Клетчатые фигуры, квадратичные формы и class number

Листок 2

Теорема Ферма-Эйлера о сумме двух квадратов. Уравнение $x^2 + y^2 = p$, где $p = 4k + 1$ — простое, имеет решение в натуральных числах.

Шахматное доказательство (L. Larson). Назовем расстановку p ферзей, попарно не бьющих друг друга, на доске $p \times p$ *регулярной*, если она порождена вектором (s, t) с координатами из $\mathbb{Z}_p$, т.е. ферзи стоят в клетках $(a + rs, b + rt) \in \mathbb{Z}_p \times \mathbb{Z}_p$, $r = 0, 1, 2, ..., p - 1$. Для любой регулярной расстановки найдется порождающий вектор вида $(d, 1)$, где d — разность между координатами занятых клеток в первом и нулевом рядах.

Оценим число различных регулярных расстановок (без учета поворотов и отражений). В нижнем ряду может быть занята любая из p клеток. При любом d, отличном от 0 (по модулю p) ферзи не бьют друг друга по вертикали. Ферзи бьют друг друга по диагонали, если $rd \equiv \pm r \pmod p$, или $d \equiv \pm 1$. Для того, чтобы некоторому $d \in \mathbb{Z}_p$ соответствовала регулярная расстановка ферзей, попарно не бьющих друг друга, необходимо и достаточно, чтобы $d \not\equiv 0$, $d \not\equiv \pm 1 \pmod p$, т.е. допустимыми являются $p - 3$ значений: $d = 2, 3, ..., p - 2$. Значит, всего существует $p(p - 3)$ регулярных расстановок.

Шахматная доска имеет 8 симметрий: тождественное преобразование, повороты на 90°, 180°, 270°, отражения относительно диагоналей и прямых, соединяющих середины противоположных сторон. Правильная расстановка ферзей не переходит в себя при отражениях. Применяя симметрии доски, из одной расстановки можно получить 2 (если расстановка переходит в себя при повороте на 90°, 4 (если расстановка центрально симметрична, но не переходит в себя при повороте на 90°) или 8 (если расстановка не обладает нетривиальными симметриями). Обозначим число расстановок первого, второго и третьего типа l, m, n соответственно. Тогда имеем

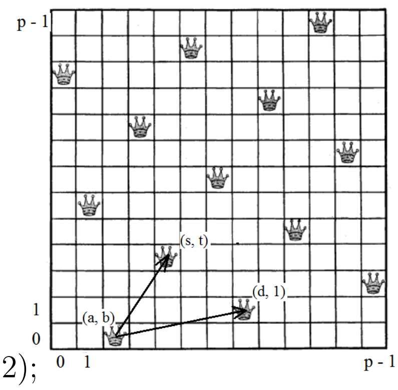

Рис. 1: .

$$2l + 4m + 8n = p(p - 3) = (4k + 1)(4k - 2);$$

$$2l + 4m + 8n \equiv 2 \pmod 4.$$

Отсюда $l > 0$, т.е. существует регулярная расстановка ферзей, переходящая в себя при повороте на 90°.

В этой расстановке занята центральная клетка (в противном случае число ферзей делилось бы на 4). Заполним бесконечную плоскость копиями доски с расставленными ферзями и соединим центр каждой занятой клетки с центрами четырех ближайших занятых клеток. Получим разбиение плоскости на квадраты площади $S = x^2 + y^2$, где (x, y) — координаты вектора с концами в центрах соседних занятых клеток.

В достаточно большом куске плоскости количество квадратов разбиения "почти совпадает" с числом ферзей, а один ферзь приходится на p клеток, поэтому $S = p$. Формализовать это рассуждение можно, например, следующим способом. Рассмотрим квадрат со стороной Np. Внутри него стоит $N^2 p$ ферзей. Сопоставим каждому ферзю квадрат разбиения, для которого ферзь стоит в верхнем углу. Пусть фигура D — объединение $N^2 p$ таких квадратов разбиения. Очевидно, D лежит внутри квадрата со стороной $(N + 1)p$ и содержит квадрат со стороной $(N - 1)p$. Отсюда имеем следующие оценки для S:

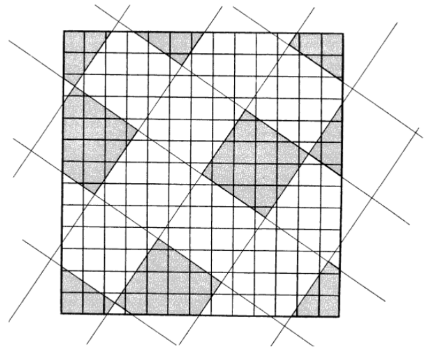

Рис. 2: .

$$\frac{(N-1)^2 p^2}{N^2 p} = p - \frac{2p}{N} + \frac{p}{N^2} < S$$

$$\frac{(N+1)^2 p^2}{N^2 p} = p + \frac{2p}{N} + \frac{p}{N^2} > S$$

При достаточно большом N единственным целым числом, удовлетворяющим обоим неравенствам, будет $S = p$. Значит, $x^2 + y^2 = p$, что и требовалось. $\square$

Действие $< f \circ g >$ на множестве "уголков". Рассмотрим граф G_p, вершины которого — решения уравнения $ab+cd = p$ в натуральных числах, удовлетворяющие либо условию $b > d$, либо $b = d = 1$ и $a > c$ (или соответствующие "уголки" и прямоугольники), а ребрами соединены те решения, которые переходят друг в друга при инволюциях f и g. К неподвижной точке инволюции присоединена петля.

Назовем геометрические фигуры, соответствующие решениям вида $(m, 1, p-m, 1)$, $m = 1, 2, \dots, \frac{p-1}{2}$ "столбцами".

Заявление 2. Для простого $p = 4k + 1$ граф G_p состоит из $k + 1$ цепочки, из которых $k - 1$ связывают два столбца; одна начинается со столбца и заканчивается в неподвижной точке f; одна начинается со столбца и заканчивается в неподвижной точке g.

Действие $< f \circ g >$ на множестве "ветряных мельниц". Полностью аналогично определим граф H_p, вершины которого — решения уравнения $b^2 + 4ac = p$ (или соответствующие геометрические фигуры). В этом случае граф имеет более сложную структуру.

Заявление 3. Для $p = 4k + 1$ граф H_p содержит цепочку, концы которой — (единственные) неподвижные точки f и g.

Интересно, что примерно для $3/4$ простых чисел вида $4k + 1$, не превосходящих 10^9, граф H_p состоит из одной цепочки. Т.е., начав с "креста", составленного из полосок ширины 1, и применяя по очереди f и g, мы переберем все p-клеточные "ветряные мельницы". Последней встретится та, которая состоит из 5 квадратов.

Квадратичные формы. Целая бинарная квадратичная форма (далее для краткости — просто квадратичная форма) — полином вида $ax^2 + bxy + cy^2$, где $a, b, c \in \mathbb{Z}$. Назовем квадратичные формы $P(x, y)$ и $Q(x, y)$ эквивалентными, если их множества значений (при подстановке всевозможных пар целых чисел) совпадают.

Заявление 4. Преобразования коэффициентов a, b, c из доказательства с "ветряными мельницами" переводят квадратичную форму $ax^2 + bxy + c^2$ в эквивалентную.

Задачи

1. Постройте граф H_{13}. (2 б)
2. Найдите "столбик", который соединен с неподвижной точкой f в G_{13}. (2 б)
3. Пусть $R(n)$ — число регулярных расстановок n ферзей на доске $n \times n$. Найдите $R(p_1 p_2)$, где p_1, p_2 — различные простые числа. (3 б)
4. Докажите, что если p, q взаимно просты, то $R(pq) = R(p)R(q)$. (3 б)
5. Можно ли провести по аналогии "шахматное" доказательство разрешимости уравнения $x^2 + y^2 = p_1 p_2$, если p_1, p_2 — простые числа вида $4k + 1$? (2 б)
6. Докажите Заявление 2. (5 б)
7. Докажите, что в графе G_p неподвижная точка g (решение исходного уравнения) соединена со столбцом $(m, 1, p - m, 1)$, для которого $m^2 \equiv -1 \pmod p$. (7 б)
8. Найдите с помощью компьютера все простые числа вида $4k + 1$ до 10^5, для которых граф H_p содержит цикл. (7 б)
9. Докажите, что если $p = 16k^2 + 1$, $k > 1$, то H_p содержит цикл. (5 б)
10. Докажите, что преобразование координат $x' = kx + y$; $y' = x$ переводит квадратичную форму в эквивалентную. (2 б)
11. Пусть $P(x)$ и $Q(x)$ — многочлены нечетной степени. Докажите, что если $P(\mathbb{Z}) = Q(\mathbb{Z})$ (т.е. совпадают множества значений в целых точках), то $P(x) = Q(\pm x + k)$, где k — некоторое целое число. (5 б)