Prof. Friedrich Eisenbrand
Nicolai Hähnle

Discussions from: April 27, 2010

Computer Algebra

Spring 2010

Assignment Sheet 5

Exercises marked with a ⋆ can be handed in for bonus points. Due date is May 11.

Exercise 1 (⋆)
Let $f = x^2 + 2x - 5$ and $g = x^2 + 3x + 2$. Let $N = 17$ and $\omega = 2 \in \mathbb{Z}_N$.

1. Show that ω is an 8-th primitive root of unity in $\mathbb{Z}_N$.
2. Use the discrete Fourier transform to compute $f(\omega^i)$ and $g(\omega^i) \mod N$, $i = 0 \ldots 7$.
3. Use the inverse discrete Fourier transform on $f(\omega^i)g(\omega^i)$. Can you use the result to find fg?

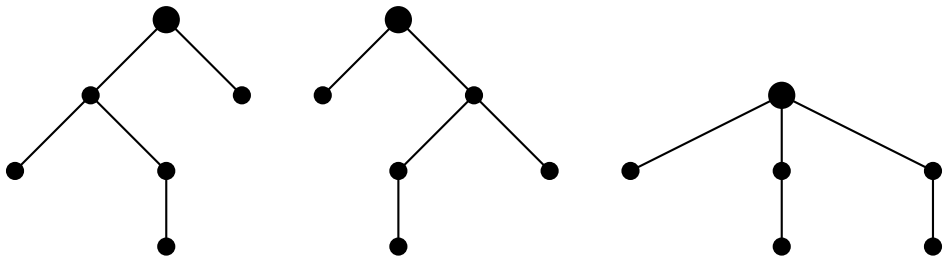
Exercise 2
Let

$$A = \begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 1 \\ 0 & 2 & 2 \end{pmatrix}$$

1. Use Gauss elimination modulo p to compute the determinant of A modulo p, for $p = 3, 5, 7$.
2. Combine the results of the previous step to find $\det(A)$ modulo 105.
3. Use the Hadamard bound to show that $2|\det(A)| + 1 \leq 105$. Conclude that you can directly obtain $\det(A)$ from the previous results.
4. Sketch a generalization of this approach into an algorithm that computes the determinant of a matrix $A \in \mathbb{Z}^{n \times n}$ while using only arithmetic with small integers (except for a final combination step that computes the final result).

Exercise 3
Two rooted trees T_1 and T_2 are said to be isomorphic is there exists a bijection f from the vertices of T_1 to those of T_2 satisfying the following conditions: the root of T_1 is mapped to the root of T_2, and for each vertex v of T_1 with children $v_1, \ldots, v_k$, the vertex $f(v)$ has as children exactly the vertices $f(v_1), \ldots, f(v_k)$. Observe that no ordering is assumed on the children of any internal vertex.

Of the following three examples, the first two are isomorphic, while the last example is isomorphic to neither of the first two.



Associate to each vertex v a polynomial f_v recursively: for a leaf vertex, set $f_v = x_0$. For an internal vertex v of height h with children $v_1, \ldots, v_k$, set

$$f_v = (x_h - f_{v_1})(x_h - f_{v_2}) \cdots (x_h - f_{v_k})$$

Note that the number of indeterminates corresponds to the height of the tree.

1. Show that two rooted trees are isomorphic if and only if the polynomials associated to their roots are equal.

2. Devise an efficient randomized algorithm for testing whether two rooted trees are isomorphic and analyze its running time and probability of success.

Exercise 4 ($\star$)
Let k be a field, $A \in k^{n \times n}$ and $b \in k^n$. Define sequences $a = (A^j)_{j \in \mathbb{N}}$ and $a^\star = (A^j b)_{j \in \mathbb{N}}$. Recall that $f = \sum_{j=0}^{d} f_j x^j \in k[x]$ is a characteristic polynomial of a sequence σ if and only if $\sum_{j=0}^{d} f_j \sigma_{m+j} = 0$ for all $m \in \mathbb{N}$.

1. Prove that $f \in k[x]$ is a characteristic polynomial of a if and only if $f(A) = 0$.

2. Prove that $f \in k[x]$ is a characteristic polynomial of $a^\star$ if and only if $f(A)b = 0$.

3. Let $a^{\star\star} = (u^T A^i b)_{i \in \mathbb{N}}$, where $u \in k^n$. Find concrete values of f, A, b, and u such that $u^T f(A) b = 0$, but f is *not* a characteristic polynomial of $a^{\star\star}$.