CS 235: Algebraic Algorithms, Spring 2021

Practice Problems for Final Exam

Exam Date: 6:00PM, Tuesday, May 05^{th}, 2021.

Problem 1. Merten's Theorem. For each positive integer k, let P_k denote the product of the first k primes. Show that $\varphi(P_k) = \Theta(P_k/\log\log P_k)$.

Solution. Let $\{p_i\}_{i=1}^k$ denotes the set of first k primes which gives $P_k = \Pi_{i=1}^k p_i$. Then, by Theorem 2.11, we have

$$\varphi(P_k) = P_k \cdot \Pi_{i=1}^k (1 - 1/p_i) = P_k \cdot \Pi_{p_i \leq p_k}(1 - 1/p)$$

Note that for $p_i \geq 2$, $(1 - 1/p_i) < 1$ and $P_k > \log P_k$. Thus, we obtain the following

$$\varphi(P_k) = P_k \cdot \Pi_{p_i \leq p_k}(1 - 1/p_i) \leq P_k \cdot \Pi_{p_i \leq \log p_k}(1 - 1/p_i)$$

By Theorem 5.13, we have $P_k \cdot \Pi_{p_i \leq \log p_k}(1 - 1/p_i) = \Theta(P_k/\log\log P_k)$ which implies that $\varphi(P_k) = \Theta(P_k/\log\log P_k)$

Problem 2. Group Theory.

1. List the cosets of $\langle 7\rangle$ in $\mathbb{Z}_{16}^*$. Is the quotient group $\mathbb{Z}_{16}^*/\langle 7\rangle$ cyclic?

   Solution. We have $\langle 7\rangle = \{1, 7\}$ and $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$. Thus, the cosets are $\langle 7\rangle = \{1, 7\}$, $3\langle 7\rangle = \{3, 5\}$, $9\langle 7\rangle = \{9, 15\}$, and $11\langle 7\rangle = \{11, 13\}$.

   Note that $|\mathbb{Z}_{16}^*/\langle 7\rangle| = 4$ and $order(3\langle 7\rangle) = 4$ which implies that $\mathbb{Z}_{16}^*/\langle 7\rangle$ is a cyclic group.

2. Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{36}$ and $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_9$ isomorphic?

   Solution. We know that if two integers n, m are relatively primes, we have $\mathbb{Z}_{mn} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. This also applies for more than two integers as long as they are relatively primes. Notice that $12 = 3 \cdot 4$ and $36 = 4 \cdot 9$, then we can "decompose" the group as direct product of cyclic groups, namely, $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{36} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9$. Similarly, $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_9 \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$. Finally, we can see that both groups have the same order of 864 which implies that $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{36} \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_9$.

Problem 3. Ring Theory.

1. Let F be a field and let $f(x)$ be a non-zero polynomial in $F[x]$. Show that $f(x)$ is a unit in $F[x]$ if and only if $deg(f(x)) = 0$.

   Solution. " $\Longrightarrow$:" Assume $deg(f(x)) = 0$, then let $f(x) = c \neq 0_F$, some constant, which is a nonzero element of the field F. Since F is a field and $c \neq 0_F$, its inverse c^{-1} exists which implies that $f(x) = c$ is a unit in $F[x]$.

   " $\Longleftarrow$:" Given that $f(x)$ is a unit, then it is easy to see that $f(x) \neq 0_{F[x]}$. Suppose, for the sake of contradiction, that $deg(f(x)) > 0$, then let $deg(f(x)) \geq 1$. Since F is a field, $F[x]$ is also a field, which implies that there exists some $g(x)$ such that $f(x)g(x) = 1_{F[X]} = 1_F$. Also, observe that $deg(1_F) = deg(1_{F[x]}) = deg(f(x)g(x)) = deg(f(x)) + deg(g(x)) = 0$. Since we assume that $deg(f(x)) \geq 1$, it must be the case that $deg(g(x)) \leq -1$ which is a contradiction since a degree of a polynomial cannot be negative. Thus, our assumption is wrong which means $deg(f(x)) = 0$.

2. Which of the following are subrings of the field $\mathbb{R}$ of real numbers.

   a. $A = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}$, and n is even$\}$

   b. $B = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}$, and n is odd$\}$

   Solution. A is a subring of the field $\mathbb{R}$. Let $a = m + n\sqrt{2}$ and $b = r + s\sqrt{2}$, where m, n, s, t are some integers n, s are even, and $a, b \in A$. Then, $a+b = (m+r)+(n+s)\sqrt{2}$ which implies that $a + b \in A$ because $(n + s)$ must be an even number. Similarly, $ab = (mr + 2ns) + (ms + nr)\sqrt{2} \in A$ because $(ms + nr)$ must be even as well. We have $-a = -m + (-n)\sqrt{2} \in A$ since $-n$ is obviously even based on our assumption. Finally, $1_{\mathbb{R}} = 1 + 0\sqrt{2}$ which implies that $1_{\mathbb{R}} \in A$. Thus, A satisfies all condition of a subring of the field $\mathbb{R}$.

   B is not a subring of the field $\mathbb{R}$ because it violates the closure of addition. Namely, consider $b = \sqrt{2} = 0 + 1\sqrt{2}$ which implies that $b \in B$. But $b + b = 0 + 2\sqrt{2}$ which implies that $b + b \notin B$ because 2 is an even number.

3. Prove the following ring isomorphism: $\mathbb{Z}[X]/(n, X) \cong \mathbb{Z}_n$, where (n, X) is the principal ideal of $\mathbb{Z}[X]$ generated by n and X, for $n \geq 2$.

   Solution. Consider the following mapping function $\rho : \mathbb{Z}[X] \to \mathbb{Z}_n$. Note that ring isomorphism is an equivalence relation (see Exercise 7.48, the proof should be similar to that of Exercise 6.22 about group isomorphism, which was introduced in Discussion 7) which implies transitivity. Thus, we can "decompose" ρ as follows: $\rho_1 : \mathbb{Z}[X] \to \mathbb{Z}$ and $\rho_2 : \mathbb{Z} \to \mathbb{Z}_n$. Specifically, $\rho_1(f(X)) = f(0) = p$ where $f(X) \in \mathbb{Z}[X]$ and $p \in \mathbb{Z}$, and $\rho_2(n) = q$ where $q \in \mathbb{Z}_n$. It is easy to see that ρ_1 is homomorphic (proof ideas are very simple and similar to those introduced in Discussion 9), and ρ_2 simply does the modulo

n arithmetic which is homomorphic by default. Thus, ρ has to be homomorphic as well.

For some integers $q \in Z_n$, we have some $f(X) \in \mathbb{Z}[X]$ such that $\rho(f(X)) = q \in \mathbb{Z}$ and observe that $\mathbb{Z} \subset \mathbb{Z}[X]$ because we can treat $\mathbb{Z}$ as the set of constant functions. This means that ρ is surjective which implies that the image of ρ, $Im(\rho) = \mathbb{Z}_n$ (i.e. the surjective relation guarantees that all elements in $\mathbb{Z}_n$ can be mapped to).

By definition of kernel of ρ, $Ker(\rho) = \{f(X) \in \mathbb{Z}[X] \mid \rho(f(X)) = 0 \in Z_n\}$. This means that ρ_1 maps $f(X)$ to some integer $p \in \mathbb{Z}$ which is a multiple of n, namely $p = na$ for some integer a, which is congruent to $0 \in \mathbb{Z}_n$.

By definition of principal ideal of $\mathbb{Z}[X]$, $(n, X) = \{nf(X) + Xf(X) \mid f(X) \in \mathbb{Z}[X]\}$. Notice that ρ_1 does the mapping by substituting $X = 0$ which gives $nf(0) + Xf(0) = nf(0) \in \mathbb{Z}$, a multiple of n. Then, ρ_2 obviously maps such $nf(0) \in \mathbb{Z}$ to $0\mathbb{Z}_n$ because it does modulo n arithmetic. Therefore, we can easily see that $Ker(\rho) = (n, X)$.

By Theorem 7.27 (First isomorphic theorem), we have $\mathbb{Z}[X]/Ker(\rho) \cong Im(\rho)$ which completes the proof of $\mathbb{Z}[X]/(n, X) \cong \mathbb{Z}_n$.

Problem 4. Topics at Midterm.

1. Is there a number x which is congruent to $1, 2, 2, 1$ under modulo $2, 3, 4, 5$ respectively?

   Solution. Assume there exists such x, we have the following system of congruences.

   $$x \equiv 1 \bmod 2$$
   $$x \equiv 2 \bmod 3$$
   $$x \equiv 2 \bmod 4$$
   $$x \equiv 1 \bmod 5$$

   Note that we cannot apply the Chinese Remaindering Theorem (CRT) here because the $\gcd(2, 4) = 2$, in other words, the modulos are not relatively prime.

   From the first congruence in the system, we have $x = 2n + 1$ which implies that x is an odd number. However, from the third congruence, we have $x = 4n' + 2 = 2(n' + 1)$ which implies that x is an even number. Thus, we obtain a contradiction as a number cannot be both even and odd, which implies that our assumption is wrong.

2. Find an integer n where $n > 4 \cdot \varphi(n)$

   Solution. Recall from Theorem 2.11, we have $\varphi(n) = n \cdot \Pi_{i=1}^{r}(1 - 1/p_i)$ if we have the following prime factorization of $n = \Pi_{i=1}^{r} p_i^{e_i}$.

   We want to find a number such that $n > 4 \cdot n \cdot \Pi_{i=1}^{r}(1 - 1/p_i)$, or equivalently, we find p_i's such that $1/4 > \cdot \Pi_{i=1}^{r}(1 - 1/p_i)$ (as it is easy to see that the cancellation law applies in this case). Note that $\Pi_{i=1}^{r}(1 - 1/p_i)$ gets smaller as we have larger values of p_i, so we make the following observation

   $$r = 1 \implies (1 - 1/2) = 1/2 > 1/4$$
   $$r = 2 \implies (1 - 1/2)(1 - 1/3) = 1/2 \cdot 1/3 > 1/4$$
   $$r = 3 \implies (1 - 1/2)(1 - 1/3)(1 - 1/5) = 1/2 \cdot 1/3 \cdot 4/5 > 1/4$$
   $$r = 4 \implies (1 - 1/2)(1 - 1/3)(1 - 1/5)(1 - 1/7) = 1/2 \cdot 1/3 \cdot 4/5 \cdot 6/7 < 1/4$$

   Thus, if we choose $r = 4$, $\{p_i\}_{i=1}^{4}$ to be the first four primes and and $\{e_i\}_{i=1}^{4}$ to be all 1's, then $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and $\varphi(n) = \varphi(210) = 210 \cdot 1/2 \cdot 1/3 \cdot 4/5 \cdot 6/7 = 48$, which satisfies $n > 4 \cdot \varphi(n)$ as $210 > 4 \cdot 48 = 192$.

3. Find integers x and y such that $1064s + 856t = gcd(1064, 856)$

   Solution. Use Extended Euclidean Algorithm (EEA), try to enumerate the steps yourself. One possible answer is $s = -37, t = 46$, and $\gcd(1064, 856) = 8$. Note that your pair of s, t is not unique, using EEA in the textbook gives you one possibility.