Prof. Friedrich Eisenbrand
Yuri Faenza

Discussions from: April 23, 2013

Computer Algebra

Spring 2013

Assignment Sheet 5

Exercises marked with a $\star$ can be handed in for bonus points. Due date is May 07.

Exercise 1 ($\star$)
Develop an algorithm that, given an odd-degree polynomial $f \in \mathbb{Z}[x]$ and $\varepsilon > 0$, computes an interval of length at most ε enclosing a root of f using binary search. This algorithm has to run in polynomial time in the encoding length of f and ε. Prove the correctness of your algorithm.

Exercise 2
Let $R = \mathbb{Z}_7$ and $S = \mathbb{Z}_{11}$ and consider the product ring $T = R \times S \cong \mathbb{Z}_{77}$. Consider the following example about how roots of unity in the product ring *don't* relate to roots of unity in the component rings (compare also the next exercise!).

1. Show that $\omega_1 = 2$ is a primitive 3-rd root of unity modulo 7.
2. Show that $\omega_2 = 4$ is a primitive 5-th root of unity modulo 11.
3. Let $\omega = 37$. Prove that $\omega \equiv \omega_1 \pmod 7$ and $\omega \equiv \omega_2 \pmod{11}$ and that ω is a 15-th root of unity modulo 77 (that is, $\omega^{15} \equiv 1 \pmod{77}$, and $\omega^k \not\equiv 1 \pmod{77}$ for $1 \leq k < 15$).
4. Prove that ω is *not* a primitive root of unity modulo 77.

Exercise 3
Let R and S be commutative rings and consider their product ring $T = R \times S$. Let $\omega = (\omega_R, \omega_S) \in T$. Prove that ω is a primitive n-th root of unity if and only if ω_R and ω_S are primitive n-th roots of unity in R and S, respectively.

Exercise 4 ($\star$)
Let $R = \mathbb{Z}_{21}$. For every element $x \in R$, determine whether it is in R^* (that is, whether it is invertible) and whether it is a zero divisor. Determine the order of every element $x \in R^*$. Finally, determine which elements are primitive roots of unity.

Exercise 5
Let $n \in \mathbb{N}$. Show that 2 is a primitive $2n$-th root of unity modulo $2^n + 1$ if and only if n is a power of 2.

Exercise 6

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 $g(\omega^i) \mod N$, $i = 0 \dots 7$.
3. Use the inverse discrete Fourier transform on $f(\omega^i)g(\omega^i)$. Can you use the result to find $fg \in \mathbb{Z}[x]$?

Exercise 7

In this exercise we will use Fast Fourier Transform to prove the following:

($\bullet$) *The product of two* $N-$*bits integers can be computed in time* $O(N \log^{\log 6} N)$.

(a) Let U, V be two N-bit integers with $N = 2^n$ for some $n \in \mathbb{N}$. Also, let $k = \lfloor n/2 \rfloor$ and $\ell = \lceil n - k \rceil$. Write U and V as vectors $\tilde{U}$ and $\tilde{B}$ respectively, with $K = 2^k$ components each.

(b) Consider the polynomials $p(x) = \sum_{j=0}^{K-1} \tilde{U}_j x^j$ and $q(x) = \sum_{j=0}^{K-1} \tilde{V}_j x^j$. Show that from the knowledge of the coefficients of their product $r(x) \in \mathbb{Z}_M$ with M appropriate one can reconstruct the product of U and V in time $O(N)$.

(c) Show how to compute the coefficients of $r(x)$ using FFT and conclude the proof of ($\bullet$).

(d) Based on ($\bullet$) and on results seen in class, deduce an appropriate complexity bound for computing the product of two polynomials in $\mathbb{Z}_M$ with $M = 2^L + 1$ and in $\mathbb{Z}$, respectively.