Finite fields. Jacobi sums. Counting solutions of equations mod p

November 8, 2012

1 Reading: [I-R] Chapter 7; Chapter 8 sections 1-4

2 Homework set due November 15

1. Page 87, Exercises 18 and 21-23
2. Page 105 Exercises 1-3

3 Further exercises not to be handed in:

1. Page 105 Exercise 8
2. Page 106 Exercise 15

4 Recall: constructions

Construct finite fields crudely as cyclotomic field extensions of prime fields. Now use the appropriate power of "Frobenius" to show that it is what you want. Prove that $\mathbf{F}_{p^d} = \mathbf{F}_p[\mu_{p^d-1}]$. Describe hierarchy of finite fields. Automorphism groups and fixed fields.

Theorem 1 *The polynomial*

$$X^{p^n} - X$$

is the product of all monic irreducible polynomials in $\mathbf{F}_p[X]$ *of degrees dividing* n.

Letting $N_d :=$ the number of monic irreducible polynomials in $\mathbf{F}_p[X]$ of degree d, then we have

$$p^n = \sum_{d \mid n} dN_d$$

and therefore, by Moebius inversion

$$N_n = \frac{1}{n} \sum_{d \mid n} \mu(n/d) p^d.$$

5 Introduction to Generalized Gauss Sums, and Jacobi Sums

5.1 Characters

Consider homomorphisms

$$\chi : \mathbf{F}_q^* \to \mathbf{C}^*.$$

Example: $\chi(a) = \left(\frac{a}{p}\right)$. Discuss the **character group** and duality.

5.2 Summation results

Consider summing $\chi(x)$ either for a fixed nontrivial character over all $x \in \mathbf{F}_q^*$; or for a fixed nontrivial x over all characters χ. Both summations vanish:

$$\sum_{\chi} \chi(x) = 0 \quad \text{(fixed } x \text{ nontrivial)}$$

$$\sum_{x} \chi(x) = 0 \quad \text{(fixed } \chi \text{ nontrivial)}.$$

5.3 Trigonometric sums

Back to $q = p$.

Define, for any character χ, the "Gauss Sum,"

$$g_a(\chi) := \sum_{x \in \mathbf{F}_p^*} \chi(a) e^{2\pi i x a/p}.$$

Put $g(\chi) := g_1(\chi)$.

Example: When $\chi(a) = \left(\frac{a}{p}\right)$, $g_a(\chi)$ is the *quadratic Gauss sum.*

Suppose that neither a nor χ are trivial. Then

$$\chi(a)g_a(\chi) = g_1(\chi) = g(\chi)$$

So,

$$g_a(\chi)\overline{g_a(\chi)} = |g(\chi)|^2,$$

and—as with quadratic Gauss sums– suppose that χ is nontrivial, and sum over all nontrivial a, the same computation as with quadatic Gauss sums gives:

Corollary 2 *If χ is nontrivial,*

$$|g(\chi)| = \sqrt{p}.$$

5.4 Jacobi Sums

If χ, ρ are two characters, define

$$J(\chi, \rho) := \sum_{a+b=1} \chi(a)\rho(b).$$

Theorem 3 *1. If χ is nontrivial, then*

$$J(\chi, \chi^{-1}) = -\chi(-1).$$

2. If χ, ρ and $\chi\rho$ are nontrivial. Then

$$J(\chi, \rho) = \frac{g(\chi)g(\rho)}{g(\chi\rho)}$$

Corollary 4 *If χ, ρ and $\chi\rho$ are nontrivial, then*

$$|J(\chi, \rho)| = \sqrt{p}.$$

5.5 How Jacobi sums are connected to counting numbers of solutions of equations modulo p; and how they are, at the same time, connected to Gauss sums

Let $P(x, y) \in \mathbf{F}_p[x, y]$ be a polynomial with coefficients in $\mathbf{F}_p$. Define

$$\mathbf{N}\langle P(x, y)\rangle := |\{(a, b) \in \mathbf{F}_p \times \mathbf{F}_p \mid P(a, b) = 0\}|.$$

So, for example, letting χ denote the Legendre symbol, $\chi(a) = \left(\frac{a}{p}\right)$,

- $$\mathbf{N}\langle x^2 - a)\rangle = 1 + \left(\frac{a}{p}\right) = 1 + \chi(a),$$
- $$\mathbf{N}\langle x^2 + y^2 - 1)\rangle = \sum_{a+b=1} \mathbf{N}\langle x^2 - a)\rangle \mathbf{N}\langle x^2 - b)\rangle = p + J(\chi, \chi) = p \pm 1,$$

  the sign depending on whether p is congruent to -1 or $+1$ mod p.
- (*)
$$\mathbf{N}\langle x^3 + y^3 - 1)\rangle = p - 2 + 2\mathrm{Re}\{J(\chi, \chi)\}.$$