Primes - Problem Sheet 7 - Solutions

Composition of quadratic forms

Q1) Let $f = (a, b, c)$ be a primitive form, and M any integer. Show that f represents some integer coprime to M. Show also that we can assume f properly represents some integer coprime to M.

Solution: Pick a prime p dividing M. There are 3 (overlapping) cases to consider:

If $p \nmid a$, then we can pick x, y such that $p \nmid x$ and $p \mid y$. Then $f(x, y) = ax^2 + bxy + cy^2$ is not divisible by p, so is prime to p.

Similarly if $p \nmid c$.

Otherwise $p \mid a, c$, so $p \nmid b$. Then pick x, y such that $p \nmid x, y$. And $f(x, y)$ is coprime to p.

Do this for every prime, and choose compatible x, y. Then $f(x, y)$ is coprime to M.

Q2) Suppose that F is (a) direct composition of f and g. If $f \sim f'$ and $g \sim g'$, and $F' \sim F$, show that F' is a direct composition of f' and g'. So we can use the Dirichlet composition to find the direct composition with explicit bilinear forms.

Solution: We sketch the details only. If $f(px + qy, rx + sy) = f'(x, y)$, and

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w)) ,$$

then

$$\begin{aligned} f'(x, y)g(z, w) &= f(px + qy, rx + sy)g(z, w) \\ &= F(B_1(px + qy, rx + sy; z, w), B_2(px + qy, rx + sy; z, w)) , \end{aligned}$$

where

$$\begin{aligned} B_1(px + qy, rx + sy; z, w) &= a_1(px + qy)z + b_1(px + qy)w + c_1(rx + sy)z + d_1(rx + sy)w \\ &= (a_1p + c_1r)xz + (b_1p + d_1r)xw + (a_1q + c_1s)yz + (b_1q + d_1r)yw \end{aligned}$$

is another integral bilinear form.

This show that F is the composition of f' and g. To be direct, we need that

$$f'(1, 0) = +(a'_1b'_2 - a'_2b'_1) .$$

But $f'(1, 0) = f(p, r) = ap^2 + bpr + cr^2$, and

$$\begin{aligned} a'_1b'_2 - a'_2b'_1 &= (a_1p + c_1r)(b_2p + d_2r) - (a_2p + c_2r)(b_1p + d_1r) \\ &= (\underbrace{a_1b_2 - a_2b_1}_{=a})p^2 + (a_1d_2 + c_1b_2 - a_2d_1 - c_2b_1)pr + (\underbrace{\ c_1d_2 - c_2d_1\ }_{c\text{, see next exercise}})r^2 \\ &\vdots \\ &= f'(1, 0) . \end{aligned}$$

For g, we have $g(1,0) = a_1c_2 - a_2c_1$, and

$$\begin{aligned} a_1'c_2' - a_2'c_1' &= (a_1p + c_1r)(a_2q + c_2s) - (a_1q + c_1s)(a_2p + c_2r) \\ &(a_1c_2 - a_2c_1)(ps - qr)\,, \end{aligned}$$

since $ps - qr = 1$ as the equivalence is proper.

Finally, if $F(x,y) = F'(ax + by, cx + dy)$, then

$$f(x,y)g(z,w) = F'(aB_1(x,y;z,w) + bB_2(x,y;z,w), cB_1(x,y;z,w) + dB_2(x,y;z,w))\,.$$

But a linear combination of two bilinear forms, is bilinear. Hence F' is a composition of f and g. For directness, we have

$$\begin{aligned} aB_1 + bB_2 &= (aa_1 + ba_2)xz + (ab_1 + bb_2)xw + (ac_1 + bc_2)yz + (ad_1 + bd_2)yw \\ cB_1 + dB_2 &= (a_1c + a_2d)xz + (b_1c + b_2d)xw + (cc_1 + c_2d)yz + (cd_1 + dd_2)yw\,. \end{aligned}$$

And

$$\begin{aligned} a_1'b_2' - a_2'b_1' &= (aa_1 + ba_2)(b_1c + b_2d) - (a_1c + a_2d)(ab_1 + bb_2) \\ &= (a_1b_2 - b_1a_2)(ad - bc) \\ &= a_1b_2 - a_2b_1 = f(1,0) \end{aligned}$$

since the transformation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant $ad - bc = 1$. Similary for g.

Q3) Suppose that $pq = X^2 + 14Y^2$ and $q = 2a^2 + 7b^2$. By considering the composition

$$\begin{aligned} p(2a^2 + 7b^2)(2a^2 + 7b^2) &= (X^2 + 14Y^2)(2a^2 + 7b^2) \\ &= 2(aX + 7bY)^2 + 7(-bX + 2aY)^2\,. \end{aligned}$$

By reducing $2a^2 + 7b^2$, and $X^2 + 14Y^2$ modulo q, show that we may choose the sign $\pm a, \pm b, \pm X, \pm Y$, so that

$$q \mid aX + 7bY, -bX + 2aY\,,$$

hence conclude that p is represented by $2x^2 + 7y^2$.

Solution: We can assume $q \neq 2, 7$. If $q = 2$, and $2p = X^2 + 14Y^2$, then $2 \mid X$, meaning $X = 2X'$, and so we get

$$2p = 4(X')^2 + 14Y^2 \implies p = 2(X')^2 + 7Y^2\,.$$

Similarly for $q = 7$.

Let us reduce $2a^2 + 7b^2$ and $X^2 + 14Y^2$ modulo q. We have

$$X^2 + 14Y^2 \equiv 2a^2 + 7b^2 \equiv 0 \pmod{q}\,,$$

so

$$\begin{aligned} 14 &\equiv -(X/Y)^2 \pmod{q} \\ 7/2 &\equiv -(a/b)^2 \pmod{q} \\ 14 &\equiv -(2a/b)^2 \pmod{q} \\ 14 &\equiv -(7b/a)^2 \pmod{q} \end{aligned}$$

and we get

$$\begin{aligned} X/Y \equiv \pm 2a/b &\implies Xb \pm 2aY \equiv 0 \\ X/Y \equiv \pm 7b/a &\implies Xa \pm 7bY \equiv 0\,. \end{aligned}$$

We have

$$2a/b = \pm 7b/a \implies 2a^2 = \pm 7b^2\,,$$

so the sign must be $-$. (If also $2a^2 - 7b^2 \equiv 0$, then we obtain $4a^2 \equiv 0 \pmod q$), which means $q \mid a$, which then leads to $q \mid b$, and a contradiction.)

Overall, we have

$$\begin{aligned} Xb \pm 2aY &\equiv 0 \\ Xa \mp 7bY &\equiv 0 \end{aligned}$$

Changing the sign of Y swaps the ± signs, so we can assume the first sign is $-$ and the second is $+$. Hence we get the required divisibility conditions.

Then

$$q^2 p = 2(aX + 7bY)^2 + 7(-bX + 2aY)^2$$

implies

$$p = 2(\frac{aX + 7bY}{q})^2 + 7(\frac{-bX + 2aY}{q})^2$$

so p is represented by $2x^2 + 7y^2$, as claimed.

Q4) Suppose that $F = (A, B, C)$ is the composition of $f = (a, b, c)$ and $g = (a', b', c')$ via

$$\begin{aligned} f(x, y)g(z, w) = F(&a_1xz + b_1xw + c_1yz + d_1yw, \\ &a_2xz + b_2xw + c_2yz + d_2yw)\,. \end{aligned}$$

Suppose all 3 forms have the same discriminant $D \neq 0$.

i) By specialising variables x, y, w, z prove that

$$\begin{aligned} aa' &= Aa_1^2 + Ba_1a_2 + Ca_2^2 \\ ac' &= Ab_1^2 + Bb_1b_2 + Cb_2^2 \\ ab' &= 2Aa_1b_1 + B(a_1b_2 + a_2b_1) + 2Ca_2b_2\,. \end{aligned}$$

Hint: try $x = z = 1, y = w = 0$ for the first.

ii) Prove that $a^2(b'^2 - 4a'c') = (a_1b_2 - a_2b_1)^2(B^2 - 4AC)$, hence conclude

$$f(1, 0) = a = \pm(a_1b_2 - a_2b_1)\,.$$

iii) Prove that

$$g(1, 0) = a' = \pm(a_1c_2 - a_2c_1)$$

Solution: a) With $x = z = 1, y = w = 0$, we get

$$f(1, 0)g(1, 0) = F(a_1, a_2) \implies aa' = Aa_1^2 + Ba_1a_2 + Ca_2^2\,.$$

For the second use $x = 1, y = 0, z = 0, w = 1$. For the third, use $x = 1, y = 0$, and $z = 1 = w$, to get

$$\begin{aligned} a(a' + b' + c') &= F(a_1 + b_1, a_2 + b_2) \\ &= A(a_1 + b_1)^2 + B(a_1 + b_1)(a_2 + b_2) + C(b_1 + b_2)^2 \end{aligned}$$

then subtract the first two results.

b) Then follows directly by taking $(ab')^2 - 4(aa')(ac')$ from above. Then take square roots.

c) We also have

$$ca' = Ac_1^2 + Bc_1c_2 + Cc_2^2 \quad (x,y,z,w) = (0,1,1,0)$$
$$ba' = 2Aa_1c_2 + (c_1a_2 + a_1c_2)B + 2a_2c_2B \quad (1,1,1,0) - (1,0,1,0) - (0,1,1,0)\,.$$

Then forming

$$(a'b)^2 - 4(a'a)(a'c)$$

gives the result after taking square roots.

Extra) We also obtain, by similar means

$$c = \pm(c_2d_1 - c_1d_2)$$
$$c' = \pm(b_2d_1 - b_1d_2)$$

Q5) Recall that a group of order 4 is is isomorphic to either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or to $\mathbb{Z}/4\mathbb{Z}$. Determine the class group $\mathcal{C}(D)$ for $D = -56$, $D = -68$, $D = -84$, $D = -96$. Do you see any connection between $\mathcal{C}(D)$ and when genus theory works? Hint: to distinguish between $\mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ you only need to check whether some form is not properly equivalent to its inverse. Why? This is easy to do using reduced forms.
Solution: To distinguish between $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$, we need to find an element of order 4. This means an element whose square is not the identity. An element which squares to the identity is its own inverse, which means the form and its inverse will be properly equivalent. The inverse of (a,b,c) is $(a,-b,c)$. Assume (a,b,c) is a reduce form, then $(a,b,c) \sim (a,-b,c)$ iff $(a,-b,c)$ is not reduced.

For $D = -56$, the reduced forms are $x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2$. We see that $(3,\pm 2,5)$ are non-equivalent as they are both reduced. Hence $\mathcal{C}(-56) \cong \mathbb{Z}/4$.

For $D = -68$, the reduced forms are $(1,0,17)$, $(2,2,9)$, $(3,-2,6)$, $(3,2,-6)$. Again $(3,\pm 2,-6)$ are inverses but are not properly equivalence. Hence $\mathcal{C}(-68) \cong \mathbb{Z}/4\mathbb{Z}$.

For $D = -84$, the reduced forms are $(1,0,21),(2,2,11),(3,0,7),(5,4,5)$. Every form is properly equivalent to its inverse since $(a,-b,c)$ and (a,b,c) do not appear together on the list. Hence $\mathcal{C}(-84) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

For $D{-}96$, the reduced forms are $(1,0,24),(3,0,8),(4,4,7),(5,2,5)$, so again $\mathcal{C}(-96) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Once can observe that genus theory works when $\mathcal{C} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and does not work when $\mathcal{C} \cong \mathbb{Z}/4\mathbb{Z}$. Generally it is true that genus theory works when $\mathcal{C} \cong (\mathbb{Z}/2\mathbb{Z})^n$.

Q6) It is known that any *ternary* quadratic form $f(x,y,z)$ of determinant $\det(f) = 1$ is properly equivalent to $x^2+y^2+z^2$. (See Corollary 2 [Cassels 2008, p. 138].) Assuming this, show that there is no (nice!) notion of composition of integral ternary quadratic forms of fixed determinant. Hint: we would (want to) have

$$(x^2+y^2+z^2)(u^2+v^2+w^2) = (B_1(x,y,z;u,v,w))^2+(B_2(x,y,z;u,v,w))^2+(B_3(x,y,z;u,v,w))^2\,,$$

where $B_i(x,y,z;u,v,w) = a_{1,1}xu + \cdots + a_{3,3}zw$ are integral bilinear forms. Consider representations of $15 = 3 \times 5$ by $x^2 + y^2 + z^2$.
Solution: If such a composition existed, then we would have a way of writing $15 = 3 \times 5$ as a sum of 3 squares: we take the representations $3 = 1^2 + 1^1 + 1^2$

and $5 = 2^2 + 1^2 + 0^2$, and run them through the composition. But 15is not the sum of 3 squares: $15 = x^2 + y^2 + z^2$ implies $x, y, z \leq 3$. A brute force check shows that this is not possible.

Q7) Suppose $D < 0$ is a discriminant, and that q is a prime such that $\left(\frac{D}{q}\right) = 1$. Show that

$$h(D) \geq \log\left(\frac{1}{4}(|D|)\right) / \log q\,.$$

Hint: some $g(x, y)$ of discriminant D represents q. If g has order M in the class group, then q^M is represented by the principal form. Put a bound on q^M.
Remark: With slightly stronger analysis, one can prove the bound

$$h(D) - 1 \geq \log\left(\frac{1}{4}(|D| + 1)\right) / \log(q)\,.$$

For this, see the paper "Über die Klassenzahl imaginär-quadratischer Zahlkörper", Nagel 1922.
Solution: We have $g(x, y) = q$. Let g have order M, so $q^M = x^2 + xy + (1 - D)/4y^2$ or $x^2 - D/4y^2$. (Represented by the principal form as $g^M =$ principal.) Since q is prime, $y = 0$ cannot be a solution. So we get

$$q^m = x^2 + xy + (1 - D)/4y^2 = (x + y/2)^2 - D(y/2)^2 \geq 0 - D \cdot (1/2)^2 = -D/4 = |D|/4$$

(Same bound holds if we have the form $x^2 - D/4y^2$.)

Now m divides $h(D)$, which means $h(D) \geq m$. We find that

$$h(D) \geq m = \log(-D/4)/\log(q)\,.$$