# Primes - Problem Sheet 4 - Solutions

## Properties of quadratic forms

Q1) Let $f(x_1, \dots, x_n)$ be a quadratic form (with coefficients over some ring $R \supset \mathbb{Z}$). Show that

$$f \text{ is integral implies } 2f \text{ is } \textit{classically} \text{ integral.}$$

**Solution:** Integral means

$$\mathrm{mat}(f) = \begin{pmatrix} a_{11} & \frac{1}{2}a_{ij} \\ \frac{1}{2}a_{ij} & a_{nn} \end{pmatrix}$$

implies

$$\mathrm{mat}(2f) = \begin{pmatrix} 2a_{11} & a_{ij} \\ a_{ij} & 2a_{nn} \end{pmatrix},$$

which means $2f$ is classically integral.

Q2) Suppose that $f(x_1, \dots, x_n)$ is a non-primitive integral quadratic form. Show that $f(x_1, \dots, x_n)$ can represent at most one prime.
**Solution:** Since $f$ is not primitive, let $d = \gcd(r_i j)$ be the common divisor of all coefficients. Then for any $a_i \in \mathbb{Z}^n$ we have $d \mid f(a_1, \dots, a_i)$.

If $f$ represents the prime $p$, then $d \mid p$, so $d = p$. Hence all values represented by $f(x_1, \dots, x_n)$ are divisible by $p$. The only prime divisible by $p$ is $p$ itself.

Q3) Suppose $f(x, y) = ax^2 + bxy + cy^2$ is an integral binary quadratic form, with discriminant $D = b^2 - 4ac$.

i) Show that $f$ is indefinite if $D > 0$.

ii) Show that $f$ is positive (respectively negative) definite if $D < 0$ and $a > 0$ (respectively $a < 0$).

iii) What happens when $D = 0$? What happens if $D > 0$ is a perfect square?
Hint: Complete the square!
**Solution:** We write

$$af(x, y) = a(ax^2 + bxy + cy^2) = (ax + by/2)^2 - \underbrace{(b^2/4 - ac)}_{D/4} y^2 .$$

If $D < 0$, then $af(x, y)$ is the sum of two squares, so is $\geq 0$. It equals 0 if and only if $y = 0$ and $ax + by/2 = 0$, i.e. $x = y = 0$. So $f(x, y) = \frac{1}{a}((ax+by/2)^2 - \underbrace{(b^2/4 - ac)}_{D/4} y^2)$ is positive-definite if $a > 0$ and negative definite if $a < 0$. Since $D < 0$, we cannot have $a = 0$.

For $D > 0$, not a perfect square, we must have $a \neq 0$. (Else $D = b^2$.) Write $f(x, y) = \frac{1}{a}(ax + by/2)^2 - \frac{D}{4a}y^2$. Taking $y = 0$, and $x = 1$ gives $a$. Taking $y = 2a$ and $x = b$ gives $f(b, -2a) = -\frac{D}{4a}(2a)^2$, which has the opposite sign to $a$. Hence $f(x, y)$ is indefinite.

For $D$ a perfect square, then we can factor the polynomial (over $\mathbb{Q}$ at first, and so over $\mathbb{Z}$ by the Gauss lemma for polynomials). If $D = 0$, then the root $r = \frac{\beta}{\alpha}$ of $f(x,1)$ is repeated, so we factor $f(x,y)$ as $a(\beta x - \alpha y)^2$. (Note $f(x,y) = y^2 f(x/y,1)$.) If $a = 0$ the polynomial is identically 0. If $a > 0$ it is positive-semidefinite by taking $y = \beta, y = \alpha$. If $a < 0$, it is negative-semidefinite.

If $D \neq 0$, then $f(x,1)$ takes some positive values and some negative values, between the roots and outside the roots we get different signs! Let $x = p/q$ give a positive, and $x = r/s$ a negative. Then $f(p,q) = q^2 f(p/q,1) > 0$ and $f(r,s) = s^2 f(r/s,1) < 0$. So $f(x,y)$ is indefinite (and non-trivially represents 0). (Perhaps this should be semi-indefinite?)

Q4) Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form, of discriminant $D = b^2 - 4ac$. Show that $D \equiv 0,1 \pmod 4$, and that every such $D$ occurs.
**Solution:** By reducing modulo 4, we see that $D \equiv b^2 \pmod 4$, and the squares modulo 4 are $0^2, (\pm)1^2, 2^2 \equiv 0,1 \pmod 4$. Conversely, if $D = 4k$, then $x^2 - ky^2$ has discriminant $4k$. Whereas for $D = 4k+1$, $x^2 + xy - ky^2$ has discriminant $4k+1$.

Q5) Show that $R$-equivalence is an equivalence relation on $n$-ary quadratic forms over $R$. Show
i) The form $f$ is equivalent to $f$,

ii) If $f$ is equivalent to $g$, then $g$ is equivalent to $f$, and

iii) If $f$ equivalent to $g$, and $g$ equivalent to $h$, then $f$ equivalent to $h$.
Check also for $\mathrm{SL}_n(\mathbb{Z})$-equivalence, when $R = \mathbb{Z}$.

**Solution:**
- The identity matrix $B = I_n$ shows $f$ is $\mathrm{SL}_n(\mathbb{Z})/\operatorname{GL}_n(\mathbb{Z})$ -equivalent to $f$.
- If $B$ gives equivalence of $f$ to $g$ then $B^{-1}$ gives equivalence of $g$ to $f$. As $\det(B) = \det(B^{-1})$, this works for $\mathrm{SL}_n(\mathbb{Z})$ equivalence too.
- If $B$ gives equivalence $f$ to $g$, and $C$ gives equivalence $g$ to $h$. Then $BC$ gives the equivalence $f$ to $h$. Since $\det(BC) = \det(B)\det(C)$, this holds for $\mathrm{SL}_n(\mathbb{Z})$ equivalence too.

Q6) Suppose $f$ and $g$ are $\mathrm{GL}_n(R)$-equivalent quadratic forms. Show
i) $\det(f)$ and $\det(g)$ differ by a square

$$\det(f) = \lambda^2 \det(g)\,,$$

for some $\lambda \neq 0 \in R^*$. How does $\lambda$ arise from the equivalence of $f$ to $g$?

ii) For $R = \mathbb{Z}$, conclude $\det(f) = \det(g)$, and explain why $\mathrm{GL}_n(\mathbb{Z})$-equivalent integral binary quadratic forms have the same discriminant.

**Solution:** Let $B$ give the equivalence, then $\mathrm{mat}(g) = B^\top \mathrm{mat}(f) B$. Taking determinants gives

$$\det(g) = \det(B)^2 \det(f)\,.$$

So $\lambda = \det(B)^{-1} \in R^*$.

Since $\mathbb{Z}^* = \{\pm 1\}$, we get $\lambda^2 = 1$, meaning equivalent integral forms have the same discriminant.

Q7) Suppose $f$ and $g$ are $\mathrm{GL}_n(R)$-equivalent quadratic forms. Show

i) $f$ represents $r \in R$ if and only if $g$ represents $r \in R$.

ii) For $R = \mathbb{Z}$, $f$ represents $n \in \mathbb{Z}$ properly, if and only if $g$ represents $n \in \mathbb{Z}$ properly. Check also for $\mathrm{SL}_n(\mathbb{Z})$-equivalence.

Use this to show that

$$x^2 + 14y^2 \text{ , } 2x^2 + 7y^2 \text{ and } 3x^2 + 2xy + 5y^2$$

are not $\mathrm{GL}_n(\mathbb{Z})$-equivalent.

**Solution:** If $r = f(a_1, \dots, a_n)$, and $g(\vec{x}) = f(B\vec{x})$, then $g(B^{-1}\vec{x}) = f(\vec{x})$. So we can write $g(B^{-1}(a_1, \dots, a_n)^\top) = f(a_1, \dots, a_n) = r$, to see $(a'_1, \dots, a'_n)^\top = B^{-1}(a_1, \dots, a_n)^\top$ gives a representation of $r$ by $g$.

By symmetry, we get $f$ represents $r$ if and only if $g$ represents $r$.

This holds for $Bin\, \mathrm{GL}_n(R)$, and also for proper equivalence $B \in \mathrm{SL}_n(\mathbb{Z})$.

If $\gcd(a_i) = 1$, then we cannot have $\gcd(a'_i) > 1$. For if $\gcd(a'_i) = d$, then $(a_1, \dots, a_n)^\top = B^{-1}(a'_1, \dots, a'_n)^\top$ and each entry is divisible by $d$, showing $\gcd(a_1, \dots, a_n) \geq d$. So $f(a_1, \dots, a_n)$ is a proper representation of $r$ implies $g(a'_1, \dots, a'_n)$ is a proper representation of $r$.

Q8) Suppose $f$ and $g$ are integral $n$-ary quadratic forms. Then $2f$ and $2g$ are classically integral. Show that

$f$ is $\mathrm{GL}_n(\mathbb{Z})$-equivalent to $g$ if and only if $2f$ is $\mathrm{GL}_n(\mathbb{Z})$-equivalent to $2g$.

Check also for $\mathrm{SL}_n(\mathbb{Z})$-equivalence.

**Solution:** Suppose $f$ is equivalent to $g$ via $B$. The matrix of $2f$ is given by $2\,\mathrm{mat}(f)$. Then

$$g(\vec{x}) = x^\top G x = x^\top B^\top G B x = x^\top F x = f(B\vec{x})$$

if and only if

$$2g(\vec{x}) = x^\top (2G) x = x^\top B^\top (2G) B x x^\top 2(B^\top G B) x = x^\top 2F x = (2f)(B\vec{x})\,.$$

So $2f$ is equivalent to $2g$ via $B$. And conversely.

Q9) Suppose $f, g, h$ are integral quadratic forms. Suppose $f$ and $g$ are improperly equivalent, and $g$ and $h$ are improperly equivalent. Show that $f$ and $h$ are *properly* equivalent.

**Solution:** Matrix $B$ gives improper equivalence between $f$ and $g$. Matrix $C$ gives improper equivalence between $g$ and $h$. Then $B, C \in \mathrm{GL}_n(\mathbb{Z})$ with $\det(B) = \det(C) = -1$.

The matrix $CB$ gives equivalence between $f$ and $h$, and $\det(CB) = \det(C)\det(B) = (-1)^2 = 1$. This is a proper equivalence between $f$ and $g$.