Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #9

As in class, we use the convention that $a \bmod n$ is the integer in $\{1, \ldots, n\}$ congruent to a modulo n.

Problem 1. Let $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ be a uniformly random permutation. Show that the average length of the cycle containing 1 is $(n+1)/2$.

Problem 2. Let $n \geqslant 1$ be a squarefree integer. Choose $a_0, \ldots, a_{n-1} \in \mathbb{Z}/n\mathbb{Z}$ uniformly at random and let $f(X) = a_{n-1}X^{n-1} + \cdots + a_0$. Show that the resulting random map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sending x to $f(x)$ has the same probability distribution as the map constructed in Theorem 15.1.2.

Problem 3. Let $n = p_1^{e_1} \cdots p_k^{e_k}$ with distinct primes $p_1, \ldots, p_k$. Let $q_1 < \cdots < q_r$ be primes not dividing n let and $t \geqslant 1$ and $s \geqslant 2$ such that $q_r^{st} \leqslant n$. Show that the number of residue classes $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $(a^s \bmod n)$ is of the form $q_1^{f_1} \cdots q_r^{f_r}$ is at least

$$\frac{r^{st}}{s^{k(s-2)}(st)!}.$$

Problem 4. Consider integers $k_1, \ldots, k_n \geqslant 2$ and distinct prime numbers $q_1, \ldots, q_m$. Let $q_j^{e_{ij}}$ be the largest power of q_j dividing k_i. Show that we can compute a list of all $e_{ij} > 0$ in quasi-linear time

$$\widetilde{\mathcal{O}}(\log k_1 + \cdots + \log k_n + \log q_1 + \cdots + \log q_m).$$

Hint: Use a product tree and remainder trees. Also, use the integer analog of Problem 3 on problem set 5.

Problem 5.

a) Show that you can implement Dixon's random squares method to run in time
$$\widetilde{\mathcal{O}}(\exp(C \cdot \sqrt{(\log n)(\log\log n)}))$$
with $C = 3/\sqrt{2}$.
Hint: Apply Problem 4 to speed up step 1.

b) (bonus) Improve the constant to $C = 2$.
Hint: Use Wiedemann's algorithm (see for example chapter 12.4 in "Modern Computer Algebra") to speed up solving the system of linear equations in $\mathbb{F}_2$.