# ELEMENTARY NUMBER THEORY

HOMEWORK 6

(1) Compute $h(-23)$.

Let $(A, B, C)$ be a reduced form of discriminant $-23$. Then $0 < A < \sqrt{23/3} < 3$, hence $A = 1$ or $A = 2$. Moreover, $B^2 - 4AC = -23$ implies that $B$ is odd. Thus we have the possibilities $(A, B) \in \{(1, 1), (2, -1), (2, 1)\}$. Computing $C$ from $B^2 - 4AC = -23$ in these cases we find that $h(-23) = 3$, and that the reduced forms are $(1, 1, 6)$ and $(2, \pm 1, 3)$.

(2) Compute $h(-52)$.

Here $0 < A < 5$, and $B$ is even. Here it turns out that there are exactly two reduced forms, namely $(1, 0, 13)$ and $(2, 2, 7)$, hence $h(-52) = 2$. You can save some work by observing that $A = 3$ is impossible since $-52 = B^2 - 4AC \equiv B^2 \bmod A$ shows that $-13$ must be a square mod $A$ if $A$ is odd. Also, $A = 4$ is impossible since $-52 \equiv B^2 \bmod 16$ implies $-13 \equiv (B/2)^2 \bmod 4$, which is not true.

(3) Reduce the form $(15, 40, 27)$.

Observe that this form has discriminant $\Delta = 40^2 - 4 \cdot 15 \cdot 27 = -20$. Thus the form must be equivalent to $(1, 0, 5)$ or $(2, 2, 3)$.

Let $Q = (15, 40, 27)$ and use $S = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$; then $Q|_S = (15, 40 - 2 \cdot 15, 15 - 40 + 27) = (15, 10, 2)$. Next $(15, 10, 2) \sim (2, -10, 15) = Q'$. This time use $S = \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right)$ and get $Q'|_S = (2, 2, 3)$.

In `pari`, you only have to enter `qfbred(Qfb(15,40,27))`.

(4) Reduce the form $(101, 20, 1)$.

Here the discriminant is $-4$, so the form must be equivalent to $(1, 0, 1)$.

Running through the algorithm, we get $(101, 20, 1) \sim (1, -20, 101)$, and then $(1, -20, 101) \sim (1, 0, 1)$.

(5) Consider the form $Q = (1, 0, 13)$. Show that if $p$ is a prime $\neq 13$ represented by $Q$, then $\left(\frac{-13}{p}\right) = +1$ and $p \equiv 1 \bmod 4$.

If $p = x^2 + 13y^2$, then $x^2 \equiv -13y^2 \bmod p$, and clearly $p \nmid y$. Thus $\left(\frac{-13}{p}\right) = +1$.

Moreover, $p = x^2 + 13y^2 \equiv x^2 + y^2 \equiv 0, 1 \bmod 4$, and since $p$ is prime, we must have $p \equiv 1 \bmod 4$.