LMS Undergraduate Summer School
Binary quadratic forms
Exercise sheet 1

Alex Bartel

25–26 August 2022

1. Show that if x is any integer, then one has $x^2 \equiv 0$ or 1 or $4 \pmod 8$, and in particular $x^2 \equiv 0$ or $1 \pmod 4$. Show also that if x is an integer, then $x^2 \equiv 0$ or $1 \pmod 3$ and $x^2 \equiv 0$ or 1 or $-1 \pmod 5$.

2. Generalising the previous exercise, show that if p is an odd prime number, then half of all non-zero remainders modulo p are realised by a square of an integer, and half are not. How many remainders modulo p are cubes? **Hint:** You may use without proof the fact that the group $(\mathbb{Z}/p\mathbb{Z})^\times$ of non-zero remainders modulo p under multiplication is cyclic.

3. Fill in all details in Zagier's proof of Fermat's sum-of-two-squares theorem.

4. Prove one direction in each of Lagrange's theorems, Theorem 1.3.

5. Let B be the set of binary quadratic forms. Show that the function $\mathrm{SL}_2(\mathbb{Z}) \times B \to B$,

$$\begin{pmatrix} r & t \\ s & u \end{pmatrix} \cdot f(x,y) \mapsto \begin{pmatrix} r & t \\ s & u \end{pmatrix} \cdot f(x,y) = f\left((x,y) \cdot \left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)\right)$$

   defines a left group action of $\mathrm{SL}_2(\mathbb{Z})$ on B, i.e. for all M, $N \in \mathrm{SL}_2(\mathbb{Z})$ and all $f \in B$ we have $M \cdot (N \cdot f) = (M \cdot N) \cdot f$.

6. For each of the following pairs f, g of binary quadratic forms, determine whether they are equivalent:

   (a) $f(x,y) = x^2 + xy + 3y^2$, $g(x,y) = x^2 + xy + y^2$;

   (b) $f(x,y) = x^2 + 7y^2$, $g(x,y) = x^2 + 2xy + 8y^2$;

   (c) $f(x,y) = x^2 + 5y^2$, $g(x,y) = 2x^2 + 2xy + 3y^2$.

7. Complete the proof of Proposition 2.8.

8. An integer d is called a *fundamental discriminant* if either

   - $d \equiv 1 \pmod 4$ and d is square-free (i.e. not divisible by the square of any integer > 1), or
   - $d \equiv 0 \pmod 4$ and $d/4 \equiv 2$ or $3 \pmod 4$ and is square-free.

   Show that if d is a fundamental discriminant, then every binary quadratic form of discriminant d is primitive. (This was a missing step in the proof of Proposition 2.11.)