CS 235: Algebraic Algorithms, Spring 2021

Final Exam Solution

Date: 06:00PM, Wednesday, May 05, 2021.

Problem 1. What fraction (within a constant factor) of n-bit strings the product of two primes make? Explain.

Solution. This problem asks you to find the fraction of numbers that can be represented as a product of two prime over all possible numbers that can be represented as an n-bit string. In other words, let t be such number, then from 1 to t, we want to know how many numbers in that range that can be represented as the product of exactly two primes, and calculate the fraction of those products over all numbers from 1 to t, broadly speaking.

Consider the product of two primes, one with some length k, the other one with length $n-k$; in other words, k is (really) strictly smaller than n. Note that there are 2^k possibilities for binary strings (i.e. something like 10011101) of length k because at each position (i.e. bit) of the string, there can only be two possibilities, either a 0 or a 1. Similarly there are 2^{n-k} possibilities for a binary string of length $n-k$. Therefore, by the prime number theorem, the number of possible primes that can be presented as a k-bit binary string is $\sim 2^k/k$; similarly, we obtain the number of possible primes represented as a $n-k$-bit strings is $\sim 2^{n-k}/(n-k)$. Thus, the number of possible products of two such primes is given by

$$2^k/k \cdot 2^{n-k}/(n-k) = 2^n/(nk-k^2) \approx 2^n/nk$$

as we assume $k < n$ which means that $k^2 < nk$ and so nk dominates k^2 as n gets large. To get a tight bound in terms of n, we approximate $1/k$ by summing all possible $1/k$ for $k < n/2$; namely, we have $1/k \leq \Sigma_{k<n} 1/k = \Theta(\log n)$ (this is Calculus, see Sum of Harmonic Series). Thus, we obtain the following

$$2^n/nk = \Theta(2^n \cdot \log n/n)$$

Therefore, the fraction of possible numbers that can be represented as product of two primes over all numbers that can be represented as an n-bit string is $\Theta(\frac{2^n \cdot \log n/n}{2^n}) = \Theta(\frac{\log n}{n})$.

Problem 2. State carefully Merten's Theorem.

Solution. The statement of Merten's Theorem is as follows

$$\Pi_{p \leq x}(1 - 1/p) = \Theta(1/\log x)$$

A meaningful thing described by this theorem is that this equation tells us more about how primes are distributed along the number line. Namely, they can't be too close and too far which reflects by the fact that the probability that you find a prime not being a factor less than x on the number line is asymptotically close to $1/\log n$ as n gets large. In other words, this probability is very close to 0 with large n which means that you can almost always find the opposite of such prime p.

Problem 3. What is the exponent of the group $\mathbb{Z}_{245}^*$. Explain.

Solution. We know that $\mathbb{Z}_{245}^* \cong \mathbb{Z}_{49}^* \times \mathbb{Z}_5^*$. Thus, the exponent of $\mathbb{Z}_{245}^*$ is given by $\mathsf{lcm}(\mathsf{exp}(\mathbb{Z}_{49}^*), \mathsf{exp}(\mathbb{Z}_5^*))$ (by Theorem 6.40). Observe that $\mathsf{exp}(\mathbb{Z}_{49}^*) = \varphi(49) = \varphi(7^2) = 42$ and $\mathsf{exp}(\mathbb{Z}_5^*) = 4$ (by Theorem 2.10). Thus, $\mathsf{exp}(\mathbb{Z}_{245}^*) = \mathsf{lcm}(42, 4) = 84$.

Problem 4. Give examples of an integral domain that is not a field and of a non-trivial ring that cannot be extended to a field. Explain

Solution.

- $\mathbb{Z}$ is an integral domain (see example 7.18), but not a field because there are only two units in $\mathbb{Z}$, namely $-1, 1$ (see example 7.10).
- $\mathbb{Z}_2$ is a non-trivial ring that cannot be extended to a field. In fact, any ring that has zero divisor should do (example: $\mathbb{Z}_2, \mathbb{Z}_6, \mathbb{Z}_{15}, etc.$) because the definition of zero divisor violates the condition forming of a field.