MOP 2018: EQUATIONS MOD p AND WEIL (06/19, K)

VICTOR WANG

Throughout these notes, p denotes a prime.

1. Counting points on curves

Here is an example.

Problem 1.1 (ISL 2012 N8)**.** If p is sufficiently large (e.g. $p > 100$), and $r \in \mathbb{F}_p$ is a constant, prove that $y^2 = x^5 + r$ has a solution $(x, y) \in \mathbb{F}_p^2$.

Question 1.2. How well can you estimate the number of solutions?

2. Exponential sums

References: `https://www.encyclopediaofmath.org/index.php/Exponential_sum_estimates`; `https://mathoverflow.net/q/138193/25123`.

Problem 2.1 (van der Corput, Weil)**.** If $f \in \mathbb{F}_p[x]$, estimate the magnitude of $\sum_{n\in\mathbb{F}_p} e_p(f(n))$, where $e_p(x) := e^{2\pi i x/p}$. When can you compute it exactly?

Question 2.2. What if $f \in \mathbb{F}_p(x)$ is a *rational* function instead?

Problem 2.3 (Non-density Ramsey theory)**.** Find a set of size $\Omega(p)$ in $\mathbb{F}_p$ with no solutions to $x + y = z^2$.

Remark 2.4. Still, Lindqvist proved the "partition regularity" of such equations.

3. The zeta function of an algebraic variety

Reference: Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions.*

Definition 3.1. The *zeta function* of a variety $X/\mathbb{F}_q$ is

$$Z_X(T) := \exp\left(\sum_{n\geq 1} \frac{|X(\mathbb{F}_{q^n})|}{n} T^n\right) \in \mathbb{Q}[[T]].$$

Question 3.2. Does this feel natural to you? Can you relate $Z_X(T)$ to other natural candidates?

Problem 3.3. Let $X/\mathbb{F}_q$ be defined by some polynomials $f_1, \ldots, f_d$ in n variables with $\mathbb{F}_q$ coefficients.

(1) Prove that $Z_X(T) \in \mathbb{Z}[[T]]$.
(2) Dwork showed, using p-adic methods, that a hypersurface in $\mathbb{A}^n$ (i.e. the $d = 1$ case) has a *rational* zeta function $Z_X(T) \in \mathbb{Q}(T)$. Extend this to arbitrary d.