# Finite fields and more Quadratic residues

November 1, 2012

## 1 Hour-and-a-half Exam: this coming Tuesday, November 6.

Fair game will be topics covered in the handouts and in the homework sets between the first hour exam and now; [I-R] Chapter 5, and sections 1-3 of Chapter 6; Continued Fractions.

## 2 Reading:

Make sure that you have read sections 1-3 of Chapter 6. Read all of Chapter 7.

## 3 Suggested Reading (after the exam!):

Read Sections 1-4 of the chapter on Quadratic Forms of H. Davenport's *The Higher Arithmetic* (any edition) Cambridge University Press.

## 4 Brief "recall" of field extensions, degree, and constructions

## 5 Cyclotomic Polynomials; cyclotomic fields in general

Discuss separability issues. Recall the theorem of Gauss that the cyclotomic polynomial $f_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ is irreducible over $\mathbf{Q}$. Discuss automorphism groups.

## 6 Finite Fields

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 $\mathbf{F}_{p^d} = \mathbf{F}_p[\mu_{p^d-1}]$.

**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

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

## 7 Proof of Quadratic Reciprocity via Gauss sums

Let $p$, $q$ be odd (and different) primes. Let $g = g_1$ be the Gauss sum relative to the prime $p$ (as above, so it is living in $\mathbf{Z}[\zeta_p]$). But watch out: we will be working in $\mathbf{Z}[\zeta_p]$ *modulo* $q \cdot \mathbf{Z}[\zeta_p]$ *in a moment. This is the ring*

$$\mathbf{Z}[\zeta_p]/q\mathbf{Z}[\zeta_p] = \mathbf{Z}/q\mathbf{Z}[X]/(f_p(X)) = \mathbf{F}_q[X]/(f_p(X))$$

*where* $f_p(X)$ *is the cyclotomic polynomial as in section 5 above. Note that in this ring we have the Frobenius endomorphism* $z \mapsto z^q$ *and this will be playing a role. But let's go on for a second, in the ring* $\mathbf{Z}[\zeta_p]$*:*

*Form* $g^{q-1} = (p^*)^{(q-1)/2}$ *noting that it is an ordinary integer in* $\mathbf{Z}[\zeta_p]$*. Now pass to its image in* $\mathbf{F}_q[X]/(f_p(X))$ *and note that it is nothing more nor less than* $\binom{p^*}{q} \in \mathbf{F}_q \subset \mathbf{F}_q[X]/(f_p(X))$*.*

*Now multiply by* $g$ *to get:*

$$g^q = \binom{p^*}{q} g,$$

*We evaluate* $g^q$ *as the image under the Frobenius endomorphism of* $g$*, i.e.,*

$$g^q = (\sum_{k=0}^{p-1} \binom{k}{p} \zeta_p^k)^q = \sum_{k=0}^{p-1} \binom{k}{p} \zeta_p^{qk} \equiv g_q = \binom{q}{p} g,$$

*so*

$$\left(\frac{q}{p}\right) g \;=\; \left(\frac{p^*}{q}\right) g.$$

*We're not yet done because we want to get rid of the factor $g$, but no problem: multiply by $g$ to get:*

$$\left(\frac{q}{p}\right) p^* = \left(\frac{q}{p}\right) g^2 \;=\; \left(\frac{p^*}{q}\right) g^2 = \left(\frac{p^*}{q}\right) p^*,$$

*and since $p^*$ is a unit mod $q$, we're done.*

*Note: we could have done all this work in a finite field extension of $\mathbf{F}_q$ that contains the values of the Gauss sum $g$. This is the content of Section 3 of Chapter 7 of* [**I-R**].

## 8 Introduction to binary quadratic forms

***Definition 1*** *A* **binary quadratic form** *over a commutative ring $R$ is a homogeneous form*

$$F(x, y) = ax^2 + bxy + cy^2 \in R[x, y],$$

*of degree two in two variables with coefficients in $R$.*

*We will be considering–this hour—binary quadratic forms for $R = \mathbf{Z}$, i.e., over the integers, and—for short—we'll omit saying that they are over $\mathbf{Z}$ and just call them "binary quadratic forms." We denote an $F$ as above with coefficients $a, b, c$ as above, by the symbol $(a, b, c)$ (for short).*

***Definition 2*** *Two binary quadratic forms $(a, b, c)$ and $(a', b', c')$ will be called* **orientation-equivalent** *if there is a matrix*

$$T := \begin{pmatrix} u & v \\ w & t \end{pmatrix}$$

*in $\mathrm{SL}_2(\mathbf{Z})$ such that if we make the linear change of variables:*

$$\begin{pmatrix} u & v \\ w & t \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$$

*and define the binary quadratic form $G(x, y) := F(x', y')$ we have that $G(x, y) = a'x^2 + b'xy + c'y^2$.*

## 9 Formulas:

$a' = au^2 + buw + cw^2$

...

**Exercise not to be handed in:** *Work out the formulas for $b', c'$.*

*We denote orientation-equivalence by a "tilde" as in:*

$$(a, b, c) \;\sim\; (a', b', c').$$

## 10 Invariant(s)

*The discriminant; the set of properly represented integers.*

***Definition 3*** $\Delta(a,b,c) := b^2 - 4ac$.

***Definition 4*** $\mathcal{N}(a,b,c) \subset \mathbf{Z}$ *is the set of integers of the form* $axu^2 + buv + cv^2$ *for* $u, v$ *relatively prime integers. An integer in* $\mathcal{N}(a,b,c)$ *will be referred to as an integer that is* **properly represented by** $(a,b,c)$.

*Compute* $\Delta$ *for the fundamental quadratic forms.*

**Completing the square:**

*Making the transformation (now over* $\mathbf{Q}$ *rather than over* $\mathbf{Z}$*)*

$$x \mapsto x - \frac{b}{2a}y; \qquad y \mapsto y$$

*we have the quadratic form (over* $\mathbf{Q}$*):*

$$ax^2 + \frac{-\Delta}{4a}y^2$$

*which is definite if* $\Delta < 0$ *and indefinite if* $\Delta > 0$. *A definite form is* **positive** *or* **negative** *definite according to the sign of "a."*

***Theorem 2*** *If* $(a,b,c) \sim (a',b',c')$ *then*

$$\Delta(a,b,c) = \Delta(a',b',c')$$

*and*

$$\mathcal{N}(a,b,c) = \mathcal{N}(a',b',c').$$

***Theorem 3*** *If* $a' \in \mathcal{N}(a,b,c)$ *then there are integers* $b', c'$ *such that* $(a,b,c) \sim (a',b',c')$. *Equivalently, any integer represented by a quadratic form* $(a,b,c)$ *can be taken as the first coefficient of a form equivalent to* $(a,b,c)$.

*Relate the signs of elements in* $\mathcal{N}(a,b,c)$ *to the question of whether or not the binary quadratic form is positive definite, negative definite, or indefinite.*

## 11 Congruence conditions

***Theorem 4*** *If $n \in \mathcal{N}(a, b, c)$ then $\Delta$ is a quadratic residue modulo $4|n|$. Conversely, if an integer $\Delta$ is a quadratic residue modulo $4|n|$ then there is a binary quadratic form $(a, b, c)$ with $\Delta(a, b, c) = \Delta$, with respect to which $n$ is properly representable.*

*Moral: If $\Delta$ is such that there is only one equivalence class of binary quadratic forms with discriminant $\Delta$, the above gives a complete solution to the problem of representing numbers by that quadratic form.*

## 12 Examples:

1. *$\Delta = -4$. $x^2 + y^2$ is the only positive definite form (up to equivalence); so $n > 0$ is properly represented by it if and only if $-1$ is a square mod $n$. We know this... but let's go through the proof.*
2. *$\Delta = -7$. $x^2 + xy + 2y^2$ is the only positive definite form (up to equivalence); supposing that $n > 0$ is odd, we see that it is properly represented by $x^2 + xy + 2y^2$ if and only if $-7$ is a square mod $4n$. This happens if and only if $n$ has no prime factor congruent to $3, 5,$ or $6$ mod $7$ and is not divisible by $49$.*
3. *$\Delta = 8$ (an indefinite form). $x^2 - 2y^2$ is the unique quadratic form of that discriminant: $n$ must have no prime factor congruent to $\pm 1$ mod $8$ and must not be divisible by $4$.*

## 13 Positive definite forms

*We now restrict to these.*

***Definition 5*** *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 5*** *Any positive definite form is equivalent to a reduced positive definite form*

***Theorem 6*** * *There is a unique reduced positive definite form in every equivalence class of positive definite forms*