

# Assignment Number 3.

April 10, 2008

*NOTE: Due Date for submission is Thursday, 24th April.*

## Notation and Preliminaries.

In this set of exercises we will often need to use the following fact: all the fundamental arithmetic operations: viz addition, multiplication, division (computing the quotient and remainder) can be done in NC. Also, we will use here a generalization of the matrix inverse in NC result: given a system of linear equations (where the number of equations need not be the same as the number of unknowns), we can find a solution, if it exists, in NC.

A polynomial  $a(x) \in \mathbb{F}[x]$  of degree  $d$  is said to be *monic* if the coefficient of  $x^d$  in  $a(x)$  is 1. That is,  $a(x)$  is monic iff its the coefficient of the largest monomial is 1.

## Exercises

1. In this exercise we show that computing the gcd of two polynomials with integer coefficients can be computed in NC. More specifically, suppose we are given two monic polynomials  $a(x)$  and  $b(x)$  of degree  $d$  with coefficients which are integers between  $-H$  and  $H$ . Thus the size of the input is  $2d \cdot \log H$ .

- (a) Let  $m$  be the degree of  $\gcd(a(x), b(x))$ .  $0 \leq m \leq d$ . Then show that there exists a *unique* monic polynomial  $h(x) \in \mathbb{Q}[x]$  of degree  $m$  such that

$$f(x) \cdot a(x) + g(x) \cdot b(x) = h(x),$$

where  $f(x)$  and  $g(x)$  both have degree at most  $(d - 1)$ . Deduce that if in addition to  $a(x)$  and  $b(x)$  we are also given  $m$  then we can find the gcd of  $a(x)$  and  $b(x)$  in NC.

- (b) Show that we can compute the value of  $m$  in NC. This will show that overall, gcd of two monic polynomials with integer coefficients can be computed in NC.
2. A positive integer  $n$  is said to be a *perfect power* if there exist two positive integers  $a$  and  $b \geq 2$  such that  $n = a^b$ . Devise a polynomial-time algorithm to test if an integer is a perfect power.
  3. In this exercise, we show that determining whether a number is a perfect power can in fact be done in NC.
    - (a) Show that in NC we can reduce the problem to the problem of determining if a number is a  $b$ -th power, where  $b$  is a *fixed* integer.

- (b) Show how to determine if a number is perfect square ( $b = 2$ ) in NC. (Hint: Use the Taylor series expansion for  $\sqrt{1+x}$ ).
  - (c) Show how to determine if a number is a perfect cube ( $b = 3$ ) in NC.
  - (d) Generalize to arbitrary  $b$ .
4. In this exercise we will design an algorithm that computes the derivative of a univariate polynomial specified via an arithmetic circuit. Suppose we are given an arithmetic circuit  $C$  that computes a univariate polynomial  $f(x)$ . Show that we can efficiently compute another circuit  $D$  which computes  $f'(x)$ , the derivative of  $f(x)$ .

## Algebra part.

In this series of exercises we will gain a better understanding of the structure of finite fields and in particular show that any two finite fields of the same size are isomorphic.

### Structure of a finite field

1. Let  $\mathbb{F}_q$  be a finite field with  $q$  elements. Show that  $q$  must be of the form  $q = p^r$  for some prime  $p$  and that for every  $\alpha \in \mathbb{F}_q$ , it must happen that  $p \cdot \alpha = 0$ . (This prime  $p$  is called the characteristic of the finite field  $\mathbb{F}_q$ ). Deduce that the elements of  $\mathbb{F}_q$  may be viewed as vectors of dimension  $r$  over the field  $\mathbb{F}_p$ .
2. Consider any  $\gamma \neq 0 \in \mathbb{F}_q$ . Show that there must exist a polynomial  $g(z) \in \mathbb{F}_p[z]$  of degree at most  $r$  so that  $g(\gamma) = 0$ . Further show that the smallest degree monic polynomial satisfied by  $\gamma$  is unique. (A monic polynomial is a polynomial where the coefficient of the largest monomial is 1.) The smallest degree monic polynomial satisfied by  $\gamma$  is called the minimal polynomial of  $\gamma$  over  $\mathbb{F}_p$ .
3. Show that the minimal polynomial  $g(z)$  of an element  $\gamma \in \mathbb{F}_q$  must be irreducible. We now fix this minimal polynomial  $g(z)$  and let's say it has degree  $d$ .
4. Let  $\mathbb{F}_p(\gamma) \subseteq \mathbb{F}_q$  be the set of all elements in  $\mathbb{F}_q$  generated by  $\gamma$ . That is  $\mathbb{F}_p(\gamma)$  consists of all elements in  $\mathbb{F}_q$  of the form

$$(a_0 + a_1 \cdot \gamma + a_2 \cdot \gamma^2 + \dots + a_d \cdot \gamma^d), \quad d \in \mathbb{Z}_{\geq 0}, \quad a_i \in \mathbb{F}_p \text{ for every } i, \quad 0 \leq i \leq d.$$

Show that the set of elements  $\mathbb{F}_p(\gamma)$  is closed under addition and multiplication.

5. Show that  $\alpha^q = \alpha$  for every  $\alpha \in \mathbb{F}_q$ . Deduce that the polynomial  $y^q - y \in \mathbb{F}_q[y]$  factors over  $\mathbb{F}_q$  as:

$$y^q - y = \prod_{\alpha \in \mathbb{F}_q} (y - \alpha).$$

Deduce also that  $\gamma^{-1} \in \mathbb{F}_p(\gamma)$ .

6. Show that the inverse of every nonzero element in  $\mathbb{F}_p(\gamma)$  is also in  $\mathbb{F}_p(\gamma)$  and that therefore  $\mathbb{F}_p(\gamma)$  forms a subfield of  $\mathbb{F}_q$ .
7. Show that this field  $\mathbb{F}_p(\gamma)$  is isomorphic to the field  $\mathbb{F}_p[z]/\langle g(z) \rangle$ , where  $g(z)$  is the minimal polynomial of  $\gamma$ .
8. Show that  $\gamma^{p^d - 1} = 1$ .

### Isomorphism of two finite fields of same size.

In the next few exercises we will show that any two finite fields of the same size are isomorphic. We will use the following fact, without proving it explicitly that any finite field on  $q = p^r$  elements is of the form  $\mathbb{F}_p[y]/\langle f(y) \rangle$ , where  $f(y) \in \mathbb{F}_p[y]$  is a monic irreducible polynomial of degree  $r$ . So let  $f(y)$  and  $g(z)$  be two irreducible polynomials of the same degree  $r$  and the fields corresponding to these two irreducible polynomials be  $\mathbb{F} = \mathbb{F}_p[y]/\langle f(y) \rangle$  and  $\mathbb{G} = \mathbb{F}_p[z]/\langle g(z) \rangle$ .

1. Notice that the element  $y \in \mathbb{F}$  is a root of  $f(y)$  in the field  $\mathbb{F}$ . Show that  $y^p, y^{p^2}, \dots, y^{p^{r-1}}$  are also roots of  $f(y)$  in  $\mathbb{F}$ . Deduce that over  $\mathbb{F}$ , the polynomial  $f(x)$  factors as:

$$f(x) = (x - y) \cdot (x - y^p) \cdot \dots \cdot (x - y^{p^{r-1}}).$$

2. Deduce that  $f(x)$  divides  $(x^{p^r} - x)$ .
3. Show that over  $\mathbb{F}_p$ , the polynomial  $(x^{p^r} - x)$  is precisely the product of all irreducible polynomials  $h(x)$  of degree  $d$  dividing  $r$ .
4. Show that the polynomial  $g(z)$  has a root in  $\mathbb{F}$ . Deduce that  $\mathbb{F} \cong \mathbb{G}$ .