9:40 p.m. January 1, 2011

Notes on DA, §§267–292: ternary quadratic forms

♦ **Reduction of positive definite binary forms.** As a preliminary, I explain binary reduction, which Gauss applies to arbitrary binary forms, both definite and indefinite. The definite ones are treated in several sections starting with §171, the other in several sections starting with §183. I'll deal here only with definite forms.

For Gauss an integral quadratic form is of the form $ax^2 + 2bxy + cy^2$ with a, b, c all integers, but I'll allow b to be a half-integer.

I'll explain binary form reduction in my own terminology. Let

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$
$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

By applying S and T repeatedly we can get a reduced form with $0 < a \le c$, $-a \le b \le a$.

(1) If $a > c$ we apply S:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} c & -b/2 \\ -b/2 & a \end{bmatrix}.$$

getting $cx^2 - bxy + ay^2$. Note that $|b|$ does not change in this.

(2) If $|b| > a$ we apply T^{-n}:

$$\begin{bmatrix} 1 & 0 \\ -n & 1 \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & -na + b/2 \\ -na + b/2 & n^2a - nb + c \end{bmatrix}.$$

The new b is $b - 2na$. so if we pick n such that $|-na + b/2| \le a/2$ we get a new form with $-a \le b \le a$. For this we require:

$$\begin{aligned} -a/2 \le -na + b/2 &\le a/2 \\ 0 \le -2na + (a+b) &\le 2a \\ n \le (a+b)/(2a) &\le n+1 \\ -n \le -(a+b)/(2a) + 1 &\le -n+1 \end{aligned}$$

so

$$n = \begin{cases} \lfloor (a+b)/(2a) \rfloor & \text{if } a+b \ge 0 \\ -\lfloor 1 - (a+b)/(2a) \rfloor & \text{if } a+b < 0. \end{cases}$$

This step does not change a. So at each step, the previous simplification is not erased, and eventually we must get a reduced form.

If f is reduced, then

$$4a^2 \le 4ac = D + b^2 \le D + a^2, \quad 3a^2 \le D, \quad a \le \sqrt{D/3}$$

so a is bounded. But then b is bounded—in fact we must have $D \le D + b^2 \le D + a^2$ must be a multiple of $4a$—and $c = (D + b^2)/4a$ is determined. So there are only a finite number of reduced positive definite forms with a given discriminant D.

♦ **Binary forms and the upper half plane.** How do positive definite binary forms relate to Möbius transforms on the upper half-plane? The complex number z corresponds to the lattice spanned by 1 and z, with quadratic form

$$(m + nz)(m + \overline{z}) = m^2 + 2mn\,\mathrm{RE}(z) + n^2|z|^2\,.$$

These are all the real positive definite forms $ax^2 + bxy + cy^2$ with $a = 1$. If we start with an arbitrary form $ax^2 + bxy + cy^2$ we can simply scale it to $x^2 + (b/a)xy + (c/a)y^2$, and then map it to $p + qi$ with

$$\begin{aligned} 2p &= (b/a) \\ p^2 + q^2 &= (c/a) \\ q &= \sqrt{(c/a) - (b/2a)^2} \\ &= \frac{\sqrt{4ac - b^2}}{2a}\,, \end{aligned}$$

which is OK since the determinant $ac - b^2/4$ is positive. So the reduction process agrees with the fact that $|z| \ge 1$, $|\mathrm{RE}(z)| \le 1/2$ is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathcal{H}$.

♦ **Genera.** Two forms are said to be in the same genus if the are equivalent modulo all p^n. If p does not divide the discriminant, then the discriminant alone determines the equivalence modulo p, then by Hensel's Lemma modulo all p^n. So we just have to figure out what happens for p dividing D. And in fact probably modulo p^k if p^k is the p-factor of D, presumably by the singular form of Hensel's Lemma?

Cassel tells us how to decide: if p is odd all forms over $\mathbb{Z}_p$ are sums of $p^n Q_i$ where Q_i one of the two canonical forms over $\mathbb{Z}/p$—a sum of hyperbolic planes plus zilch, x^2, ax^2 with $a/p = -1$, or the norm of a quadratic extension. (This by Minkowski.)

If $p = 2$, we get a sum of 2^k times x^2, $3x^2$, $5x^2$, $7x^2$, xy, or $x^2 + xy + y^2$.

♦ **Outline of Gauss.**

§§262–270: Introduction to ternary forms

§§271–277: Reduction

§§278–292: Representations of numbers and binary forms by ternary forms

♦ **266.** Basic idea. As for binary forms, his forms correspond to integral matrices.

♦ **267.** Terminology and adjoint forms (in my own terminology). If a linear transformation T has matrix

$$M = \begin{bmatrix} m_{1,1} & m_{1,2} & m_{1,3} \\ m_{2,1} & m_{2,2} & m_{2,3} \\ m_{3,1} & m_{3,2} & m_{3,3} \end{bmatrix}$$

with respect to basis e_i then its adjoint is the matrix of the transformation $\wedge^2 T$ with respect to the (properly oriented) dual basis $e_2 \wedge e_3$, $e_3 \wedge e_1$, $e_1 \wedge e_2$

$$\begin{bmatrix} m_{2,2}m_{3,3} - m_{3,2}m_{2,3} & \dots m_{3,2}m_{1,3} - m_{1,2}m_{3,3} \\ m_{1,2}m_{2,3} - m_{2,2}m_{1,3} & \end{bmatrix} .$$

Why this choice of basis? Given V of dimension n and a form ω in $\wedge^n V$, $\wedge^k V$ and $\wedge^{n-k}$ are dual:

$$u \wedge v = \langle u, v \rangle \omega \, .$$

We also have

$$(\wedge^i T u) \wedge (\wedge^j T v) = \wedge^{i+j}(u \wedge v)$$

and the fact that M times the transposed adjoint of M is equal to $\det(M) \cdot I$ is just a transliteration of $\wedge^k T \wedge^{n-k} T = \wedge^n T = \det(T) \cdot I$. The product in this case represents the equation

$$T e_i \wedge T e_j^{\wedge} = \det(T)(e_i \wedge e_j^{\wedge}) \, .$$

(I. e./ a matrix represents all kinds of things, here a bilinear pairing). *Transposed* adjoint because $T e_i$ is rendered as a row vector in a matrix multiplication.

What Gauss says is that the form

$$f = \begin{bmatrix} a & b'' & b' \\ b'' & a' & b \\ b' & b & a'' \end{bmatrix}$$

has as adjoint the form

$$F = \begin{bmatrix} b^2 - a'a'' & a''b'' - bb' & a'b' - bb'' \\ a''b'' - bb' & b'b' - aa'' & ab - b'b'' \\ a'b' - bb'' & ab - b'b'' & b''b'' - aa' \end{bmatrix} = \begin{bmatrix} A & B'' & B' \\ B'' & A' & B \\ B' & B & A'' \end{bmatrix} .$$

Gauss' matrix gives a symmetric bilinear form $B(x,y)$ with $Q(x) = B(x,x)$. This is an isomorphism from $\mathbb{Z}^3$ to $\mathbb{Z}^3$, presumably the matrix of the form. It takes u to the linear function $T(u)$ defined by

$$\langle T(u), v\rangle = B(u,v),\ \langle T(e_i), e_j\rangle = B(e_i,e_j)\,,$$

so $T(e_i)$ has its expression in the dual basis f_i equal to the column of the matrix. It induces another bilinear form on $\wedge^2\mathbb{Z}^3$. Is it Gauss'?

$$\begin{aligned}
T(e_2\wedge e_3) &= (b''f_1 + a'f_2 + bf_3)\wedge(b'f_1 + bf_2 + a''f_3)\\
&= (f_2\wedge f_3)(a'a'' - bb) + (f_3\wedge f_1)(bb' - a''b'') + (f_1\wedge f_2)(b''b - a'b')\\
T(e_3\wedge e_1) &= (af_1 + b''f_2 + b'f_3)\wedge(b'f_1 + bf_2 + a''f_3)\\
&= (f_2\wedge f_3)(bb' - b''a'') + (f_3\wedge f_1)(aa'' - b'b') + (f_1\wedge f_2)(b'b'' - ab)\\
T(e_1\wedge e_2) &= (af_1 + b''f_2 + b'f_3)\wedge(b''f_1 + a'f_2 + bf_3)\\
&= (f_2\wedge f_3)(b''b - b'a') + (f_3\wedge f_1)(b'b'' - ab) + (f_1\wedge f_2)(aa' - b''b'')
\end{aligned}$$

with matrix

$$-\begin{bmatrix} A & B'' & B'\\ B'' & A' & B\\ B' & B & A''\end{bmatrix} = -F\,.$$

The adjoint of the adjoint is fD, where D is $\det f$.

His D is the negative determinant.

♦ **268.** Substitute

$$\begin{bmatrix} x\\ x'\\ x''\end{bmatrix} = \begin{bmatrix} \alpha & \beta & \gamma\\ \alpha' & \beta' & \gamma'\\ \alpha'' & \beta'' & \gamma''\end{bmatrix}\begin{bmatrix} y\\ y'\\ y''\end{bmatrix}\,.$$

We get a new form

$${}^txQx = {}^ty{}^tSQSy$$

There is no distinction between equivalence and proper equivalence, since $-I$ is in the orthogonal group.

Effect of transforms on adjoints. He calls transforms transpositions.

♦ **269.** Equivalent if transforms of each other. Two forms are equivalent if and only if their adjoints are equivalent.

♦ **270.** Composite of transforms by matrix multiplication.

♦ **271.** Leading to Theorem that there are only a finite number of ternary classes with a given determinant (which will be proved in §276).

Criteria for definite forms, positive ones, negative ones.

♦ **272.** Still leading to reduction. The basic idea is to transform f to g by some S, with g simpler in some sense. Look at adjoints F, G, transformed by adjoint of S (§269).

I. First we apply the reduction process for binary forms to

$$\begin{bmatrix} a & b'' \\ b'' & a' \end{bmatrix}.$$

by taking

$$S = \begin{bmatrix} \alpha & \beta & 0 \\ \alpha' & \beta' & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

This gives us $|a| \leq (4/3)\sqrt[3]{D}$.

II. Next take S of the form

$$S = \begin{bmatrix} 1 & 0 & 0 \\ 0' & \beta' & \gamma' \\ 0 & \beta'' & \gamma'' \end{bmatrix}.$$

and apply the binary reduction to

$$\begin{bmatrix} A'' & B \\ B & A' \end{bmatrix}.$$

This gives us $|A''| \leq (4/3)\sqrt[3]{D^2}$.

III. If neither of these reductions can be applied, ... we must therefore have $|a| \leq (4/3)\sqrt[3]{D}$ and $|A''| \leq (4/3)\sqrt[3]{D^2}$.

IV. Apply these alternately.

Any ternary form of determinant D may be reduced to an equivalent form with the property that $|a| \leq (4/3)\sqrt[3]{D}$ and $|A''| \leq (4/3)\sqrt[3]{D^2}$.

♦ **273.** An example:

$$f = \begin{bmatrix} 19 & 1 & 28 \\ 121 & 15 & \\ 28 & 15 & 50 \end{bmatrix}.$$

Another example:

$$f = \begin{bmatrix} 10 & 4 & 0 \\ 426 & 7 & \\ 0 & 7 & 2 \end{bmatrix}.$$

♦ **274.** After these, a further reduction can be made by applying

$$S = \begin{bmatrix} 1 & \beta & \gamma \\ 0 & 1 & \gamma' \\ 0 & 0 & 1 \end{bmatrix} .$$

♦ **275.** The previous examples continued.

♦ **276.** **Theorem.** *The number of classes into which all ternary forms of a given determinant are distributed is always finite.*

♦ **277.**

♦ **278.** We now have the following problems:

I. To find all representations of a given number by a given ternary form.

II. To find all representations of a given binary form by a given ternary form.

III. To judge whether or not two given ternary forms are equivalent, and if they are to find all transformations taking one to the other.

IV. To find whether or not a given ternary form implies another, and if it does to find all transformations of the first into the second.

In this book he will not be complete, but reduce I to II, reduce II to III, give some simple examples, and not discuss IV at all.

♦ **279.** **Lemma.** *Given any three integers a, a', a'' (not all 0) how to find six others B, B', B'', C, C', C'' such that*

$$B'C'' - B''C' = a, \quad B''C = BC'' = a', \quad BC' - B'C = a"" \ ?$$

♦ **291.** To find all representations of $M > 0$ by $x^2 + y^2 + z^2 = M$, or $-M$ by $-x^2 - y^2 - z^2 = f$.

subsecI First find all binary forms of determinant $-M$ represented by $X^2 + Y^2 + Z^2$. When $M \equiv 0$, 4, or 7 modulo 8 there are none, and M cannot be expressed as a sum of three mutually prime squares.