Homogenous Forms over finite fields

November 29, 2012

1 Recall 'Hour-and-a-half' Exam December 4 2012

2 Course evaluations now open!

3 Specific reading:

Section 3 of Chapter 10; section 7 of Chapter 17.

4 Recall finite cyclic groups and their character groups

Let C be a finite cyclic group of order N (which we'll write multiplicatively). Recall the following basic facts:

- If $g\ inC$ is a generator of C, then

$$C \ = \ \{1, g, g^2, \ldots, g^{N-1}\}.$$

  The elements of C that are generators of C are the elements g^a with $1 \leq a \leq N-1$ and a relatively prime to N. There are $\Phi(N)$ distinct generators of C.

- The subgroups of C are determined by their orders, and these are precisely the positive divisors of N. The subgroup of order d where $d \mid N$ consists of the elements of C that are powers of $g^{N/d}$.

- If $h_m : C \to C$ is the homomorphism given by raising to the m-th power (i.e., $h_m(x) := x^m$) then h_m is an isomorphism if and only if $(m, N) = 1$. If m divides N then the mapping $h_m : C \to C$ is $m - to - one$.

- Suppose m divides N. Then if $y \in h_m(C)$—or equivalently: if there exists an $x \in C$ such that $x^m = y$—then

- there are precisely m such x's in C, and
- If $\chi : C \to \mathbf{C}^*$ is a *character*–i.e., a homomorphism–of order dividing m, we have

$$\chi(y) = \chi(x^m) = \chi(x)^m = \chi^m(x) = 1.$$

- Suppose m divides N. There are exactly m distinct characters of C of order dividing m.
- $$\sum_{\chi;\chi^m=1} \chi(y) = m \text{ or } 0$$

  depending on whether or not $y \in h_m(C)$.

Example: $C = \mathbf{F}_q^*$. .

5 Recall: Jacobi Sums

If $\chi, \rho : \mathbf{F}_q^* \to \mathbf{C}^*$ are two characters, define

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

Theorem 1 *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 2 *If χ, ρ and $\chi\rho$ are nontrivial, then*

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

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

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

So, for example, let $q = p$, and χ denote the Legendre symbol, $\chi(a) = \binom{a}{p}$.

$$\mathbf{N}\langle x^2 - a\rangle = 1 + \binom{a}{p} = 1 + \chi(a) = \sum_{\chi;\ \chi^2=1} \chi(a)$$

More generally, over $\mathbf{F}_q$, if $m \mid q-1$,

$$\mathbf{N}\langle x^m - a)\rangle \ = \sum_{\chi;\ \chi^m=1} \chi(a) =$$

Or, fixing a *generating character* ψ of order m; i.e., a character such that the powers ψ^k with $k = 0, 1, \ldots, m-1$, we have:

$$\mathbf{N}\langle x^m - a\rangle \ = \ \sum_{k=0}^{N-1} \psi^k(a).$$

Corollary 3

$$\mathbf{N}\langle x^m + y^m - 1\rangle \ = \ \sum_{k,\ j=0}^{N-1} \quad \sum_{a,\ b;\ \ a+b=1} \psi^k(a)\psi^j(b) \ = \ \sum_{k,\ j=0}^{m-1} J(\psi^k, \psi^j).$$

So, let's separate summands:

$$\sum_{k,\ j \text{ general}} \ = \ \sum_{k+j=0;\ k\neq 0} \ + \ \sum_{k\neq 0 \text{ general},\ j=0} \ + \ \sum_{j\neq 0 \text{ general},\ k=0} \ + t \sum_{j=0;\ k=0} \ + \ \sum_{k+j\neq 0;\ j\neq 0;\ k\neq 0} .$$

OK, these five summands of the RHS are evaluated, in order:

1. $$\sum_{k+j=0;\ k\neq 0} J(\psi^k, \psi^j) = \sum_{k\neq 0} J(\psi^k, \overline{\psi^k}) \ = \ -\sum_{k\neq 0} \psi^k(-1) \ = 1 - \mathbf{N}\langle x^m + 1\rangle.$$

2. $$\sum_{k\neq 0 \text{ general},\ j=0} J(\psi^k, \mathbf{1}) = \sum_{k\neq 0} \sum_{a} \psi^k(a) = 0.$$

3. $$\sum_{j\neq 0 \text{ general},\ k=0} J(\mathbf{1}, \psi^j) = \sum_{j\neq 0} \sum_{a} \psi^j(a) = 0.$$

4.

$$\sum_{j=0;\ k=0} J(\mathbf{1},\mathbf{1}) \ = q.$$

5.

$$\sum_{k+j\neq 0;\ j\neq 0;\ k\neq 0} J(\psi^k,\psi^j).$$

Note:

$$|\sum_{k+j\neq 0;\ j\neq 0;\ k\neq 0} J(\psi^k,\psi^j)| \quad \leq \quad (m-2)(m-1)\sqrt{q}.$$

Let's examine these terms. First introduce this curious terminology:

$$\mathbf{N}_{\text{projective}}\langle x^m+y^m+z^m\rangle := \quad \mathbf{N}\langle x^m+y^m-1\rangle \quad + \quad \mathbf{N}\langle x^m+1\rangle.$$

Note: the subscript in $\mathbf{N}_{\text{projective}}$ means that we will be counting points on the *projective curve* defined by the homogenous form $x^m+y^m+z^m$. Discuss this. The claim is the RHS counts exactly those points.

So, we have:

$$\mathbf{N}_{\text{projective}}\langle x^m+y^m+z^m\rangle \quad = \quad (1+q) \quad + \quad \sum_{k+j\neq 0;\ j\neq 0;\ k\neq 0} J(\psi^k,\psi^j).$$

Clearly, if we want, we could change that to:

$$\mathbf{N}_{\text{projective}}\langle x^m+y^m+z^m\rangle \quad = \quad (1+q) \quad + \quad \sum_{k+j\neq 0;\ j\neq 0;\ k\neq 0} Re\{J(\psi^k,\psi^j)\}.$$

where $Re(z)$ denotes the"real part' of the complex number z.

It is enlightening to think of the "$1+q$" in the formula above as the **dominant term** and the $\sum_{k+j\neq 0;\ j\neq 0;\ k\neq 0} J(\psi^k,\psi^j)$ as the **error term**, in view of the possibility of *keeping the homogeneous form* $x^m+y^m+z^m$ *fixed*, i.e., viewing it as, say, a form with coefficients in the ring $\mathbf{Z}$, and 'varying' the choice of q (subject to the restriction that $q\equiv 1 \bmod m$) and then noting, given what we have proved, that the dubbed "error term" is a constant times the square root of the dubbed "dominant term."