CS681: Computational Number Theory

Midsem 1

31st August 2007

1. (10 marks) Let $f(X)$ and $g(X)$ be two irreducible polynomials over $\mathbb{F}_q$ of degree d. We know that the finite fields $L = \mathbb{F}_q[X]/f(X)$ and $K = \mathbb{F}_q[X]/g(X)$ are both isomorphic. Use factoring algorithms for polynomials over $\mathbb{F}_q$ to give an efficient algorithm to find the explicit isomorphism. (i.e, choose appropriate basis for L and K and compute the matrix that gives this isomorphism) Give key ideas for the algorithm and brief but convincing argument for the correctness.

2. Let N be an integer given as a product of k distinct primes. Given a monic (i.e leading coefficient is 1) polynomial $f(X)$ in $\mathbb{Z}[X]$ of degree d, give the best possible algorithms for teh following tasks. (the key ideas are sufficient, not entire pseudo code)

   (a) (5 marks) Check if $f(X)$ has a root modulo N.

   (b) (5 marks) If $f(X)$ has a root modulo N, compute one such root.

   Mentino waht the running time of the algorithm is (i.e say whether it is polynomial in d and N, polynomial in d and $\log N$, exponential in both, randomized/deterministic)

3. An algebraically closed field is a field where every polynomial has a root (e.g $\mathbb{C}$). Say whether the following statements are true or false (justify your answer by either giving a counter example or a short proof). Answer with no justifications carry no marks.

   (a) (5 marks) Any finite field cannot be algebraically closed. (Hint: cardinality arguments)

   (b) (5 marks) Any field of finite characteristic cannot be algebraically closed.

Solutions

Problem 1

We know that $\mathbb{F}_q[X]/f(X)$ is isomorphic to $\mathbb{F}_q[X]/g(X)$. Suppose α is a root of f and β a root of g, then the first field is just $\mathbb{F}_q(\alpha)$ and the second field is just $\mathbb{F}_q(\beta)$. Therefore, to find an explicit isomorphism, we just need to hunt for the β in $\mathbb{F}_q(\alpha)$.

For this, look at the field $\mathbb{F}_q[X]/f(X)$. We want the β here. Therefore, factorize $g(Y)$ thinking of it as a polynomial in $(\mathbb{F}_q[X]/f(X))[Y]$. Now we know that β is somewhere in this field. And therefore, that should isolate as a linear factor $Y - \hat{g}(X)$ when we factorize.

Thus, we have the following isomorphism from $\mathbb{F}_q[X]/g$ to $\mathbb{F}_q[X]/f$ which is just taking X to $\hat{g}(X)$.

The central idea is to take the root α from $\mathbb{F}_q(\alpha)$ to the corresponding element in $\mathbb{F}_q(\beta)$. The trick is to just find the root α in $\mathbb{F}_q(\beta)$.

Problem 2

Suppose $f(X) = 0$ modulo N, then by the chinese remainder theorem, this is equivalent to saying $f(X) = 0$ for each p_i. Therefore, a root of f modulo N is equivalent to saying you want a root of f modulo each of the p_is.

Now note that $\mathbb{Z}/p_i\mathbb{Z}$ is a field and we can factorize f over this field using one of the algorithms we did in class. How will we know that f has a root say α_i in $\mathbb{Z}/p_i\mathbb{Z}$? If α was a root, then $(X - \alpha)$ divides $f(X)$ and therefore, this would be one of the factors if we factorize f.

Therefore, the solution to the first subdivision (to check if there is a root modulo N) doing distant degree factorization to get all the degree 1 factors. If it outputs something other than 1 for each p_i, then you know that there is a linear factor modulo each p_i and therefore has a solution modulo N.

The second subdivision is just a small extension: factorize them over each p_i and look for linear terms. Once we get linear terms $(X - \alpha_i)$ for each $\mathbb{Z}/p_i\mathbb{Z}$, we have a vector $(\alpha_1, \alpha_2, \cdots, \alpha_k)$ where each α_i is a root of f modulo p_i. Just take the inverse map of the chinese remaindering, and we get the root of f modulo N.

The first is deterministic and the second is randomized, both running in time polynomial in $\log N$ and $deg(f)$.

Problem 3

Subdivision 1

The statement is true. If K is a finite field, then K cannot be algebraically closed. The proof of this fact is just the existence of irreducible polynomials.

Suppose $K = \mathbb{F}_q$ was algebraically closed, then every polynomial f over K has all its roots in K. Which means that for any polynomial f, since its roots $\alpha_1, \alpha_2, \cdots, \alpha_d$ lie in K, f should split as $(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_d)$ in K. But the very definition of irreducible polynomials mean that they don't split.

Thus the existence of irreducible polynomials show that a finite field cannot be algebraically closed.

Or for a more explicit example, consider the polynomial $(X^q - X) + 1$ over $\mathbb{F}_q$. For ever $a \in \mathbb{F}_q$, we know that it satisfies $X^q - X = 0$ and therefore cannot be a root of the above polynomial. And therefore, this polynomials has no roots in $\mathbb{F}_q$.

Subdivision 2

The earlier argument(s) don't work when the size if the field is infinite. Every field F has something known as its *algebraic closure.* The algebraic closure of F is the smallest field K that contains F and is algebraically closed. For example, the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$. And also, note that the algebraic closure of $\mathbb{Q}$ is not $\mathbb{C}$, it's a much smaller subfield of all algebraic numbers over $\mathbb{Q}$.

Such an algebraic closure exists for every field F, and in particular for $\mathbb{F}_p$. And since $\mathbb{F}_p$ has characteristic p, so will teh algebraic closure. And the algebraic closure is an example of a field with characteristic p that is algebraically closed.

One can think of the algebraic closure of $\mathbb{F}_p$ as the infinite union [1].

$$\mathbb{F} = \bigcup_{d \geq 1} \mathbb{F}_{p^d}$$

[1] some work needs to be done before I can even write such an outrageous infinite union without mathematical rigour, but for the moment just take it for granted that it can be done. The proof involves a certain lemma called the Zorn's Lemma or the axiom of choice.