HUMBOLDT–UNIVERSITÄT ZU BERLIN

MATHEMATISCH-NATURWISSENSCHAFTLICHE FAKULTÄT II

INSTITUT FÜR MATHEMATIK

PROF. ANDREAS GRIEWANK PHD,

DR. LUTZ LEHMANN

Humboldt-Universität zu Berlin, Institut für Mathematik, Unter den Linden 6, D-10099 Berlin

Berlin, den May 26, 2008

Exercises for the lecture "Introduction to Computer Algebra"

Series 3. (Return on Monday, June 9th 2008)

Task 1: If two natural integers $a, p \in \mathbb{N}$ have no common divisor, then the extended euclidean algorithm provides euclidean coefficients $s, t \in \mathbb{Z}$ with $s\,a + t\,p = 1$. In the remainder arithmetics modulo p this implies $s\,a \equiv 1 \bmod p$. Thus in the remainder class ring $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z})$, the class $[s]_p$ is the multiplicative inverse of the class $[a]_p$.

Compute the inverse of a) 29 modulo 19, b) of 625 modulo 1103 and c) of 1234 modulo 10009. **6 pts.**

Task 2: Let $p \in \mathbb{N}$ be a prime number.

Prove that all binomial coefficients $\binom{p}{k}$, $k = 1, \ldots, p-1$ are divisible by p. **4 pts.**

(b) Conclude that for any $a, b \in \mathbb{N}$ the relation $(a+b)^p \equiv a^p + b^p \bmod p$ holds. **2 pts.**

(c) Further conclude that $a^p \equiv a \bmod p$, and that even $a^{p-1} \equiv a \bmod p$ if a is no multiple of p. **4 pts.**

(d) The last relation, the "little theorem" of Fermat, has as interpretation that a^{p-2} is the inverse of a in $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z})$. This number can be computed by repeated squaring and reduction mod p.

Use this method to compute the inverses for the same examples as in task 1. Compare the numbers of multiplications under the assumption that the long division has the same cost as two multiplications. **9 pts.**

Task 3: The chinese remainder theorem also applies to univariate polynomials with coefficients in a field $\mathbb{F}$. Let $z_1, z_2, \ldots, z_n \in \mathbb{F}$ be pairwise different numbers.

(a) Compute the inverse of $(X - z_2)(X - z_3)\ldots(X - z_n)$ modulo $(X - z_1)$. **4 pts.**

(b) Determine the reconstruction formula for the chinese remainder problem $p(X) \equiv y_k \bmod (X - z_k)$, $k = 1, \ldots, n$, with $y_1, \ldots, y_n \in \mathbb{F}$ given. Compare this formula with the Lagrange interpolation formula. **4 pts.**

(c) Estimate the operation count for determining the coefficients of $p(X)$ in the naive way (directly from the interpolation formula, without precomputed results). **6 pts.**

(d) Devise a "divide and conquer" method for a faster computation of these coefficients, again without precomputed results. **8 pts.**

Task 4: Let $n, B \in \mathbb{N}$ and coefficients $a_0, \dots, a_n, b_0, \dots, b_n \in \mathbb{Z}$ with $|a_k| < B$, $|b_k| < B$ be given. Furthermore, let $c = ab$ be the product of both polynomials $a = a_0 + a_1 x + \cdots + a_n x^n$ and $b = b_0 + b_1 x + \cdots + b_n x^n$.

(a) Find a tight bound on the coefficients c_i in terms of n and B. **2 pts.**

(b) Give an algorithm for the computation of c using modular arithmetics modulo a sufficient number of small primes and reconstruction using the chinese remainder theorem. (It may contain a size bound leading to an "overflow error".) **8 pts.**

(c) Trace the steps of the algorithm on the computation of the product of **6 pts.**

$$a = 261\,x^3 + 458\,x^2 + 204\,x - 696 \text{ and } b = 602\,x^3 - 756\,x^2 + 53\,x - 771\,.$$

phone: 030/2093-5820 fax: 030/2093-5848
e-mail: griewank@math.hu-berlin.de llehmann@math.hu-berlin.de