Math 286X: Arithmetic Statistics

Spring 2020

Problem set #1

Problem 1. Fix a polynomial $f(X) \in \mathbb{Z}[X]$ of degree 1 or 2. Show that

$$\mathbb{P}(f(x) \text{ squarefree} \mid x \in \mathbb{Z}) = \prod_{p \text{ prime}} \mathbb{P}(f(x) \not\equiv 0 \mod p^2 \mid x \in \mathbb{Z}).$$

(Also think about what goes wrong in the proof for large degrees.)

Problem 2. For each prime number p, fix a residue class $c_p \in \mathbb{F}_p$. Show that

$$\mathbb{P}(x \not\equiv c_p \mod p \quad \forall p \mid x \in \mathbb{Z}) = 0.$$

Problem 3. Fix an odd prime l. Order the quadratic number fields K by $|\operatorname{disc}(K)|$. Show that

$$\mathbb{P}(K \text{ unramified at } l \mid K \text{ quadratic number field}) = \frac{l}{l+1}.$$

Problem 4. Let $n \geqslant 2$. Show that the number of squarefree monic polynomials $f(X) \in \mathbb{F}_q[X]$ of degree n is $q^n - q^{n-1}$. (Hint: Every monic polynomial $a(X)$ can be written uniquely as $a(X) = f(X)g(X)^2$, where $f(X)$ is squarefree and both $f(X)$ and $g(X)$ are monic.)

Problem 5. Show that there are sets $S_p \subseteq \mathbb{F}_p$ (for prime p) such that

$$\mathbb{P}((x \bmod p) \in S_p \quad \forall p \mid x \in \mathbb{Z}) = 0,$$

but

$$\prod_p \mathbb{P}(x \in S_p \mid x \in \mathbb{F}_p) > 0.$$

Problem 6. Order pairs $(x, y) \in \mathbb{N}^2$ by $\max(x, y)$. What is

$$\mathbb{P}(\gcd(x, y) = 1 \mid (x, y) \in \mathbb{N}^2)?$$

Problem 7 (If you know about Dirichlet series and how to make use of their complex analysis)**.** Use Dirichlet series to prove that

$$\mathbb{P}(x \text{ squarefree} \mid x \in \mathbb{N}) = \frac{1}{\zeta(2)}.$$

Problem 8. For any $t \in \mathbb{F}_q$, the discriminant of the polynomial $f_t(X) = X^3 - tX^2 + (t-3)X + 1$ is a square: $\operatorname{disc}(f_t) = (9 - 3t + t^2)^2$. Assuming the discriminant is nonzero (the polynomial $f_t(X)$ is squarefree), this implies that either $f_t(X)$ splits into linear factors, or its Galois group is the cyclic group $A_3 \subset S_3$ of degree three. Show that

$$\lim_{q\to\infty} \mathbb{P}(f_t(X) \text{ splits into linear factors} \mid t \in \mathbb{F}_q) = \mathbb{P}(g = \mathrm{id} \mid g \in A_3) = \frac{1}{3}.$$

Problem 9. Here are two ways to estimate the number $N(T)$ of pairs $(x, y) \in \mathbb{N}^2$ such that $x^2 y \leqslant T$:

$$a) \quad N(T) = \sum_{1\leqslant x\leqslant\sqrt{T}} \#\{1 \leqslant y \leqslant \frac{T}{x^2}\} \approx \sum_{1\leqslant x\leqslant\sqrt{T}} \frac{T}{x^2} \approx T \cdot \sum_{x=1}^{\infty} \frac{1}{x^2} = \zeta(2) \cdot T.$$

$$b) \quad N(T) = \sum_{1\leqslant y\leqslant T} \#\{1 \leqslant x \leqslant \sqrt{\frac{T}{y}}\} \approx \sum_{1\leqslant y\leqslant T} \sqrt{\frac{T}{y}} \approx \sqrt{T} \cdot \sum_{1\leqslant y\leqslant T} y^{-1/2} \approx 2 \cdot T.$$

Which is better for large T? Can you give an error bound for the better one?

Problem 10. Let a, b, c be a 2-cycle, an $(n-1)$-cycle, and an n-cycle in S_n (where $n \geqslant 2$). Show that they together generate the entire symmetric group S_n.