Computer Science 345
The Efficient Universe

Homework 2
Due Wednesday, March 1, 2006

No collaboration is permitted for this homework.

It is very important that you provide clear and concise answers. Read your answers to make sure they articulate your understanding. A few sentences or pseudo-code suffice for each of the problems. When you are asked to attempt to do something, please give it your best shot and describe (again clearly and concisely) your thoughts, even if you didn't succeed. No points will be deducted if you don't.

1 Euclidean Algorithm

In this section we study Euclidean Algorithm.

Algorithm 1 Euclidean Algorithm

Input: positive integers a and b.
Output: $\gcd(a, b)$ — the greatest common divisor of a and b.

- Let $a_0 = a$; $b_0 = b$.
- Let $i = 0$.
- while $(a_i \neq 0)$
  - Let $a_{i+1} = b_i \mod a_i$.
  - Let $b_{i+1} = a_i$.
  - Let $i = i + 1$.
- Return b_i.

Problem 1

1. Prove that the algorithm always terminates.
2. Prove that the algorithm performs at most $O(n)$ iterations, where $n = |a| + |b| \approx \log a + \log b$ is the total input length; $|a|$ denotes the length of the number a in binary. Is this algorithm efficient?
3. Prove the following loop invariant:

   $$\gcd(a_i, b_i) = \gcd(a, b),$$

   for every i.
4. Prove the correctness of the algorithm: the value returned by the algorithm is indeed the greatest common divisor of a and b.

Problem 2 *

1. Prove that a_{i+1} is a linear combination (with integer coefficients) of a_i and b_i.
2. Modify the algorithm, so that it returns two integer numbers k and m s.t.

   $$k \cdot a + m \cdot b = \gcd(a, b).$$

2 Groups

Definition 1 *A set G with an operation $*\colon G \times G \to G$ is a group if it satisfies the following properties.*

- *Associativity: for all elements x, y and z*

$$(x * y) * z = x * (y * z).$$

- *There exists an identity element e such that for all elements x*

$$x * e = e * x = x.$$

- *For every x in G, there exists an inverse element y such that*

$$x * y = y * x = e.$$

Remark: *The inverse element y is denoted by x^{-1}.*

We say that the group G is Abelian (or commutative) if for all x and y

$$x * y = y * x.$$

Problem 3 Denote by $\mathbb{Z}_m^*$ the set of integer numbers from 1 to m coprime to m:

$$\mathbb{Z}_m^* = \{x \in \mathbb{Z} : 1 \leq x < m \text{ and } \gcd(x, m) = 1\}.$$

1. Show that for every x and y in $\mathbb{Z}_m^*$, the number $z = x \cdot y \mod m$ belongs to $\mathbb{Z}_m^*$.
2. Prove that the set $\mathbb{Z}_m^*$ with the multiplication operation defined as follows

$$a * b = a \cdot b \mod m$$

is an Abelian group (prove all group properties!).

Hint: Use problem 2, to show that every element has an inverse.

3. Design an efficient algorithm that given an element finds its inverse.

3 Classes $\mathcal{P}$, $\mathcal{NP}$ and $\mathcal{EXP}$

First we recall some definitions from the class.

Definition 2 *An algorithm M is a polynomial time algorithm, if there exists a polynomial $p(n)$ such that for every binary string $x \in \{0,1\}^*$, the running time of M on input x is at most $p(|x|)$, where $|x|$ denotes the length of the string.*

Definition 3 *A set (language) L belongs to the class $\mathcal{P}$ if there exists a polynomial time algorithm M such that for every binary string x:*

- *if $x \in L$, $M(x) = 1$ (M accepts x);*
- *if $x \notin L$, $M(x) = 0$ (M rejects x).*

Definition 4 *A set L belongs to the class $\mathcal{NP}$ if there exists a polynomial time algorithm M (with two parameters) and a polynomial $q(n)$ satisfying the following properties:*

- *If $x \in L$, then there exists a witness w of length at most $q(|x|)$ s.t. $M(x,w) = 1$ (M accepts the witness/proof w).*
- *If $x \notin L$, then for every w, $M(x,w) = 0$ (M rejects the witness w).*

Remark: This definition says, that if an element x belongs to the set L, then there exists a short proof w that "$x \in L$". If, however, x does not belong to L, then there is no valid proof that "$x \in L$".

Problem 4

1. Construct an $\mathcal{NP}$-proof (discussed in class) that 67 is a prime number.
2. Does the set of composite numbers belong to $\mathcal{NP}$? Find a short proof that 57 is composite.
3. If L is in $\mathcal{P}$, is it in $\mathcal{NP}$? Why?

Definition 5 *Similarly to $\mathcal{P}$, we can define the class of languages decidable in exponential time. A set L belongs to the class $\mathcal{EXP}$ if there there exists a polynomial $p(n)$ and an algorithm M satisfying the following properties.*

- *The running time of M on input x is bounded by $e^{p(|x|)}$.*
- *If $x \in L$, $M(x) = 1$ (M accepts x).*
- *If $x \notin L$, $M(x) = 0$ (M rejects x).*

Problem 4.4 Prove that $\mathcal{NP} \subset \mathcal{EXP}$.