Math 152 Notes

Lucas Garron

November 5, 2009

20091105

On webpage:
Lecture notes from Tuesday
Statement about Midterm
Next (short homework)

A binary quadratic form is $f(x,y) = ax^2 + bxy + cy^2$ $(a,b,c \in \mathbb{Z})$
Studied by Gauss, who introduced the notion of class numbers $h(d)$ where d is some discriminant.
$d = b^2 - 4ac$ is called the discriminant of f. You can change the quadratic form by a linear change of variables.
$x = mx' + ny'$
$y = tx' + uy'$
This change of variables multiplies d by $(mu - nt)^2$
Best kind of variable change: $(mu - nt) = 1 \Rightarrow d$ discriminant unchanged (unimodular change of variables).
$f(x,y) = a'(x')^2 + b'x'y' + c'(y')^2$, where $(b')^2 - 4a'c' = (mu - nt)^2(b^2 - 4ac)$
Proof:
$ax^2 + bxy + cy^2 = (x,y)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$
$(x,y)\begin{pmatrix} ax + \frac{b}{2}y \\ \frac{b}{2}x + cy \end{pmatrix} = ax^2 + \frac{b}{2}y + \frac{b}{2}xy + cy^2$
$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} m & n \\ t & u \end{pmatrix}\begin{pmatrix} x' \\ t \end{pmatrix}$
$\xi = M\xi'$
$(x', y')\begin{pmatrix} m & t \\ n & u \end{pmatrix} = (x,y)$
$\xi = \begin{pmatrix} x \\ y \end{pmatrix}$
$\begin{pmatrix} m & n \\ t & u \end{pmatrix} = M$
$\xi' = \begin{pmatrix} x' \\ y' \end{pmatrix}$
$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = Q$ symmetric.

$(\begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} = Q'?)$
$f(x,y) = \xi^t Q \xi$
$= (M\xi')^t Q (M\xi')$
$(\xi')^t M^t Q M \xi'$ (call $M^tQM = Q'$))
$det(Q) = \frac{1}{4}(b^2 - 4ac) = -\frac{d}{4}$

Two binary quadratic forms f and f' are considered equivalent if they are related by a unimodular change of variables.
$f(x,y) = f'(x',y')$
$x = mx' + ny', y = tx' + uy'$
$m, n, t, u \in \mathbb{Z}, mu - nt = 1$
In this case they have the same discriminant $d = b^2 - 4ac = (b')^2 - 4a'c'$
Same Discriminant $\not\Rightarrow$ equivalent. Example:
$2x^2 + 2xy + 3y^2$ and $x^2 + 5y^2$ doth have $d = -20$, but not equivalent.
The number of BQFs with discriminant d is called a class number $h(d)$
$h(-20) = 2$. This is related to the failure of unique factorization in the ring $\mathbb{Z}[\sqrt{-5}]$

Read 3.4 and 3.5

Representations by sum of squares.
Let $r(m) = \#(x,y) \in \mathbb{Z}^2 | x^2 + y^2 = n$
($r(0) = 1$, IGNORE)
$r(1) = 4$ ($(\pm 1)^2 + 0^2$, $0^2 + (\pm 1)^2$)
$r(2) = 4$
$r(3) = 0$
$r(4) = 4$
$r(5) = 8$
If $x^2 + y^2 = n$ is a solution, then associate $x + iy \in R = \mathbb{Z}[i]$ in the Gaussian integers.
$n = N(x+iy)$; $z = x + iy$ have four different solutions corresponding to $z, iz, -z, -iz\{\epsilon Z | \epsilon \in R^\times\}$
($R^\times$ units $\pm 1, \pm i$)
Special case $r(p)$, p odd prime. In this case, claim:
$r(p) = 8$ if $p \equiv 1 \bmod 4$
$r(p) = 0$ if $p \equiv 3 \bmod 4$

Claim: If $p \equiv 1 \bmod 4$, there are two Gaussian primes dividing p. (π, π' are associates, $\pi' = \epsilon\pi, \epsilon$ a unit). Think of these as representing the same primes.
$5 = (1 + 2i)(1 - 2i)$ (distinct Gaussian primes dividing 5)
Proposition: If $p \equiv 1m4$ prime in $\mathbb{Z}$ ($\Rightarrow$ by Fermat, $p = a^2 + b^2$). $p = \pi\overline{\pi} = (a + bi)(a - bi)$ where π is a Gaussion prime. $\pi, \overline{\pi}$ are not associative but any Gaussian prime dividing p is (an associate of) π or π'
Remark: If $\kappa \in R$, $N(\kappa)$ prime in $\mathbb{Z} \Rightarrow \kappa$ is prime in $R = \mathbb{Z}[i]$
(However, this is not $\Leftrightarrow$ since 3 is prime in R but $N(3) = 9q$ is not prime in $\mathbb{Z}$.)
Proof of remark: $If \kappa = \kappa_1\kappa_2 \Rightarrow N(\kappa) = N(\kappa_1)N(\kappa_2) \Rightarrow N(\kappa_1)$ or $N(\kappa_2) = 1 \Rightarrow \kappa_1$ or κ_2 is a unit.
Proof of proposition:
If κ is a prime dividing p ($\kappa | p$), then $\kappa | \pi\overline{\pi}$ (Note $\pi, \overline{\pi}$ are prime by remark, $N(\pi) = a^2 + b^2 = p$)
So $\kappa | \pi$ or $\kappa | \pi'$

κ, π prime $\Rightarrow \kappa$ is an associate of π or π'

Define $\chi(n) =$
$0(n$ even$)$
$1(n \equiv 1 \bmod 4)$
$-1(n \equiv 3 \bmod 4)$
i.e. $\xi(n) = \frac{(-1}{2})$ ("Kronecker Symbol")

Theorem: $r(n) = 4\sum_{d|n} \chi(d)$

Proof: $\frac{1}{4}\left(\sum_{\text{nonzero Gaussian integers}} \frac{1}{N(d)^2} = Z(R)\right)$ (s some complex number $re(s) > 1$ will guarantee convergence.)
(1/4 accounts for $\alpha, i\alpha, -\alpha, -i\alpha$ having same norm.)
$Z(R) = \sum_{\text{ideals I of R}} \frac{1}{NI^s}$ (Dedekind zeta function of R)
Every ideal is of the form (α) = all multiples of α because R is a principal ideal domain.
$(\alpha) = (\beta) \Rightarrow \alpha = \epsilon\beta$ $(\epsilon \in R^\times)$. Passing to ideals removes need to divide by 4.
$\xi(R) = \sum_{\text{ideals I of } \mathbb{Z}} \frac{1}{NI^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}$
Every ideas has a unique factorization into ideals. This means... ξ first. Ideals of $\mathbb{Z}$ are (n) with $n > 0$ and each has a unique factorization into primes.
$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - \frac{1}{p^s})^{-1}$
Because RHS $= \prod_p (1 + \frac{1}{p^s} + \frac{1}{p^2 s} + ...)$ (multiplying out gives each $\frac{1}{n^2}$ exactly once.)
$\frac{1}{1-x} = 1 + 1x + x^2 + ...$
$\xi(s) = \sum n^{-s} = \prod_p (1 - p^{-s})^{-1}$

$\frac{1}{4}\sum_{n=1}^{\infty} r(n)n^{-s} = Z(s) = \prod_{\text{prime Ideals P of R}} (1 - \frac{1}{NP^s})^{-1}$ ($\frac{1}{4}r(n) = \#$ of ideals with norm $N(I) = n$)
Prime ideals of R:
One ideal $(1+i)$ with $N(P) = 2$
Two ideals $(a+bi), (a-bi)$ with $NP = p$, $p \equiv 1 \bmod 4$ with $NP = p^2$, $p \equiv 3 \bmod 4$
$(N(P) = N(\alpha)$ with $P = (\alpha))$
One ideal (p)
$2, 3, 1+2i, 1-2i, 7$
$\prod_{\text{prime Ideals P of R}} (1 - \frac{1}{NP^s})^{-1}$
$= (1 - \frac{1}{2^s})^{-1} \left(\prod_{p \equiv 1 \bmod 4} (1 - \frac{1}{p^s})^{-1}(1 - \frac{1}{p^s})^{-1}\right) \left(\prod_{p \equiv 3 \bmod 4} (1 - \frac{1}{p^s})^{-1}\right)$

$$\prod_{\chi(p)=0}(1-\frac{1}{p^s})^{-1}(1-\frac{\chi(p)}{p^s})^{-1}\prod_{\chi(p)=1}(1-\frac{1}{p^s})^{-1}(1-\frac{\chi(p)}{p^s})^{-1}\prod_{\chi(p)=-1}(1-\frac{1}{p^s})^{-1}(1-\frac{\chi(p)}{p^s})^{-1}$$