Check whether the exam is complete: it should have 7 pages (Exercises 1–7). Write your name on the title page. Solutions have to be written below the exercises. Solutions must be comprehensible. In case of lack of space, additional paper can be asked from the exam supervision.

Use neither pencil nor red colored pen!

Duration: 180 min

Exercise 1: (Multiple Choice, points \{-1, 0, 1\} each)
No justifications needed. Mark ‘yes’ or ‘no’. \textbf{Wrong answers cause negative points!} Total number of points achieved cannot be negative.

\begin{tabular}{l|c|c|c|c|c|c|c|c|c|c}
Exercise: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & Σ \\
max points: & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 48 \\
achieved points: & & & & & & & & & \\
\end{tabular}

a) Let \( f, g : \mathbb{N} \to \mathbb{R}_+ \) be monotone increasing functions. If \( f = O(g) \), then \( f(n) \leq g(n) \) for all sufficiently large \( n \).

\( \circ \) yes \circ no

b) Given two natural numbers \( a, b \in \mathbb{N} \), one can test whether \( a \) is a factor of \( b \) in polynomial time in the bit-size of \( a \) and \( b \).

\( \circ \) yes \circ no

c) Given two natural numbers \( a, b \in \mathbb{N} \), one can compute \( a^b \in \mathbb{N} \) in polynomial time in the bit-size of \( a \) and \( b \).

\( \circ \) yes \circ no

d) For all \( n \in \mathbb{N} \) and for all \( x \in \mathbb{Z}_n^* \) one has \( x^{n-1} \equiv 1 \pmod{n} \).

\( \circ \) yes \circ no

e) Let \( R \) be a commutative ring and \( \omega \in R \) a primitive \( n \)-th root of unity. Then \( \omega^{n-1} \) is a primitive \( n \)-th root of unity.

\( \circ \) yes \circ no

f) Let \( F \) be a field and let \( f \in F[x_1, x_2] \) be a non-zero polynomial of total degree \( d \). Then \( f \) has at most \( d \) zeros.

\( \circ \) yes \circ no

g) Every non-trivial lattice contains at least two non-zero shortest vectors.

\( \circ \) yes \circ no

h) If \( F \) is a field of characteristic \( n \), then there exists a primitive \( n \)-th root of unity \( \omega \in F^* \).

\( \circ \) yes \circ no
Exercise 2: (8 points)

Consider the following algorithm:

\[
\text{ABC}(a, n) \\
\text{Input: } a \in \mathbb{N}, \ n = 2^k \text{ a power of two.} \\
1. \ \text{Print the pair } (a, n) \\
2. \ \text{if } n > 1 \\
3. \ \ \text{then } \text{ABC}(a + 1, n/2) \\
4. \ \ \text{ABC}(a + 2, n/2)
\]

1. Write down, in the correct order, everything that is printed by the call ABC(1, 8).
2. Let \( T(n) \) be the number of pairs printed in total by the call ABC\((a, n)\) for any \( a \). Derive an exact formula for \( T(n) \).

Solution:

1. \((1, 8), (2, 4), (3, 2), (4, 1), (5, 1), (4, 2), (5, 1), (6, 1), (3, 4), (4, 2), (5, 1), (6, 1), (5, 2), (6, 1), (7, 1)\)

2. We have \( T(1) = 1 \) and \( T(n) = 2T(n/2) + 1 \) for \( n = 2^k \geq 2 \) a power of two. This gives us

\[
T(n) = 2T(2^{k-1}) + 1 = 4T(2^{k-2}) + 2 + 1 \\
= 2^jT(2^{k-j}) + \sum_{i=0}^{j-1} 2^i \\
= 2^kT(1) + \sum_{i=0}^{k-1} 2^i = 2^k + 2^k - 1 \\
= 2n - 1
\]

Use reverse side if you need more space
Exercise 3: (8 points)
Let \( N = pq, \ p \neq q \) primes. Show that \( N \) is not a Carmichael number.

**Solution:**
Here is a very direct way of proving this.
Consider first any \( x \in \mathbb{Z}_N^* \) and keep in mind that \( \mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^* \). Looking at \( x \pmod{p} \) one gets
\[
X^{N-1} = X^{pq-1} = X^{(p-1)q + q-1} = X^{q-1} \pmod{p}
\]
So if \( q < p \), which we can assume without loss of generality, and \( x \), viewed as an element of \( \mathbb{Z}_p^* \), is a generator of \( \mathbb{Z}_p^* \), then \( X^{N-1} \not\equiv 1 \pmod{p} \) (because \( x \) has order \( p-1 > q-1 \)) and thus \( X^{N-1} \not\equiv 1 \pmod{N} \).
With this in mind and using the CRT, we simply choose \( x \) such that it is a generator of \( \mathbb{Z}_p^* \) modulo \( p \) and an arbitrary unit modulo \( q \), say 1, and the \( x \) so chosen will not be a Fermat liar modulo \( N \), which means that \( N \) is not Carmichael.
Exercise 4: (8 points)
Let $R$ be a ring and let $\omega \in R$ be a primitive $n$-th root of unity where $n \geq 3$ is an odd number. Prove that $\omega^2$ is a primitive $n$-th root of unity.

Solution:
Call $\eta = \omega^2$. We need to prove three things: $\eta^n = 1$, $\eta^k \neq 1$ for all $1 \leq k < n$, and $\eta^{n/t} - 1$ is not a zero divisor for proper divisors $t$ of $n$ ($n \in R^*$ is clear from the fact that $\omega$ is a primitive $n$-th root of unity).

1. $\eta^n = \omega^{2n} = (\omega^n)^2 = 1$. Assume $\eta^k = 1$. This implies $\omega^{2k} = 1$ which implies $2k$ is a multiple of $n$, so since $n$ is odd this means that $k$ is a multiple of $n$, contradiction.

2. We can factor

$$\omega^{n/t} - 1 = (\omega^{2n/t} - 1)(1 + \omega^{2n/t} + \omega^{4n/t} + \cdots + \omega^{(t-1)n/t})$$

To see that this is true, observe that because $n$ is odd, $t$ must be odd and so $t - 1$ is even, so the right factor is really a sum of powers of $\omega^{2n/t}$ which means that all terms cancel except for the lowest power and the highest power, i.e. the right factor multiples out to

$$\omega^{2n + (t-1)n/t} - 1 = \omega^{(t+1)n/t} - 1 = \omega^{n/t} - 1$$

So we see that $\eta^{n/t} - 1$ is a factor of an element which is not a zero divisor, and so it is also not a zero divisor. (If it were, then $(\eta^{n/t} - 1)x = 0$ for some non-zero $x \in R$, and then the above equality would show that also $(\omega^{n/t} - 1)x = 0$.)
Exercise 5: (8 points)
Let $F$ be a field and let $V$ be an $F$-vector space. For $f = \sum_{j=0}^{n} f_j x^j \in F[x]$ and $a = (a_i)_{i \in \mathbb{N}} \in V^\mathbb{N}$ we set
\[
 f \star a = \left( \sum_{j=0}^{n} f_j a_{i+j} \right)_{i \in \mathbb{N}} \in V^\mathbb{N}
\]
Let $a \in V^\mathbb{N}$ be linearly recurrent with minimal polynomial $f \in F[x]$. Furthermore, let $g \in F[x]$ be the minimal polynomial of $x^m \star a$. Prove that $f = x^k g$ for some $0 \leq k \leq m$.

Solution:
First observe that
\[
x^m \star a = (a_{i+m})_{i \in \mathbb{N}}
\]
Let $g = \sum_{j=0}^{n} g_j x^j$ be the minimal polynomial of $x^m \star a$. Consider the polynomial
\[
x^m g = \sum_{j=m}^{m+n} g_{j-m} x^j
\]
Since for any starting offset $s \in \mathbb{N}_0$ one has
\[
(x^m g \star a)_s = \sum_{j=m}^{m+n} g_{j-m} a_{s+j} = \sum_{j=0}^{n} g_j a_{s+j+m} = 0
\]
due to the fact that $g$ is a characteristic polynomial of $x^m \star a$. Thus $x^m g$ is a characteristic polynomial of $a$.
It remains to show that $g$ divides the minimal polynomial $f = \sum_{j=0}^{n} f_j x^j$ of $a$.
\[
(f \star (x^m \star a))_s = \sum_{j=0}^{r} f_j a_{s+j+m} = (f \star a)_{s+m} = 0
\]
It follows that $f$ is a characteristic polynomial of $x^m \star a$ and so is divided by $g$.
To summarize, $f = pg$ for some polynomial $p \in F[x]$, but furthermore $x^m g = qf = pqg$ for some polynomial $q \in F[x]$. It follows that $pq = x^m$, and so $f = x^k g$ for some $0 \leq k \leq m$.

Use reverse side if you need more space
Exercise 6: (8 points)
The Euclidean algorithm applied to natural numbers $r_0 \geq r_1$ uses division with remainder to compute finite sequences $(r_j)_{j=0}^m$ and $(q_j)_{j=2}^m$ of natural numbers where $r_{j-2} = q_j r_{j-1} + r_j$ until $r_m = 0$.

1. Perform the Euclidean algorithm starting with $r_0 = 57$ and $r_1 = 42$. Explicitly write down the sequences $(r_j)$ and $(q_j)$ that you obtain. (Note: You should get $m = 5$ and the last $q_j$ is $q_5 = 4$.)

2. Is $42 \in \mathbb{Z}^*_5$? Why? If it is, what is its inverse?

3. For arbitrary $a_1 \in \mathbb{N}_0, a_2, \ldots, a_\ell \in \mathbb{N} \geq 1$ we define the continued fraction

$$[a_1, \ldots, a_\ell] := a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots + \frac{1}{a_\ell}}}}$$

Show that $\frac{r_0}{r_1} = [q_2, \ldots, q_m]$, where $(q_j)_{j=2}^m$ is the sequence computed by the Euclidean algorithm started with $r_0 \geq r_1$.

Solution:

1. $r = (57, 42, 15, 12, 3, 0), q = (1, 2, 1, 4)$.

2. No, because the above calculation shows $\gcd(42, 57) = 3$.

3. Proof by induction on $m$, i.e. essentially number of iterations of the Euclidean algorithm. Since the first division by remainder is always performed, we always have $m \geq 2$.

In the base case $m = 2$, we get $r_0 = q_2 r_1$, i.e. $\frac{r_0}{r_1} = q_2 = [q_2]$.

In the general case, first observe that the sequences of $q_j$ and $r_j$ that we get when starting the Euclidean algorithm with $r_1$ and $r_2$ are really the same as the sequences that we get when starting at $r_0$ and $r_1$ (except for the first step). So by induction hypothesis, we already know that

$$\frac{r_1}{r_2} = [q_3, \ldots, q_m]$$

Furthermore, from $r_0 = q_2 r_1 + r_2$ we deduce

$$\frac{r_0}{r_1} = q_2 + \frac{r_2}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}} = q_2 + \frac{1}{[q_3, \ldots, q_m]} = [q_2, \ldots, q_m]$$
Exercise 7: (8 points)
Let $\alpha > 0$ be a real number and let $L_\alpha = \{ t \left( \frac{1}{\alpha} \right) \mid t \in \mathbb{R} \}$ be the line in the plane of slope $\alpha$ through the origin. Consider the following algorithm that intends to approximate $\alpha$ with a rational number:

**APPROXIMATE($\alpha$)**

1. $x^{(0)} \leftarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}, y^{(0)} \leftarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
2. for $k \leftarrow 1, 2, \ldots$
3. do $x^{(k)} \leftarrow x^{(k-1)} + a_k \cdot y^{(k-1)}$, where $a_k \in \mathbb{N}_0$ is maximal such that $x^{(k)}$ does not lie above $L_\alpha$
4. Stop if $x^{(k)}$ lies on $L_\alpha$
5. $y^{(k)} \leftarrow y^{(k-1)} + b_k \cdot x^{(k)}$, where $b_k \in \mathbb{N} \geq 1$ is maximal such that $y^{(k)}$ does not lie below $L_\alpha$
6. Stop if $y^{(k)}$ lies on $L_\alpha$

Prove:

1. The numbers $a_k$ and $b_k$ are well-defined in the sense that the respective maximal natural number exists.
2. $\{x^{(k)}, y^{(k)}\}$ and $\{x^{(k+1)}, y^{(k)}\}$ are bases of the lattice $\mathbb{Z}^2$ for all $k$ where they are defined. Furthermore, the half-open parallelepiped $P^{(k)}$ spanned by $x^{(k)}$ and $y^{(k)}$ contains no integer point except the origin. Here, $P^{(k)} = \{ \lambda x^{(k)} + \mu y^{(k)} \mid 0 \leq \lambda < 1, 0 \leq \mu < 1 \}$.
3. The line $L^{(k)}$ through the origin and $x^{(k)}$ is a best approximation of $L_\alpha$ from below in the following sense: Among all lines through the origin with rational slope $p/q \leq \alpha$ with $0 < q \leq x^{(k)}_1$, $L^{(k)}$ minimizes $|\alpha - \frac{p}{q}|$. 


Solution:

1. To see that the possible values of $a_k$ and $b_k$ are bounded from above, observe that as long as the algorithm doesn’t stop, $x^{(k)}$ is strictly below and $y^{(k)}$ is strictly above $L_\alpha$. The ray

$$\{ x^{(k-1)} + \lambda y^{(k-1)} \mid \lambda \geq 0 \}$$

starts below $L_\alpha$ and has slope strictly greater than $\alpha$, so it eventually intersects $L_\alpha$, i.e. the possible values for $a_k$ are bounded from above, and similarly for $b_k$.

To see that there are feasible values for $a_k$, it is enough to see that obviously 0 is a feasible value. For $b_k$, we have to argue that 1 is a feasible value: $y^{(k-1)} + 1 \cdot x^{(k)} = x^{(k-1)} + (a_k + 1)y^{(k-1)}$ is strictly above the line $L_\alpha$ by line 3 of the algorithm.

2. Clearly $\{x^{(0)}, y^{(0)}\}$ is a basis of $\mathbb{Z}^2$. From this, the other pairs of vectors are derived using successive elementary column operations, so they are also bases. $P^{(k)}$ is the fundamental parallelepiped corresponding to the lattice basis $\{x^{(k)}, y^{(k)}\}$, so it contains no lattice point besides 0.

3. Consider the triangle with vertices 0, $x^{(k)}$, and the intersection of $L_\alpha$ and the vertical line through $x^{(k)}$. This triangle is fully contained in $P^{(k)}$ except for the point $x^{(k)}$ itself, because the first coordinate of $y^{(k)}$ is greater than that of $x^{(k)}$.

Any rational line through the origin between $L^{(k)}$ and $L_\alpha$ with slope $\frac{p}{q}$ must contain an integer point with first coordinate at most $q$. In particular, this integer point lies in the triangle described above and so by the previous part, the only non-zero integer point in that region is $x^{(k)}$ itself. So the line must have been $L^{(k)}$ itself.