Foundations of Computer Algebra. CS424b: Quiz 2. UWO, March 9, 2005.

Student ID number:
Student Last Name:

Guidelines. Every printed document is allowed but computers and calculators are not. The duration of the quiz is 40 minutes. The quiz consists of three exercises located on pages 2, 3, 4. 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 an integer $n \in \mathbb{Z}$ the set of the multiples of n (all of them: positive, null or negative) is denoted by $n\mathbb{Z}$. For an integer $n \in \mathbb{Z}$ the residue class of the binary relation $(a, b) \longmapsto a \equiv b \mod n$ is denoted by $\mathbb{Z}/n\mathbb{Z}$, 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

$$(\forall x \in R) \quad \begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \iff x \equiv c \mod m\,n \tag{1}$$

where a convenient c is given by

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

Therefore, for every $a, b \in R$ the system of equations

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \tag{3}$$

has a solution.

Exercise 1. Solve in $\mathbb{Z}$ the following equations or systems of equations.

1. $2x \equiv 2 \mod 6$, with unknown x,
2. $5x \equiv 2 \mod 6$, with unknown x,
3. $3x + 2y = 5$, with unknown (x, y),
4. $12x + 15y = 14$, with unknown (x, y),
5. $\begin{cases} x & \equiv & 2 & \mod 3 \\ x & \equiv & 4 & \mod 5 \end{cases}$

Answer 1

Exercise 2. We consider the following algorithm, which computes the gcd of two integer numbers.

$\gcd(a : \mathbb{Z}, b : \mathbb{Z}) : \mathbb{Z}$ ==

if $a = b$ **then return** a
if $a \equiv 0 \mod 2$ **and** $b \equiv 0 \mod 2$ **then return** $\gcd(a/2, b/2)$
if $a \equiv 0 \mod 2$ **and** $b \equiv 1 \mod 2$ **then return** $\gcd(a/2, b)$
if $a \equiv 1 \mod 2$ **and** $b \equiv 0 \mod 2$ **then return** $\gcd(a, b/2)$
if $a > b$ **then return** $\gcd((a - b)/2, b)$ **else return** $\gcd((b - a)/2, a)$

1. Let n_a and n_b the number of bits (in binary-expansion) of a and b respectively. Give an upper bound for the number of reursive calls needed to compute $\gcd(a, b)$?

2. Give an upper bound for the number of machine word operations needed for computing $\gcd(a, b)$.

Answer 2

Answer 3

Exercise 3. Let a and b be two univariate polynomials in $\mathbb{Z}[x]$. We assume that b is **monic** and has degree $n > 0$ and that a has degree $n + k$ whith $k \geq 0$. We define $a = a_{n+k}x^{n+k} + \cdots + a_n x^n + \cdots + a_1 x + a_0$ and $b = b_n x^n + \cdots + b_1 x + b_0$. We are interesting in computing the remainder r of the Euclidean division of a by b (regarding them as polynomials in $\mathbb{Q}[x]$), by a modular method. Let p be a prime number and Φ_p be the application that maps every integer z with its residue class $\Phi_p(z)$ in $\mathbb{Z}/p\mathbb{Z}$. We extend this application to a map denoted Φ_p again, from $\mathbb{Z}[x]$ to $\mathbb{Z}/p\mathbb{Z}[x]$, such that x is mapped to x.

1. Explain why the remainder r belongs to $\mathbb{Z}[x]$, that is no fractions appears during the computations.
2. Consider $a = x^2 + 7x + 1$ and $b = x + 4$. Compute q and r.
3. Consider $p = 3$. Compute $\Phi_p(a)$ and $\Phi_p(b)$. Then compute the quotient and the remainder of $\Phi_p(a)$ by $\Phi_p(b)$.
4. In the general case, what is the relation between r and the remainder of $\Phi_p(a)$ by $\Phi_p(b)$?
5. Design a modular method to compute r.

Answer 4

Answer 5