{1/2}x^{-3/10}$$

and using (5.45) implies also that

$$R_1 \ll x^{2/15} + \frac{L}{\log x}$$

concluding the proof.

(d) ▹ *Bounds for* R_2. In the range $]L, (64x)^{1/8}]$, we use Theorem 5.23 (i) with $k = 3$ giving

$$\begin{aligned}&\mathcal{R}\Big(\Big(\frac{x}{a^2}\Big)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\Big)\\ &\quad\ll \big(A^7x\big)^{1/18} + \big(A^2x^{-1}y^3\big)^{1/12} + y\big(x^{-2}A\big)^{1/3} + A\big(yx^{-1}\big)^{1/2}\end{aligned}$$

so that

$$\begin{aligned}&\max_{L<A\leqslant(64x)^{1/8}} \mathcal{R}\Big(\Big(\frac{x}{a^2}\Big)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\Big)\\ &\quad\ll x^{5/48} + y^{1/4}x^{-1/16} + yx^{-5/8} + y^{1/2}x^{-3/8}.\end{aligned}$$

In the range $](64x)^{1/8}, (2x)^{1/5}]$, we use Theorem 5.26 implying that

$$\begin{aligned}&\mathcal{R}\Big(\Big(\frac{x}{a^2}\Big)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\Big)\\ &\quad\ll \big\{(Ax)^{1/10} + \big(A^4x^3\big)^{1/15} + y\big(Ax^{-2}\big)^{1/3} + \big(A^{-2}xy^3\big)^{1/24}\\ &\qquad + \big(A^8x^{-1}y^3\big)^{1/21} + \big(Ax^{-1}y^2\big)^{1/5} + A\big(yx^{-1}\big)^{1/2}\big\}(\log A)^{2/5}\end{aligned}$$

so that

$$\max_{(64x)^{1/8}<A\leqslant(2x)^{1/5}} \mathcal{R}\Big(\Big(\frac{x}{a^2}\Big)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\Big)$$

$$\ll \{x^{3/25} + yx^{-3/5} + x^{1/32}y^{1/8} + x^{1/35}y^{1/7} + y^{2/5}x^{-4/25} + y^{1/2}x^{-3/10}\}(\log x)^{2/5}$$

and the lower bound of (5.46) implies that

$$R_2 \ll x^{3/25}(\log x)^{2/5} + \frac{L}{\log x}.$$

▹ *Bounds for* R_1. In the range $]L, (16x)^{1/6}]$, we use Theorem 5.23 (i) with $k = 3$ giving

$$\mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll \big(B^3x\big)^{1/12} + \big(yB^{-1}\big)^{1/4} + y(Bx)^{-1/2} + B\big(yx^{-1}\big)^{1/2}$$

so that

$$\max_{L<B\leqslant(16x)^{1/6}} \mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll x^{1/8}(\log x)^{1/8} + y^{1/2}x^{-1/4}(\log x)^{1/4} + y^{1/2}x^{-3/8}.$$

In the range $](16x)^{1/6}, (2x)^{1/5}]$, we use Theorem 5.26 implying that

$$\mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll \big\{\big(xB^{-1}\big)^{3/20} + (Bx)^{1/10} + y(Bx)^{-1/2} + \big(xy^2B^{-3}\big)^{1/16} + (By)^{1/7} + \big(x^{-1}y^4B^{-3}\big)^{1/10} + B\big(yx^{-1}\big)^{1/2}\big\}(\log B)^{2/5}$$

so that

$$\max_{(16x)^{1/6}<B\leqslant(2x)^{1/5}} \mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll \{x^{1/8} + yx^{-7/12} + x^{1/32}y^{1/8} + x^{1/35}y^{1/7} + y^{2/5}x^{-3/20} + y^{1/2}x^{-3/10}\}(\log x)^{2/5}$$

and the lower bound of (5.46) implies that

$$R_1 \ll x^{1/8}(\log x)^{2/5} + \frac{L}{\log x}.$$

The proof is complete.

Remark Splitting R_1 into more parts and using Theorem 5.28 in the "critical" part, the author [Tri02] proved that, under a more restricted range than (5.46), the exponent $1/8$ may be reduced to $19/154 \approx 0.123\,33\ldots$ Note that the result obtained for

R_2 above shows that we might expect to get the bound $3/25 = 0.12$. However, this estimate for R_1 still remains open.

7. Let $r \geqslant 2$ be an integer and define the multiplicative function $\tau^{(r)}$ by

$$\tau^{(r)}(n) = \sum_{d^r|n} 1.$$

Clearly, we have $\tau^{(r)}(p^\alpha) = 1 + [\alpha/r]$ so that $\tau^{(r)}$ satisfies the hypotheses of Theorem 4.62. Furthermore, we have using Lemma 5.2

$$\begin{aligned}
\mathcal{R}\Big(\frac{x}{n^r}, N\delta\Big) &\leqslant \sum_{N\leqslant d\leqslant 2N} \left(\left[\frac{x}{d^r} + \delta\right] - \left[\frac{x}{d^r} - \delta\right]\right) = \sum_{N\leqslant d\leqslant 2N} \sum_{x-d^r\delta < md^r \leqslant x+d^r\delta} 1 \\
&\leqslant \sum_{N\leqslant d\leqslant 2N} \sum_{x-(2N)^r\delta\leqslant md^r\leqslant x+(2N)^r\delta} 1 = \sum_{x-(2N)^r\delta\leqslant n\leqslant x+(2N)^r\delta} \sum_{\substack{d^r|n\\ N\leqslant d\leqslant 2N}} 1 \\
&\leqslant \sum_{x-(2N)^r\delta\leqslant n\leqslant x+(2N)^r\delta} \tau^{(r)}(n) \\
&\ll \frac{2^{r+1}N^r\delta}{\log x} \exp\Big(\sum_{p\leqslant x} \frac{\tau^{(r)}(p)}{p}\Big) + x^\varepsilon \ll_{r,\varepsilon} N^r\delta
\end{aligned}$$

where we used Theorem 4.62 with the fact that $r \geqslant 2$, and Corollary 3.50.

8.

(a) Using respectively the inequalities $\delta^{-1} \geqslant c_0^{-1}N$ and $N^{-1} > (c_0^{-1}x)^{-1/3}$, we get

$$\frac{A}{R} = N^{-2/3}x^{1/6}\delta^{-1/6} \geqslant c_0^{-1/6}N^{-1/2} > c_0^{-1/6}\big(c_0^{-1}x\big)^{-1/6}x^{1/6} = 1$$

and similarly using $N \geqslant 2(x\delta)^{-1/2}$, we obtain

$$\frac{N}{2A} = 2^{-2/3}N^{1/3}(x\delta)^{1/6} \geqslant (x\delta)^{1/6}(x\delta)^{-1/6} = 1$$

so that

$$R < A \leqslant \frac{N}{2}.$$

(b) Inserting this value of A in the proof of Theorem 5.30 we get

$$|T| \ll \big(N^2\delta x\big)^{1/6} + \big(x\delta^{-2}N^{-4}\big)^{1/3} + \big(x\delta^7N^{11}\big)^{1/9}$$

implying the asserted result.

(c) For all $c_0^{-1}y \leqslant N \leqslant (c_0^{-1}x)^{1/3}$, we infer that

$$\mathcal{R}\Big(\frac{x}{n^2}, N, \frac{y}{N^2}\Big) \ll x^{1/5} + (xy)^{1/6} + \big(xy^{-2}\big)^{1/3} + \big(xy^7N^{-3}\big)^{1/9}$$

so that

$$\max_{c_0^{-1}y \leqslant N \leqslant (c_0^{-1}x)^{1/3}} \mathcal{R}\Big(\frac{x}{n^2}, N, \frac{y}{N^2}\Big) \ll x^{1/5} + (xy)^{1/6} + \big(xy^{-2}\big)^{1/3} + \big(xy^4\big)^{1/9}$$
$$\ll \big(xy^4\big)^{1/9}$$

since $x^{1/5} \leqslant y \leqslant x^{1/3}$. Furthermore, it has been proved in Corollary 5.35 that

$$\max_{2\sqrt{y} \leqslant N \leqslant c_0^{-1}y} \mathcal{R}\Big(\frac{x}{n^2}, N, \frac{y}{N^2}\Big) \ll x^{1/10}y^{2/5} + (xy)^{1/7} + y^{2/3} + \big(x^{-1}y^4\big)^{1/3}$$
$$\ll \big(xy^4\big)^{1/9}$$

since $x^{1/5} \leqslant y \leqslant x^{1/3}$. Finally, by (5.29), we have

$$\max_{N \leqslant 2c_0^{2/3}x^{1/3}} \mathcal{R}\Big(\sqrt{\frac{x}{n}}, N, \frac{y}{\sqrt{Nx}}\Big) \ll x^{1/5}(\log x)^{2/5}$$

if c_0 is sufficiently small. Clearly $y^{1/2} \leqslant (xy^4)^{1/9}$, so that Lemma 5.3 with $A = 2\sqrt{y}$ and $B = (c_0^{-1}x)^{1/3}$ implies the asserted result. Note also that, since $y \geqslant x^{1/5}$, then

$$x^{1/15}y^{2/3} \geqslant \big(xy^4\big)^{1/9}.$$

9. Using Theorem 5.22 we get for all $4y < N \leqslant x$

$$\mathcal{R}\Big(\frac{x}{n}, N, \frac{y}{N}\Big) \ll x^{1/3} + y + (xy)^{1/2}N^{-1} + N\big(yx^{-1}\big)$$

so that

$$\max_{4y < N \leqslant x} \mathcal{R}\Big(\frac{x}{n}, N, \frac{y}{N}\Big) \ll x^{1/3} + y + \big(xy^{-1}\big)^{1/2}$$

and the second term dominates the others in view of $y \geqslant x^{1/3}$.

10. We use induction on k, the case $k = 2a$ coming from (5.26) and the fact that $k = 2a \geqslant 4$. Assume that the estimate is true for some $k \geqslant 2a$. By induction hypothesis and (5.26) used with $k+1$ instead of k, we get $\mathcal{R}(f, N, \delta) \ll \min(E, F)$ where

$$E = \max\big(T^{\frac{2}{(k+1)(k+2)}}N^{\frac{k}{k+2}},\ N\delta^{\frac{2}{k(k+1)}},\ N\big(\delta T^{-1}\big)^{\frac{1}{k+1}}\big) = \max(e_1, e_2, e_3)$$

and

$$F = \max\big(T^{\frac{2}{k(k+1)}} N^{\frac{k-1}{k+1}},\ N\delta^{\frac{1}{a(2a-1)}}\big) = \max(f_1, f_2)$$

say. The result is proved except in the cases $\min(e_2, f_1)$ and $\min(e_3, f_1)$. As in Proposition 5.24, the following inequality

$$\min(x, y) \leqslant x^a y^{1-a}$$

with $0 \leqslant a \leqslant 1$, is used.

▹ *Case* $\min(e_2, f_1)$. We choose $a = \frac{k-2a}{(k-a)(k+2)} \in [0, 1]$ which gives

$$\mathcal{R}(f, N, \delta) \ll T^{\frac{2}{(k+1)(k+2)}} N^{\frac{k}{k+2}} \big(T N^{-a} \delta^{1-2a/k}\big)^{\frac{2}{(k-a)(k+1)(k+2)}} \ll T^{\frac{2}{(k+1)(k+2)}} N^{\frac{k}{k+2}}$$

by (5.50) and the fact that $k \geqslant 2a$ and $\delta < \frac{1}{4}$.

▹ *Case* $\min(e_3, f_1)$. We choose $a = \frac{2}{k+2}$ which gives

$$\mathcal{R}(f, N, \delta) \ll T^{\frac{2}{(k+1)(k+2)}} N^{\frac{k}{k+2}} \big(N\delta T^{-1}\big)^{\frac{2}{(k+1)(k+2)}} \ll T^{\frac{2}{(k+1)(k+2)}} N^{\frac{k}{k+2}}$$

by (5.50) again. This completes the proof.

Using this result with $a = 2$ we get

$$\mathcal{R}(f, N, \delta) \ll T^{\frac{2}{k(k+1)}} N^{\frac{k-1}{k+1}} + N\delta^{1/6}$$

if $N\delta \leqslant T \leqslant N^2$. This result is useful since the condition $T \leqslant N^2$ (i.e. $\lambda_2 \leqslant 1$) is often satisfied in the usual applications.

A.6 Chapter 6

1.

(a) We have

$$\big|e(x) - e(y)\big| = \big|e(y)\big| \times \big|e(x-y) - 1\big| = \big|e(x-y) - 1\big| = 2\big|\sin \pi(x-y)\big|$$

and we conclude using Exercise 2 in Chap. 5.

(b) If $\alpha \in \mathbb{Z}$, then $e(\alpha n + \beta) = e(\beta)$ so that

$$\left|\sum_{n=M+1}^{N} e(\alpha n + \beta)\right| = \left|\sum_{n=M+1}^{N} 1\right| = N - M.$$

Assume that $\alpha \notin \mathbb{Z}$. Using the previous inequality we get

$$\left|\sum_{n=M+1}^{N} e(\alpha n + \beta)\right| = \left|\sum_{n=M+1}^{N} e(\alpha n)\right| = \frac{|e(N\alpha) - e(M\alpha)|}{|e(\alpha) - 1|} \leqslant \frac{2}{4\|\alpha\|} = \frac{1}{2\|\alpha\|}$$

as asserted.

2.

(a) We have

$$\Big|\sum_{N<n\leqslant N_1} e\big(\pm f(n)\big)\Big| \leqslant \Big|\sum_{\substack{N<n\leqslant N_1\\ \|f'(n)\|<\delta}} e\big(\pm f(n)\big)\Big| + \Big|\sum_{\substack{N<n\leqslant N_1\\ \|f'(n)\|\geqslant\delta}} e\big(\pm f(n)\big)\Big|$$

$$\leqslant \mathcal{R}\big(f', N, \delta\big) + \Big|\sum_{\substack{N<n\leqslant N_1\\ \|f'(n)\|\geqslant\delta}} e\big(\pm f(n)\big)\Big|.$$

Since f' is non-decreasing and $f'(N_1) - f'(N) \ll N\lambda_2$ by the mean-value theorem, the interval $f'([N, N_1])$ has at most $\ll N\lambda_2 + 1$ integers by Proposition 1.11 (vi). It follows that the set $\{x \in [N, N_1] : \|f'(x)\| \geqslant \delta\}$ can be partitioned in at most $\ll N\lambda_2 + 1$ subintervals, and the Kusmin–Landau inequality (Corollary 6.7) applied on each of these intervals implies the asserted estimate.

(b) Applying Theorem 5.6 we get

$$\sum_{N<n\leqslant N_1} e\big(f(n)\big) \ll N\lambda_2 + N\delta + \delta\lambda_2^{-1} + N\lambda_2\delta^{-1} + \delta^{-1} + 1$$

$$\ll N\lambda_2\delta^{-1} + N\delta + \delta\lambda_2^{-1} + \delta^{-1}$$

and choosing $\delta = \lambda_2^{1/2}$ gives

$$\sum_{N<n\leqslant N_1} e\big(f(n)\big) \ll N\lambda_2^{1/2} + \lambda_2^{-1/2}$$

as required.

3. Squaring out we get

$$\Big|\sum_{h=0}^{H-1} e(ha)\Big|^2 = \sum_{h_1=0}^{H-1} e(h_1 a) \sum_{h_2=0}^{H-1} e(-h_2 a) = \sum_{h_1=0}^{H-1}\sum_{h_2=0}^{H-1} e\big((h_1 - h_2)a\big).$$

Now set $h_1 = h + k$ and $h_2 = k$ so that

$$\begin{cases} 0 \leqslant h_1 \leqslant H-1, \\ 0 \leqslant h_2 \leqslant H-1 \end{cases} \iff \begin{cases} 0 \leqslant k \leqslant H-1, \\ -h \leqslant k \leqslant H-1-h \end{cases}$$

$$\iff \begin{cases} |h| \leqslant H-1, \\ 0 \leqslant k \leqslant H-1-|h| \end{cases}$$

and hence

$$\left|\sum_{h=0}^{H-1} e(ha)\right|^2 = \sum_{|h|\leqslant H-1} \sum_{k=0}^{H-1-|h|} e(ha) = \sum_{|h|\leqslant H-1} (H-|h|)e(ha)$$

as required.

4. We may obviously assume that $\mathcal{R}(f,N,\delta)\neq 0$, otherwise the inequality (6.29) is trivial.

(a) There exist $m\in\mathbb{Z}$ and $\delta_0\in\mathbb{R}$ such that $f(n)=m+\delta_0$ with $|\delta_0|<\delta$, so that

$$hf(n) = hm + h\delta_0 \quad \text{with} \quad |h\delta_0| < (H-1)\delta \leqslant (K-1)\delta \leqslant \frac{1}{8}$$

and thus

$$\mathrm{Re}\big\{e\big(hf(n)\big)\big\} = \cos\big(2\pi hf(n)\big) = \cos(2\pi hm + 2\pi h\delta_0) = \cos(2\pi h\delta_0) > \frac{\sqrt{2}}{2}$$

since $2\pi|h\delta_0|<\pi/4$.

(b) Summing the previous inequality over n and h running respectively through the whole set $\mathcal{S}(f,N,\delta)$ and the integers $\{0,\dots,H-1\}$, we obtain

$$\begin{aligned} H\mathcal{R}(f,N,\delta) &\leqslant \sqrt{2}\sum_{n\in\mathcal{S}(f,N,\delta)} \mathrm{Re}\left(\sum_{h=0}^{H-1} e\big(hf(n)\big)\right) \\ &\leqslant \sqrt{2}\sum_{n\in\mathcal{S}(f,N,\delta)} \left|\sum_{h=0}^{H-1} e\big(hf(n)\big)\right|. \end{aligned}$$

Applying the Cauchy–Schwarz inequality gives

$$\begin{aligned} \mathcal{R}(f,N,\delta) &\leqslant \frac{\sqrt{2}}{H}\left(\sum_{n\in\mathcal{S}(f,N,\delta)} 1\right)^{1/2}\left(\sum_{n\in\mathcal{S}(f,N,\delta)} \left|\sum_{h=0}^{H-1} e\big(hf(n)\big)\right|^2\right)^{1/2} \\ &= \frac{\sqrt{2}}{H}\mathcal{R}(f,N,\delta)^{1/2}\left(\sum_{n\in\mathcal{S}(f,N,\delta)} \left|\sum_{h=0}^{H-1} e\big(hf(n)\big)\right|^2\right)^{1/2} \end{aligned}$$

so that squaring out we get

$$\mathcal{R}(f,N,\delta) \leqslant \frac{2}{H^2}\sum_{n\in\mathcal{S}(f,N,\delta)} \left|\sum_{h=0}^{H-1} e\big(hf(n)\big)\right|^2 \leqslant \frac{2}{H^2}\sum_{N\leqslant n\leqslant 2N} \left|\sum_{h=0}^{H-1} e\big(hf(n)\big)\right|^2$$

as asserted.

Now using Exercise 3 we obtain

$$\mathcal{R}(f,N,\delta) \leqslant \frac{2}{H^2} \sum_{N\leqslant n\leqslant 2N} \sum_{|h|\leqslant H-1} (H-|h|)e\big(hf(n)\big)$$

and treating the cases $h=0$ and $h\neq 0$ separately we get

$$\begin{aligned}
\mathcal{R}(f,N,\delta) &\leqslant \frac{2(N+1)}{H} + \frac{2}{H^2} \sum_{N\leqslant n\leqslant 2N} \sum_{\substack{|h|\leqslant H-1\\ h\neq 0}} (H-|h|)e\big(hf(n)\big) \\
&\leqslant \frac{4N}{H} + \frac{2}{H} \sum_{N\leqslant n\leqslant 2N} \sum_{\substack{|h|\leqslant H-1\\ h\neq 0}} \Big(1-\frac{|h|}{H}\Big)e\big(hf(n)\big) \\
&= \frac{4N}{H} + \frac{2}{H} \sum_{h=1}^{H-1} \Big(1-\frac{h}{H}\Big) \sum_{N\leqslant n\leqslant 2N} \big\{e\big(hf(n)\big) + e\big(-hf(n)\big)\big\} \\
&\leqslant \frac{4N}{H} + \frac{4}{H} \sum_{h=1}^{H-1} \mathrm{Re}\Big(\sum_{N\leqslant n\leqslant 2N} e\big(hf(n)\big)\Big) \\
&\leqslant \frac{4N}{H} + \frac{4}{H} \sum_{h=1}^{H-1} \Big| \sum_{N\leqslant n\leqslant 2N} e\big(hf(n)\big)\Big|
\end{aligned}$$

completing the proof of (6.29).

5. By Definition 6.34 and the inequality (6.29), we get for all integers $1\leqslant H\ll \delta^{-1}$

$$\begin{aligned}
\mathcal{R}(f,N,\delta) &\ll NH^{-1} + H^{-1} \sum_{h\leqslant H} \big((hT)^k N^{l-k} + N(hT)^{-1}\big) \\
&\ll NH^{-1} + (HT)^k N^{l-k} + NT^{-1} \ll NH^{-1} + (HT)^k N^{l-k}
\end{aligned}$$

since $N\leqslant 8T$. We conclude the proof by using Lemma 5.5.

6.

▹ *Squarefree problem.* Let x, y be real numbers satisfying (5.5). Using the exponent pair (6.19), we get for all $N\leqslant 2x^{1/3}$

$$\mathcal{R}\Big(\sqrt{\frac{x}{n}}, N, \frac{y}{\sqrt{Nx}}\Big) \ll \big(x^{97}N^{167}\big)^{1/696} + \big(x^{97}N^{-27}\big)^{1/502} + y\big(Nx^{-1}\big)^{1/2}$$

so that

$$\max_{N\leqslant 2x^{1/3}} \mathcal{R}\Big(\sqrt{\frac{x}{n}}, N, \frac{y}{\sqrt{Nx}}\Big) \ll x^{229/1044} + yx^{-1/3}.$$

Next we apply the transformation BA to Huxley's exponent pair $(\frac{32}{205}+\varepsilon, \frac{1}{2}+\frac{32}{205}+\varepsilon)$ giving the exponent pair

$$\left(\frac{269}{948}+\varepsilon,\ \frac{269}{474}+\varepsilon\right)$$

where the small real number $\varepsilon > 0$ need not have the same occurrence at each computation. This implies for all $2\sqrt{y} < N \leqslant 2x^{1/3}$ and all $\varepsilon > 0$

$$\mathcal{R}\left(\frac{x}{n^2}, N, \frac{y}{N^2}\right) \ll x^{269/1217+\varepsilon} + \left(xN^{-1}\right)^{269/948+\varepsilon} + yN^{-1}$$

so that

$$\max_{x^{1/4}<N\leqslant 2x^{1/3}} \mathcal{R}\left(\frac{x}{n^2}, N, \frac{y}{N^2}\right) \ll x^{269/1217+\varepsilon} + y^{1/2}.$$

The exponent pair $(\frac{1}{6}, \frac{2}{3})$ provides the bound

$$\mathcal{R}\left(\frac{x}{n^2}, N, \frac{y}{N^2}\right) \ll \left(N^2x\right)^{1/7} + (Nx)^{1/6} + yN^{-1}$$

for all $2\sqrt{y} < N \leqslant 2x^{1/3}$, so that

$$\max_{2\sqrt{y}<N\leqslant x^{1/4}} \mathcal{R}\left(\frac{x}{n^2}, N, \frac{y}{N^2}\right) \ll x^{3/14} + y^{1/2}.$$

Hence using Lemma 5.3 with $A = 2\sqrt{y}$ and $B = x^{1/3}$ we get for all x, y satisfying (5.5) and $\varepsilon > 0$

$$\sum_{x<n\leqslant x+y} \mu_2(n) = \frac{y}{\zeta(2)} + O_\varepsilon\left(x^{269/1217+\varepsilon} + y^{1/2}\right).$$

▹ *Square-full problem.* We take up the notation of Exercise 6 in Chap. 5 and let x, y be real numbers satisfying (5.45). Using the exponent pair (6.19), we get

$$\mathcal{R}\left(\left(\frac{x}{a^2}\right)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\right) \ll \left(x^{97}A^{202}\right)^{1/1044} + \left(x^{97}A^{-89}\right)^{1/753} + y\left(Ax^{-2}\right)^{1/3}$$

so that

$$\max_{L<A\leqslant(2x)^{1/5}} \mathcal{R}\left(\left(\frac{x}{a^2}\right)^{1/3}, A, \frac{y}{(Ax)^{2/3}}\right) \ll x^{229/1740} + yx^{-3/5}.$$

Using (6.19) again, we get

$$\mathcal{R}\left(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\right) \ll \left(x^{97}B^{-27}\right)^{1/696} + \left(x^{97}B^{-221}\right)^{1/502} + \frac{y}{\sqrt{Bx}}$$

so that

$$\max_{x^{59/313}<B\leqslant(2x)^{1/5}} \mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll x^{124/939} + yx^{-186/313}.$$

The exponent pair $BA^2B(0,1) = (\frac{2}{7}, \frac{4}{7})$ provides the estimate

$$\mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll (Bx)^{1/9} + \big(xB^{-1}\big)^{1/7} + \frac{y}{\sqrt{Bx}}$$

valid for all $L < B \leqslant (2x)^{1/5}$, so that

$$\max_{x^{1/8}<B\leqslant x^{59/313}} \mathcal{R}\Big(\sqrt{\frac{x}{b^3}}, B, \frac{y}{\sqrt{xB^3}}\Big) \ll x^{124/939} + yx^{-9/16}.$$

Completing the proof with the trivial bound for R_1 in the range $]L, x^{1/8}]$ we finally get for all x, y satisfying (5.45)

$$\sum_{x<n\leqslant x+y} s_2(n) = \frac{\zeta(3/2)}{2\zeta(3)}\frac{y}{x^{1/2}} + O\big(x^{124/939}\log x + L\big).$$

7.

(a) This is [GK91, Lemma 2.11].

(b) Let $1 \leqslant T < t$ and let (k, l) be an exponent pair. We have

$$\begin{aligned}
\Big|\sum_{n\leqslant t} n^{-\sigma-it}\Big| &\leqslant \Big|\sum_{n\leqslant T} n^{-\sigma-it}\Big| + \Big|\sum_{T<n\leqslant t} n^{-\sigma-it}\Big| \\
&\ll \sum_{n\leqslant T} n^{-\sigma} + \max_{T<N\leqslant t}\Big|\sum_{N<n\leqslant 2N} n^{-\sigma-it}\Big|\log t \\
&\ll \sum_{n\leqslant T} n^{-\sigma} + \max_{T<N\leqslant t} N^{-\sigma}\max_{N\leqslant N_1\leqslant 2N}\Big|\sum_{N\leqslant n\leqslant N_1} n^{-it}\Big|\log t \\
&\ll T^{1-\sigma} + \max_{T<N\leqslant t} N^{-\sigma}\max_{N\leqslant N_1\leqslant 2N}\big(t^k N^{l-k} + Nt^{-1}\big)\log t \\
&\ll T^{1-\sigma} + \max_{T<N\leqslant t}\big(t^k N^{l-k-\sigma} + t^{-1}N^{1-\sigma}\big)\log t.
\end{aligned}$$

Now since $l - k \leqslant \frac{1}{2}$ and $\frac{1}{2} \leqslant \sigma \leqslant 1$, we deduce that $k + \sigma \geqslant l$. This implies that

$$\sum_{n\leqslant t} n^{-\sigma-it} \ll T^{1-\sigma} + t^k T^{l-k-\sigma}\log t$$

and the choice of $T = t^{\frac{k}{1+k-l}}$ gives

$$\sum_{n \leqslant t} n^{-\sigma - it} \ll t^{\frac{k(1-\sigma)}{1+k-l}} \log t.$$

Note that $0 \leqslant k \leqslant \frac{1}{2} \leqslant l \leqslant 1$ and $l - k \leqslant \frac{1}{2}$ imply that $\frac{1}{2} \leqslant 1 + k - l \leqslant 1$. Using the previous question, we get

$$\zeta(\sigma + it) \ll \left(t^{\frac{k(1-\sigma)}{1+k-l}} + t^{1-2\sigma}\right) \log t$$

and the second term is clearly absorbed by the first one. With $\sigma = \frac{1}{2}$ this gives for all $t \geqslant 3$

$$\zeta\left(\frac{1}{2} + it\right) \ll t^{\frac{k}{2(1+k-l)}} \log t$$

and Huxley's exponent pair $(\frac{32}{205} + \varepsilon, \frac{1}{2} + \frac{32}{205} + \varepsilon)$ provides the bound

$$\zeta\left(\frac{1}{2} + it\right) \ll t^{32/205+\varepsilon}$$

for all $t \geqslant 3$ and $\varepsilon > 0$, which is the best result up to now.

A.7 Chapter 7

1. Let $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$. Suppose that 3 is not an irreducible so that $3 = rs$ with $N_{\mathbb{K}/\mathbb{Q}}(r) \neq 1$ and $N_{\mathbb{K}/\mathbb{Q}}(s) \neq 1$. Since $9 = N_{\mathbb{K}/\mathbb{Q}}(3) = N_{\mathbb{K}/\mathbb{Q}}(r)\, N_{\mathbb{K}/\mathbb{Q}}(s)$, we must then have $N_{\mathbb{K}/\mathbb{Q}}(r) = N_{\mathbb{K}/\mathbb{Q}}(s) = 3$ and hence $a^2 + 5b^2 = 3$ for some $a, b \in \mathbb{Z}$. This implies that $b = 0$ and thus $a^2 = 3$ which is impossible.

Similarly, if $7 = rs$ where neither r nor s is a unit, then we must have $a^2 + 5b^2 = 7$, implying that either $b = 0$ and $a^2 = 7$ or $b = \pm 1$ and $a^2 = 2$, both cases being impossible.

If $1 \pm 2\sqrt{-5} = rs$ where neither r nor s is a unit, then

$$21 = N_{\mathbb{K}/\mathbb{Q}}(1 \pm 2\sqrt{-5}) = N_{\mathbb{K}/\mathbb{Q}}(r)\, N_{\mathbb{K}/\mathbb{Q}}(s)$$

and hence either $N_{\mathbb{K}/\mathbb{Q}}(r) = 3$ or $N_{\mathbb{K}/\mathbb{Q}}(s) = 3$, which is impossible as was seen above.

2. θ is algebraic over $\mathbb{Q}$ as sum of two algebraic numbers over $\mathbb{Q}$. This gives the answer to the exercise, but does not provide the minimal polynomial of θ.

To do this, one may use the following lemma, useful for small degrees (see [Coh00, Proposition 2.1.7]).

Lemma *Let α, β be algebraic over $\mathbb{Q}$ and $P, Q \in \mathbb{Q}[X]$ such that $P(\alpha) = Q(\beta) = 0$. Then the resultant*

$$R = \mathrm{Res}_Y\big(P(X), Q(Y - X)\big)$$

satisfies $R \in \mathbb{Q}[Y]$ and $R(\alpha + \beta) = 0$.

Proof We have clearly $R \in \mathbb{Q}[Y]$. Furthermore, R is equal to zero if and only if P and Q have a common root. But $R(\alpha+\beta)$ is the resultant of $P(X)$ and $Q(\alpha+\beta-X)$ which have α as a common root, and hence $R(\alpha + \beta) = 0$. □

Applying this result with $P = X^5 - 2$ and $Q = X^3 - 2$ we get

$$R = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 \\ -1 & 3Y & -3Y^2 & Y^3-2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 3Y & -3Y^2 & Y^3-2 & 0 & 0 & 0 \\ 0 & 0 & -1 & 3Y & -3Y^2 & Y^3-2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 3Y & -3Y^2 & Y^3-2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 3Y & -3Y^2 & Y^3-2 \end{vmatrix}$$

$$= Y^{15} - 10Y^{12} - 6Y^{10} + 40Y^9 - 360Y^7 - 80Y^6 + 12Y^5 - 1080Y^4 + 80Y^3 - 240Y^2 - 240Y - 40.$$

Furthermore, this polynomial is irreducible over $\mathbb{Z}$ by applying Ore's criterion since $|P(m)|$ is prime for

$$m \in \{-653, -579, -532, 459, -447, -429, -427, -367, -337, -271, -81, -43 \\ 51, 209, 213, 339, 423, 509, 521, 581\}.$$

Hence $\deg(2^{1/3} + 2^{1/5}) = 15$.

3. P is irreducible over $\mathbb{Z}$ since $\deg P = 3$ and P has no rational root. Indeed, if P has such a root, then it must be ± 1 by using Exercise 17 in Chap. 3, and $P(\pm 1) = 1$. This implies that $2\alpha^2 - 3\alpha + 2 \neq 0$ and then β is well-defined. Furthermore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $\{1, \alpha, \alpha^2\}$ is a $\mathbb{Q}$-base of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Therefore there exist $x, y, z \in \mathbb{Q}$ such that

$$\frac{1}{2\alpha^2 - 3\alpha + 2} = x + y\alpha + z\alpha^2.$$

This may be written as $(2\alpha^2 - 3\alpha + 2)(x + y\alpha + z\alpha^2) = 1$ and expanding the product and using the relations $\alpha^3 = \alpha - 1$ and $\alpha^4 = \alpha^2 - \alpha$ we get

$$\alpha^2(2x - 3y + 4z) + \alpha(-3x + 4y - 5z) + 2x - 2y + 3z - 1 = 0$$

implying that $x = z = 1$ and $y = 2$, so that

$$\frac{1}{2\alpha^2 - 3\alpha + 2} = 1 + 2\alpha + \alpha^2.$$

This gives $\beta^2 = 7\alpha^2 + 7\alpha - 3$ and $\beta^3 = 25\alpha^2 + 15\alpha - 24$, so that

$$\beta^3 - 5\beta^2 + 10\beta - 1 = 0.$$

One easily checks that the polynomial $Q = X^3 - 5X^2 + 10X - 1$ is irreducible over $\mathbb{Z}$, and hence Q is the minimal polynomial of β.

4. Set $\theta = \sqrt{5} + \sqrt[4]{2}$. We have obviously $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt[4]{2})$. Conversely, since $(\theta - \sqrt{5})^4 = 2$, expanding the product we get

$$\theta^4 + 30\theta^2 + 23 = \sqrt{5}\big(4\theta^3 + 20\theta\big)$$

so that

$$\sqrt{5} = \frac{\theta^4 + 30\theta^2 + 23}{4\theta^3 + 20\theta}$$

and hence $\sqrt{5} \in \mathbb{Q}(\theta)$. Thus

$$\sqrt[4]{2} = \theta - \sqrt{5} \in \mathbb{Q}(\theta, \sqrt{5}) \subseteq \mathbb{Q}(\theta).$$

Therefore we get

$$\mathbb{Q}\big(\sqrt{5}, \sqrt[4]{2}\big) \subseteq \mathbb{Q}\big(\sqrt{5} + \sqrt[4]{2}\big)$$

as required. Now using the lemma of Exercise 2 we infer that θ is a root of the polynomial

$$P = X^8 - 20X^6 + 146X^4 - 620X^2 + 529$$

and $|P(m)|$ is prime for $\pm m \in \{6, 12, 18, 60, 66, 120, 132\}$ so that P is irreducible over $\mathbb{Z}$ by Proposition 7.28. Hence

$$\big[\mathbb{Q}\big(\sqrt{5} + \sqrt[4]{2}\big) : \mathbb{Q}\big] = 8.$$

5. We first have

$$F_n = n!\, P_n = \sum_{k=0}^{n} \frac{n!}{k!} X^k.$$

1. Let p be a prime factor of $n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!}$. Therefore for all $0 \leqslant k \leqslant n-m$, p divides $(n!/k!)$ which is the coefficient of X^k in $F_n(X)$, so that $F_n(X) \bmod p$ is divisible by X^{n-m+1}.

If $F_n = A_m B$ with $B \in \mathbb{Z}[X]$ is monic such that $\deg B = n - m$, then X^{n-m+1} divides $\overline{A_m} \times \overline{B}$ in $\mathbb{F}_p[X]$. Since $\deg \overline{B} = n - m$, we get $X \mid \overline{A_m}$. This implies that $\overline{A_m}(0) = \overline{0}$ as required.

2. a. First note that $\theta \in \mathcal{O}_{\mathbb{K}}$ since A_m is monic. By the previous question, we get

$$N_{\mathbb{K}/\mathbb{Q}}(\theta) = \pm a_0 \equiv 0 \pmod{p}$$

so that $p \mid \mathcal{N}_{\mathbb{K}/\mathbb{Q}}((\theta))$.

b. Since $F_n(\theta) = 0$, we have

$$-n! = \sum_{k=1}^{n} \frac{n!\theta^k}{k!}$$

hence there exists an index $k \in \{1, \ldots, n\}$ such that

$$v_{\mathfrak{p}}\left(\frac{n!\theta^k}{k!}\right) \leqslant v_{\mathfrak{p}}(n!).$$

Since

$$v_{\mathfrak{p}}\left(\frac{n!\theta^k}{k!}\right) = v_{\mathfrak{p}}(n!) + k\alpha - v_{\mathfrak{p}}(k!) = v_{\mathfrak{p}}(n!) + k\alpha - ev_p(k!)$$

we get

$$k\alpha - ev_p(k!) \leqslant 0.$$

c. By Exercise 12 in Chap. 3, we get

$$k\alpha \leqslant \frac{e(k-1)}{p-1}$$

and hence

$$(p-1)\alpha \leqslant \frac{e(k-1)}{k} < e \leqslant m$$

so that

$$p < \frac{m}{\alpha} + 1 \leqslant m + 1$$

implying that $p \leqslant m$.

3. By the first question, all the prime factors of $n, n-1, \ldots, n-m+1$ divide a_0 and the previous question shows that each of these prime factors is $\leqslant m$. Thus the numbers $n, n-1, \ldots, n-m+1$ form a sequence of m consecutive integers all greater than m which have no prime factor greater than m, contradicting Lemma 7.183.

Remark In [Col87], the author provided an elegant proof of Schur's result based upon the theory of Newton polygons for polynomials belonging to $\mathbb{Q}_p[X]$. Let us

compute the discriminant of P_n. If $\alpha_1, \ldots, \alpha_n$ are the roots of P_n in an algebraic closure of $\mathbb{Q}$, we have by Definition 7.36

$$\operatorname{disc}(P_n) = (n!)^{2-2n} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

We proceed as in the proof of Proposition 7.61 (iv). Writing $P_n = (n!)^{-1} \prod_{i=1}^{n} (X - \alpha_i)$, we infer that

$$\frac{P_n'}{P_n} = \sum_{i=1}^{n} \frac{1}{X - \alpha_i}$$

so that

$$P_n' = \frac{1}{n!} \sum_{i=1}^{n} \prod_{j \neq i} (X - \alpha_j)$$

and thus for all $i \in \{1, \ldots, n\}$, we get

$$n!\, P_n'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j).$$

This implies that

$$\begin{aligned} \prod_{i=1}^{n} n!\, P_n'(\alpha_i) &= \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= \prod_{i=1}^{n} \prod_{i<j} \bigl(-(\alpha_i - \alpha_j)^2\bigr) \\ &= (-1)^{n(n-1)/2} (n!)^{2n-2} \operatorname{disc}(P_n). \end{aligned}$$

Note that $P_n' = P_{n-1}$ and $P_n(X) = P_{n-1}(X) + x^n/n!$ so that

$$P_n'(\alpha_i) = P_n(\alpha_i) - \frac{\alpha_i^n}{n!} = -\frac{\alpha_i^n}{n!}$$

and hence

$$\begin{aligned} \operatorname{disc}(P_n) &= (-1)^{n(n-1)/2} (n!)^{2-2n} \prod_{i=1}^{n} \bigl(-\alpha_i^n\bigr) \\ &= (-1)^{n(n-1)/2+n} (n!)^{2-2n} \left(\prod_{i=1}^{n} \alpha_i \right)^n \\ &= (-1)^{n(n-1)/2+n} (n!)^{2-2n} \bigl((-1)^n n!\bigr)^n \\ &= (-1)^{n(n-1)/2} (n!)^{2-n}. \end{aligned}$$

We deduce that if $n \equiv 2$ or $3 \pmod 4$, then $\operatorname{disc}(P_n) < 0$ and hence $\operatorname{disc}(P_n)$ is not a square in $\mathbb{Q}$. If $n \equiv 0 \pmod 4$, then $n-2$ is even and thus $\operatorname{disc}(P_n)$ is a square in $\mathbb{Q}$. Now assume that $n \equiv 1 \pmod 4$. By Corollary 3.44, for all $n \geqslant 2$, there exists a prime number p such that $n/2 < p \leqslant n$, so that $v_p(n!) = 1$. This implies that $v_p((n!)^n) = n$ is odd, and thus $(n!)^n$ is not a square in $\mathbb{Q}$ if $n \equiv 1 \pmod 4$ and $n \geqslant 2$. Therefore $\operatorname{disc}(P_n)$ cannot be a square in $\mathbb{Q}$ in this case. Furthermore, it can be proved that $\operatorname{Gal}(P_n/\mathbb{Q})$ contains a p-cycle for some prime number satisfying $n/2 < p < n-2$ (see [Col87] for instance). Using Lemma 7.144, we get the following result due to Schur too.

Proposition (Schur) *Let $n \in \mathbb{Z}_{\geqslant 2}$. Then*

$$\operatorname{Gal}(P_n/\mathbb{Q}) \simeq \begin{cases} \mathcal{A}_n, & \text{if } n \equiv 0 \pmod 4, \\ \mathcal{S}_n, & \text{otherwise.} \end{cases}$$

6.

(a) Since $\theta^n = -a_{n-1}\theta^{n-1} - \cdots - a_1\theta - a_0$ and $p \mid a_i$, we infer that $\theta^n/p \in M \subseteq \mathcal{O}_{\mathbb{K}}$ and that $N_{\mathbb{K}/\mathbb{Q}}(\theta) = a_0 \not\equiv 0 \pmod{p^2}$ by assumption.

(b) Since $p \mid f$, we deduce that there is an element of order p in $\mathcal{O}_{\mathbb{K}}/M$ by Theorem 7.1 (ii), so that there exists $\alpha \in \mathcal{O}_{\mathbb{K}}$ such that $\alpha \notin M$ and $p\alpha \in M$. Hence

$$p\alpha = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}$$

where not all the b_i are divisible by p, otherwise $\alpha \in M$.

(c) $\beta \in \mathcal{O}_{\mathbb{K}}$ since both α and $b_0 p^{-1} + \cdots + b^{j-1}\theta^{j-1}p^{-1}$ are in $\mathcal{O}_{\mathbb{K}}$. This implies that

$$\beta\theta^{n-j-1} = \frac{b_j\theta^{n-1}}{p} + \frac{\theta^n}{p}\left(b_{j+1} + b_{j+2}\theta + \cdots + b_n\theta^{n-j-2}\right)$$

is also in $\mathcal{O}_{\mathbb{K}}$. Now by the first question $\theta^n/p \in \mathcal{O}_{\mathbb{K}}$ and also $b_{j+1} + b_{j+2}\theta + \cdots + b_n\theta^{n-j-2} \in \mathcal{O}_{\mathbb{K}}$, so that

$$\frac{b_j\theta^{n-1}}{p} \in \mathcal{O}_{\mathbb{K}}.$$

By Proposition 7.55, we infer that the norm of this element must be an integer. But

$$N_{\mathbb{K}/\mathbb{Q}}\left(\frac{b_j\theta^{n-1}}{p}\right) = \left(\frac{b_j}{p}\right)^n N_{\mathbb{K}/\mathbb{Q}}(\theta)^{n-1} = \frac{b_j^n a_0^{n-1}}{p^n}$$

cannot be an integer since $p \nmid b_j$ and $p^2 \nmid a_0$.

7.

(a) P is irreducible over $\mathbb{Z}$ by Eisenstein's criterion with $p = 7$.

(b) Since $189 = 3^3 \times 7$ and $756 = 2^2 \times 3^3 \times 7$, we have $\mathbb{K} = \mathbb{Q}(\alpha)$ where $\alpha = \theta/3$ is a root of $Q = X^3 - 21X + 28$. We have $\operatorname{disc}(Q) = 2^2 \times 3^4 \times 7^2$ and use Proposition 7.70. The largest square n^2 dividing $\operatorname{disc}(Q)$ for which the system of congruences

$$\begin{cases} x^3 - 21x + 28 \equiv 0 \pmod{n^2}, \\ 3x^2 - 21 \equiv 0 \pmod{n} \end{cases}$$

is solvable for x is given by $n = 2$ and we get $x = 1$, so that

$$\left\{1, \alpha, \frac{-1 + \alpha + \alpha^2}{2}\right\} = \left\{1, \frac{\theta}{3}, -\frac{1}{2} + \frac{\theta}{6} + \frac{\theta^2}{18}\right\}$$

is an integral basis for $\mathbb{K}$.

(c) Since $\operatorname{disc}(P)$ is a square in $\mathbb{Q}$, we get $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathcal{A}_3 \simeq C_3$ by Lemma 7.145 (ii) or Lemma 7.140.

Since $(r_1, r_2) = (3, 0)$, we have $\mathcal{O}_{\mathbb{K}}^* \simeq W_{\mathbb{K}} \times \mathbb{Z}^2$ by Dirichlet's unit theorem (Theorem 7.74). Using Theorem 7.105 we get

$$(3) = \mathfrak{p}_3^3$$

with $\mathfrak{p}_3 = (3, \theta/3 + 1)$ and using the PARI/GP system we obtain

$$(6 - \theta) = \mathfrak{p}_2 \mathfrak{p}_3^4 \quad \text{and} \quad (12 - \theta) = \mathfrak{p}_2^3 \mathfrak{p}_3^3$$

with $\mathfrak{p}_2 = (2, \theta)$. This implies that

$$(6 - \theta)^3 = (3)^3 (12 - \theta)$$

and hence there exists a unit u such that $(6-\theta)^3 = 27u(12-\theta)$. Now expanding $(6 - \theta)^3$ and using $\theta^3 = 189\theta - 756$, we deduce that

$$18\theta^2 - 297\theta + 972 = 27u(12 - \theta)$$

so that

$$9(\theta - 12)(2\theta - 9) = 27u(12 - \theta)$$

and then $u = 3 - 2\theta/3$. Using PARI, the second unit is $u' = \theta^2/9 - 5\theta/3 + 5$ so that

$$\mathcal{R}_{\mathbb{K}} = \left| \det \begin{pmatrix} \log|3 - 2\theta/3| & \log|\theta^2/9 - 5\theta/3 + 5| \\ \log|3 - 2\theta'/3| & \log|\theta'^2/9 - 5\theta'/3 + 5| \end{pmatrix} \right| \approx 12.594\,188\,956\ldots$$

8. Since $-2 \not\equiv 1 \pmod 4$, we have $d_{\mathbb{K}} = -8$.

(a) ▹ Since $-8 \equiv 1 \pmod 3$, we get $(-8/3) = (1/3) = 1$ so that 3 splits completely in $\mathbb{K}$ by Proposition 7.108 and then

$$(3) = \mathfrak{p}_3 \overline{\mathfrak{p}_3}$$

where $\mathfrak{p}_3 = (1 + \sqrt{-2})$ and $\overline{\mathfrak{p}_3} = (1 - \sqrt{-2})$.

▹ Since $(1-\sqrt{-2})^2 = -1-2\sqrt{-2}$, we infer that $\mathfrak{a} = \overline{\mathfrak{p}_3}^2$, so that the equality $(1+2\sqrt{-2})^n = 3^n$ contradicts Theorem 7.88.

(b) Suppose that $\arccos(1/3)/\pi \in \mathbb{Q}$. There exists $(p,q) \in \mathbb{Z} \times \mathbb{Z}_{\geqslant 1}$ such that $(p,q) = 1$ and

$$\arccos\left(\frac{1}{3}\right) = \frac{p\pi}{q}.$$

Since

$$1+2\sqrt{-2} = 3e^{i\arccos(1/3)} = 3e^{ip\pi/q}$$

we have

$$(1+2\sqrt{-2})^{2q} = 3^{2q}$$

contradicting the previous question. Therefore, $\arccos(1/3)/\pi \notin \mathbb{Q}$.

9. First note that, if $\mathbb{k}_1 = \mathbb{Q}(\sqrt{a})$ and $\mathbb{k}_2 = \mathbb{Q}(\sqrt{b})$, then by assumption on a and b we get $d_{\mathbb{k}_i} \equiv 1 \pmod 3$, so that 3 splits completely in $\mathbb{k}_1$ and in $\mathbb{k}_2$ by Proposition 7.108. This implies that 3 splits completely in $\mathbb{K}$. Now assume that $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$ for some $\theta \in \mathbb{K}$. Then $\mathbb{K} = \mathbb{Q}(\theta)$ and the minimal polynomial μ of θ is of degree 4. By the previous observation, we infer that the reduction $\overline{\mu}$ in $\mathbb{F}_3[X]$ can be expressed as a product of four distinct monic linear polynomials, which is impossible since $\mathbb{F}_3$ has only three distinct elements.

10. We use Proposition 7.118.

▹ **Type I.** We have $\nu_{\mathbb{K}}(p^\alpha) = \mathcal{D}_{(1,1,1)}(\alpha) = \binom{\alpha+2}{2}$.

▹ **Type II.** In this case, p is inert so that by Remark 7.120 we get

$$\nu_{\mathbb{K}}\big(p^\alpha\big) = \begin{cases} 1, & \text{if } 3 \mid \alpha, \\ 0, & \text{otherwise.} \end{cases}$$

▹ **Type III.** We have $\nu_{\mathbb{K}}(p^\alpha) = \mathcal{D}_{(1,2)}(\alpha)$ which can be computed by using Theorem 2.32 or Popoviciu's result of Exercise 12 in Chap. 2. For instance, applying Popoviciu's theorem with $a=1$, $b=2$ and $n=\alpha$, we get $\overline{a}=1$ and thus

$$\nu_{\mathbb{K}}\big(p^\alpha\big) = \frac{\alpha}{2} + 1 - \left\{\frac{\alpha}{2}\right\} = \begin{cases} (\alpha+2)/2 & \text{if } \alpha \equiv 0 \pmod 2, \\ (\alpha+1)/2, & \text{if } \alpha \equiv 1 \pmod 2. \end{cases}$$

▹ **Type IV.** We have $\nu_{\mathbb{K}}(p^\alpha) = \mathcal{D}_{(1,1)}(\alpha) = \binom{\alpha+1}{1} = \alpha+1$.

▹ **Type V.** We have $g=1$ and thus we may use Remark 7.120, and since $e=3$, we get

$$\nu_{\mathbb{K}}\big(p^\alpha\big) = 1.$$

11.

(a) This is done in the proof of Proposition 7.138 using Corollary 7.130.
(b) We have $f_n(\sigma) = \sigma^{n+1}\pi^{-n\sigma/2}\Gamma(\sigma/2)^n$ and hence

$$g_n(\sigma) = \frac{2}{n} - (\log\pi + \gamma)\sigma + \sum_{k=1}^{\infty}\left(\frac{\sigma}{k} - \frac{\sigma}{k+\sigma/2}\right)$$

and thus

$$g_n''(\sigma) = 8\sum_{k=1}^{\infty}\frac{k}{(\sigma+2k)^3} > 0$$

so that g_n is convex on $]0, +\infty[$.
(c) For all $\sigma \in [1, 2]$, we deduce that

$$\begin{aligned} g_n(\sigma) &\leqslant \max\bigl(g_n(1),\ g_n(2)\bigr) \\ &= \max\left(2 - \gamma - \log(4\pi) + \frac{2}{n},\ 2\left(1 - \gamma - \log\pi + \frac{1}{n}\right)\right) \end{aligned}$$

and since $n \geqslant 2$ we obtain

$$g_n(\sigma) \leqslant \max\bigl(3 - \gamma - \log(4\pi),\ 3 - 2(\gamma + \log\pi)\bigr) < 0.$$

(d) The previous question implies that f_n is decreasing on $[1, 2]$ so that

$$f_n(\sigma_0) \leqslant f_n(1) = 1.$$

Therefore

$$\kappa_{\mathbb{K}} \leqslant \frac{d_{\mathbb{K}}^{(\sigma_0-1)/2}}{(\sigma_0-1)^{n-1}} = \left(\frac{e\log d_{\mathbb{K}}}{2n-2}\right)^{n-1}$$

and (7.21) gives then (7.23).

12. Since $\mathbb{K}$ is real, we have $(r_1, r_2) = (n, 0)$, $w_{\mathbb{K}} = 2$ and every character of $X(\mathbb{K}) = X$ is even, so that the class number formula seen in Remark 7.164 can be written in this case as

$$h_{\mathbb{K}}\mathcal{R}_{\mathbb{K}} = \frac{d_{\mathbb{K}}^{1/2}}{2^{n-1}}\prod_{\substack{\chi\in X\\ \chi\neq\chi_0}} L\bigl(1, \chi^\star\bigr)$$

where $\chi^\star$ is the primitive even Dirichlet character that induces χ. Now using (7.37) and the arithmetic-geometric mean inequality, we get

$$\prod_{\substack{\chi\in X\\ \chi\neq\chi_0}} \bigl|L\bigl(1, \chi^\star\bigr)\bigr| \leqslant \left(\frac{1}{2n-2}\sum_{\substack{\chi\in X\\ \chi\neq\chi_0}} \log f_{\chi^\star}\right)^{n-1}$$

and the conductor–discriminant formula (Theorem 7.162) implies that

$$\prod_{\substack{\chi\in X\\ \chi\neq\chi_0}} \left|L\big(1,\chi^\star\big)\right| \leqslant \left(\frac{\log d_{\mathbb{K}}}{2n-2}\right)^{n-1}$$

as required.

13. We proceed as in Example 7.175. We have $15 \equiv 3 \pmod 4$, the order $\mathcal{O} = \mathbb{Z}[\sqrt{-15}]$ has discriminant -60 and conductor $f = \sqrt{60/15} = 2$. By Lemma 7.172 (i), the class number of $\mathcal{O}$ is given by

$$h_{\mathcal{O}} = 2 \times 2 \times \left(1 - \frac{1}{2}\left(\frac{-15}{2}\right)\right) = 2$$

and, by Lemma 7.172 (ii), representatives of the two classes of invertible fractional ideals of $\mathcal{O}$ are

$$(1, \sqrt{-15}) \quad \text{and} \quad (3, \sqrt{-15})$$

and hence using PARI/GP we obtain

$$H_{\mathcal{O}} = X^2 - \big(3^3 \times 5^3 \times 10\,968\,319\big)X + \big(3^2 \times 5 \times 29 \times 41\big)^3.$$

By Corollary 7.174, we infer that a prime $p \geqslant 7$ can be expressed in the form $p = x^2 + 15y^2$ if and only if $(-15/p) = 1$ and the equation

$$x^2 - \big(3^3 \times 5^3 \times 10\,968\,319\big)x + \big(3^2 \times 5 \times 29 \times 41\big)^3 \equiv 0 \pmod p$$

has a solution in $\mathbb{Z}$.

References

[AS82] Adams W, Shanks D (1982) Strong primality tests that are not sufficient. Math Comput 39:255–300

[Bor06] Bordellès O (2006) An inequality for the class number. JIPAM J Inequal Pure Appl Math 7:87

[Coh00] Cohen H (2000) Advanced topics in computational algebraic number theory. GTM, vol 193. Springer

[Col87] Coleman R (1987) On the Galois groups of the exponential Taylor polynomials. Enseign Math 33:183–189

[GK91] Graham SW, Kolesnik G (1991) Van der Corput's method of exponential sums. London math. soc. lect. note series, vol 126. Cambridge University Press, Cambridge

[Gou72] Gould HW (1972) Combinatorial identities. A standardized set of tables listing 500 binomial coefficients summations. Morgantown, West Virginia

[HT88] Hall RR, Tenenbaum G (1988) Divisors. Cambridge University Press, Cambridge

[HW38] Hardy GH, Wright EM (1938) An introduction to the theory of numbers. Oxford, London

[Rn62] Rosser JB, Schœnfeld L (1962) Approximate formulas for some functions of prime numbers. Ill J Math 6:64–94

[Tri02] Trifonov O (2002) Lattice points close to a smooth curve and squarefull numbers in short intervals. J Lond Math Soc 65:309–319

Index

O. Bordellès, *Arithmetic Tales*, Universitext,
DOI 10.1007/978-1-4471-4096-2, © Springer-Verlag London 2012