Matematiska Institutionen, KTH   Friday, December 21, 08:00 – 13:00 in M21, M22

Final Exam in Diskret Matematik och algebra (SF2714)

With Solutions

Examiner: Petter Brändén.
No calculators, textbooks or notes are allowed.
There are 5 problems for a total of 58 points.
For full credit you must show all your work.

Problem 1. (12p).

(a) State the Chinese remainder theorem (you don't have to prove it).
(b) Solve the following system of congruences.

$$\begin{aligned} x &\equiv 1 \mod 3, \\ x &\equiv 2 \mod 4, \\ x &\equiv 5 \mod 7. \end{aligned}$$

Solution. Since $3, 4, 7$ (pairwise) have no common non-trivial divisors there is a unique solution modulo $3 \cdot 4 \cdot 7 = 84$. Using the notation in the Chinese remainder theorem we have: $M_1 = 84/3 = 28, M_2 = 84/4 = 21, M_3 = 84/7 = 12$. Next step is to solve

$$\begin{aligned} 28x_1 &\equiv 1 \mod 3, \\ 21x_2 &\equiv 1 \mod 4, \\ 12x_3 &\equiv 1 \mod 7. \end{aligned}$$

We may choose $x_1 = x_2 = 1$, $x_3 = 3$. By the Chinese remainder theorem the solution is given by

$$x \equiv 1 \cdot 28 \cdot 1 + 2 \cdot 21 \cdot 1 + 5 \cdot 12 \cdot 3 \equiv 82 \mod 84.$$

Problem 2. (12p).

(a) Determine if the polynomial $q(x) = x^4 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$. If possible, find the inverse of $x^2 + x + 1$ in $\mathbb{Z}_2[x]/(q)$.
(b) Determine if the polynomial $q(x) = x^4 + x^2 + 2$ is irreducible in $\mathbb{Z}_3[x]$. If possible, find the inverse of $x^2 + x + 1$ in $\mathbb{Z}_3[x]/(q)$.

Solution. (a). We have $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$, so $q(x)$ is reducible. Since $(x^2+x+1)^2 = 0$ in $\mathbb{Z}_2[x]/(q)$ the polynomial x^2+x+1 is not invertible (remember that $p(x)$ is invertible in $F[x]/(q)$ if and only if $\gcd(p, q) = 1$).

(b). Note that $q(0) = 2, q(1) = q(2) = 1$, so q has no divisors of degree 1 by the factor theorem. Suppose that $q(x)$ is the product of two polynomials of degree 2. It follows that

$$x^4 + x^2 - 1 = x^4 + x^2 + 2 = (x^2 + ax + 1)(x^2 + bx - 1)$$

for some $a, b \in \mathbb{Z}_3$. Identifying the coefficient on both sides of the above equation we see that $a + b = 0$, $ab = 1$ and $b - a = 0$. The first and third equations imply that $a = b = 0$, which conflicts with the second equation. This contradiction means that $q(x)$ has no factors of degree two either. Hence $q(x)$ is irreducible. Since $q(x)$ is irreducible it follows that $\mathbb{Z}_3[x]/(q)$ is a field which guarantees the existence of the inverse of $x^2 + x + 1$. Using the Euclidian algorithm we find that the inverse is $2x^2 + x + 2$.

Problem 3. (12p). Prove the following theorem.

Theorem. Suppose that a, b are positive integers. Then there are two unique non-negative integers q, r such that

$$a = bq + r \quad \text{and} \quad 0 \le r < b.$$

Problem 4. (10p). Suppose that we are given bricks of dimensions $1 \times 1 \times 3$, $1 \times 1 \times 4$ and $1 \times 1 \times 5$. Let a_n be the number of ways to build a tower of size $1 \times 1 \times n$ using these bricks. Also, define $a_0 = 1$. ($a_1 = a_2 = 0, a_3 = a_4 = a_5 = 1, a_{11} = 6$). Determine the generating function $F(x) = \sum_{n=0}^{\infty} a_n x^n$.

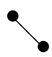
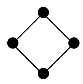
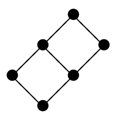
Solution. Let $\mathcal{T}$ be set of all towers that we can build as described and let $\mathcal{T}_j$, $j = 3, 4, 5$, be the set of towers whose first has dimensions $1 \times 1 \times j$. Moreover, let $F_j(x)$, $j = 3, 4, 5$, be the corresponding generating functions. Then $F(x) = 1 + F_3(x) + F_4(x) + F_5(x)$ and $F_3(x) = x^3 F(x)$, $F_4(x) = x^4 F(x)$, $F_5(x) = x^5 F(x)$, which combined gives $F(x) = 1 + x^3 F(x) + x^4 F(x) + x^5 F(x)$ i.e.,

$$F(x) = \frac{1}{1 - x^3 - x^4 - x^5}.$$

Problem 5. (12p). Let k be a positive integer. Let $G_k = (V_k, E_k)$ be the graph determined by

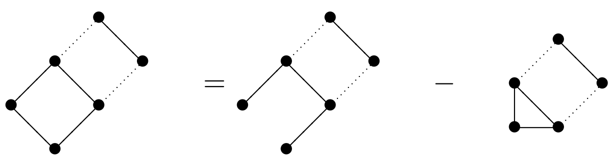
$$V_k = \Big\{(x, y) : x \in \{1, \ldots, k\}, y \in \{1, 2\}\Big\}, \quad E_k = \Big\{\{(x_1, y_1), (x_2, y_2)\} : |x_1 - x_2| + |y_1 - y_2| = 1\Big\}.$$

(a) Determine for which $k \ge 1$ there exists an Eulerian walk in G_k,
(b) Find a formula for the chromatic polynomial of G_k, valid for all $k \ge 1$,
(c) Determine the number of acyclic orientations of G_k, $k \ge 1$.

$G_1 =$  $G_2 =$  $G_3 =$ 

Solution. (a). Apply Euler's Königsberg theorem. Eulerian walks exist for $k = 1, 2, 3$ but not for $k > 3$ since then more than 2 vertices have degree 3.

(b). Let $P_k(x)$ be the chromatic polynomial of G_k. Hence $P_1(x) = x(x-1)$. By the recursive formula for the chromatic polynomials we have the following recursion (in symbols):



This gives the recursion

$$P_k(x) = (x-1)^2 P_{k-1}(x) - (x-2) P_{k-1}(x) = (x^2 - 3x + 3) P_{k-1}(x),$$

so

$$P_k(x) = x(x-1)(x^2-3x+3)^{k-1}, \quad k \geq 1.$$

(c). The number of acyclic orientations is given by $|P_k(-1)| = 2 \cdot 7^{k-1}$.