**ADVANCED TOPICS IN ALGORITHMS** **March, 2008**

# Assignment 2

1. Show that for prime $p \geq 3$, $m, n \geq 1$, $(x^{p^m-1} - 1)|(x^{p^n-1} - 1)$ if and only if $m|n$. □

2. Let $F$ be an extension field of (that is, a field containing) $Z_p$. Show that the elements of $F$ are roots of the polynomial $x^{p^n} - x = 0$ in $Z_p[X]$ for some positive integer $n$. Conversely, show that for any extension field $F$ of $Z_p$ the set of elements in $F$ that satisfy the polynomial $x^{p^n} - x = 0$ forms a subfield. Conclude (using the previous question) that subfields of a field of $p^n$ elements are precisely fields of $p^m$ elements for each $m|n$. □

3. Let $m(x)$ be an irreducible polynomial of degree $n$ in $Z_p[X]$. Show that in the field $F = Z_p[X]/m(x)$ the polynomial $m(x)$ has a root. How many roots does the polynomial have in $F$? Express the other roots as polynomials of the first root. □

4. Show that an irreducible polynomial $m(x)$ of degree $d$ divides $x^{p^n} - x$ if and only if $d$ divides $n$. □

5. Let $\alpha \in F$, $F$ extension of $Z_p$ of degree $n$, let $m(x)$, the minimal polynomial of $\alpha$ have degree $n$. Show that $d = ord(\alpha)$ in $F^*$ must satisfy $d|(p^n - 1)$, but $d$ does not divide $p^m - 1$ for any $m < n$. How many irreducible polynomials of degree $d$ exist? How many of them are monic (that is leading coefficient is $1$)? [Note: The last part counts polynomials which are constant multiples of each other only once. Hint: Note that there are $\phi(d)$ elements in $F$ of order $d$.] □

6. Let $F$ be a finite extension field of $Z_p$ and let $m(x) \in Z_p[X]$ be an irreducible polynomial of degree $d$ with a root $\alpha \in F$. Show that $m(x)$ has $d$ (distinct) roots in $F$. Show that all other roots of $m(x)$ can be expressed in terms of $\alpha$. (Show that $\alpha, \alpha^p, \alpha^{p^2} ..., \alpha^{p^d}$ are distinct and are roots of $m(x)$. To prove that $m(x)$ has no other roots, let $q(x) = \prod_{i=1}^{d}(x - \alpha^{p^i})$. Show that $q(x)^p = q(x^p)$ and conclude that the coefficients of $q(x)$ must be in $Z_p$). □

7. Let $F$, $F'$ be two extension fields of $Z_p$ of $p^n$ elements. Let $\alpha$ generate $F^*$. Let $m_\alpha(x)$ be the minimal polynomial of $\alpha$. Show that degree of $m_\alpha(x) = n$. Since $m_\alpha(x)$ divides $x^{p^n} - x$ and elements in $F'$ also are roots of $x^{p^n} - x = 0$, there must be some $\beta \in F'^*$ such that $m_\alpha(x)$ is the minimal polynomial of $\beta$. (Here we are assuming that factorization of $x^{p^n} - x$ is unique in $F_p[X]$.) Show that the map $g : F \longrightarrow F'$ mapping $g(\alpha) = \beta$ defines an isomorphism between $F$ and $F'$. As a consequence, we see that there is atmost one field of $p^n$ elements. □

8. This question derives the Möbius inversion formula. Let $f$,$g$ and $h$ be functions defined from $Z^+$ to $Z^+$. Define the Dirichlet convolution between functions $(f * g)(n) = \Sigma_{d|n} f(d)g(n/d)$. Show that convolution is associative. Define the identify function $I(1) = 1$, $I(n) = 0, n > 1$ and the Möbius function $\mu(1) = 1$ , $\mu(n) = 0$ if the square of a prime number divides $n$ and $\mu(n) = (-1)^k$ when $n$ is square free product of $k$ distinct primes. Show that $I * f = f$ for all $f$ and $\mu * u = I$. Hence conclude that if $f = g * u$ (i.e., $f(n) = \Sigma_{d|n} g(d)$) then $f * \mu = g$ (i.e., $g(n) = \Sigma_{d|n} f(d)\mu(n/d)$). □

9. Let $I_p(d)$ be the number of irreducible polynomials of degree $d$ over $Z_p$. Note that by a previous question, $x^{p^n} - x$ splits into all monic irreducible factors of degree $d$ for each $d|n$. Counting degrees, conclude that $p^n = \Sigma_{d|n} d I_p(d)$. (Each factor on the right side raises the degree of the product on the RS by $d$ for some $d|n$). Use Möbius inversion to show that $I_p(n) = \frac{1}{m}\Sigma_{d|n}\mu(d)p^{n/d}$. Show that $\frac{1}{m}\Sigma_{d|n}\mu(d)p^{n/d} > 0$ for all $n > 0$. (Hint: $\Sigma_{d|n}\mu(d)p^{n/d} > (p^n - p^{n/2} - p^{n/3} - ...) > 0$). Hence conclude that there exists an irreducible polynomial of degree $n$ in $Z_p[X]$ for all $n$. This shows the existance of a finite field of $p^n$ for every $n$. Use the formula to find the number of monic irreducible polynomials of degree $4$ in $F_{16}$. □

10. Find all the irreducible factors of $x^{16} - x$ in $F_2[X]$. Find the order (in the multiplicative group) of the roots of each irreducible factor. □

11. How many elements in $F_{27}$ are contained in no proper subfield of $F_{27}$? □