

Algebraic Number Theory Lecture Notes

Brendan Hassett

January 24, 2003

5 Chevalley-Warning Theorem

5.1 Review of finite fields

We review some basic facts about finite fields which may be found in any basic algebra book.

Let F be a finite field.

1. For some prime p , F contains $\mathbb{Z}/p\mathbb{Z}$ as a subfield.
2. We can consider F as a vector space over $\mathbb{Z}/p\mathbb{Z}$: It has elements e_1, \dots, e_n so that each $x \in F$ has a unique expression as a linear combination

$$x = a_1e_1 + \dots + a_n e_n, \quad a_j \in \mathbb{Z}/p\mathbb{Z},$$

where $n = \dim_{\mathbb{Z}/p\mathbb{Z}}(F)$. It follows that $|F| = p^n$.

3. F^* is a cyclic group of order $p^n - 1$, so we have a factorization

$$\Phi_{p,n}(x) := x^{p^n-1} - 1 = \prod_{\alpha \in F^*} (x - \alpha).$$

4. There is a unique finite field with p^n elements, up to isomorphism, denoted \mathbb{F}_{p^n} . It is characterized as the field generated over \mathbb{F}_p by the roots of the polynomial $\Phi_{p,n}(x)$.
5. Let m be relatively prime to p . Then there exists an n so that $\mathbb{F}_{p^n}^*$ contains a *primitive m th root of unity*, i.e., an element α of order precisely

m in $\mathbb{F}_{p^n}^*$. We can take n to be order of $p \pmod{m}$, i.e., the smallest n so that

$$p^n \equiv 1 \pmod{m}.$$

Example 5.1 Find the smallest n so that \mathbb{F}_{5^n} has a primitive 13th root of unity:

First, observe that $5^4 \equiv 1 \pmod{13}$ but $5^2 \not\equiv 1 \pmod{13}$, so $\mathbb{F}_{5^4} = \mathbb{F}_{625}$ has a primitive 13 root of unity.

5.2 Statement of the Theorem and Corollaries

Our motivation is to ‘automate’ the solution of congruences. For example, given integers A, B, N we shall see that the congruence

$$Ax^2 + By^2 \equiv N \pmod{p}$$

is guaranteed to have solutions for almost all primes p . This coincides with our experience in solving these problems: the primes dividing A, B , or N tend to be the only ones useful for showing integrals solutions do not exist.

Let \mathbb{F}_q denote the finite field with $q = p^N$ elements.

Theorem 5.2 (Chevalley-Warning) *Consider a set of polynomials in n variables over a finite field*

$$\{f_\alpha\} \subset \mathbb{F}_q[x_1, \dots, x_n]$$

so that

$$\sum_{\alpha} \deg(f_\alpha) < n.$$

Let

$$V = \{(a_1, \dots, a_n) \in \mathbb{F}_q^n : f_\alpha(a_1, \dots, a_n) = 0 \text{ for each } \alpha\}.$$

Then $\#V \equiv 0 \pmod{p}$.

Corollary 5.3 Retain the assumptions of Theorem 5.2 and suppose that the f_α are all homogeneous of positive degree, i.e.,

$$f_\alpha = \sum_{i_1 + \dots + i_n = \deg(f_\alpha)} c_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}, \quad c_{i_1, \dots, i_n} \in \mathbb{F}_q, \quad \deg(f_\alpha) > 0.$$

Then V contains a *nontrivial* common zero, i.e.,

$$V \supsetneq \{(0, 0, \dots, 0)\}.$$

Of course, V contains $(0, \dots, 0)$ so $\#V > 0$. But since $p \nmid \#V$, we must have at least $(p - 1)$ other zeros.

Example 5.4 Consider the equations

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 = 0 \quad x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3 = 0$$

over the finite field \mathbb{F}_{243} . These are guaranteed to have a common nonzero solution.

5.3 Proof of the Theorem

We follow J.P. Serre's *Course in Arithmetic*, ch. I, loosely.

Lemma 5.5 Fix $u \geq 0$ an integer. Then we have

$$S(x^u) := \sum_{x \in \mathbb{F}_q} x^u = \begin{cases} -1 & u \geq 1, (q-1) \mid u \\ 0 & \text{otherwise} \end{cases}.$$

We use the convention $x^0 = 1$ for all $x \in \mathbb{F}_q$, even $x = 0$.

proof of Lemma: The case $u = 0$ is clear, as $q = 0$ in \mathbb{F}_q . For positive u divisible by $(q - 1)$, we have $x^u = 1$ for $x \neq 0$, hence

$$\sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q^*} x^u = q - 1 = -1.$$

For u not divisible by $(q - 1)$, we can find $y \in \mathbb{F}_q^*$ so that $y^u \neq 1$, e.g., a generator of the cyclic group of units. Then we have

$$\sum_{x \in \mathbb{F}_q^*} x^u = \sum_{j=1}^{q-1} y^{ju} = y^u \sum_{j=0}^{q-2} y^{ju} = y^u \sum_{x \in \mathbb{F}_q^*} x^u,$$

where the last equation entails reordering the elements of \mathbb{F}_q^* . Since $y^u \neq 1$, the summation necessarily vanishes. \square

proof of Theorem Consider the polynomial

$$P(x_1, \dots, x_n) = \prod_{\alpha} (1 - f_{\alpha}^{q-1}),$$

which has degree $\leq (q-1) \sum \deg(f_\alpha) < (q-1)n$. This is a characteristic function for V , i.e.,

$$P(a_1, \dots, a_n) = \begin{cases} 1 & \text{if } (a_1, \dots, a_n) \in V \\ 0 & \text{if } (a_1, \dots, a_n) \notin V \end{cases},$$

which means

$$\#V \equiv \sum_{(x_1, \dots, x_n) \in \mathbb{F}_q^n} P(x_1, \dots, x_n) \pmod{p}.$$

Consider the linear operator

$$\begin{aligned} \tilde{S} : \mathbb{F}_q[x_1, \dots, x_n] &\rightarrow \mathbb{F}_q \\ P &\rightarrow \sum_{(x_1, \dots, x_n) \in \mathbb{F}_q^n} P(x_1, \dots, x_n). \end{aligned}$$

We claim this vanishes on polynomials of degree $< n(q-1)$. It suffices to check monomials $x_1^{u_1} \dots x_n^{u_n}$ with $u_1 + \dots + u_n < (q-1)n$. We know that $u_j < q-1$ for some j , so we have

$$\tilde{S}[x_1^{u_1} \dots x_n^{u_n}] = \sum_{x_j \in \mathbb{F}_q} x_j^{u_j} \cdot \sum_{x_1, \dots, \widehat{x_j}, \dots, x_n \in \mathbb{F}_q} x_1^{u_1} \dots \widehat{x_j^{u_j}} \dots x_n^{u_n}$$

which vanishes by the Lemma above. \square

5.4 Extensions

Can we ‘geometrize’ the assumptions of the Chevalley-Warning Theorem and its corollary? That is, can we replace the *algebraic* assumption on the degrees of the defining equations f_α with a *geometric* assumption on V .

Theorem 5.6 (Esnault’s Theorem) *Let V be a smooth projective variety over \mathbb{F}_q , so that the determinant of the tangent bundle of V*

$$\bigwedge^{\dim(V)} T_V$$

is positive (i.e., ample). Then V has a point over \mathbb{F}_q .

See ‘Varieties over a finite field with trivial Chow group of 0-cycles have a rational point’, H. Esnault, math.AG 0207022, to appear in *Inventiones mathematicae*