Ideal Composition in Quadratic Fields:

from Bhargava to Gauss

Duncan Buell

Department of Computer Science and Engineering

University of South Carolina

1 Quadratic Forms

- Everything is an integer (except $\sqrt{\Delta}$).
- *Binary quadratic form* $f(x,y) = ax^2 + bxy + cy^2 = (a,b,c)$ of *discriminant* $\Delta = b^2 - 4ac$.
- *Primitive* if $\gcd(a,b,c) = 1$; we usually consider only primitive forms. (For imprimitive forms we can usually just factor out the common term, do the theory on the resulting primitive form, and then put the factor back in.)
- Forms $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ are *equivalent* if there exists $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ such that we have a matrix equivalence $M^T \cdot \begin{pmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{pmatrix} \cdot M = \begin{pmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{pmatrix}$
- Alternatively, $M : f_1(x_1, y_1) \to f_2(x_2, y_2)$ under

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

with explicit change of variables

$$\begin{aligned} a_2 &= a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 \\ b_2 &= b_1(\alpha\delta + \beta\gamma) + 2(a_1\alpha\beta + c_1\gamma\delta) \\ c_2 &= a_1\beta^2 + b_1\beta\delta + c_1\delta^2 \end{aligned} \tag{1}$$

- $f = (a, b, c)$ *represents* an integer m if there exist x, y such that $m = ax^2 + bxy + cy^2$.
- *Primitive representation* if $\gcd(x, y) = 1$)

Theorem 1.1. *Primitive representation is equivalent to equivalence.*

Because if $a_2 = a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2$ with $\gcd(\alpha, \gamma) = 1$, then we can find β, δ with $\alpha\delta - \beta\gamma = 1$ and we have the matrix from the modular group for the equivalence (1).

Theorem 1.2. *The classes of forms of a fixed discriminant Δ form the finite abelian group that is the ideal class group of the quadratic order of discriminant Δ in the quadratic field $\mathbb{Q}(\Delta)$.*

Theorem 1.3. *A primitive form can represent some integer relatively prime to any chosen integer.*

(In deep obscurity mode, this is the Cebotarev Density Theorem, but it can be proven directly in this simple case.)

• Special cases for the generators of the modular group:

$$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} : (a, b, c) \to (a, \quad b + 2a\beta, \quad a\beta^2 + b\beta + c)$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : (a, b, c) \to (c, \quad -b, \quad a)$$

2 Quadratic Fields

- Let $\Delta \in \mathbb{Z}$, $\Delta \equiv 0, 1 \pmod 4$ be the discriminant of a quadratic number field $K = \mathbb{Q}(\sqrt{\Delta})$.
- We have the ring of integers $\mathcal{O}$ in K, ideals in $\mathcal{O}$, and the class group of ideals modulo principal ideals.
- Essentially, ideals are $\mathbb{Z}$-modules

$$\left[a, \frac{-b + \sqrt{\Delta}}{2}\right]$$

with some conditions added, for $a, b \in \mathbb{Z}$.

- "Essentially", meaning:
  - ◇ narrow versus wide ideals
  - ◇ invertible ideals
  - ◇ nonfundamental discriminants, orders not the principal order
  - ◇ etc.

3 Forms and Ideals

• The form $f = (a, b, c)$ of discriminant Δ corresponds to the $\mathbb{Z}$-module $\left[a, \frac{-b+\sqrt{\Delta}}{2}\right]$.

• For positive discriminant, classes of forms correspond to the *narrow* classes of ideals modulo principal ideals of *positive* norm (an extra 2 to 1 mapping).

• For nonfundamental discriminants of orders, classes of primitive forms of that disc are crisply and simply defined, but modules and ideals require some extra conditions.

• I have always preferred forms, in part because having the third coefficient c explicitly presented is useful, especially in what now follows.

4 Composition of forms/Multiplication of ideals

- In essence,

$$(a_1, b_1, c_1) \circ (a_2, b_2, c_2) \sim (fudge \cdot a_1 a_2, *, *)$$

and

$$\left[a_1, \frac{-b_1 + \sqrt{\Delta}}{2}\right] \cdot \left[a_2, \frac{-b_2 + \sqrt{\Delta}}{2}\right] \sim \left[fudge \cdot a_1 a_2, \frac{* + \sqrt{\Delta}}{2}\right]$$

- The real substance of a composition algorithm is to be able precisely to determine the value of $fudge$.

5 Dirichlet's United Forms

• Assume $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ of the same discriminant Δ.

• If

$$\begin{aligned} f_1 = (a_1, \quad b_1, \quad c_1) &\sim (a_1, \quad b_1 + 2a_1\beta_1, \quad C_1) = (a_1, \quad B, \quad C_1) \\ f_2 = (a_2, \quad b_2, \quad c_2) &\sim (a_2, \quad b_2 + 2a_2\beta_2, \quad C_2) = (a_2, \quad B, \quad C_2) \end{aligned} \tag{2}$$

then necessarily we have

$$f_1 \sim (a_1, \quad B, \quad a_2C)$$

$$f_2 \sim (a_2, \quad B, \quad a_1C)$$

and the composition $f_1 \circ f_2 \sim (a_1a_2, \quad B, \quad C)$.

• Dirichlet defined two forms to be *united* if $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$, and a solution to (2) can be shown to be guaranteed if the forms are united.

• This is the simplest of the composition algorithms. For existential purposes, since we can always cite Theorem 1.3 and argue that we can find $f_3 \sim f_2$ with $\gcd(a_3, a_1) = 1$, we can in theory always do composition using Dirichlet united forms.

• This is unsatisfactory because this isn't an algorithmically explicit composition.

6 Arndt's Algorithm

• Dirichlet united forms is not "algorithmic" in that we have to specify that we find some form with a relatively prime lead coefficient.

• **Arndt's method:** Assume $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ of discriminant Δ. Let $\beta = \frac{b_1+b_2}{2}$ and $n = \gcd(a_1, a_2, \beta)$, and solve $a_1 t + a_2 u + \beta v = n$ for t, u, v.

Then

$$\begin{aligned} B &\equiv b_1 \pmod{2a_1/n} \\ B &\equiv b_2 \pmod{2a_2/n} \\ \frac{\beta B}{n} &\equiv \frac{b_1 b_2 + \Delta}{2n} \pmod{2a_1 a_2/n^2} \end{aligned} \tag{3}$$

has the simultaneous solution

$$B = \frac{a_1 b_2 t + a_2 b_1 u + v(b_1 b_2 + \Delta)/2}{n}$$

and the composition is

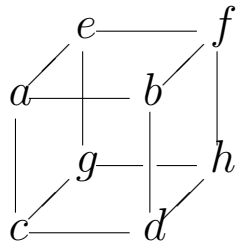
$$f_1 \circ f_2 \sim (a_1 a_2/n^2, \quad B, \quad *).$$

United forms, fudged to allow for $n \neq 1$: find the "most nearly united" B possible.

Hold that thought!

7 Bhargava's cubes

- Bhargava defines a cube



and three pairs of matrices derived from the three orientations of faces of the cube:

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix} \qquad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix} \tag{4}$$

$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix} \qquad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}$$

- From these we get forms

$$Q_i(x, y) = -Det(M_i x - N_i y)$$

which explicitly are

$$\begin{aligned} Q_1 &= x^2(-ad+bc)+xy(ah-bg-cf+de)+y^2(-eh+fg) \\ Q_2 &= x^2(-ag+ce)+xy(ah+bg-cf-de)+y^2(-bh+df) \\ Q_3 &= x^2(-af+be)+xy(ah-bg+cf-de)+y^2(-ch+dg) \end{aligned} \tag{5}$$

all of discriminant

$$\Delta = a^2h^2+b^2g^2+c^2f^2+d^2e^2+$$

$$2(abgh+cdef+acfh+bdeg+adeh+bcfg)+4(adfg\ \ +bceh)$$

• We let $SL_2(\mathbb{Z})\oplus SL_2(\mathbb{Z})\oplus SL_2(\mathbb{Z})$ act on these cubes: in the i-th factor, we have

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} : (M_i, N_i) \to (rM_i+sN_i, tM_i+uN_i)$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : (M_i, N_i) \to (M_i+N_i, N_i) \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : (M_i, N_i) \to (-N_i, M_i)$$

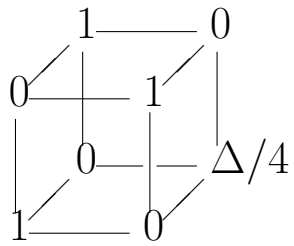
Bhargava (continued)

• The action of $SL_2(\mathbb{Z}) \oplus SL_2(\mathbb{Z}) \oplus SL_2(\mathbb{Z})$ is the action of equivalence on the derived forms.

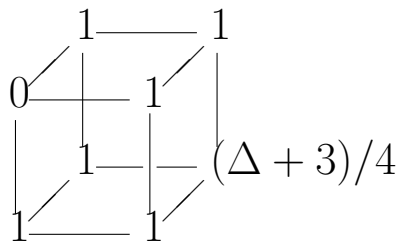
Theorem 7.1. *We have composition in the group of classes of forms as follows.*

$$Q_1 \circ Q_2 \circ Q_3 \sim Id.$$

Bhargava's identity is

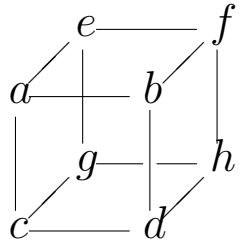


or



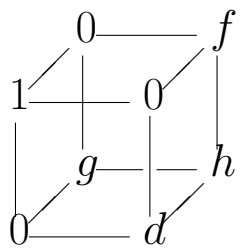
Theorem 7.2. *Bhargava reduces to Dirichlet united forms.*

Proof. Bhargava defines projectively the cube



so we may assume that $\gcd(a, b, c, d, e, f, g, h) = 1$. Use this fact and invoke the extended Euclidean algorithm. That is, apply modular group transformations to get $a = 1$. Apply further transformations with the left face to get a 0 for the "b" location; apply transformations with the top face to get a 0 for for the "c" location; and apply transformations with the front face to get a 0 for for the "e" location.

This yields



Ba Da Bing! The three forms are now

$$Q_1 = -dx^2 + hxy + fgy^2$$

$$Q_2 = -gx^2 + hxy + dfy^2$$

$$Q_3 = -fx^2 + hxy + dgy^2$$

□

• Note that Gauss/Dirichlet/Arndt/Matthews/Buell would have written the third form as the equivalent form $Q_3 = dgx^2 - hxy - fy^2$; it is typical of doing the computations in Bhargava fashion that we get the product written this way.

Bhargava (continued)

• In theory, then, Bhargava subsumes Gauss.

• But given two forms, how do we find a cube on which both live, and then which among the compounded forms in the class shows up as the third form from the cube?

• That is, how do we make this algorithmic instead of existential?

• In fact, Arndt's method works just fine. There are no doubt other methods, but with eight variables and three sets of quadratic equations, showing how, where, and why the old method works is a good start.

• Remember:

$$Q_1 = x^2(-ad + bc) + xy(ah - bg - cf + de) + y^2(-eh + fg)$$

$$Q_2 = x^2(-ag + ce) + xy(ah + bg - cf - de) + y^2(-bh + df)$$

$$Q_3 = x^2(-af + be) + xy(ah - bg + cf - de) + y^2(-ch + dg)$$

and we are asking for ways to solve this if we are given explicit coefficients for Q_1 and Q_2.

Theorem 7.3 (Unproven?)**.** *A given octuple a, b, c, d, e, f, g, h uniquely determines a set of three forms (forms, not classes) and conversely.*

• If I could prove this, things would be a little simpler.

8 Bhargava continued–The old algorithm still works

• Necessary Conditions for the Algorithm

To compound two forms (A_1, B_1, C_1) and (A_2, B_2, C_2) by putting them on a cube:

- Let $\beta = \frac{B_1+B_2}{2}$ and set $n = \gcd(A_1, A_2, \beta)$.
- Start by choosing relatively prime values of a_0 and c_0.
- Now solve

$$\begin{aligned} -a_0 d + c_0 b &= A_1/n = A_{10} \\ -a_0 g + c_0 e &= A_2/n = A_{20} \\ a_0 h - c_0 f &= \beta/n = \beta_0 \end{aligned} \tag{6}$$

Bhargava continued (continued)

• We get general solutions

$$\begin{aligned} a &= n \cdot a_0 \\ c &= n \cdot c_0 \\ b &= b_0 + a_0\lambda \\ d &= d_0 + c_0\lambda \\ e &= e_0 + a_0\mu \\ g &= g_0 + c_0\mu \\ f &= f_0 + a_0\nu \\ h &= h_0 + c_0\nu \end{aligned} \tag{7}$$

• We now have three equations to solve, one for B_1, one for C_1, and one for C_2. (We get B_2 by combining the formula for B_1 with the formula for β.)

Bhargava continued (continued)

• First,

$$\begin{aligned} B_1 &= a(h_0 + c_0\nu) - (b_0 + a_0\lambda)(g_0 + c_0\mu) - c(f_0 + a_0\nu) + (d_0 + c_0\lambda)(e_0 + a_0\mu) \\ &= ah_0 - b_0g_0 - cf_0 + d_0e_0 + \lambda(-a_0g_0 + c_0e_0) + \mu(a_0d_0 - c_0b_0) \\ &= ah_0 - b_0g_0 - cf_0 + d_0e_0 + \lambda A_{20} - \mu A_{10} \end{aligned}$$

We have

$$B_1 - (ah_0 - b_0g_0 - cf_0 + d_0e_0) = \lambda A_{20} - \mu A_{10} \tag{8}$$

or, written another way,

$$\frac{B_1 - B_2}{2} + b_0g_0 - d_0e_0 = \lambda A_{20} - \mu A_{10} \tag{9}$$

• **We assume that we can solve (9);** assuming this, then the solutions are

$$\begin{aligned} \lambda &= \lambda_0 + A_{10}\eta \\ \mu &= \mu_0 + A_{20}\eta \end{aligned} \tag{10}$$

for yet another parameter η.

Bhargava continued (continued)

- Next,

$$C_1 = -(e_0 + a_0\mu)(h_0 + c_0\nu) + (f_0 + a_0\nu)(g_0 + c_0\mu)$$

which reduces to

$$C_1 + e_0h_0 - f_0g_0 = -\beta_0\mu - A_{20}\nu$$

and then to

$$C_1 + e_0h_0 - f_0g_0 + \beta_0\mu_0 = A_{20}[-\beta_0\eta - \nu] \tag{11}$$

- Finally,

$$C_2 = -(b_0 + a_0\lambda)(h_0 + c_0\nu) + (d_0 + c_0\lambda)(f_0 + a_0\nu)$$

which reduces to

$$C_2 + b_0h_0 - d_0f_0 + \beta_0\lambda_0 = A_{10}[-\beta_0\eta - \nu] \tag{12}$$

The Algorithm

Leaving aside a fair number of issues about greatest common divisors and the resulting ability to do the extended Euclidean algorithm, the process is:

1. Compute n, and then choose a_0 and c_0 relatively prime.

2. Solve equations (6) to get the general forms of the variables, as in (7). This we are guaranteed to be possible by our choice of a_0 and c_0.

3. Solve (9) to get λ and μ as in (10). This is not guaranteed. However, in the development of the composition algorithm, especially that of united forms, there is a role to be played by $\gcd(A_1, A_2)$, so I am not overly concerned here. It is also possible here that one would need to use a good choice of a_0 and c_0 and not an arbitrary choice.

4. Solve (11) and (12) for ν and η. This is really one equation

$$\begin{aligned}\beta_0\eta + \nu &= -\left(\frac{1}{A_{20}}\right)(C_1 + e_0h_0 - f_0g_0 + \beta_0\mu_0)\\ &= -\left(\frac{1}{A_{10}}\right)(C_2 + b_0h_0 - d_0f_0 + \beta_0\lambda_0)\end{aligned}$$

9 A Specific Version of an Algorithm

- To compound two forms (A_1, B_1, C_1) and (A_2, B_2, C_2) by putting them on a cube:
- Let $\beta = \frac{B_1+B_2}{2}$ and set $n = \gcd(A_1, A_2, \beta)$.
- Start by choosing relatively prime values of a_0 and c_0. Specifically, choose

$$\begin{aligned} a_0 &= 1 \\ c_0 &= 0 \end{aligned} \tag{13}$$

- Now solve

$$\begin{aligned} -a_0 d + c_0 b &= A_1/n = A_{10} \\ -a_0 g + c_0 e &= A_2/n = A_{20} \\ a_0 h - c_0 f &= \beta/n = \beta_0 \end{aligned} \tag{14}$$

• We get general solutions

$$\begin{aligned} a = n \cdot a_0 &= n \\ c = n \cdot c_0 &= 0 \\ b = b_0 + a_0\lambda &= 0 + \lambda \\ d = d_0 + c_0\lambda &= -A_{10} + 0\lambda \\ e = e_0 + a_0\mu &= 0 + \mu \\ g = g_0 + c_0\mu &= -A_{20} + 0\mu \\ f = f_0 + a_0\nu &= 0 + \nu \\ h = h_0 + c_0\nu &= \beta_0 + 0\nu \end{aligned} \tag{15}$$

• We now have three equations to solve, one for B_1, one for C_1, and one for C_2. (We get B_2 by combining the formula for B_1 with the formula for β.)

• First,

$$\begin{aligned} B_1 &= a(h_0 + c_0\nu) - (b_0 + a_0\lambda)(g_0 + c_0\mu) - c(f_0 + a_0\nu) + (d_0 + c_0\lambda)(e_0 + a_0\mu) \\ &= ah_0 - b_0g_0 - cf_0 + d_0e_0 + \lambda(-a_0g_0 + c_0e_0) + \mu(a_0d_0 - c_0b_0) \\ &= ah_0 - b_0g_0 - cf_0 + d_0e_0 + \lambda A_{20} - \mu A_{10} = n\beta_0 + \lambda A_{20} - \mu A_{10} \end{aligned}$$

• That is,

$$B_1 - \beta = \lambda A_{20} - \mu A_{10} \tag{16}$$

or, written another way,

$$\frac{B_1 - B_2}{2} = \lambda A_{20} - \mu A_{10} \tag{17}$$

• **We know that we can solve (17).** This is because we have

$$\beta_0 \left(\frac{B_1 - B_2}{2} \right) = \left(\frac{B_1 + B_2}{2n} \right) \left(\frac{B_1 - B_2}{2} \right) = A_{10} C_1 - A_{20} C_2. \tag{18}$$

Any common factor of A_{10} and A_{20} on the right hand side cannot divide β_0 by the definition of n, so it must divide $\frac{B_1 - B_2}{2}$. This is enough to guarantee that we can solve (17), and then the solutions must be of the form

$$\begin{aligned} \lambda &= \lambda_0 + \eta A_{10}/p \\ \mu &= \mu_0 + \eta A_{20}/p \end{aligned} \tag{19}$$

for yet another parameter η, and where $p = \gcd(A_{10}, A_{20})$.

• Next,

$$C_1 = -(e_0 + a_0\mu)(h_0 + c_0\nu) + (f_0 + a_0\nu)(g_0 + c_0\mu)$$

which reduces to

$$C_1 = -\beta_0\mu - A_{20}\nu \tag{20}$$

and then to

$$C_1 + \beta_0\mu_0 = -(A_{20}/p)(-\beta_0\eta - p\nu) \tag{21}$$

• **We know that we can solve (20) and (21).**

• To see this, we refer again to (18). Any common factor of β_0 and A_{20} must divide $A_{10}C_1$ and must therefore divide C_1 by the definition of n.

• Finally,

$$C_2 = -(b_0 + a_0\lambda)(h_0 + c_0\nu) + (d_0 + c_0\lambda)(f_0 + a_0\nu)$$

which reduces to

$$C_2 = -\beta_0\lambda - A_{10}\nu \tag{22}$$

and then to

$$C_2 + \beta_0\lambda_0 = -(A_{10}/p)(-\beta_0\eta - p\nu) \tag{23}$$

- **We know that we can solve (22) and (23)** by an argument analogous to that for equation (20).
- **We know that we can simultaneously solve (17), (20), and (22).**
- What we have is a matrix equation

$$\begin{pmatrix} A_{20} & -A_{10} & 0 \\ -\beta_0 & 0 & -A_{10} \\ 0 & -\beta_0 & -A_{20} \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = \begin{pmatrix} \frac{B_1 - B_2}{2} \\ C_2 \\ C_1 \end{pmatrix}$$

which reduces to

$$\begin{pmatrix} A_{20} & -A_{10} & 0 \\ 0 & -\beta_0 A_{10} & -A_{10}A_{20} \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = \begin{pmatrix} \frac{B_1 - B_2}{2} \\ C_2 A_{20} + \beta_0 \left(\frac{B_1 - B_2}{2} \right) \\ \beta_0 \left(\frac{B_1 - B_2}{2} \right) + C_2 A_{20} - C_1 A_{10} \end{pmatrix}$$

and then by applying (17) this becomes

$$\begin{pmatrix} A_{20} & -A_{10} & 0 \\ 0 & -\beta_0 & -A_{20} \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = \begin{pmatrix} \frac{B_1 - B_2}{2} \\ C_1 \\ 0 \end{pmatrix}$$

so our solutions to (17), (20), and (22) will in fact work.

• As a comment on "proper" composition, we note that $Q_3 = (A_3, B_3, C_3)$ has $C_3 = -ch + dg = A_{10}A_{20} = A_1A_2/n^2$, just as is usually done with the standard composition algorithms. Of course, the usual algorithms produce a form with this as the *lead* coefficient, but the usual algorithms produce the compounded form, not its inverse. If we take the compounded form to be $(A_3, -B_3, C_3) \sim (C_3, B_3, A_3)$, then this composition is essentially the same as "ordinary" composition.

10 The Specific Algorithm Is the Standard Algorithm

• The specific algorithm above for putting two forms on a Bhargava cube is in fact the "standard" algorithm for composition.

• The standard algorithm, from my book, as done by Arndt and presented in Mathews, is as follows. (Arndt/Mathews do an algorithm for the Gauss forms with the middle coefficient required to be even; the algorithm in my book is the same algorithm but for Eisenstein forms with arbitrary middle coefficient.)

• **Arndt's Method:** To compound forms $F_1 = (A_1, B_1, C_1)$ and $F_2 = (A_2, B_2, C_2)$, we let $\beta = \frac{B_1+B_2}{2}$, we let $n = \gcd(A_1, A_2, \beta)$, and we solve

$$A_1 t + A_2 u + \beta v = n$$

for t, u, and v.

• We let

$$A_3 = A_1 A_2 / n^2,$$
$$B_3 = \frac{A_1 B_2 t + A_2 B_1 u + v(B_1 B_2 + \Delta)/2}{n}.$$

The composition is

$$F_1 \circ F_2 \sim (A_3, B_3, *)$$

with the third coefficient computed from the discriminant (or painfully from the formulas above).

- This works because we have

$$B_3 \equiv B_1 \pmod{2(A_1/n)} \tag{24}$$

and

$$B_3 \equiv B_2 \pmod{2(A_2/n)} \tag{25}$$

and

$$\beta B_3 \equiv \frac{B_1 B_2 + \Delta}{2} \pmod{2A_1A_2/n} \tag{26}$$

and this is essentially the united forms method of Dirichlet, adjusted slightly for the case that $n \neq 1$.

Bhargava can be derived from Arndt

• As above, let

$$\begin{aligned} a &= n \\ c &= 0 \\ d &= -A_{10} \\ g &= -A_{20} \\ h &= \beta_0 \end{aligned} \tag{27}$$

I have somewhat overcomplicated the notation by introducing $b = \lambda$ and $e = \mu$, but I will stick with that.

• If we now solve equation (16)

$$B_1 - \beta = \lambda A_{20} - \mu A_{10}$$

this leads to

$$B_1 + 2A_{10}\mu = B_2 + 2A_{20}\lambda.$$

In other words, we have solved congruences (24) and (25) and the common value of this expression is our desired B_3. The final solution, solving (20) (or (22)) for f in Bhargava's cube, is what gives us a value for B_3 that also satisfies congruence (26) in Arndt's method.