Homogenous Forms over finite fields

November 27, 2012

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

2 Specific reading:

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

3 Some readings for general culture:

1. - Read up on quadratic forms over fields in any of your favorite Algebra texts; e.g., M.Artin: Chapter 7 sections 1,2
   - Read Chapter XX of Hardy and Wright's *Introduction to the theory of numbers*
   - Read sections 5-9 (pages 319-325) of my article *Algebraic Numbers* in *The Princeton Companion to Mathematics* (Ed: T. Gowers) Princeton University Press, 2008. You can download the article from my web-page http://abel.math.harvard.edu/m̃azur/.
2. Read Sections 1-4 of Chapter IV of H. Davenport's *The Higher Arithmetic* (any edition) Cambridge University Press.

4 Five useful exercises but don't hand in

(Note: Exercises 4, 5 are dispersed below)

Exercise 1 *Show that* $13x^2 + 36xy + 25y^2$ *and* $58x^2 + 82xy + 29y^2$ *are each equivalent to* $x^2 + y^2$.

Exercise 2 *Show that* $ax^2 + \pm bxy + cy^2$ *are not properly equivalent to one another if* $-a < b < a < c$ *and* $b \neq 0$.

Exercise 3 *How many properly inequivalent forms are there with $|\Delta| = 5$? Prove your assertion.*

5 Recall: Chevalley's Theorem about zeroes of polynomial equations over finite fields; the theorem of Chevalley-Warning

Let F be a finite field of cardinality $q = p^\nu$ and $P(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ a polynomial (in the n variables) of degree $d < n$ with "no constant term." That is, $P(0, 0, \ldots, 0) = 0$. The theorem of Chevalley says that there is at least one "nontrivial" zero of P rational over the field F.

Corollary 1 *A quadratic form over a finite field in three or more variables has a nontrivial zero.*

Note that this is not true for quadratic forms in *two* variables, but we have all the tools to understand this case!

6 Chevalley-Warning

Let $N_P :=$ the number of solutions of $P(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ and put:

$$\bar{N}_P := N_P \text{ modulo } p.$$

Theorem 2 *Suppose that the degree of P is srictly less than the number of variables n. $N_P \equiv 0$ modulo p; i.e., $\bar{N}_P = 0$.*

Proof: We start with the observation that:

$$\bar{N}_P = \sum_{(a_1, a_2, \ldots, a_n)} (1 - P(a_1, a_2, \ldots, a_n)^{q-1}).$$

Now, express $(1 - P(X_1, X_2, \ldots, X_n)^{q-1})$ as a sum of monomials in the X_i. Note that each such monomial, $\prod_i X_i^{d_i}$, is of total degree $< d(q-1)$. Since $d < n$ this means that each monomial, $\prod_i X_i^{d_i}$, has at least one of its exponents d_j that is **less than** $q - 1$. For any monomial, with one of its exponents d_j less than $q - 1$, we have:

Lemma 1

$$\sum_{(a_1, a_2, \ldots, a_n)} \prod_i a_i^{d_i} \ = \ 0.$$

This concludes the proof!

7 Representation of integers by forms

This is a basic problem. One has the general **(Waring's Problem):** Representation of positive integers as sums of "4 squares, 9 cubes, 19 biquadrates, 'and so on'. More specifically, for example: given a quadratic form what integers does it represents—i.e., as values? E.g., Is there a simple description of the set of integers can be expressed as a sum of three square integers? In how many ways can such an integer be so represented? How often can primes be represented as a sum of n squares?

Such questions show up as useful pieces of knowledge in many branches of mathematics. We've been dealing with examples of this.

8 Sums of n squares

Theorem 3 *Any squarefree (positive) number is a sum of two squares if and only if it has no prime factor congruent to* -1 *mod* 4.

Theorem 4 (Lagrange) *Any positive integer is expressible as a sum of four squares.*

Formulate this in quaternion language.

If:

$$x = x_1 + i \cdot x_2 + j \cdot x_3 + k \cdot x_4$$

and

$$\bar{x} = x_1 - i \cdot x_2 - j \cdot x_3 - k \cdot x_4,$$

then put:

$$N(x) := x \cdot \bar{x} = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Lemma 2 *1.*

$$\overline{\alpha \cdot \beta} = \overline{\beta} \cdot \overline{\alpha}.$$

2.

$$N(x \cdot y) = N(x) \cdot N(y).$$

Proof: Just compute to see that (1) holds; which implies (2). So, the set $\mathcal{N}$ of numbers representable as a sum of four squares is closed under multiplication.

Corollary 5 *To show Lagrange's theorem suffices to show that all odd primes are in* $\mathcal{N}$. *(Or even just all primes congruent to* -1 *mod* 4.*)*

From now on, suppose that our primes p are odd.

Lemma 3 *For any prime p, a multiple of p is in $\mathcal{N}$.*

Proof: Show that $x_1^2 + x_2^2 + 1^2 + 0^2 \equiv 0 \mod p$ has a solution for any (odd) prime p. One can do this by (a version of) Dirichlet's box principle since there are $(p+1)/2$ quadratic residues (counting 0) and $(p+1)/2$ congruence classes of the form $-1 - x^2$ (again counting 0) so there has to be an ovewrlap of these two subsets of $\mathbf{F}_p$.

Or use Chevalley's Theorem.

Lemma 4 *Let $n > 1$ be an odd number. Suppose that some multiple of n is in $\mathcal{N}$, i.e., is representable as a sum of four squares. Then there is an integer m with $0 < m < n$ such that $n \cdot m \in \mathcal{N}$.*

Proof: Our hypothesis gives

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod n,$$

so choose representatives $y_i \equiv x_i \mod n$ for $n/2 < y_i < n/2$ giving

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \mod n,$$

where the left hand side is strictly less then n^2.

More generally, the above holds for even numbers n, taking $n/2 < y_i \leq n/2$ with *one exceptional case:* when all the y_i are equal to $n/2$, giving

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = n^2.$$

Call this case the "worst scenario."

8.1 Inductive Step:

Let p be a prime, and $m_0 \cdot p > 0$ be the smallest multiple in $\mathcal{N}$. We want to show that $m_0 = 1$, so suppose $m_0 > 1$ and we'll find a contradiction. We have $m_0 < p$ with

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = pm_0.$$

Lemma 5 (Switching the roles of p and m_0)

1. *Either we are in the "worst case scenario" (see above) or else there are integers y_1, y_2, y_3, y_4 ("least residues" mod m_0) such that $y_i \equiv x_i$ modulo m_0 ($i = 1, 2, 3, 4$) we have:*

   $$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1$$

   with $m_1 < m_0$.

2. *We are not in the "worst case scenario."*

—bf Proof: The proof of (1) follows from the discussion above, while the proof of (2) goes as follows. Suppose the above set-up, but that we're in the worst case scenario. Then

$$x_i = y_i + u_i m_0 = m_0/2 + u_i m_0$$

for integers u_i. Squaring, gives:

$$x_i^2 = m_0^2/4 + u_i m_0^2 + u_i^2 m_0^2$$

, or:

$$pm_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod m_0^2$$

so m_0 divides p, an impossibility unless $m_0 = 1$ since $m_0 < P$ and p is a prime.

Now, reverting to quaternion language: define

$$z := x \cdot y = z_1 + i \cdot z_2 + j \cdot z_3 + k \cdot z_4$$

so $N(z) = m_0^2 m_1 p$.

Exercise 4 *Check that z_1, z_2, z_3, z_4 are each divisible by m_0.*

Putting

$$t_\iota := \frac{z_\iota}{m_0}$$

for $\iota = 1, 2, 3, 4$ and considering the quaternion

$$t = t_1 + i \cdot t_2 + j \cdot t_3 + k \cdot t_4,$$

we have

$$N(t) = t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 \cdot p$$

with $m_1 < m_0$, which completes our inductive protocol (and/or gives our contradiction).

9 Sums of three squares

Exercise 5 *Show that any number congruent to 7 mod 8 is not a sum of three squares. Show that if a number $n \equiv 0$ mod 4 is sum of three squares*

$$n = a^2 + b^2 + c^2,$$

then a, b, c are all even. Show that any number congruent to 28 mod 32 is also not a sum of three squares. Show, more generally that any number congruent to $7 \cdot 4^e$ mod 2^{e+3} (for $e \geq 0$) is not a sum of three squares[1].

[1] By the way, the above condition is necessary and sufficient; but this is a deep theorem due to the efforts of Legendre, Dirichlet, Gauss.

Theorem 6 *If a number n is not of the above form, i.e., congruent to $7 \cdot 4^e$ mod 2^{e+3}, then n is a sum of three squares.*

10 Sums of 24 squares

Discuss

$$N(p) \approx \frac{16}{691}(p^{11}+1).$$