The Chevalley-Warning Theorem

Let $\mathbb{F}$ denote a finite field. The goal of this talk is to give sufficient conditions for the existence of points on certain varieties defined over finite fields. The kind of arguments involved are mostly combinatorial in nature. We begin with an easy warm-up problem.

Problem 1. Any element of $\mathbb{F}$ is a sum of two squares.

Problem 1 states that the equation $x^2 + y^2 = a$ admits solutions (x, y) for every value of $a \in \mathbb{F}$. For our purposes it is easier to restrict our attention to homogeneous polynomials. Note that the homogeneous equation associated to $x^2 + y^2 = a$ is the equation $X^2+Y^2 = aZ^2 \in \mathbb{F}[X, Y, Z]$; in terms of solutions to the original equation, the homogeneous one has the "added solutions" for which $Z = 0$, since any solution of $X^2 + Y^2 = aZ^2$ either has $Z = 0$ or can be rescaled to have $Z = 1$.

Going back to Problem 1, we found solutions to several degree two homogeneous polynomials in three variables. Thus we may wonder more generally: is it true that every homogeneous polynomial $q \in \mathbb{F}[x_0, x_1, x_2]$ of degree two admits a solution over $\mathbb{F}$?

Problem 2. Every homogeneous polynomial $q \in \mathbb{F}[X, Y, Z]$ of degree two has a solution in $\mathbb{F}$. Thus every homogeneous polynomial $p \in \mathbb{F}[x_0, \ldots, x_n]$ has a solution in $\mathbb{F}$ if $n \geq 2$.

Problem 3. Let V be a finite dimensional vector space over $\mathbb{F}$ and let $q\colon V \to \mathbb{F}$ be a quadratic form on V, that is q is a homogeneous polynomial of degree two in the coordinates of V.

(a) Show that there exists a non-negative integer $k \leq n/2$ and a basis $z_1, w_1, z_2, w_2, \ldots, z_k, w_k, y_{2k+1}, y_{2k+2}, \ldots, y_n$ of V^* such that q has one of the following forms:
- $z_1w_1 + \cdots + z_kw_k$;
- $z_1w_1 + \cdots + z_{k-1}w_{k-1} + (z_k^2 + z_kw_k + aw_k^2)$ with $x^2 + x + a$ irreducible over $\mathbb{F}$;
- $z_1w_1 + \cdots + z_kw_k + y_{2k+1}^2$.

Choose any basis $x_0, \ldots, x_n$ of V^* and write $q = \sum a_{ij}x_ix_j$ with $a_{ij} \in \mathbb{F}$.

(b) Suppose that $\mathrm{char}(\mathbb{F}) \neq 2$. Can you give an easy criterion in terms of the coefficients of q that determines which of the three forms above q may have? *Hint:* Use the symmetric bilinear form associated to q.

(c) *Challenge:* Do the same over a field of characteristic two.

Note that there are homogeneous polynomials of degree two in two variables over $\mathbb{F}$ admitting no root (can you show this?); in this sense the result of Problem 2 is sharp. This leads us to wonder what is the situation for higher degree polynomials.

Problem 4. Is there always a solution to a homogeneous polynomial $f \in \mathbb{F}[x_0, x_1, x_2]$ of degree three?

Misleading (?) hint: A smooth plane cubic is a curve of genus one. Remember from George's talk that genus one curves always have a point over a finite field.

We are now ready to state the Chevalley-Warning Theorem.

Theorem 5 (Chevalley-Warning)**.** *Let $f_1, \ldots, f_r \in \mathbb{F}[x_0, \ldots, x_n]$ be homogeneous polynomials of degree $d_1, \ldots, d_r$ respectively. If $d_1 + \cdots + d_r \leq n$, then there is a non-zero solution to $f_1(x) = \cdots = f_r(x) = 0$.*

The argument is very simple and I will go over it in the talk. Here are enough hints that should allow you to prove it yourself. Let N be the number of $a \in \mathbb{F}^{n+1}$ such that $f_1(a) = \cdots = f_r(a) = 0$; thus N counts the solution $(0, \ldots, 0)$ as well as every "rescaled" solution. If we show that $N \equiv 0 \pmod{\mathrm{char}(\mathbb{F})}$, then we deduce that there is a non-zero solution to $f_1(x) = \cdots = f_r(x) = 0$ since $(0, \ldots, 0)$ is a solution and $\mathrm{char}(\mathbb{F}) > 1$.
Step 1: Find a polynomial $\chi \in \mathbb{F}[t]$ of smallest degree such that

$$\chi(\alpha) = \begin{cases} 0 & \text{if } \alpha \neq 0 \\ 1 & \text{if } \alpha = 0. \end{cases}$$

Note that a polynomial of degree $|\mathbb{F}| - 1$ suffices; this determines χ uniquely. In particular we have

$$N \equiv \prod_{i=1}^{r} \Big(\sum_{a \in \mathbb{F}^{n+1}} \chi(f_i(a)) \Big) \pmod{\mathrm{char}(\mathbb{F})} \tag{1}$$

and to conclude it suffices to show that $\prod_i \big(\sum_a \chi(f_i(a)) \big) = 0$.
Step 2: For every non-negative integer j evaluate the sum

$$\sum_{a \in \mathbb{F}} a^j. \tag{2}$$

Step 3: Expand $\prod_i \chi(f_i(x))$ as a sum of monomials and deduce, from the condition that $d_1 + \cdots + d_r \leq n$, that every monomial must contain a variable raised to a small exponent.
Hint: "Small exponent" means that the exponent is smaller than $|\mathbb{F}| - 1$.
Step 4: Using (1) and (2), prove that $\mathrm{char}(\mathbb{F}) \mid N$ and conclude.

Remark. The argument sketched above shows that if in the statement of the Chevalley-Warning Theorem we drop the assumption that the polynomials $f_1, \ldots, f_r$ are homogeneous, then the number of solutions of the system $f_1(x) = \cdots = f_r(x) = 0$ is divisible by $\mathrm{char}(\mathbb{F})$. This is Warning's Theorem. Chevalley's Theorem is the statement that if $f_1, \ldots, f_r$ are polynomials without constant term and the above restrictions on the degrees, then there is a non-zero solution to the system $f_1(x) = \cdots = f_r(x) = 0$.

Depending on the amount of time left and the interests of the people attending the talk, further topics include Tsen's Theorem or applications of the Chevalley-Warning Theorem to the proof of Wedderburn's Theorem or of the Erdős-Ginzburg-Ziv Theorem.

Theorem 6 (Tsen's Theorem)**.** *Let k be an algebraically closed field and let $K \supset k$ be a finitely generated field of transcendence degree one. If $f_1, \ldots, f_r \in K[x_0, \ldots, x_r]$ are homogeneous polynomials of degrees $d_1, \ldots, d_r$ respectively such that $d_1 + \cdots + d_r \leq n$, then there is a non-zero solution of the system $f_1(x) = \cdots = f_r(x) = 0$.*

Theorem 7 (Wedderburn's Theorem)**.** *Let A be a finite integral domain. Then A is a field.*

Theorem 8 (Erdős-Ginzburg-Ziv Theorem)**.** *Let n be a positive integer and let $a_1, \ldots, a_{2n-1} \in \mathbb{Z}$. There exists a subset $I \subset \{1, \ldots, 2n-1\}$ such that*

- $|I| = n$, *and*
- $\sum_{i \in I} a_i \equiv 0 \pmod{n}$.