Problem Set 2: Part B

- Due Date: **29 Mar, 2022**
- The points for each problem is indicated on the side. The total available in this part of the set is **70 points** and you can choose to **answer any 50 points** worth of questions for a full score (anything above this threshold will be bonus points and counted towards your aggregate).
- The problem set has a fair number of questions so please do not wait until close to the deadline to start on them. Try and do one question every couple of days.
- Turn in your solution to this part electronically (PDF; either LaTeXed or scanned etc.) on Acadly.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring to sources other than the class notes is strongly discouraged. But if you do use an external source (eg., other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources (including collaborators) in your writeup. This will NOT affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.
- Be clear in your writing.

1. **[Fast interpolation]** (10)

   Assume that n is a power of 2. Given as input distinct field elements $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{F}$ and arbitrary field elements $\beta_0, \ldots, \beta_{n-1} \in \mathbb{F}$, computes the coefficients of the unique polynomial $f(x) \in \mathbb{F}[x]$ of degree less than n such that $f(\alpha_i) = \beta_i$ in time $O(n \cdot \text{poly}\log(n))$ (assuming that all field operations are unit time operations).

   [Hint: Suppose $Z_L(x)$ is the polynomial that is zero on the first half of α's and $Z_R(x)$ is teh polynomial that is zero on the second half, and if you were to write $f(x) = f_L(x)Z_R(x) + f_R(x)Z_L(x)$, what should f_L and f_R be?]

2. **[Convolutions and wrapped convolutions]** (2 + 6 + 6 + 6)

   Let n be a power of 2 and let R be a ring in which we can divide by 2.

   Given two "vectors" $f = [f_0, \ldots, f_{n-1}]$ and $g = [g_0, \ldots, g_{n-1}]$ in R^n (a tuple of n elements from a ring R), the n-length convolution is defined as the following $2n$-length "vector" $h = [h_0, \ldots, h_{2n-1}]$ with $h_{2n-1} = 0$ and

   $$h_\ell = \sum_{j=0}^{2n-1} f_j g_{\ell-j} \quad \text{for all } \ell = 0, \ldots, 2n-2.$$

   (Any subscript that is out-of-bounds is set to zero.)

   As you can see, convolution is just polynomial multiplication of f and g.

In various applications, the following two *wrapped* versions are very useful. The n-length *positively wrapped convolution (PWC)* of f and g, and the n-length *negatively wrapped convolution (NWC)* is given by the n-length vectors $h^+ = [h_0^+, \ldots, h_{n-1}^+]$ and $h^- = [h_0^-, \ldots, h_{n-1}^-]$ given by

$$h_\ell^+ = h_\ell + h_{n+\ell} \qquad \text{for all } \ell = 0, \ldots, n-1,$$
$$h_\ell^- = h_\ell - h_{n+\ell} \qquad \text{for all } \ell = 0, \ldots, n-1,$$

where $h = [h_0, \ldots, h_{2n-1}]$ is the n-length convolution of f and g.

(a) Observe that $\mathrm{PWC}(f, g)$ is the unique polynomial $h^+(x)$ of degree less than n such that $h^+(x) = f(x)g(x) \bmod x^n - 1$, and similarly $h^-(x)$ is the unique polynomial of degree less than n with $h^-(x) = f(x)g(x) \bmod x^n + 1$.

(b) Suppose R contains an n-PROU ω. Suppose $p(x), q(x) \in R[x]$ are two polynomials of degree less than n such that $p(\omega^i) = q(\omega^i)$ for all $i = 0, \ldots, n-1$. Show that $p(x) = q(x)$.

[Hint: Note that you are only working over a ring and not a field and so, generally speaking, the degree mantra DOES NOT hold. But, on the other hand, you are given that 2 is invertible in R and that ω is an n-PROU.]

(c) Assume the fact that $\prod_{i=0}^{n-1}(x - \omega^i) = x^n - 1$. Come up with an algorithm to compute $\mathrm{PWC}(f, g)$ for $f, g \in R^n$ that performs

- $O(n \log n)$ additions in R,
- $O(n \log n)$ multiplications of the form $R \times \omega^i$,
- n multiplications of the form $R \times R$.

[Hint: Note that computing the product fg and then going modulo $x^n + 1$ may have worked, but that requires an $2n$-PROU, and also ends up using $2n$ multiplications of the form $R \times R$. What *can* you do with just an n-PROU?]

(d) Now, suppose $\tau \in R$ is a $2n$-PROU. Assume that $\tau^n = -1$. Come up with an algorithm to compute $\mathrm{NWC}(f, g)$ for $f, g \in R^n$ that performs

- $O(n \log n)$ additions in R,
- $O(n \log n)$ multiplications of the form $R \times \tau^i$,
- n multiplications of the form $R \times R$.

[Hint: $(\tau x)^n - 1 = -(x^n + 1)$. Can you massage f, g into different polynomials $\tilde{f}, \tilde{g}$ such that you can recover $\mathrm{NWC}(f, g)$ from $\mathrm{PWC}(\tilde{f}, \tilde{g})$?]

3. **[Quotients in groups and rings]** (2 + 3 + 5 + 5)

Let G be a group and let $H \trianglelefteq G$ be a normal subgroup. We would like to define a product operation on cosets of H:

$$aH \cdot bH := (ab)H$$

(a) Show that the above product is well-defined. That is, if the cosets $aH = a'H$ and $bH = b'H$, then cosets $(ab)H = (a'b')H$. This shows that the set of cosets of H in G, when H is normal in G, forms a group itself and is denoted by $\frac{G}{H}$.

(b) Let $\varphi : G_1 \to G_2$ be a homomorphism between two groups. Show that the homomorphism φ is one-to-one if and only if $\ker(\varphi)$ is trivial (only consists of the identity element). Also, show that

$$\mathrm{Im}(\varphi) = \{g_2 \in G_2 \ : \ \exists g_1 \in G_1 \text{ such that } \varphi(g_1) = g_2\}$$

is a subgroup of G_2. Is this always a normal subgroup of G_2?

(c) Two groups G_1 and G_2 are isomorphic (denoted by $G_1 \cong G_2$) if we can find a homomorphism $\varphi : G_1 \to G_2$ that is one-to-one and onto. Given a homomorphism $\sigma : G_1 \to G_2$, prove formally that

$$\frac{G_1}{\ker(\sigma)} \cong \mathrm{Im}(\sigma).$$

That is, construct a map φ from $\frac{G_1}{\ker(\sigma)}$ to $\mathrm{Im}(\sigma)$, prove it is well-defined and is a homomorphism, and prove that it is one-to-one and onto.

(d) Along similar lines, if $\sigma : R_1 \to R_2$ is a homomorphism between two rings, show that

$$\frac{R_1}{\ker(\sigma)} \cong \mathrm{Im}(\sigma).$$

4. **[Counting the number of irreducible polynomials over $\mathbb{F}_p$]** (10)

Suppose $f, g : \mathbb{N} \to \mathbb{R}$ such that $f(n) = \sum_{d|n} g(d)$. Then,

$$g(n) = \sum_{d|n} f(d)\mu(n/d)$$

where $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is the Möbius function given by

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is a product of an odd number of distinct primes,} \\ -1 & \text{if } n \text{ is a product of an even number of distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

This is referred to as the *Möbius inversion formula*, and you may assume this fact for this question.

Fix a prime p and suppose r is large enough. Use the above inversion formula and the equation

$$x^{p^r} - x = \prod_{\substack{\gamma \text{ monic, irred.} \\ \deg(\gamma)|r}} \gamma(x)$$

to show that the number of monic irreducible polynomials of degree r is at least $\frac{p^r}{r} \cdot (1 - o(1))$.

5. **[Computing square-roots of modulo x^k]** (15)

In class we saw an algorithm that, given $g(x)$ such that $g(0) = 1$, and an integer k, we could compute a polynomial $h(x)$ such that $g(x)h(x) = 1 \bmod x^k$ in time near-linear time.

Modify that approach to find square-roots modulo x^k. That is, you are given a polynomial $g(x) \in \mathbb{F}[x]$ with $g(0) = 1$, and an integer k. Compute a polynomial $h(x)$ such that

$$g(x) = (h(x))^2 \bmod x^k$$

in time $\tilde{O}(n)$ where $n = \max(\deg(g), k)$.
