More binary quadratic forms; Homogenous Forms over finite fields

November 19, 2012

1 Reading:

1. Read section 2 of Chapter 10.
2. Read section 7 of Chapter 17.

2 Already in last handout; recall: First Part of Homework set due Tuesday Nov 27

1. Show that given any pair of relatively prime integers (a, b) there is a matrix

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $A \in \mathrm{SL}_2(\mathbf{Z})$.

2. Prove that the discriminant of a binary quadratic form is invariant under orientation-equivalence.
3. Find a negative discriminant such that there is more than one reduced binary quadratic form of that discriminant.
4. (Not to be handed in or graded, but think about this:)
   (a) How might you show that your reduced binary quadratic forms (of the previous exercise) are *not* orientation-equivalent?
   (b) Do the exercise in that handout.

3 Second Part of Homework set due Tuesday Nov 27

1. (a) Factor $X^9 - X \in \mathbf{F}_3[X]$ into a product of irreducible polynomials (the factorization should be over the field $\mathbf{F}_3$).

(b) Consider the polynomial in ten variables,

$$P(X_1, X_2, \ldots, X_{10}) := \sum_{i=1}^{10} X_i^5 \in \mathbf{F}_7[X_1, X_2, \ldots, X_{10}].$$

How many solutions does the equation $P(X_1, X_2, \ldots, X_{10}) = 2$ have over the field $\mathbf{F}_7$?

2. Page 86 Exercises 10,11.

4 Recall: positive definite forms

Definition 1 *A* **reduced positive definite form** *is a form (a, b, c) such that*

$$-a < b \leq a \leq c$$

and such that if $a = c$ then $b \geq 0$.

Theorem 1 *Any positive definite form is equivalent to a reduced positive definite form*

Theorem 2 * *There is a unique reduced positive definite form in every equivalence class of positive definite forms*

5 Computations for small values

Let $\Delta := -D$ for some (small) positive number D, and let (a, b, c) be a reduced positive definite form of discriminant Δ, with $a, c > 0$; and let's compute. We have:

$$(\mathbf{1}) \quad b^2 = 4ac - D,$$

and since

$$-a < b \leq a \leq c,$$

we also have:

$$(\mathbf{2}) \quad 0 \leq b^2 \leq ac.$$

Putting **(1)** and **(2)** together, we get:

$$(\mathbf{3}) \quad 3ac \leq D.$$

In particular, if $\Delta = -4, -7, -8$ there is only one reduced positive definite quadratic form. Therefore, (at least) in these three cases a positive number n is properly represented by the unique

(positive definite) binary quadratic form of discriminant Δ if and only if Δ is a quadratic residue mod $4n$. With -7, then we are dealing with the positive definite form

$$X^2 + XY + 2Y^2.$$

Noting that -7 is a square modulo 4, we get that and odd positive number n is representable as $n = x^2 + xy + 2y^2$ if and only if -7 is a square modulo n; e.g., for odd primes $n = p$ this is determined by

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right).$$

That is: yes if $p \equiv 1, 2, 4 \bmod 7$ and no otherwise.

6 *Back to finite fields:* 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. We'll build up to this.

Discuss the distinction between P as a polynomial, and P as a function $\bar{P} : F \times F \times \ldots \times F$ to F. Note that $P \mapsto \bar{P}$ is *not* one:one! I.e., $\bar{P}$ *does not* determine P. Basic example. Now note that this "basic example" clears the way for:

Lemma 1 *If you restrict to P's that are of degree strictly less than q in each variable x_i, then $\bar{P}$ does determine P. Equivalently, if—for such a polynomial— $\bar{P}$ is identically zero, then so is P.*

Proof: Induction on n.

Let $P(x, x_1, x_2, \ldots x_{n-1})$ be a polynomial in $F[x, x_1, x_2, \ldots, x_{n-1}]$ that is *identically zero* as a function on F^n, and is such that every monomial that occurs in P is of degree $< q$ in each of the variables, $x, x_1, x_2, \ldots, x_{n-1}$.

So write

$$P(x, x_1, x_2, \ldots x_{n-1}) = x^d p_d(x_1, x_2, \ldots x_{n-1}) + x^{d-1} p_{d-1}(x_1, x_2, \ldots x_{n-1}) + \ldots + p_0(x_1, x_2, \ldots x_{n-1}).$$

Now just note that by induction we can find specialized values $a_1, a_2, \ldots, a_{n-1} \in F$ where some of the coefficients $p_j(a_1, a_2, \ldots a_{n-1})$ don't vanish. But then we are faced with a nontrivial polynomial $P(x, a_1, a_2, \ldots a_{n-1}) \in F[x]$ of degree $< q$ having every element of F (and there are q of them!) as root. This is absurd. QED

Discuss *reduction of polynomials*. Define the equivalence relation: $P \sim Q$ if $\bar{P} = \bar{Q}$. **Proof of Chevalley's Theorem:** Let P be a counterexample. So

$$1 - P^{q-1} \sim \prod_{j=1}^{n}(1 - x_j^{q-1})$$

since the polynomials on the RHS and LHS both, as functions on $F \times F \times \ldots \times F$ take $(0, 0, \ldots, 0)$ to 1 and everything else to 0.

Now reduce $1 - P^{q-1}$ to a "reduced" polynomial $H \sim 1 - P^{q-1}$. Note that

$$\text{degree}(H) \leq d(q-1).$$

We have that

$$H - \prod_{j=1}^{n}(1 - x_j^{q-1}) \ \sim \ 0$$

and therefore—since the LHS of the above equation is *reduced*, by Lemma 1

$$H - \prod_{j=1}^{n}(1 - x_j^{q-1}) \ = \ 0$$

or

$$H \ = \ \prod_{j=1}^{n}(1 - x_j^{q-1}).$$

In particular,

$$\text{degree}(H) = n(q-1).$$

Contradiction since $d < n$; so there is *no* counterexample P. QED.

Corollary 3 *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!

7 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 4 *$N_P \equiv 0$ 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 2

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

This concludes the proof!

8 Homogeneous forms; Quadratic forms

- Discuss in general.
- Bilinear forms on vector spaces.
- Discuss issues over $\mathbf{Z}$.
- Quadratic forms over $\mathbf{R}, \mathbf{F}_q, \mathbf{Q}$ and $\mathbf{Z}$
- Conics over $\mathbf{Q}$
- Representation of numbers as a sum of two squares.:
- Intro to **(Waring's Problem):** Representation of positive integers as sums of "4 squares, 9 cubes, 19 biquadrates, 'and so on'.