MATH 542 NUMBER THEORY
Problems to Think About #5
CH. 5, #1-7

Russell Jahn

(1)

Let us call:

$\alpha : (a,b,c) \to (c,-b,a)$ for $f \in (1)$ or (3)

$\beta : (a,b,c) \to (a, b+2ka, ak^2+bk+c)$ for $f \in (2)$ or (5) where $k = [[\frac{a-b}{2a}]]$

$\gamma : (a,b,c) \to (a, b-2ka, ak^2-bk+c)$ for $f \in (4)$ or (7) where $k = [[\frac{a+b}{2a}]]$

$\delta : (a,b,c) \to (a, b+2a, a+b+c) = (a,a,c)$ for $f \in (6)$

First, we need to show that each is unimodular: Recall $F = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$

(α) Let $U_\alpha = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Rightarrow \det U_\alpha = 1$ and $U_\alpha^T F U_\alpha = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$

(β) Let $U_\beta = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \Rightarrow \det U_\beta = 1$ and $U_\beta^T F U_\beta = \begin{pmatrix} a & 1/2(b+2ka) \\ 1/2(b+2ka) & ak^2+bk+c \end{pmatrix}$

(γ) Let $U_\gamma = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \Rightarrow \det U_\gamma = 1$ and $U_\gamma^T F U_\gamma = \begin{pmatrix} a & 1/2(b-2ka) \\ 1/2(b-2ka) & ak^2-bk+c \end{pmatrix}$

(δ) Let $U_\delta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow \det U_\delta = 1$ and $U_\delta^T F U_\delta = \begin{pmatrix} a & 1/2(b+2a) \\ 1/2(b+2a) & a+b+c \end{pmatrix}$

$\therefore$ Each is unimodular.

Let the transformed BQF be $Ax^2 + Bxy + Cy^2$.

$f \in (6)\ \ (a < c, b = -a) \overset{\delta}{\to} A < C, B = A \Rightarrow$ reduced.

$f \in (3)\ \ (a = c, -a \le b < 0) \overset{\alpha}{\to} A = C, 0 < B \le A \Rightarrow$ reduced.

$$f \in (1)\ \ (a > c) \overset{\alpha}{\to} A < C \begin{cases} -A < B \le A \Rightarrow \text{reduced} \\ B = -A \overset{\delta}{\to} A < C, B = A \Rightarrow \text{reduced} \\ |B| > A \text{ (need to go to } \beta \text{ or } \gamma) \end{cases}$$

In (β), $k = [[\frac{a-b}{2a}]] \Rightarrow \frac{a-b}{2a} - 1 \le k < \frac{a-b}{2a} \Rightarrow -a \le b + 2ka < a$

So, $a \to A$, $-A \le B < A$.

In (γ), $k = [[\frac{a+b}{2a}]] \Rightarrow \frac{a+b}{2a} - 1 \le k < \frac{a+b}{2a} \Rightarrow -a < b - 2ka \le a$

So, $a \to A$, $-A < B \leq A$.

We will demonstrate $f \in (2)$ $(a = c, b < -a)$ ($f \in (5)$ with (β) and $f \in (4)$ or (7) with (γ) are entirely analogous).

$$f \in (2)\ (a = c, b < -a) \stackrel{\beta}{\to} \begin{cases} A < C, -A < B < A \Rightarrow \text{reduced} \\ A < C, B = -A \stackrel{\delta}{\to} A < C, B = A \Rightarrow \text{reduced} \\ A = C, 0 \leq B < A \Rightarrow \text{reduced} \\ A = C, -A \leq B < 0 \stackrel{\alpha}{\to} A = C, 0 < B \leq A \Rightarrow \text{reduced} \\ A > C, -A \leq B < A \stackrel{\alpha}{\to} A < C \begin{cases} -A < B \leq A \Rightarrow \text{reduced} \\ B = -A \stackrel{\delta}{\to} A < C, B = A \Rightarrow \text{reduced} \\ \text{otherwise, } |B| > A \text{ and we are back} \\ \text{to apply } \beta \text{ or } \gamma \end{cases} \end{cases}$$

Each time we get to a possible $A > C$ (and then apply α), if not reduced we end up with $A < C, |B| > A$, but now A is strictly less than its predecessor. Also, $0 \leq |B| \leq A$ after each application of β or γ. Therefore, if f not already reduced, $|B|$ will eventually equal 0 after a finite number of steps, in which case f is either reduced or reduced after one more application of α.

Therefore, f gets reduced after a finite number of steps in all cases.

(2)-(7) mathematica programs attached

(7)

$p \equiv 1 (\text{mod } 4)$

Just to summarize the theory of infinite descent for two squares, which is very similar to the case of four squares but simpler:

Since $\left(\frac{-1}{p}\right) = 1$, $\exists\ x \in [0, p-1) \ni x^2 \equiv -1 (\text{mod } p)$.

$\therefore \exists\ m \ni mp = x^2 + 1$. Furthermore, $m \in [1, p-1]$ as in four square case. Find an m (by brute force).

The rest is identical to the case of four squares, but we do not have to worry about pairing up like parity addends when m is even, since m even implies both addends are odd or both are even.