Sample problems for the final exam: 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: $x = 27 + 210n$, $n \in \mathbb{Z}$.

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). Suppose $1 = 42n_1 + 35n_2 + 30n_3$ for some integers n_1, n_2, n_3. Then the numbers $x_1 = 42n_1$, $x_2 = 35n_2$ and $x_3 = 30n_3$ satisfy the following systems of congruences:

$$\begin{cases} x_1 \equiv 1 \bmod 5, \\ x_1 \equiv 0 \bmod 6, \\ x_1 \equiv 0 \bmod 7, \end{cases} \qquad \begin{cases} x_2 \equiv 0 \bmod 5, \\ x_2 \equiv 1 \bmod 6, \\ x_2 \equiv 0 \bmod 7, \end{cases} \qquad \begin{cases} x_3 \equiv 0 \bmod 5, \\ x_3 \equiv 0 \bmod 6, \\ x_3 \equiv 1 \bmod 7. \end{cases}$$

It follows that $x_0 = 2x_1 + 3x_2 + 6x_3$ is a solution of the given system.

Let us apply the generalized Euclidean algorithm (in matrix form) to 42, 35 and 30. We begin with the augmented matrix of a system

$$\begin{cases} y_1 = 42, \\ y_2 = 35, \\ y_3 = 30. \end{cases}$$

At each step, we choose two numbers in the rightmost column, divide the larger of them by the smaller, and replace the dividend with the remainder. This can be done by applying an elementary row operation to the matrix:

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

The first row of the last matrix corresponds to a linear equation $3y_1 - y_2 - 3y_3 = 1$. Since elementary row operations preserve the solution set of any system, it follows that $(y_1, y_2, y_3) = (42, 35, 30)$ is a solution of that equation. In other words,

$$1 = 42 \cdot 3 + 35 \cdot (-1) + 30 \cdot (-3).$$

Let x_1, x_2, x_3 be the terms in this expansion of 1: $x_1 = 42 \cdot 3 = 126$, $x_2 = 35 \cdot (-1) = -35$ and $x_3 = 30 \cdot (-3) = -90$. By the above, one solution of the given system of congruences is

$$x_0 = 2x_1 + 3x_2 + 6x_3 = 2 \cdot 126 + 3(-35) + 6(-90) = -393.$$

Another solution is $-393 + 2 \cdot 210 = 27$. The general solution is $x = 27 + 210n$, $n \in \mathbb{Z}$.

Alternative solution: We can solve the system inductively, handling one congruence at a time. With this approach, it is convenient (though not necessary) to go from larger moduli to smaller ones. Hence we begin with the last congruence $x \equiv 6 \bmod 7$. Its general solution is $x = 6 + 7k$, $k \in \mathbb{Z}$. Substituting this into the second congruence, we obtain a linear congruence in k:

$$6 + 7k \equiv 3 \bmod 6 \quad \Longleftrightarrow \quad k \equiv 3 \bmod 6.$$

The general solution of the latter congruence is $k = 3+6m$, $m \in \mathbb{Z}$. Then $x = 6+7k = 6+7(3+6m) = 27 + 42m$. We obtain that $x = 27 + 42m$, $m \in \mathbb{Z}$ is the general solution of a system formed by the second and the third congruences of the given system. Substituting this into the first congruence, we obtain a linear congruence in m:

$$27 + 42m \equiv 2 \bmod 5 \quad \Longleftrightarrow \quad 2m \equiv 0 \bmod 5.$$

Since the number 2 is coprime with 5, we have $2m \equiv 0 \bmod 5$ if and only if $m \equiv 0 \bmod 5$. Therefore the general solution is $m = 5n$, $n \in \mathbb{Z}$. Then $x = 27 + 42m = 27 + 42(5n) = 27 + 210n$. We conclude that $x = 27 + 210n$, $n \in \mathbb{Z}$ is the general solution of the system formed by all three congruences.

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:

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

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 $3 \cdot 27 = 81 \equiv 1 \bmod 40$). 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 $b_1 \equiv 4^3 \bmod 55$, $b_2 \equiv 7^3 \bmod 55$, and $0 \le b_1, b_2 < 55$. We find that $b_1 = 9$, $b_2 = 13$.

Problem 5. 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 6. For any positive integer n let $n\mathbb{Z}$ denote the set of all integers divisible by n.

(i) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under addition? Does it form a group?

(ii) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under multiplication? Does it form a group?

Solution: Under addition, $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ is neither a semigroup nor a group. Under multiplication, $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ is a semigroup but not 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.

Each of the sets $3\mathbb{Z}$, $4\mathbb{Z}$ and $7\mathbb{Z}$ is closed under multiplication by any integer. Hence their union S is also closed under multiplication by any integer. In particular, S is a semigroup with respect to multiplication. It is not a group since it does not contain 1 (and 1 is the only number that can be the multiplicative identity element unless $S = \{0\}$).

Problem 7. Given a group G, an element $c \in G$ is called *central* if it commutes with any element of the group: $cg = gc$ for all $g \in G$. 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.

To show that the center $C(G)$ is a subgroup of G, we need to check that $C(G)$ contains the identity element e, is closed under the group operation, and is closed under taking the inverse.

Clearly, the identity element of the group G commutes with all elements of G. Hence $e \in C(G)$.

Assume $c_1, c_2 \in C(G)$. Then for any $g \in G$ we have $c_1 g = g c_1$ and $c_2 g = g c_2$. It follows that $(c_1 c_2)g = c_1(c_2 g) = c_1(g c_2) = (c_1 g)c_2 = (g c_1)c_2 = g(c_1 c_2)$. Hence $c_1 c_2$ is central as well.

Assume $c \in C(G)$. Then for any $g \in G$ we have $cg = gc$. It follows that $c^{-1}g = c^{-1}g(cc^{-1}) = c^{-1}(gc)c^{-1} = c^{-1}(cg)c^{-1} = (c^{-1}c)gc^{-1} = gc^{-1}$. Hence c^{-1} is central as well.

To show that the subgroup $C(G)$ is normal, we need to check that each left coset of $C(G)$ is also a right coset. Take any $g \in G$. Then $gc = cg$ for all $c \in C(G)$. As a consequence, the left coset $gC(G)$ coincides with the right coset $C(G)g$.

Problem 8. Find a direct product of cyclic groups that is isomorphic to G_{16} (multiplicative group of all invertible congruence classes modulo 16).

Solution: $G_{16} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

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 $p_1^{m_1}, p_2^{m_2}, \ldots, p_k^{m_k}$ of the cyclic groups is unique up to rearranging its terms. Note that the order of the Abelian group is the same as the order of the direct product, which equals $p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$.

A congruence class $[a]_{16}$ is invertible if and only if the number a is coprime with 16, that is, if a is odd. Hence there are 8 congruence classes in G_{16}: [1], [3], [5], [7], [9], [11], [13] and [15]. Up to rearranging the factors, there are 3 ways to represent the number 8 as a product of prime powers: $8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2$. It follows from the classification that the group G_{16} is isomorphic to $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. These three groups are distinguished by orders of their elements: $\mathbb{Z}_8$ has

elements of order 1, 2, 4 and 8; $\mathbb{Z}_4 \times \mathbb{Z}_2$ has elements of order 1, 2 and 4; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has only elements of order 1 and 2.

Since any isomorphism of groups preserves orders of elements, we can classify the group G_{16} by finding orders of all its elements. Note that conceivable orders are 1, 2, 4 and 8 (due to Lagrange's Theorem). We obtain that

$$
\begin{aligned}
&[1]^1 = [1];\\
&[3]^2 = [9], \quad [3]^4 = [9]^2 = [81] = [1];\\
&[5]^2 = [25] = [9], \quad [5]^4 = [9]^2 = [81] = [1];\\
&[7]^2 = [49] = [1];\\
&[9]^2 = [-7]^2 = [49] = [1];\\
&[11]^2 = [-5]^2 = [25] = [9], \quad [11]^4 = [9]^2 = [81] = [1];\\
&[13]^2 = [-3]^2 = [9], \quad [13]^4 = [9]^2 = [81] = [1];\\
&[15]^2 = [-1]^2 = [1].
\end{aligned}
$$

Hence the congruence class [1] has order 1, congruence classes [7], [9] and [15] have order 2, and congruence classes [3], [5], [11] and [13] have order 4. Thus the group G_{16} has elements of order 1, 2 and 4, but no element of order 8. We conclude that $G_{16} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Problem 9. Complete the following Cayley table of a group of order 9:

$*$	A	B	C	D	E	F	G	H	I
A	I								F
B		F						G	
C			H				E		
D				G		A			
E					E				
F				A		B			
G			E				A		
H		G						D	
I	F								C

First we observe that E is the identity element as $E^2 = E$.

Next we observe that $A^2 = I$ and $A^3 = A^2A = IA = F$. It follows from Lagrange's Theorem that the order of any element in the group is a divisor of 9 (1, 3 or 9). Note that the order of the element A is neither 1 (as $A \neq E$) nor 3 (as $A^3 \neq E$). Hence A has order 9. We conclude that the group is cyclic and A is a generator.

Our next task is to represent every element of the group as a power of A. We already have that $E = A^0$, $A = A^1$, $I = A^2$ and $F = A^3$. Using the Cayley table, we obtain that

$$
\begin{aligned}
&B = F^2 = (A^3)^2 = A^6,\\
&C = I^2 = (A^2)^2 = A^4,\\
&H = C^2 = (A^4)^2 = A^8,\\
&D = H^2 = (A^8)^2 = A^{16} = A^7,\\
&G = D^2 = (A^7)^2 = A^{14} = A^5.
\end{aligned}
$$

Now that every element of the group is represented as a power of A, completing the table is a routine task. For example, $DH = A^7A^8 = A^{15} = A^6 = B$.

Remark. Since the group is generated by the element A, it follows that a map $f : \mathbb{Z}_9 \to \{A, B, C, D, E, F, G, H, I\}$ given by $f([n]_9) = A^n$ for all $n \in \mathbb{Z}$ is an isomorphism of groups. When each element of the group was represented as a power of A, we had essentialy computed the function f as well as its inverse. The inverse function f^{-1} is also an isomorphism. Hence $f^{-1}(XY) = f^{-1}(X) + f^{-1}(Y)$ for all X and Y. Then $XY = f\big(f^{-1}(X) + f^{-1}(Y)\big)$. For example, $DH = f\big(f^{-1}(D) + f^{-1}(H)\big) = f([7]_9 + [8]_9) = f([6]_9) = B$.

Problem 10. 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 11. Find all prime numbers p such that a polynomial $x^4 - x^3 + x^2 - x + 1$ is divisible by $x + 2$ in $\mathbb{Z}_p[x]$.

Solution: 3 and 5.

The polynomials $f(x) = x^4 - x^3 + x^2 - x + 1$ and $g(x) = x + 2$ can be considered over any field $\mathbb{F}$. We know that $f(x)$ is divisible by $x + 2$ in $\mathbb{F}[x]$ if and only if $f(-2) = 0$ in $\mathbb{F}$. We obtain that

$$f(-2) = (-2)^4 - (-2)^3 + (-2)^2 - (-2) + 1 = 15$$

in any field $\mathbb{F}$. Hence $f(x)$ is divisible by $x + 2$ in $\mathbb{Z}_p[x]$ if and only if $15 \equiv 0 \bmod p$. That is, if the integer number 15 is divisible by p. The number 15 has two prime divisors, 3 and 5.

Problem 12. Factorise the polynomial $p(x) = x^4 - 2x^3 - x^2 - 2x + 1$ into irreducible factors over the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

Solution: $p(x) = (x^2 - 3x + 1)(x^2 + x + 1)$ over $\mathbb{Q}$,
$p(x) = \left(x - \frac{3+\sqrt{5}}{2}\right)\left(x - \frac{3-\sqrt{5}}{2}\right)(x^2 + x + 1)$ over $\mathbb{R}$,
$p(x) = \left(x - \frac{3+\sqrt{5}}{2}\right)\left(x - \frac{3-\sqrt{5}}{2}\right)\left(x - \frac{-1+i\sqrt{3}}{2}\right)\left(x - \frac{-1-i\sqrt{3}}{2}\right)$ over $\mathbb{C}$,
$p(x) = (x + 1)^2(x^2 + x + 1)$ over $\mathbb{Z}_5$,
$p(x) = (x - 2)(x + 3)(x^2 - 3x + 1)$ over $\mathbb{Z}_7$.

First consider p as a function on $\mathbb{C}$. For any $x \neq 0$ we have

$$\frac{p(x)}{x^2} = x^2 - 2x - 1 - \frac{2}{x} + \frac{1}{x^2} = \left(x^2 + \frac{1}{x^2}\right) - 2\left(x + \frac{1}{x}\right) - 1.$$

Let $y = x + \frac{1}{x}$. Then $y^2 = x^2 + 2 + \frac{1}{x^2}$ so that $x^2 + \frac{1}{x^2} = y^2 - 2$. Consequently,

$$\frac{p(x)}{x^2} = (y^2 - 2) - 2y - 1 = y^2 - 2y - 3.$$

The quadratic polynomial $y^2 - 2y - 3$ admits a factorisation $y^2 - 2y - 3 = (y - 3)(y + 1)$. It follows that

$$p(x) = x^2(y - 3)(y + 1) = x^2\Big(x + \frac{1}{x} - 3\Big)\Big(x + \frac{1}{x} + 1\Big) = (x^2 - 3x + 1)(x^2 + x + 1).$$

We have obtained the above factorisation of p as an equality of functions on $\mathbb{C} \setminus \{0\}$. Now we can check by direct multiplication that, in fact,

$$x^4 - 2x^3 - x^2 - 2x + 1 = (x^2 - 3x + 1)(x^2 + x + 1)$$

over any field. Depending on the field, any of the two quadratic factors either is irreducible (if it has no roots) or else splits as a product of two linear factors.

Over the field $\mathbb{C}$, the polynomial $x^2 - 3x + 1$ has roots $\alpha_{1,2} = \frac{1}{2}(3 \pm \sqrt{5})$ and the polynomial $x^2 + x + 1$ has roots $\beta_{1,2} = \frac{1}{2}(-1 \pm i\sqrt{3})$. Hence the factorisation into irreducible factors over $\mathbb{C}$ is $p(x) = (x - \alpha_1)(x - \alpha_2)(x - \beta_1)(x - \beta_2)$. Note that the numbers β_1 and β_2 are not real while α_1 and α_2 are real but not rational. Since $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, it follows that over $\mathbb{R}$, the factorisation into irreducible factors is $p(x) = (x - \alpha_1)(x - \alpha_2)(x^2 + x + 1)$, and over $\mathbb{Q}$, it is $p(x) = (x^2 - 3x + 1)(x^2 + x + 1)$.

In the case of a finite field, we find roots by trying all elements of the field. We obtain that over the field $\mathbb{Z}_5$, the polynomial $x^2 + x + 1$ is irreducible while

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

Over the field $\mathbb{Z}_7$, the polynomial $x^2 - 3x + 1$ is irreducible while

$$x^2 + x + 1 = x^2 + x + 1 - 7 = x^2 + x - 6 = (x - 2)(x + 3).$$