Division and Binary Quadratic Forms

William C. Jagy

December 13, 2008

1 Hi There

This all must go back to people such as Legendre, Dirichlet, and Gauss. I have no idea, really.

We use $\langle \alpha, \beta, \gamma \rangle$ to denote the (positive) binary quadratic form $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$. The discriminant Δ is given by $\Delta = \beta^2 - 4\alpha\gamma$ and so is negative for positive forms. We insist that our forms be primitive, that is $\gcd(\alpha, \beta, \gamma) = 1$.

For discriminant $\Delta = -23$, the entire class group

$$H(-23) = \{\langle 1, 1, 6\rangle, \langle 2, 1, 3\rangle, \langle 2, -1, 3\rangle\}$$

has only three elements, written $h(-23) = 3$.

There is an binary operation called composition that takes two primitive forms of the same discriminant to a third. Composition is commutative and associative, and makes the set of forms into a group, with identity $\langle 1, 0, -\Delta/4\rangle$ for even discriminant and $\langle 1, 1, (1 - \Delta)/4\rangle$ for odd.

From page 49 of Buell [1]: if a form $\langle \alpha, \beta, \gamma \rangle$ represents a number r primitively, that is $r = \alpha x^2 + \beta xy + \gamma y^2$ with $\gcd(x, y) = 1$, then the form can be rewritten as ('is equivalent to') some $\langle r, s, t\rangle$ of the same discriminant, still primitive.

From page 64 of Buell [1], the Shanks algorithm: if a form f_1 primitively represents a number a_1 and a form f_2 of the same discriminant primitively represents a number a_2, then the composition $f_1 \circ f_2$ does represent $a_1 a_2$ but perhaps not primitively.

Indeed, from pages 55-57 of Buell [1]: suppose $f_1 = \langle a_1, b_1, c_1\rangle$ and $f_2 = \langle a_2, b_2, c_2\rangle$ are "united" in the sense of Dirichlet, that is $\gcd(a_1, a_2, (b_1 +$

$b_2)/2) = 1$. Then (Prop. 4.5) there exist integers B, C such that $f_1 \sim \langle a_1, B, a_2 C\rangle$ and $f_2 \sim \langle a_2, B, a_1 C\rangle$. Furthermore,

$$f_1 \circ f_2 \sim \langle a_1 a_2, B, C\rangle$$

which means that $a_1 a_2$ is represented primitively by $f_1 \circ f_2$.

So this is the most favorable aspect of the picture: if two numbers are represented primitively by primitive united forms, then the product of the numbers is represented primitively by the composition of the forms, itself primitive. Kind of a semigroup homomorphism.

In particular, if the identity form $1 \sim \langle 1, \star, \star\star\rangle$ represents a prime number p that does not divide the discriminant Δ, then $1 \sim \langle p, b_1, c_1\rangle$ and $1 \sim \langle p, -b_1, c_1\rangle$ as the identity is ambiguous. Note that p does not divide b_1. Given some $f_2 = \langle a_2, b_2, c_2\rangle$, if $(b_1 + b_2)/2 \equiv 0 \bmod p$, then $(b_1 - b_2)/2 \not\equiv 0 \bmod p$. Either way, f_2 and at least one version of 1 are united forms, $1 \circ f_2 = f_2$, and so f_2 primitively represents pa_2.

2 Quickie

Theorem: Suppose some form f primitively represents the product mn with $\gcd(mn, \Delta) = 1$. Then f is the composition of primitive forms g and h, where g primitively represents m and h primitively represents n.

Proof: $f \sim \langle mn, \beta, \gamma\rangle$, with $\gcd(mn, \beta) = 1$, so $\gcd(m, \beta) = 1$ and $\gcd(n, \beta) = 1$.

Define $g = \langle m, \beta, n\gamma\rangle$ and $h = \langle n, \beta, m\gamma\rangle$, since $\gcd(m, \beta) = 1$ and $\gcd(n, \beta) = 1$ the two forms are primitive.

By Dirichlet's description of composition, page 57 of Buell [1], we have

$$g \circ h \sim f.$$

3 Prime p represented by the identity

Here we wish to allow common divisors, but insist one form in the composition be the identity. We insist

$$\Delta \leq -11,$$

so that the identity form does not represent the prime 2. Note that for indefinite forms, the prime two is represented by the identity form in arbitrarily high discriminant, so we are throwing all those out. May not matter, I just don't want to think about it.

Lemma: With $\Delta \leq -11$, if the identity form represents a prime p such that $p|\Delta$, then for even discriminant, $p = -\Delta/4$, but for odd discriminant, $p = -\Delta$.

Proof: For even Δ, we have $p = x^2+Dy^2$ where $D = -\Delta/4$, and $\Delta \leq -11$ implies $D \geq 3$. If $y = 0$ then $x^2 + Dy^2$ is not prime anyway. So $y \neq 0$ and $p = x^2 + Dy^2 \geq D \geq 3$. So p is not 2, and $p| - 4D$ means $p|D$. So $p \leq D$ as well and $p = D = -\Delta/4$.

For odd Δ, we have $p = x^2 + xy + ky^2$ where $k = (1 - \Delta)/4$. Note first that with $x = 1$ and $y = -2$, $x^2 + xy + ky^2 = 4k - 1$. Next, $\Delta \leq -11$ implies $k \geq 3$. In $p = x^2 + xy + ky^2$, if we had $y = 0$ we would get $p = x^2$ which does not result in a prime. So $y \neq 0$ and $p = x^2 + xy + ky^2 \geq (4k - 1)/4$. But p, x, y are integers so $p = x^2 + xy + ky^2 \geq k$. Meanwhile $p|4k - 1 = -\Delta$.

If $k \neq 1 \bmod 3$, then $4k - 1 \neq 0 \bmod 3$. So the smallest possible divisor of $4k - 1$ other than 1 is 5, and the largest possible divisor of $4k - 1$ other than $4k - 1$ itself is $(4k - 1)/5$. However $p \geq k > (4k - 1)/5$. So here $p = 4k - 1 = -\Delta$.

If $k \equiv 7 \bmod 9$, then $4k-1 \equiv 0 \bmod 9$. Here 3 is a divisor, and $(4k-1)/3$ is a divisor, of $4k - 1$, however $(4k - 1)/3$ is divisible by 3 and not prime.

If $k \equiv 1 \bmod 3$ but $k \neq 7 \bmod 9$, then $(4k - 1)/3$ is not divisible by 3. Let $t = (k - 1)/3$, so that $(4k - 1)/3 = 4t + 1$. Next, define the form $\langle 3, 3, t + 1\rangle$. Note that $4t + 1$ and therefore $t + 1$ are prime to 3. Now, $3x^2 + 3xy + (t + 1)y^2 = 4t + 1 = (4k - 1)/3$ when $x = 1$ and $y = -2$. As $k \geq 3$, here $k \geq 4$, and we find $t = (k - 1)/3 \geq 1$. When $k = 4$, $\langle 3, 3, 2\rangle \sim \langle 2, 1, 2\rangle$ is not the identity. When $k > 4$, actually $k \geq 10$ and $t \geq 3$, so $\langle 3, 3, t + 1\rangle$ is reduced and is not the identity. All of which is to say, when If $k \equiv 1 \bmod 3$ but $k \neq 7 \bmod 9$, if $(4k - 1)/3$ should happen to be prime it is not represented by the identity. So $p \neq (4k - 1)/3$, either $p \leq (4k - 1)/5$ or $p = 4k - 1$, so $p \geq k$ implies $p = 4k - 1 = -\Delta$.

4 Division and prime p represented by the identity

Theorem: Let the discriminant $\Delta \leq -11$, let the prime p be represented by the identity form $1 \sim \langle 1, \star, \star\star\rangle$, and let the product np be primitively represented by a primitive form f of the same Δ. Then f also primitively represents n.

Case I: When $\Delta \neq 0 \bmod p$, we have

$$f \sim \langle np, \beta_1, \gamma_1 \rangle$$

and

$$1 \sim \langle p, \beta_2, \gamma_2 \rangle.$$

We have $\beta_2 \neq 0 \bmod p$, so if we have bad luck and $(\beta_1 + \beta_2)/2 \equiv 0 \bmod p$, we merely switch (the identity form is ambiguous) β_2 to $-\beta_2$ to arrange $(\beta_1 + \beta_2)/2 \neq 0 \bmod p$.

So far we have $\gcd(p, np, (\beta_1 + \beta_2)/2) = 1$. Then, by Prop. 4.5 in Buell, there are integers B, C with

$$f \sim \langle np, B, pC \rangle$$

and

$$1 \sim \langle p, B, npC \rangle.$$

Meanwhile, the fact that f is primitive tells us that $\gcd(n, B, C) = 1$.

Define the form

$$g = \langle n, B, p^2C \rangle.$$

This is primitive as $B \neq 0 \bmod p$ and $\gcd(n, B, C) = 1$.

Compare

$$1 \sim \langle p, B, n(pC) \rangle,$$

$$g = \langle n, B, p(pC) \rangle.$$

As usual, we get

$$1 \circ g \sim \langle np, B, (pC) \rangle$$

so that

$$1 \circ g \sim f.$$

So f, g are equivalent and f primitively represents n.

Case II: $p | \Delta$ and even Δ.

$$f \sim \langle np, 2F, J \rangle$$

and

$$1 \sim \langle 1, 0, p \rangle.$$

So $\Delta = -4p = 4F^2 - 4npJ$. Then $p|F$, and

$$f \sim \langle np, 2pE, J\rangle.$$

$\Delta = -4p = 4p^2E^2 - 4npJ$ and $nJ = 1 + pE^2$.

$$1 \sim \langle p, 0, 1\rangle \sim \langle p, 2pE, 1+pE^2\rangle \sim \langle p, 2pE, nJ\rangle.$$

Define

$$g = \langle n, 2pE, pJ\rangle.$$

So

$$1 \circ g \sim \langle np, 2pE, J\rangle$$

and

$$1 \circ g \sim f.$$

So f, g are equivalent and f primitively represents n.

Case III: $p|\Delta$ and odd Δ, so $\Delta = -p$ and $1 \sim \langle 1, 1, k\rangle$.

$$f \sim \langle np, F, J\rangle.$$

Again $F \equiv 0 \bmod p$, so

$$f \sim \langle np, pE, J\rangle$$

with E odd. Meanwhile $p^2E^2 - 4npJ = -p$ and $4nJ = 1 + pE^2$. With the equivalence

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$

we find

$$1 \sim \langle p, -p, k\rangle.$$

As E is odd,

$$1 \sim \langle p, pE, nJ\rangle.$$

Define

$$g = \langle n, pE, pJ\rangle.$$

So

$$1 \circ g \sim \langle np, pE, J\rangle$$

and

$$1 \circ g \sim f.$$

So f, g are equivalent and f primitively represents n.

5 Some applications

Corollary: if an integer n is represented by $\langle 2, 1, 3 \rangle$, then n is divisible by some prime $q = 2x^2 + xy + 3y^2$.

Proof: First, perhaps n is not primitively represented. For example, this must happen if n is divisible by any prime s with Legendre symbol $(-23|s) = -1$. Well, no matter, divide the two variables by their gcd G and divide n by G^2. This factor $m = n/G^2$ is represented primitively. It follows that m is not divisible by any prime s with Legendre symbol $(-23|s) = -1$. All remaining primes are 2, 3, 23, or p with $(-23|p) = +1$. If m is divisible by any prime that is itself represented by $\langle 1, 1, 6 \rangle$, such as 23, the Theorem of the previous section shows that $\langle 2, 1, 3 \rangle$ also divides m divided by that prime. Repeat until no prime factors of shape $\langle 1, 1, 6 \rangle$ remain. As $\langle 2, 1, 3 \rangle$ does not represent 1, what is left has at least one prime factor, and all of its prime factors are of shape $\langle 2, 1, 3 \rangle$. That is, m and the original n are divisible by some prime $q = 2x^2 + xy + 3y^2$.

Corollary: if an integer n is not divisible by 2 or 3, and n is represented by $\langle 4, 2, 7 \rangle$, then n is divisible by some prime $q = 4x^2 + 2xy + 7y^2$.

Proof: First, perhaps n is not primitively represented. For example, this must happen if n is divisible by any prime s with Legendre symbol $(-108|s) = -1$. Well, no matter, divide the two variables by their gcd G and divide n by G^2. This factor $m = n/G^2$ is represented primitively. It follows that m is not divisible by any prime s with Legendre symbol $(-108|s) = -1$. All remaining primes are 2, 3, or p with $(-108|p) = +1$. But we were told that m is not divisible by 2 or 3. If m is divisible by any prime that is itself represented by $\langle 1, 0, 27 \rangle$, such as 31, the Theorem of the previous section shows that $\langle 4, 2, 7 \rangle$ also divides m divided by that prime. Repeat until no prime factors of shape $\langle 4, 2, 7 \rangle$ remain. As $\langle 4, 2, 7 \rangle$ does not represent 1, what is left has at least one prime factor, and all of its prime factors are of shape $\langle 4, 2, 7 \rangle$. That is, m and the original n are divisible by some prime $q = 4x^2 + 2xy + 7y^2$.

Note that the primes 2 and 3 are not represented by primitive forms of discriminant $\Delta = -108$. Instead they are represented by imprimitive $\langle 2, 2, 14 \rangle$ and $\langle 3, 0, 9 \rangle$. It is also worth pointing out the facts, easily checked, that $4x^2 + 2xy + 7y^2 \neq 2 \bmod 4$ and $4x^2 + 2xy + 7y^2 \neq \pm 3 \bmod 9$.

References

[1] D. A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer-Verlag, 1989.

[2] Richard H. Hudson and Kenneth S. Williams. Representation of primes by the principal form of discriminant $-D$ when the classnumber $h(-D)$ is 3. *Acta Arithmetica*, 57:131–153, 1991.

[3] Blair K. Spearman and Kenneth S. Williams. The cubic conguence $x^3 + Ax^2 + Bx + C \equiv 0 \bmod p$ and binary quadratic forms. *Journal of the London Mathematical Society*, 46:397–410, 1992.