Mid-semester examination

Due date: March 18, 2013

General instructions:

- Submit your solutions by typesetting in LaTeX.
- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly urged to solve the problems by yourself.
- If you discuss with someone else or refer to any material (other than the course notes) then please put a reference in your answer script stating clearly whom or what you have consulted with and how it has benifited you. We would appreciate your honesty.
- If we need any clarification, please ask one of the instructors.

Total: 40 points

1. (**5 points**) The structure theorem for finite commutative groups (also known as the fundamental theorem of finite abelian groups) states that every finite commutative group G is isomorphic to a group of the form

$$G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{e_k}},$$

where $\mathbb{Z}_n$ represents the cyclic group of order n, and $p_1, \ldots, p_k$ are prime numbers. Use the fundamental theorem of finite abelian groups to devise an efficient (polynomial time) deterministic algorithm that when given two sets of integers $\{d_1, d_2, \ldots, d_r\}$ and $\{c_1, c_2, \ldots, c_t\}$ (in binary) determines whether the group

$$G_1 \stackrel{\text{def}}{=} \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \ldots \oplus \mathbb{Z}_{d_r}$$

is isomorphic to the group

$$G_2 \stackrel{\text{def}}{=} \mathbb{Z}_{c_1} \oplus \mathbb{Z}_{c_2} \oplus \ldots \oplus \mathbb{Z}_{c_t}.$$

2. (**10 points**) A bijection ϕ from a ring $(\mathcal{R}, +, \cdot)$ to itself is called an automorphism if for all $a, b \in \mathcal{R}$, $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. Let n be an integer. Show the following:

(a) (**5 points**) Integer n (given in binary) can be factored in deterministic polynomial time if a nontrivial automorphism of the ring $\frac{\mathbb{Z}_n[x]}{(x^2-1)}$ can be computed in deterministic polynomial time. Here by polynomial time, we mean $\log^{O(1)} n$ bit operations.

(b) (**5 points**) Integer n (given in binary) can be factored in deterministic polynomial time if the number of automorphisms of the ring $\frac{\mathbb{Z}_n[x]}{(x^2)}$ can be counted in deterministic polynomial time, assuming n is either of the form $p \cdot q$ (for primes p and q), or there is a prime p such that p^2 divides n.

3. (**15 points**) Let $f \in \mathbb{F}_q[x]$ be a square-free polynomial of degree n that splits completely over $\mathbb{F}_q$. Let $a_1, \ldots, a_n$ be the distinct roots of f, and $\mathcal{R} = \frac{\mathbb{F}_q[x]}{(f)}$. An endomorphism of $\mathcal{R}$ is a map $\phi : \mathcal{R} \to \mathcal{R}$ satisfying the following properties - For every $g, h \in \mathcal{R}$ and $\alpha \in \mathbb{F}_q$,

   - $\phi(g + h) = \phi(g) + \phi(h)$
   - $\phi(g \cdot h) = \phi(g) \cdot \phi(h)$ and $\phi(1) = 1$, and
   - $\phi(\alpha \cdot g) = \alpha \cdot \phi(g)$.

   An endomorphism ϕ is called an automorphism of $\mathcal{R}$ if ϕ is bijective. Let X be the element $X = x \mod f$. Note that every element in $\mathcal{R}$ can be viewed as a polynomial in X of degree less than n. When we write $g(X)$, we mean an element in $\mathcal{R}$, but when we write $g(x)$ we mean an element in $\mathbb{F}_q[x]$ of degree less than n. With these conventions, prove the following:

   (a) (**4 points**) A map ϕ is an endomorphism if and only if the element $\phi(X) \in \mathcal{R}$ is such that

   $$\phi(x) = a_{\sigma_\phi(i)} \mod (x - a_i),$$

   for every $i \in \{1, \ldots, n\}$, where σ_ϕ is a map from $\{1, \ldots, n\}$ to itself.

   (b) (**3 points**) ϕ is an automorphism of $\mathcal{R}$ if and only if σ_ϕ is a permutation map on $\{1, \ldots, n\}$.

   (c) (**3 points**) Given f as a list of its n coefficients, if we can compute $n + 1$ distinct automorphisms of $\mathcal{R}$ in time T, then we can compute a proper factor of f in time $T + (n \log q)^{O(1)}$. (Computing an automorphism ϕ means, finding the image of X in $\mathcal{R}$ under the automorphism map ϕ.)

   (d) (**5 points**) If we can compute one endomorphism that is not an automorphism of $\mathcal{R}$ in time T, then we can also compute a proper factor of f in time $T + (n \log q)^{O(1)}$. (Once again, computing an endomorphism ϕ means finding $\phi(X)$ in $\mathcal{R}$.)

4. (**10 points**) There is an algorithm, due to René Schoof, which finds the square root of a given element a in a prime field $\mathbb{F}_p$ in time polynomial in $|a|$ and $\log p$. Moreover, this algorithm is 'unconditional', which means that it is not based upon the assumption of the ERH. Use Schoof's algorithm as a 'blackbox' to show the following:

   Let $\mathbb{F}_p$ be a prime field such that $p - 1 = 2^t$, for some $t > 0$. Show that there is an unconditional deterministic polynomial time algorithm to factor a given polynomial f over $\mathbb{F}_p$. (Mark the word 'unconditional' - do not assume ERH!).

   Can you make your algorithm work (in deterministic polynomial time) if $p - 1$ is of the form $2^t \cdot m$, where $m = \log^{O(1)} p$?