Формы Маркова

Определение 1. *Квадратичной формой* над $\mathbb{Z}$ называется выражение вида

$$F(x, y) = ax^2 + bxy + cy^2,$$

где x и y — переменные, принимающие только целые значения, и $a, b, c \in \mathbb{Z}$. Квадратичная форма *неразложима* над $\mathbb{Z}$, если ее нельзя представить в виде

$$F(x, y) = (\alpha x + \beta y)(\gamma x + \delta y)$$

с целыми $\alpha, \beta, \gamma, \delta$. *Дискриминантом* формы $F(x, y)$ называется выражение $D_F = b^2 - 4ac$. Форма F называется *вполне вещественная*, если $D_F > 0$.

Определение 2. Замена переменных

$$x = \alpha u + \gamma v, \qquad y = \beta u + \delta v$$

называется *допустимой*, если $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ и переменные u и v выражаются через x и y с целыми коэффициентами, т. е.

$$u = \alpha' x + \gamma' y, \qquad v = \beta' x + \delta' y$$

с $\alpha', \beta', \gamma', \delta' \in \mathbb{Z}$.

Упражнение 3. Проверьте, что замена переменных

$$x = \alpha u + \gamma v, \qquad y = \beta u + \delta v$$

допустима тогда и только тогда, когда $\alpha\delta - \beta\gamma = \pm 1$.

Определение 4. Назовем квадратичные формы $F(x, y)$ и $F'(u, v)$ *эквивалентными* ($F \sim F'$), если они получаются друг из друга допустимой заменой переменных.

Для каждой формы $F(x, y)$ положим по определению

$$m_F = \min_{(x,y)\in\mathbb{Z}^2\setminus\{0\}} |F(x, y)| \quad \text{и} \quad \mu_F = \frac{m}{\sqrt{D}}.$$

Наша цель — доказать самую простую часть теоремы Маркова, которая звучит следующим образом:

Теорема (Маркова) 5. Существует такая квадратичная форма $F_1(x, y)$ над $\mathbb{Z}$, что

$$\frac{1}{\sqrt{5}} = \mu_{F_1} \geq \mu_F$$

для любой неразложимой вполне вещественной квадратичной формы F. Причем, если $\mu_F = \mu_{F_1}$, то $F \sim \pm F_1$.

Идея доказательства состоит в том, чтобы найти форму F_1 среди тех, у которых $m_F = 1$, и показать, что если $m_F \geq 2$, то $\mu_F < \frac{1}{\sqrt{5}}$.

Доказательство. Заметим, что в результате замены переменных $x = \alpha u + \gamma v$, $y = \beta u + \delta v$ форма $ax^2 + bxy + cy^2$ примет вид

$$\begin{aligned} F(u, v) = {} & u^2(a\alpha^2 + b\alpha\beta + c\beta^2) + \\ & + uv(2a\alpha\gamma + b(\alpha\delta + \beta\gamma) + 2c\beta\delta) + \\ & + v^2(a\gamma^2 + b\gamma\delta + c\delta^2). \end{aligned} \tag{1}$$

Замечание 6. Пусть $m_F = m$. Тогда существует допустимая замена переменных, после которой форма $\pm F$ запишется как
$$F(u,v) = mu + b'uv + c'.$$

Действительно, пусть
$$F(\alpha,\beta) = a\alpha^2 + b\alpha\beta + c\beta^2 = \pm m. \tag{2}$$
Поскольку $F(dx,dy) = d^2F(x,y)$, то в случае $m = 0$ можно считать, что α и β взаимно просты. Если же $m > 0$, то α и β — уже взаимно просты (m — наименьшее значение $|F(x,y)|$).

Для взаимно простых α и β найдутся такие целые числа δ и γ, что $\alpha\delta - \beta\gamma = 1$. Значит, замена переменных
$$x = \alpha u + \gamma v, \qquad y = \beta u + \delta v$$
допустима, причем (см. формулы (1) и (2))
$$F(u,v) = \pm mu^2 + b'uv + c'v^2.$$
Более того, так как нас интересуют формы с точностью до умножения на -1, то можно считать, что
$$F(u,v) = mu^2 + b'uv + c'v^2, \qquad m = \min|F(x,u)|.$$

Следствие 7. Если $m_F = 0$, то форма разложима над $\mathbb{Z}$.

Лемма 8. Неразложимая над $\mathbb{Z}$ форма F с $m_F = m$ после подходящей допустимой замены координат принимает вид:
$$F(u,v) = mu^2 + ruv + dv^2, \qquad m = m_F > 0, \quad |r| \le m. \tag{3}$$

Доказательство. Благодаря замечанию 6 можно считать, что наша форма имеет вид
$$F(x,y) = mx^2 + bxy + cy^2.$$
(Мы воспользовались старыми обозначениями для подходящих координат.)

Разделим b на $2m$ с остатком: $b = 2md + r$, $|r| \le m$ и сделаем замену переменных:
$$x = u - dv, \qquad y = v.$$
Тогда ввиду (1), в новых координатах наша форма приобретет вид:
$$F(u,v) = mu^2 + ruv + dv^{\cdot}$$

Предложение 9. Если F — неразложимая вполне вещественная форма над $\mathbb{Z}$ с $m_F = 1$, то $\mu_F \le \frac{1}{\sqrt{5}}$. Более того, все неразложимые вполне вещественные формы над $\mathbb{Z}$ с $\mu_F = \frac{1}{\sqrt{5}}$ эквивалентны форме $F_1(x,y) = x^2 + xy - y^2$.

Доказательство. Рассмотрим форму F с $m_F = 1$. Тогда она эквивалентна форме
$$x^2 + bxy + cy^2,$$
где $|b| \le 1$. Причем $\mu_F = \frac{1}{\sqrt{D_F}}$.

Если $b = 0$, то $D_F = -4c$. Наша форма вполне вещественна, значит, $c < 0$ и $D_F = 4|c|$. При этом $D_F < 5$ только если $-c = 1$, т.е. $F(x,y) = x^2 - y^2$ — разложима.

Если $b = \pm 1$, то $D_F = 1 - 4c$ и опять получаем, что $c \ge 0$. Но если $c = 0$, то $m_F = 0$, что противоречит предположению. Поэтому $|c| \ge 1$ и минимальное значение D_F — это 5.

Осталось доказать последнее утверждение:

Предложение. 10. Пусть F — неразложимая вполне вещественная форма над $\mathbb{Z}$ с $m_F = m \geq 2$. Тогда $\mu_F \leq \frac{1}{\sqrt{5}}$. Причем, если $\mu_F = \frac{1}{\sqrt{5}}$, то $F \sim mF_1$, где форма $F_1(x,y) = x^2 + xy - y^2$.

Доказательство. Предположим, что найдется форма F с $m_F = m \geq 2$ и $\mu_F \geq \frac{1}{\sqrt{5}}$. Мы знаем, что форма F эквивалентна форме вида

$$mx^2 + bxy + cy^2, \qquad |b| \leq m. \tag{4}$$

Ее однородный минимум вычисляется как

$$\mu_F = \frac{m}{\sqrt{D_F}} = \frac{m}{\sqrt{b^2 - 4mc}}.$$

Поэтому

$$\mu_F \geq \frac{1}{\sqrt{5}} \qquad \Leftrightarrow \qquad D_F = b^2 - 4mc \leq 5m^2. \tag{5}$$

Мы хотим показать, что если последнее неравенство выполнено, то модуль одно из значений: $F(1,1)$ или $F(1,-1)$ будет меньше m (что противоречит предположению: $m_F = m$), либо равен m (что даст нам форму, эквивалентную mF_1).

Заметим, что $c = F(0,1)$ и поэтому $|c| \geq m$. Кроме того, $0 < D_F = b^2 - 4mc \leq m^2 - 4mc$ (т. к. F — вполне вещественная и $|b| \leq m$). Отсюда $c \leq m/4$, что вместе с неравенством $|c| \geq m$ дает: $c \leq -m$.

Обозначим $-c = m + \alpha$ $(\alpha \geq 0)$. Если $\alpha > m/4$, то

$$D_F = b^2 - 4mc > b^2 + 4m\left(m + \frac{m}{4}\right) \geq 5m^2.$$

Поэтому, учитывая неравенство (5), получаем оценку:

$$0 \leq \alpha \leq \frac{m}{4}. \tag{6}$$

Кроме того, из неравенства (4) можно записать:

$$|b| = m - \beta, \qquad 0 \leq \beta \leq m. \tag{7}$$

Пусть $b \leq 0$. Тогда

$$F(1,-1) = m + |b| + c = m + m - \beta - m - \alpha = m - \beta - \alpha.$$

Значит, $|F(1,-1)| \leq m$, причем $|F(1,-1)| = m \Leftrightarrow \alpha = \beta = 0$ и

$$F(x,y) = mx^2 - mxy - my^2 \sim mF_1(x,y).$$

Пусть $b > 0$. Вычислим

$$F(1,1) = m + b + c = m + m - \beta - m - \alpha = m - \beta - \alpha.$$

Опять $|F(1,1)| \leq m$, причем $|F(1,1)| = m$ только если $\alpha = \beta = 0$ и

$$F(x,y) = mx^2 + mxy - my^2 \sim mF_1(x,y).$$