Math 152 Notes

Lucas Garron

November 3, 2009

20091103

Midterm: Nov. 12
Sums of Two Squares
Special Case of binary quadratic form
BQF: If $a, b, c \in \mathbb{Z}$
$ax^2 + bxy + cy^2$ is a binary quadratic form
Their theory is closely related to the field $\mathbb{Q}(\sqrt{D})$ $(D = b^2 - 4ac)$ (could be $\pm$), case $D > 0$ easier.
Case $ax^2 + xbxy + cy^2 = 0$ $(D = -4)$
$\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(i)$ $(i = \sqrt{-1})$
Inside $\mathbb{Q}(i)$ is the ring of Gaussian integers, $R = \mathbb{Z}[i]$
$\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$
$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$
(In field theory, if F is a field, R a ring, K is a bigger field $\supset F, R$, $x \in K$, $F(x) = \{$smallest field containing $F, x\}$, $R[x]$ smallest ring containing R, x
$\mathbb{Q}(i) = \mathbb{Q}[i]$, $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$)

Review from Thursday: Theory of the norm.
F any field, $D \in F^\times \neq 0$, not a square in F.
D is a square in $K = F(\sqrt{D})$. This is constructed the same way as $\mathbb{C}$ given $\mathbb{R}$
$F(\sqrt{D}) = F[\sqrt{D}] = \{a + d\sqrt{D} | a, b \in F\}$
"Obvious" ring operations. It is a field, it is a 2-D vector space over F.
$\frac{1}{a+b\sqrt{D}} = \frac{a-b\sqrt{D}}{a^2-b^2D}$, hence a field (denom $\neq 0$ if a, b not both 0 because D not a square root in F)
$x^2 - Dy^2 = (x + y\sqrt{D})(x + y\sqrt{D}) = N(x + y\sqrt{D})$ (LHS binary Q.F. in a, b)

<u>Ex. 1</u> $(D = -1)$
$x^2 + y^2 = (x + iy)(x - iy) = N(x + iy)$ ($N : K \to F$ norm map)
$N(zw) = N(z)N(w)$ (*)
$\tau(x + iy) = x - iy$ (complex conj.): $\tau(zw) = \tau(z)\tau(w)$ (also addition)
General case: $\tau : K \to K$
$\tau(x + y\sqrt{D}) = x - y\sqrt{D}$
$\tau(zw) = \tau(z)\tau)w$ (mult both sides by zw gives (*))

Ex. 1 shows that binary quadratic forms $ax^2 + bxy + cy^2$ with $b = 0$ are sometimes norms from quadratic fields.

But $b = 0$ is unimportant, and in general, the theory of binary quadratic forms (developed by Gauss) is the same as the theory of quadratic fields $\mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}, D$ nonsquare

<u>Ex. 2</u>: $x^2 + xy + y^2$a BQY with $b \neq 0$
$\rho = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$
$\rho^2 = e^{\frac{4\pi i}{3}} = -\frac{1}{2} - \frac{\sqrt{-3}}{2}$
$\sqrt{-3} = \rho - \rho^2$
$\rho^2 + \rho + 1 = 0$
$\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$; compute norm of $x + y\rho$
$\tau : K \to K$, $\tau(x + y\sqrt{-3}y) = x - \sqrt{-3}y$
$\tau(\rho) = \rho^2$
$N(x + y\rho) = (x + y\rho)(x + y\rho^2) = x^2 + (\rho + \rho^2)xy + y\rho^2 = x^2 - xy + y^2$
$N(x - y\rho) = x^2 + xy + y^2$, so any BQR with $D = b^2 - 4ac$ nonsquare is related to a norm.
Caveat: $ax^2 + bxy + cy^2$

Questions: Which integers can be expressed as a sum of two squares?
First obseravation: $(x^2 + y^2)(z^2 + w^2) = t^2 + u^2$ for suitable t, u
$t = (xz - yw), u = (xw - yz)$
Underlying reason: $N(z_1)N(z_2) = N(z_1z_2)$ $(z_1 = x + iy,\ z_2 = z + iw)$
$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (z_1^2 + z_2^2 + z_3^2 + z_4^2)$ for suitable z_1, z_2, z_3, z_4 (similar explanation using quaternions)
So if u, v are sums of two (or four) squares, so is uv.
Thm: p prime is a sum of 2 squares $\Leftrightarrow p = 2 = 1^1 + 1^2$ or $p \equiv 1$ mod 4
Proof: If $p \equiv 3$ mod 4, p is not a sum of two squares since $u^2 = 0$ or 1, $u^2 + b^2 = 0, 1, 2$
Fermat: If $p \equiv 1$ mod 4, then $pisasumof2squares$
The Gaussian integers are a ring where unique factorization result is true.
Lemma: If $a, b \in R = \mathbb{Z}[i], b \neq 0 \Rightarrow a = bq + r, |r| < |b|$
Consider $R \cdot b =$ square lattice with vertices at $(x + iy)b,\ x, y \in \mathbb{Z}$