Foundations of Computer Algebra. CS424b: Quiz 1. UWO, February 8, 2006.

Student ID number:
Student Last Name:

Guidelines. Every printed document is allowed but computers and calculators are not. The duration of the quiz is 45 minutes. The quiz consists of four exercises located on pages 2, 3, 4 and 5. All answers should be written in the *answer boxes*. No justifications for the answers are needed, unless explicitly required. You are expected to do this quiz on your own without assistance from anyone else in the class. If possible, please avoid pencils and use pens with dark ink. Thank you.

Notations. The set of non-negative integer numbers, integer numbers and rational numbers are denoted respectively $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, as usual. For a ring $\mathbb{A}$, we denote by $\mathbb{A}[x]$ the ring of univariate polynomials in x with coefficients in $\mathbb{A}$.

Formulas. Let m and n be two relatively prime elements of an Euclidean domain R. (You may think $R = \mathbb{Z}$ or $R = \mathbb{Q}[x]$.) Let $s, t \in R$ be such that $s\,m + t\,n = 1$. For every $a, b \in R$ there exists $c \in R$ such that

$$(\forall x \in R) \quad \left\{ \begin{array}{ll} x \equiv a & \mod m \\ x \equiv b & \mod n \end{array} \right. \quad \Longleftrightarrow \quad x \equiv c \mod m\,n \tag{1}$$

where a convenient c is given by

$$c \;=\; a + (b - a)\,s\,m = b + (a - b)t\,n \tag{2}$$

Let A and B be two square matrices of order n and with coefficients in $\mathbb{Q}$ where n is a power of 2. We recall the Strassen's trick for computing AB.

(1) If $n = 1$ the matrices A et B are of the form (a) et (b) where $a, b \in \mathbb{Z}$, such that $A\,B$ equals $(a\,b)$.

(2) If $n > 1$ the matrices A and B can be decomposed as

$$A = \left(\begin{array}{cc} A_{11} & A_{12} \\ A_{21} & A_{22} \end{array} \right), \; B = \left(\begin{array}{cc} B_{11} & B_{12} \\ B_{21} & B_{22} \end{array} \right),$$

where A_{ij} and B_{ij} are square matrices of order $n/2$. Then, one computes the following 8 sums.

$$\begin{array}{ll} S_1 = A_{21} + A_{22} & T_1 = B_{12} - B_{11} \\ S_2 = S_1 - A_{11} & T_2 = B_{22} - T_1 \\ S_3 = A_{11} - A_{21} & T_3 = B_{22} - B_{12} \\ S_4 = A_{12} - S_2 & T_4 = T_2 - B_{21} \end{array}$$

(3) Next, one computes the following 7 matrix products by recursive calls to the algorithm.

$$\begin{array}{ll} P_1 = A_{11}\,B_{11} & P_5 = S_1\,T_1 \\ P_2 = A_{12}\,B_{21} & P_6 = S_2\,T_2 \\ P_3 = S_4\,B_{22} & P_7 = S_3\,T_3 \\ P_4 = A_{22}\,T_4 & \end{array}$$

(4) Finally, one computes the following 7 sums:

$$\begin{array}{ll} U_1 = P_1 + P_2 & U_5 = U_4 + P_3 \\ U_2 = P_1 + P_6 & U_6 = U_3 - P_4 \\ U_3 = U_2 + P_7 & U_7 = U_3 + P_5 \\ U_4 = U_2 + P_5 & \end{array}$$

and one returns:

$$\begin{pmatrix} U_1 & U_5 \\ U_6 & U_7 \end{pmatrix}.$$

Next, we recall the Extended Euclidean Algorithm.

Input: $a, b \in R$.

Output: $g \in R$ a gcd of a and b together with $s, t \in R$ such that $g = s\,a + t\,b$.

$r_0 := a$; $s_0 := 1$; $t_0 := 0$
$r_1 := b$; $s_1 := 0$; $t_1 := 1$
$i := 2$
while $r_{i-1} \neq 0$ **repeat**
    $q_i := r_{i-2}$ quo r_{i-1}
    $r_i := r_{i-2}$ rem r_{i-1}
    $s_i := s_{i-2} - q_i\,s_{i-1}$
    $t_i := t_{i-2} - q_i\,t_{i-1}$
    $i := i + 1$
return$(r_{i-2}, s_{i-2}, t_{i-2})$

Exercise 1. Let $m = x^3 - 1$ and $n = x^2 + 1$ be polynomials in $\mathbb{Q}[x]$. Find all polynomials p of degree less than 5 satisfying the system of equations

$$\left\{ \begin{array}{ll} p \equiv 1 & \mod m \\ p \equiv 2 & \mod n \end{array} \right. \tag{3}$$

We aim at applying the Chinese Remaindering Theorem. To do so we need

- to check that n and m are relatively prime, and, if this holds,
- to compute s, t such that $sm + tn = 1$.

Running the Extended Euclidean Algorithm with n and m as input will address these issues. We use the notations of the above algorithm. So, let us define $r_0 := m$ and $r_1 := n$. We have

$$\begin{array}{r|l} x^3 - 1 & x^2 + 1 \\ \cline{2-2} -x - 1 & x \end{array} \quad \text{and} \quad \begin{array}{r|l} x^2 + 1 & -x - 1 \\ \cline{2-2} 2 & -x + 1 \end{array}$$

Hence, we have $(r_2, q_2) = (-x - 1, x)$ and $(r_3, q_3) = (2, -x + 1)$. Thus, the algorithm give:

$$(s_2, t_2) = (-x - 1, 1, -x) \text{ and } (s_3, t_3) = (2, x - 1, -x^2 + x + 1),$$

and, we have

$$2 = (x - 1)m + (-x^2 + x + 1)n,$$

leading to $s = \frac{x-1}{2}$ and $t = \frac{-x^2+x+1}{2}$.
Let $a = 1$ and $b = 2$. Applying the recalled Formula (2), we have

$$c = a + (b - a)\, s\, m = 1 + (2 - 1)\frac{x - 1}{2}(x^3 - 1) = 1/2x^4 - 1/2x^3 - 1/2x + 3/2,$$

which has degree less than 5. All other solutions of (3) are of the form $c + q\, m\, n$, where q is a non-zero polynomial and, thus have degree at least 5.

Exercise 2. We consider the following 4 square matrices of order 2 with coefficients in $\mathbb{Q}$:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},\ B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix},\ C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \text{ and } D = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}.$$

Then we consider the following polynomials of degree 1 in X and with square matrices of order 2 for coefficients:

$$p = AX + B \text{ and } q = CX + D.$$

1. How many additions and multiplications in $\mathbb{Q}$ are needed in order to compute the product pq in a *naive way*.
2. Check that Karatsuba's trick applies here (despite of the fact that matrix multiplication is not commutative).
3. Explain briefly why we can compute pq using only 21 multiplications in $\mathbb{Q}$. How many additions in $\mathbb{Q}$ are needed in this case?
4. Explain briefly in which circumstances using the multiplication scheme of the previous question makes sense.

1. We have:

   $$pq = (AX + B)(CX + D) = ACX^2 + (AD + BC)X + BD,$$

   leading to 4 multiplications and 1 addition of 2×2 matrices. Each multiplication of 2×2 matrices, with the naive algorithm costs 8 multiplications and 4 additions in $\mathbb{Q}$. Therefore, in total, the naive approach for computing pq amounts to 32 multiplications and 20 additions in $\mathbb{Q}$.

2. Without using commutativity for the multiplication, we can write:

   $$(A+B)(C+D) - AC - BD = AC + AD + BC + BD - AC - BD = AD + BC.$$

   Therefore, Karatsuba's trick applies to polynomials with matrix coefficients.

3. Applying Karatsuba's trick. We perform

    - $4+4$ additions in $\mathbb{Q}$ for computing $A+B$ and $C+D$,
    - 3×7 multiplications in $\mathbb{Q}$and 3×15 additions in $\mathbb{Q}$ for computing each of the 3 products $(A+B)(C+D)$, AC, BD using Strassen's trick.

    Therefore, in total, this approach for computing pq amounts 21 multiplications and 61 additions in $\mathbb{Q}$.

4. If the coefficients of the input matrices are large integer numbers and if the products in $\mathbb{Z}$ are computed by a classical quadratic algorithm, then the Karatsuba-Strassen approach may perform much better than the naive approach. If the coefficients of the input matrices are rational numbers with numerators and denominators of about the same size, then which approach to use is harder to decide. Indeed, consider two rational numbers a/b and c/d in canonical form. Computing $a/b + c/d$ requires 1 GCD-with-cofactors, 2 multiplications and 1 addition. Computing $(a/b) \times (c/d)$ requires 2 GCDs-with-cofactors, and 2 multiplications. The GCD computations dominane both costs.

Exercise 3. Let $m \in \mathbb{Q}[x]$ be a non-constant polynomial of degree n. Let $R = Q[x]/\langle m \rangle$ be the set of the residue classes modulo m.

1. Let $p \in \mathbb{Q}[x]$ be a polynomial. How many elements are there in the residue class $\overline{p}$ of p modulo m with degree **less** than n?

2. Explain why we can view each element of R as a vector of n coordinates in $\mathbb{Q}$.

Given two polynomial c and a in $\mathbb{Q}[x]$ we want to decide whether there exists a polynomial f such that we have $c \equiv af \mod m$. For instance, with $m = x^3 - 1$, $c = x - 1$ and $a = x^2 - 1$, one solution is $f = x^2 + 1$. Indeed, we have $(x^2+1)(x^2-1) = x^4 - 1 \equiv x - 1 \mod x^3 - 1$. (Working modulo $x^3 - 1$ means replacing every occurrence of x^3 by 1.)

3. Assume first that $\gcd(a, m) = 1$. Explain why such a polynomial f exists and is unique.

4. Now, assume that $\gcd(a, m) = g$ where g is a non-constant polynomial. Indicate briefly a strategy for solving our problem in this case.

5. Solve our problem for the particular $m = x^3 - 1$, $c = x - 1$ and $a = x^2 + 1$.

1. Only one! The remainder in the Euclidean division of p w.r.t. m.

2. Each element of R is represented by a remainder modulo m. Such remainder has degree less than n and therefore all its coefficients fit in a vector of size n. Moreover, additions in R and multiplication by a scalar can be computed in the same way they are computed in $\mathbb{Q}^n$, that is coordinate-wise. Let us prove it for the addition. Let $\overline{r}$ and $\overline{s}$ be two elements of R represented by $r = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$ and $s = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$ Note that, as polynomials of $\mathbb{Q}[x]$, they may have degree less than $n - 1$. Clearly $(r_0 + s_0) + (r_1 + s_1)x + \cdots + (r_{n-1} + s_{n-1})x^{n-1}$ is the remainder of $r + s$ modulo m and, thus, represents $\overline{r + s}$. Hence, the sum $\overline{r} + \overline{s}$, which equals $\overline{r + s}$, can be computed coordinate-wise.

3. If $\gcd(a, m) = 1$ then a is invertible modulo m. Let u be its inverse modulo m. The equation $c \equiv af \mod m$ becomes $f \equiv uc \mod m$ showing the existence and the unicity of f.

4. Solving the equation $c \equiv af \mod m$ with f as unknown is equivalent to solve the equation $c = af + bm$ with (f, b) as unknown. Let $g = \gcd(a, m)$. Observe that g must divide c for a solution to exist. (Indeed g divides a and m, and thus divides $af + bm$.) So, let us assume that g divides c. Let c', a', m' be such that $c = gc'$, $a = ga'$ and $m = gm'$. We obtain $c' = a'f + bm'$. Let s, t be such that $1 = sa' + tm'$, computed by the Extended Euclidean Algorithm. It follows that $f = sc'$ is a solution to our original problem.

5. In this case we have $\gcd(a, m) = 1$, showing that there exists a unique solution f. Moreover, the example described in the statement tells us that
$$(x^2 + 1)(x^2 - 1) \equiv x - 1 \mod x^3 - 1$$
holds, that is $a(x^2 - 1) \equiv c \mod m$. Hence $f = x^2 - 1$ is the solution!