Sample problems for the final exam: Some solutions

Any problem may be altered or replaced by a different one!

Problem 1 The number 63000 has how many positive divisors?

Solution: 96.

First we decompose the given number into a product of primes:

$$63000 = 63 \cdot 10^3 = (7 \cdot 9) \cdot (2 \cdot 5)^3 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7.$$

An integer $n \geq 2$ is a divisor of 63000 if and only if its prime factorisation is part of the above prime factorisation, that is, if $n = 2^{m_1} 3^{m_2} 5^{m_3} 7^{m_4}$, where $0 \leq m_1 \leq 3$, $0 \leq m_2 \leq 2$, $0 \leq m_3 \leq 3$, and $0 \leq m_4 \leq 1$. Note that the divisor $n = 1$ admits this representation as well, with $m_1 = m_2 = m_3 = m_4 = 0$. By the Unique Factorisation Theorem, the quadruple (m_1, m_2, m_3, m_4) is uniquely determined by n. Thus we have a one-to-one correspondence between positive divisors of 63000 and elements of a Cartesian product $\{0,1,2,3\} \times \{0,1,2\} \times \{0,1,2,3\} \times \{0,1\}$. The Cartesian product has $4 \cdot 3 \cdot 4 \cdot 2 = 96$ elements.

Problem 2 Solve a system of congruences (find all solutions):

$$\begin{cases} x \equiv 2 \bmod 5, \\ x \equiv 3 \bmod 6, \\ x \equiv 6 \bmod 7. \end{cases}$$

Solution: $x = 27 + 210k$, $k \in \mathbb{Z}$.

The moduli 5, 6 and 7 are pairwise coprime. By the generalized Chinese Remainder Theorem, all solutions of the system form a single congruence class modulo $5 \cdot 6 \cdot 7 = 210$. It remains to find a particular solution. One way to do this is to represent 1 as an integral linear combination of $6 \cdot 7 = 42$, $5 \cdot 7 = 35$ and $5 \cdot 6 = 30$ (note that 1 is the greatest common divisor of these numbers). Let us apply the generalized Euclidean algorithm (in matrix form) to 42, 35 and 30:

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 42 \\ 0 & 1 & 0 & 35 \\ 0 & 0 & 1 & 30 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & -1 & 12 \\ 0 & 1 & 0 & 35 \\ 0 & 0 & 1 & 30 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & -1 & 12 \\ -2 & 1 & 2 & 11 \\ 0 & 0 & 1 & 30 \end{array}\right) \to \left(\begin{array}{ccc|c} 3 & -1 & -3 & 1 \\ -2 & 1 & 2 & 11 \\ 0 & 0 & 1 & 30 \end{array}\right).$$

From the first row of the last matrix we read off that $3(6 \cdot 7) - 1(5 \cdot 7) - 3(5 \cdot 6) = 1$. Then one of the solutions is $x = 2(3 \cdot 6 \cdot 7) + 3(-1 \cdot 5 \cdot 7) + 6(-3 \cdot 5 \cdot 6) = 252 - 105 - 540 = -393$. Another solution is $-393 + 2 \cdot 210 = 27$.

Problem 3 Find all integer solutions of a system

$$\begin{cases} 2x + 5y - z = 1, \\ x - 2y + 3z = 2. \end{cases}$$

Solution: $x = -3 - 13k$, $y = 2 + 7k$, $z = 3 + 9k$, where $k \in \mathbb{Z}$.

First we solve the second equation for x and substitute it into the first equation:

$$\begin{cases} 2x + 5y - z = 1, \\ x - 2y + 3z = 2 \end{cases} \iff \begin{cases} 2(2y - 3z + 2) + 5y - z = 1, \\ x = 2y - 3z + 2 \end{cases} \iff \begin{cases} 9y - 7z = -3, \\ x = 2y - 3z + 2. \end{cases}$$

For any integer solution of the equation $9y - 7z = -3$, the number y is a solution of the linear congruence $9y \equiv -3 \bmod 7$. Solving the congruence, we obtain

$$9y \equiv -3 \bmod 7 \iff 2y \equiv 4 \bmod 7 \iff y \equiv 2 \bmod 7.$$

Hence $y = 2 + 7k$, where $k \in \mathbb{Z}$. Now we find z and x by back substitution: $z = (9y + 3)/7 = (9(2 + 7k) + 3)/7 = 3 + 9k$ and $x = 2y - 3z + 2 = 2(2 + 7k) - 3(3 + 9k) + 2 = -3 - 13k$. Note that z and x are integers for all $k \in \mathbb{Z}$.

Problem 4 You receive a message that was encrypted using the RSA system with public key $(55, 27)$, where 55 is the base and 27 is the exponent. The encrypted message, in two blocks, is $4/7$. Find the private key and decrypt the message.

Solution: The private key is $(55, 3)$, the decrypted message is $9/13$.

First we find $\phi(55)$. The prime factorisation of 55 is $5 \cdot 11$, hence

$$\phi(55) = \phi(5)\phi(11) = (5 - 1)(11 - 1) = 40.$$

The private key is $(55, \beta)$, where the exponent β is the inverse of 27 (the exponent from the public key) modulo $\phi(55) = 40$. It is easy to find by inspection that $\beta = 3$ (as $3 \cdot 27 = 81 \equiv 1 \text{ mod } 40$). The standard way to find β is to apply the Euclidean algorithm (in matrix form) to 27 and 40:

$$\left(\begin{array}{cc|c} 1 & 0 & 27 \\ 0 & 1 & 40 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 27 \\ -1 & 1 & 13 \end{array}\right) \to \left(\begin{array}{cc|c} 3 & -2 & 1 \\ -1 & 1 & 13 \end{array}\right).$$

From the first row we read off that $3 \cdot 27 - 2 \cdot 40 = 1$, which implies that 3 is the inverse of 27 modulo 40.

Now that we know the private key, the decrypted message is b_1/b_2, where $b_1 \equiv 4^3 \text{ mod } 55$, $b_2 \equiv 7^3 \text{ mod } 55$, and $0 \leq b_1, b_2 < 55$. We find that $b_1 = 9$, $b_2 = 13$.

Problem 5 Consider a relation $\sim$ on the symmetric group $S(n)$ defined as follows. For any $\pi, \sigma \in S(n)$ we let $\pi \sim \sigma$ if and only if π is conjugate to σ, which means that $\pi = \tau\sigma\tau^{-1}$ for some permutation $\tau \in S(n)$. Show that $\sim$ is an equivalence relation.

We have to show that the relation $\sim$ is reflexive, symmetric, and transitive.
Reflexivity. $\pi \sim \pi$ for all $\pi \in S(n)$ since $\pi = \tau\pi\tau^{-1}$ holds for $\tau = \text{id}$ (as well as for $\tau = \pi$).
Symmetry. Assume $\pi \sim \sigma$, that is, $\pi = \tau\sigma\tau^{-1}$ for some $\tau \in S(n)$. Then

$$\sigma = \tau^{-1}\pi\tau = \tau^{-1}\pi(\tau^{-1})^{-1} = \tau_0\pi\tau_0^{-1},$$

where $\tau_0 = \tau^{-1} \in S(n)$. Hence $\sigma \sim \pi$.

Transitivity. Assume $\pi \sim \sigma$ and $\sigma \sim \rho$, that is, $\pi = \tau_1 \sigma \tau_1^{-1}$ and $\sigma = \tau_2 \rho \tau_2^{-1}$ for some $\tau_1, \tau_2 \in S(n)$. Then

$$\pi = \tau_1(\tau_2 \rho \tau_2^{-1})\tau_1^{-1} = (\tau_1\tau_2)\rho(\tau_2^{-1}\tau_1^{-1}) = (\tau_1\tau_2)\rho(\tau_1\tau_2)^{-1} = \tau\rho\tau^{-1},$$

where $\tau = \tau_1\tau_2 \in S(n)$. Hence $\pi \sim \rho$.

Problem 6 Let $\pi = (1\,2)(2\,3)(3\,4)(4\,5)(5\,6)$, $\sigma = (1\,2\,3)(2\,3\,4)(3\,4\,5)(4\,5\,6)$. Find the order and the sign of the following permutations: π, σ, $\pi\sigma$, and $\sigma\pi$.

Solution: π has order 6, σ has order 2, $\pi\sigma$ and $\sigma\pi$ have order 4. The sign of σ is $+1$, the sign of π, $\pi\sigma$ and $\sigma\pi$ is -1.

Any transposition is an odd permutation, its sign is -1. Any cycle of length 3 is an even permutation, its sign is $+1$. Since the sign is a multiplicative function, we obtain that $\operatorname{sgn}(\pi) = (-1)^5 = -1$, $\operatorname{sgn}(\sigma) = 1^4 = 1$, and $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\sigma\pi) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma) = -1$.

To find the order of a permutation, we need to decompose it into a product of disjoint cycles. First we decompose π and σ: $\pi = (1\,2\,3\,4\,5\,6)$, $\sigma = (1\,2)(5\,6)$. Then we use these decompositions to decompose $\pi\sigma$ and $\sigma\pi$: $\pi\sigma = (1\,3\,4\,5)$, $\sigma\pi = (2\,3\,4\,6)$. The order of a product of disjoint cycles equals the least common multiple of their lengths. Therefore $o(\pi) = 6$, $o(\sigma) = 2$, and $o(\pi\sigma) = o(\sigma\pi) = 4$.

Problem 7 For any positive integer n let $n\mathbb{Z}$ denote the set of all integers divisible by n. Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under addition? Does it form a group? Explain.

Solution: The set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ is neither a semigroup nor a group.

The set $S = 3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ consists of all integers divisible by at least one of the numbers 3, 4 and 7. This set is not closed under the operation of addition. For example, the numbers 4 and 7 belong to S while their sum $4 + 7 = 11$ does not. Therefore S is neither a semigroup nor a group with respect to addition.

Problem 8 Given a group G, an element $g \in G$ is called central if it commutes with any element of G. The set of all central elements, denoted $C(G)$, is called the center of G. Prove that $C(G)$ is a normal subgroup of G.

We need to show that the set $C(G)$ is nonempty, closed under the group operation, and closed under taking the inverse. Clearly, the identity element e of the group G commutes with all elements of G. Hence $e \in C(G)$. In particular, $C(G)$ is not empty.

Assume $g_1, g_2 \in C(G)$. Then for any $h \in G$ we have $g_1 h = h g_1$ and $g_2 h = h g_2$. It follows that $(g_1 g_2)h = g_1(g_2 h) = g_1(h g_2) = (g_1 h)g_2 = (h g_1)g_2 = h(g_1 g_2)$. Hence $g_1 g_2$ is central as well.

Assume $g \in C(G)$. Then for any $h \in G$ we have $gh = hg$. It follows that $g^{-1}h = g^{-1}h(gg^{-1}) = g^{-1}(hg)g^{-1} = g^{-1}(gh)g^{-1} = (g^{-1}g)hg^{-1} = hg^{-1}$. Hence g^{-1} is central as well.

Problem 9 (i) List all cyclic subgroups of the alternating group $A(4)$.

(ii) List all non-cyclic subgroups of $A(4)$.

Solution: cyclic subgroups are $\{\mathrm{id}\}$, $\{\mathrm{id},(1\,2)(3\,4)\}$, $\{\mathrm{id},(1\,3)(2\,4)\}$, $\{\mathrm{id},(1\,4)(2\,3)\}$, $\{\mathrm{id},(1\,2\,3),(1\,3\,2)\}$, $\{\mathrm{id},(1\,2\,4),(1\,4\,2)\}$, $\{\mathrm{id},(1\,3\,4),(1\,4\,3)\}$ and $\{\mathrm{id},(2\,3\,4),(2\,4\,3)\}$; non-cyclic subgroups are $\{\mathrm{id},(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$ and $A(4)$.

Problem 10 All Abelian groups of order 36 form how many isomorphism classes?

Solution: 4.

According to the classification of finite Abelian groups, any such group is isomorphic to a direct product of cyclic groups of the form $\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}}$, where $k \geq 1$, each p_i is a prime number, and each m_i is a positive integer. Moreover, the sequence of orders $p_1^{m_1}, p_2^{m_2}, \dots, p_k^{m_k}$ of the cyclic groups is unique up to to rearranging its terms. Note that the order of the Abelian group is the same as the order of the direct product, which equals $p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$.

The prime factorisation of the number 36 is $2^2 \cdot 3^2$. Up to rearranging the factors, there are 4 ways to decompose it as a product of prime powers: $36 = 2^2 \cdot 3^2 = 2 \cdot 2 \cdot 3^2 = 2^2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 3$. It follows that all Abelian groups of order 36 form 4 isomorphism classes, represented by groups $\mathbb{Z}_4 \times \mathbb{Z}_9$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$, $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Problem 11 A linear binary coding function f is defined by a generator matrix

$$G = \begin{pmatrix} 0 & \square & 0 & 1 & 1 & 0 & 1 \\ 1 & \square & 0 & 1 & 1 & 1 & 0 \\ 0 & \square & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

with some entries missing. Fill in the missing entries so that f can detect as many errors as possible. Explain.

Solution: $G = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$.

The maximal number of errors detected by a linear binary code equals $k-1$, where k is the minimal weight of nonzero codewords. Suppose

$$G = \begin{pmatrix} 0 & a_1 & 0 & 1 & 1 & 0 & 1 \\ 1 & a_2 & 0 & 1 & 1 & 1 & 0 \\ 0 & a_3 & 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

where $a_1, a_2, a_3 \in \{0, 1\}$. Codewords of f are linear combinations of rows of the matrix G (regarded as vectors in $\mathbb{Z}_2^7$). In particular, $0a_101101$ is the first row, $1(a_1+a_2)00011$ is the sum of the first two rows, and $0(a_1+a_3)10110$ is the sum of the first and the last rows. If $(a_1, a_2, a_3) \neq (1, 0, 0)$ then at least one of those three codewords has weight 3. On the other hand, in the case $(a_1, a_2, a_3) = (1, 0, 0)$ all seven nonzero codewords have weight 4: 0101101, 1001110, 0011011, 1100011, 0110110, 1010101, and 1111000. Thus the maximal possible number of detected errors is 3, achieved for a unique choice of missing entries.

Problem 12 The polynomial $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ has how many distinct complex roots?

Solution: 2.

The Fundamental Theorem of Algebra implies that any polynomial p of degree $n \geq 1$ with complex coefficients can be represented as $p(x) = c(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$, where $c, \alpha_1, \dots, \alpha_n \in \mathbb{C}$ and $c \neq 0$. The numbers $\alpha_1, \alpha_2, \dots, \alpha_n$ are roots of p, they need not be distinct. We say that α is a root of multiplicity $k \geq 1$ if $p(x)$ is divisible by $(x-\alpha)^k$ but not divisible by $(x-\alpha)^{k+1}$. An equivalent condition is that $p(x) = (x-\alpha)^k q(x)$ for some polynomial q such that $q(\alpha) \neq 0$. If this is the case then

$$p'(x) = \big((x-\alpha)^k\big)' q(x) + (x-\alpha)^k q'(x) = k(x-\alpha)^{k-1}q(x) + (x-\alpha)^k q'(x) = (x-\alpha)^{k-1}r(x),$$

where $r(x) = kq(x) + (x-\alpha)q'(x)$ is a polynomial and $r(\alpha) = kq(\alpha) \neq 0$. Hence α is a root of p' of multiplicity $k-1$ if $k > 1$ and not a root of p' if $k = 1$. We have

$$p(x) = c(x-\beta_1)^{k_1}(x-\beta_2)^{k_2}\dots(x-\beta_m)^{k_m},$$

where $\beta_1, \dots, \beta_m$ are distinct roots of p and $k_1, \dots, k_m$ are their multiplicities. It follows from the above that

$$\gcd(p(x), p'(x)) = (x-\beta_1)^{k_1-1}(x-\beta_2)^{k_2-1}\dots(x-\beta_m)^{k_m-1}.$$

As a consequence, the number of distinct roots of the polynomial p equals $\deg(p) - \deg(\gcd(p, p'))$.

To find the greatest common divisor of the polynomials $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$ and $f'(x) = 6x^5 + 15x^4 - 15x^2 + 3$, we use the Euclidean algorithm. First we divide f by f':

$$x^6 + 3x^5 - 5x^3 + 3x - 1 = (6x^5 + 15x^4 - 15x^2 + 3)\Big(\frac{1}{6}x + \frac{1}{12}\Big) - \frac{5}{4}x^4 - \frac{5}{2}x^3 + \frac{5}{4}x^2 + \frac{5}{2}x - \frac{5}{4}.$$

It is convenient to replace the remainder $r(x) = -\frac{5}{4}x^4 - \frac{5}{2}x^3 + \frac{5}{4}x^2 + \frac{5}{2}x - \frac{5}{4}$ by its scalar multiple $\tilde{r}(x) = -\frac{4}{5}r(x) = x^4 + 2x^3 - x^2 - 2x + 1$. Next we divide f' by $\tilde{r}$:

$$6x^5 + 15x^4 - 15x^2 + 3 = (x^4 + 2x^3 - x^2 - 2x + 1)(6x + 3).$$

Since f' is divisible by $\tilde{r}$, it follows that $\gcd(f, f') = \gcd(f', r) = \gcd(f', \tilde{r}) = \tilde{r}$. Thus the number of distinct complex roots of the polynomial f equals $\deg(f) - \deg(\gcd(f, f')) = 6 - 4 = 2$.