Неделимость числа классов идеалов вещественного квадратичного поля

Петр Кучерявый

Факультет математики НИУ ВШЭ

11 февраля, 2025

В 1850 году Куммер ввёл понятие регулярного простого числа и доказал, что $x^p + y^p = z^p$ не имеет нетривиальных решений в целых числах, если p регулярное.
Число называется регулярным, если p не делит число классов кругового поля $\mathbb{Q}(\zeta_p)$, где ζ_p- примитивный корень степени p из 1.
Регулярность в таком рассуждении используется так. Пусть мы знаем, что $a = I^p$, где a – главный идеал. Тогда можно сделать вывод, что I также главный, если число классов не делится на p.
Гипотеза Зигеля утверждает, что вероятность того, что простое регулярное равно $e^{-1/2} \approx 0.6$. Доказано, что существует бесконечно много иррегулярных простых, но не известно, существует ли бесконечно много регулярных простых.

Пусть D – фундаментальный дискриминант, то есть либо $D \equiv 1 \pmod 4$ и D свободно от квадратов, либо $D = 4m$, где $m \equiv 2$ или $3 \pmod 4$ и m свободно от квадратов.
Обозначим $h(D)$ – число классов идеалов поля $\mathbb{Q}(\sqrt{D})$.
Зафиксируем простое число p и зададимся вопросом, как часто $p|h(D)$.
Для $p = 2$ этот вопрос решил ещё Гаусс.

Теорема

$h(D)$ нечётное если D простое или произведение двух отрицательных простых дискриминантов.

См, например, книгу Franz Lemmermeyer "Reciprocity Laws"(Genus theory).

Эвристика Коэна-Ленстры даёт различные предсказания про структуру группы классов. Например, что $\sim 97.7575...\%$ мнимоквадратичных полей имеет циклическую нечетную часть группу классов.

Гипотеза 1

Пусть p – нечетное простое.
Вероятность, что $p \nmid h(-D)$ для отрицательного фундаментального дискриминанта равна

$$\prod_{k=1}^{\infty}(1-p^{-k}) = 1 - \frac{1}{p} - \frac{1}{p^2} + \frac{1}{p^5} + \dots$$

Вероятность, что $p \nmid h(D)$ для положительного фундаментального дискриминанта равна

$$\left(\frac{p}{p-1}\right)\prod_{k=1}^{\infty}(1-p^{-k}) = 1 - \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4} + \dots$$

Обозначим $h^*(D)$ количество элементов в группе классов, которые в степени 3 дают единицу группы классов.

Теорема (Davenport-Heilbronn, 1971)

$$\lim_{X\to\infty} \frac{\sum_{-X<-D<0} h^*(-D)}{\sum_{-X<-D<0} 1} = 2.$$

Отсюда для любого $\varepsilon > 0$ для достаточно большого X

$$\frac{|\{-X < -D < 0 : 3 \nmid h(-D)\}|}{|\{-X < -D < 0\}|} \geq \frac{1}{2} - \varepsilon.$$

Эвристика Коэна-Ленстры предсказывает $\approx 1/2 + 0.06\ldots$.

Теорема (Davenport-Heilbronn, 1971)

$$\lim_{X\to\infty} \frac{\sum_{0<D<X} h^*(D)}{\sum_{0<D<X} 1} = \frac{4}{3}.$$

Отсюда для любого $\varepsilon > 0$ для достаточно большого X

$$\frac{|\{0 < D < X : 3 \nmid h(D)\}|}{|\{0 < D < X\}|} \geq \frac{5}{6} - \varepsilon.$$

Эвристика Коэна-Ленстры предсказывает $\approx 5/6 + 0.0068\ldots$.

Теорема (Ono-Kohnen, 1999)

Пусть простое $p > 3$ и $\varepsilon > 0$. Тогда для достаточно большого $X > 0$

$$|\{-X < -D < 0 : p \nmid h(-D)\}| \geq \left(\frac{2(l-2)}{\sqrt{3}(l-1)} - \varepsilon \right) \frac{\sqrt{X}}{\log X}.$$

Теорема 1 (Ono-Byeon, 2003)

Пусть простое $p > 3$. Тогда

$$\left| \left\{ 0 < D < X : p \nmid h(D),\ p|D,\ \left| \frac{R_p(D)}{\sqrt{D}} \right|_p = 1 \right\} \right| \gg_p \frac{\sqrt{X}}{\log X}.$$

Доказательство теоремы использует свойства p-адической L-функции, которую мы сейчас определим. См. Lawrence C. Washington "Introduction to Cyclotomic fields".

Обозначим $|\cdot|$ – p-адическую норму. Она продолжается однозначно на $\overline{\mathbb{Q}}_p$. Отнормируем её так, чтобы $|p| = 1/p$. $\overline{\mathbb{Q}}_p$ не полно. Пополнение $\overline{\mathbb{Q}}_p$ будем обозначать $\mathbb{C}_p$, которое уже оказывается алгебраически замкнутым. $\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$ имеет радиус сходимости $p^{-1/(p-1)}$. Определим $\log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} X^n}{n}$. У этого ряда радиус сходимости 1.

Предложение 1 (логарифм Ивасавы)

Существует единственное продолжение $\log_p(x)$ *на всё* $\mathbb{C}_p^*$ *такое, что* $\log_p(xy) = \log_p(x) + \log_p(y)$ *для всех* $x, y \in \mathbb{C}_p^*$ *и* $\log_p(p) = 0$.

Доказательство:
Зафиксируем $p^{\mathbb{Q}}$ как подгруппу $\mathbb{C}_p^*$. Для любого $\alpha \in \mathbb{C}_p^*$ существует единственное p^r, что $|\alpha p^{-r}| = 1$. Обозначим W группу корней из единицы порядка взаимнопростого с p. Пусть $\beta \in \mathbb{C}_p^*$ и $|\beta| = 1$. Выберем $\beta_1 \in \overline{\mathbb{Q}}_p$ близкое к β. Пусть P – идеал лежащий над p в $\mathbb{Q}_p(\beta_1)/\mathbb{Q}_p$. β_1 тогда сравнимо по модулю P с некоторым элементом $(\mathcal{O}/P)^*$, то есть с корнем из 1. С помощью Леммы Гензеля его можно поднять до $u \in W$, что $|\beta_1 - u| < 1$, а значит $|\beta - u| < 1$.

Обозначим $U_1 = \{x \in \mathbb{C}_p : |x-1| < 1\}$. Докажем, что $W \cap U_1 = \{1\}$. Пусть $u \in W \cap U_1, u \neq 1$. Если $u^n = 1$, то $|u^k - 1| < 1$ для любого k. Значит $|n| = |\sum_{k=0}^{n-1} u^k - n| < 1$ – противоречие, потому что $(n,p) = 1$. Доказали, что $\mathbb{C}_p^* = p^{\mathbb{Q}} \times W \times U_1$. Если $u^n = 1$, то с необходимостью $\log_p(u) = \log_p(u^n)/n = 0$. Аналогично $\log_p(p^r) = 0$. Значит однозначно получаем для $\alpha = p^r u x \in \mathbb{C}_p^*$, $\log_p(\alpha) = \log_p(x)$. $\square$
Положим $q = p$ если $p > 2$ и $q = 4$ для $p = 2$. Для $a \in \mathbb{Z}_p, p \nmid a$ (по Лемме Гензеля) существует корень степени $\varphi(q)$ из 1, что $a \equiv \omega(a) \pmod{q}$. ω называется характером Тейхмюллера. Обозначим $\langle a \rangle = \omega(a)^{-1} a$. Имеем $\langle a \rangle \equiv 1 \pmod{q}$ и $\log_p(a) = \log_p(\langle a \rangle)$.

Предложение 2 (Свойства логарифма)

1. *Если* $|x| < p^{-1/(p-1)}$, *то* $|\log_p(1+x)| = |x|$ *и если* $|x| \leq p^{-1/(p-1)}$, *то* $|\log_p(1+x)| \leq |x|$.
2. $\log_p x = 0 \Leftrightarrow x \in p^{\mathbb{Q}} \times W \times \{1\}$.
3. *Если* $|x| < p^{-1/(p-1)}$, *то* $\log_p \exp(x) = x$, $\exp \log_p(1+x) = 1+x$.

Пусть $a \in \mathbb{Z}_p, p \nmid a$. Определим

$$\langle a \rangle^x = \exp(x \log_p \langle a \rangle) = \exp(x \log_p a)$$

Так как $|\log_p \langle a \rangle| \leq |\langle a \rangle - 1| \leq |q| = 1/q$, этот ряд сходится при $|x| < qp^{-1/(p-1)} > 1$. В частности можно проверить, что $\langle a \rangle^n$ имеет обычное определение для $n \in \mathbb{Z}$.
Как всегда

$$\binom{X}{n} = \frac{X(X-1)\dots(X-n+1)}{n!}.$$

$\binom{X}{n}$ переводит $\mathbb{Z}$ в $\mathbb{Z}$, а значит $\mathbb{Z}_p$ в $\mathbb{Z}_p$.

Теорема (Kurt Mahler, 1958)

Положим $(\Delta f)(x) = f(x+1) - f(x)$. Функция f из $\mathbb{Z}_p$ в $\mathbb{Q}_p$ непрерывна тогда и только тогда, когда

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n}, \qquad a_n \to 0$$

$$a_n = (\Delta^n f)(0) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k).$$

Предложение 3

Пусть $r < p^{-1/(p-1)} < 1$ *и*

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n}$$

и $|a_n| \leq Mr^n$ *для некоторого* M. *Тогда* $f(X)$ *может быть выражена, как степенной ряд с радиусом сходимости не меньше* $R = (rp^{1/(p-1)})^{-1} > 1$.

Доказательство: положим $P_i(X) = \sum_{n \leq i} a_n \binom{X}{n} = \sum_{n \leq i} a_{n,i} X^n$. Тогда $|a_{n,i}| \leq \max_{j \geq n} \left|\frac{a_j}{j!}\right| \leq MR^{-n}$. Также $|a_{n,i} - a_{n,i+k}| \leq MR^{-(i+1)}$. Значит $a_{n,i}$ – последовательность Коши и существует $a_{n,0} = \lim_{i \to \infty} a_{n,i}$, $|a_{n,0}| \leq MR^{-n}$. Положим $P_0(X) = \sum a_{n,0} X^n$. Это искомый ряд для f, так как если $|X| < R$, то

$$\left| \sum_{n \geq n_0} a_{n,i} X^n \right| \leq \max_{n \leq n_0} MR^{-n} |X|^n \to 0 \quad \text{при} \quad n_0 \to \infty.$$

Функцию $\langle a\rangle^s = \exp(s \log_p \langle a\rangle)$ можно разложить в биномиальный ряд

$$(1 + \langle a\rangle - 1)^s = \sum_{n=0}^{\infty} \binom{s}{n} (\langle a\rangle - 1)^n.$$

Так как $|\langle a\rangle - 1| \leq q^{-1}$, можно взять $r = q^{-1}$ и по Предложению 3 радиус сходимости не меньше $qp^{-1/(p-1)}$. Биномиальный ряд совпадает с изначальной функцией, так как они обе аналитичны по s и совпадают на всём $\mathbb{Z}$, для которого 0 является предельной точкой.

———————

Напоминание про числа Бернулли

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, \qquad \frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}$$

Пусть χ – характер Дирихле с кондуктором f. Определим обобщенные числа Бернулли.

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}$$

Так, например $\sum_{n=0}^{\infty} B_{n,1} \frac{t^n}{n!} = \frac{te^t}{e^t-1} = \frac{t}{e^t-1} + t$. $B_{1,1} = 1/2, B_1 = -1/2$.

Предложение 4

Пусть $f|F$. Тогда

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right), \qquad B_n(x) = \sum_{i=0}^{n} \binom{n}{i} B_i x^{n-i}.$$

Введём $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, $(\mathrm{Re}(s) > 1)$, и дзета-функцию Гурвица $\zeta(s,b) = \sum_{n=0}^{\infty} \frac{1}{(n+b)^s}$, $(\mathrm{Re}(s) > 1)$.

Теорема

$L(1-n,\chi) = -B_{n,\chi}/n, n \geq 1$. И более общим образом,
$\zeta(1-n,b) = -B_n(b)/n, 0 < b \leq 1$.

Возможное доказательство: рассмотреть интеграл $\frac{ze^{(1-b)z}}{e^z-1} z^{s-2}\, dz$ по контуру Ганкеля (уходящему в $+\infty$). Для $\mathrm{Re}(s) > 0$ получаем выражение через $\zeta(s,b)$. При $s = 1-n$ сокращаются интегралы вдоль вещественной оси сверху и снизу и вклад даёт интеграл по малекой окружности вокруг 0.

Положим $H(s,a,F)=\sum_{\substack{m\equiv a(F)\\ m>0}} m^{-s}=\sum_{n=0}^{\infty}\frac{1}{(a+nF)^s}=F^{-s}\zeta\left(s,\frac{a}{F}\right)$, где $s\in\mathbb{C}$. Тогда

$$H(1-n,a,F)=-\frac{F^{n-1}B_n(a/F)}{n}\in\mathbb{Q},\quad n\geq 1,$$

и у H простой полюс в $s=1$ с вычетом $1/F$.

Предложение 5

Пусть $q|F$ и $p\nmid a$. Тогда существует p-адическая мероморфная функция $H_p(s,a,F)$ на $\{s\in\mathbb{C}_p:|s|<qp^{-1/(p-1)}>1\}$, такая что

$$H_p(1-n,a,F)=\omega^{-n}(a)H(1-n,a,F),\quad n\geq 1.$$

В частности, если $\varphi(q)|n$, то $H_p(1-n,a,F)=H(1-n,a,F)$. Функция H_p аналитическаая кроме простого полюса в $s=1$ с вычетом $1/F$.

Доказательство: положим

$$H_p(s,a,F)=\frac{1}{s-1}\frac{1}{F}\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j.$$

Пользуясь Предложением 4 и предполагая сходимость:

$$H_p(1-n,a,F) = \frac{-1}{nF}\langle a\rangle^n \sum_{j=0}^{n} \binom{n}{j} (B_j) \left(\frac{F}{a}\right)^j =$$

$$-\frac{F^{n-1}\omega^{-n}(a)}{n} B_n\left(\frac{a}{F}\right) = \omega^{-n}(a) H(1-n,a,F).$$

Сходимость следует из Предложения 3, поскольку $|(B_j)(F/a)^j| \leq p|q|^j = p/q^j$. Можно взять $r = 1/q$ в Предложении 3. Здесь мы воспользовались

Предложение 6 (фон Штаудт-Клауссен)

$$B_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z},$$

В частности $|B_n|_p \leq p$.

Теперь мы готовы определить p-адическую L-функцию Куботы-Леопольда.

Теорема 2

Пусть χ характер Дирихле с кондуктором f и $qf|F$. Тогда существует p-адическая мероморфная (аналитичная при $\chi \neq 1$) функция $L_p(s,\chi)$ на $\{s \in \mathbb{C}_p : |s| < qp^{-1/(p-1)}\}$ такая что

$$L_p(1-n,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \quad n \geq 1.$$

Если $\chi = 1$, то $L(s,\chi)$ имеет простой полюс в $s = 1$ с вычетом $(1-1/p)$.
Имеет место формула

$$L_p(s,\chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j.$$

Заметим, что если $\chi = \omega^n \neq 1$, то $\chi\omega^{-n}(p) = 1$, хотя $\chi(p) = \omega^n(p) = 0$.
Теорема выводится из того, что

$$L_p(s,\chi) = \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(s,a,F).$$

Множитель $(1 - \chi\omega^{-n}(p)p^{n-1})$ это множитель в разложении Эйлера $L(s, \chi\omega^{-n})$. Если $n \equiv 0 \pmod{\varphi(q)}$, то $L_p(1-n, \chi) = (1 - \chi(p)p^{n-1})L(1-n, \chi)$.

Предложение 7

Пусть $\chi \neq 1$ и $pq \nmid f_\chi$. Тогда

$$L_p(s, \chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \dots$$

с $|a_0| \leq 1$ и $p|a_i$ при $i \geq 1$. (так как радиус сходимости этого ряда больше 1, мы априори знаем, что $a_i \to 0$ при $i \to \infty$).

Выберем F как в Теореме 2, такое что $q|F$, но $pq \nmid F$. Тогда

$$\left| \frac{B_j}{j!} \frac{F^{j-1}}{a^j} \right| \leq p^{j/(p-1)} \cdot p \cdot \frac{1}{q^{j-1}} \leq \frac{1}{q} \quad (j \geq 6).$$

Таким образом мы можем обрезать сумму до первых нескольких членов и проверить утверждение.

Следствие 1

Пусть $\chi \neq 1, pq \nmid f$. Пусть $m, n \in \mathbb{Z}$. Тогда $L_p(m, \chi) \in \mathbb{Z}_p$ и

$$L_p(m, \chi) \equiv L_p(n, \chi) \pmod{p}$$

Пусть X – конечная группа характеров Дирихле и n – НОК их кондукторов. Тогда на X можно смотреть как на харакеры группы $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Пусть H – пересечение ядер характеров из X и K – поле, неподвижное под действием H. Тогда X это в точности множество гомоморфизмов $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^*$.

Теорема (p-адическая формула числа классов)

Пусть K – абсолютно вещественное (все вложения вещественные) абелево числовое поле степени n, соответствующее группе X характеров Дирихле. Тогда

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{d(K)}} = \prod_{\substack{\chi\in X\\ \chi\neq 1}} \left(1-\frac{\chi(p)}{p}\right)^{-1} L_p(1,\chi).$$

Зафиксируем вложение $\mathbb{C}_p$ в $\mathbb{C}$. p-адический регулятор определяется как обычный регулятор: если r_1 – количество вещественных вложений в $\mathbb{C}_p$, а r_2 – пар мнимых. $r = r_1 + r_2 - 1$ и $\varepsilon_1, \ldots, \varepsilon_r$ – базис единиц K. $\sigma_1, \ldots, \sigma_{r+1}$ – вложения K в $\mathbb{C}_p$, где из пары мнимых взяли только одно вложение. Положим $\delta_i = 1$, если σ_i вещественное и $\delta_i = 2$, если σ_i мнимое. Тогда

$$R_p(K) := \det(\delta_i \log_p(\sigma_i\varepsilon_j))_{1\le i,j\le r}.$$

Гипотеза 2 (Леопольд)

$R_p(K) \neq 0$ для всех числовых полей K.

Известно, что если $K/\mathbb{Q}$ абелево, то $R_p(K) \neq 0$.
Далее нам понадобится:

Предложение 8 (Коутс)

Пусть K – абсолютно вещественное абелево числовое поле. Если p не делит $\deg(K/\mathbb{Q})$, если существует только одно простое в K, лежащее над p и если индекс ветвления p не больше $p-1$, то

$$\left| \frac{R_p(K)}{\sqrt{d(K)}} \right|_p \leq 1.$$

Для доказательства Теоремы 1 понадобится некоторые сведения о модулярных формах полуцелого веса.
Определим $\epsilon_d = 1$ для $d \equiv 1 \pmod 4$ и $\epsilon_d = i$ для $d \equiv 3 \pmod 4$.
$\lambda \in \mathbb{Z}_{\geq 0}$.
$g \in M_{\lambda+1/2}(\Gamma_0(4N), \chi)$ если для всех $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4N)$

$$g\left(\frac{az+b}{cz+d}\right) = \chi(d)\left(\frac{c}{d}\right)^{2\lambda+1}\epsilon_d^{-1-2\lambda}(cz+d)^{\lambda+\frac{1}{2}}g(z).$$

Положим $\chi_D = \left(\frac{D}{\cdot}\right)$. Определим теперь ряд Коэна-Эйзенштейна.
Пусть $r \geq 2$. Если $(-1)^r N \not\equiv 0, 1 \pmod 4$, то положим $H(r, N) := 0$.
Если $N = 0$, то положим $H(r, 0) := \zeta(1-2r) = -\frac{B_{2r}}{2r}$. Если $N > 0$ и $Dn^2 = (-1)^r N$, где D – фундаментальный дискриминант, то определим

$$H(r, N) := L(1-r, \chi_D)\sum_{d|n}\mu(d)\chi_D(d)d^{r-1}\sigma_{2r-1}(n/d).$$

В частности для $D = (-1)^r N$, получим
$H(r, N) = L(1-r, \chi_D) = -\frac{B(r, \chi_D)}{r}$.
Если $(-1)^r N = n^2$, то

$$H(r, N) = \zeta(1-r)\sum_{d|n}\mu(d)d^{r-1}\sigma_{2r-1}(n/d).$$

Предложение 9 (Коэн, 1975)

Положим $H_r(z) := \sum_{N=0}^{\infty} H(r,N)q^N$. *Тогда для* $r \geq 2$

$$H_r(z) \in M_{r+\frac{1}{2}}(\Gamma_0(4)).$$

Доказательство состоит в том, что если положить

$$E_{r+\frac{1}{2}}(z) := \sum_{n>0\,\mathrm{odd},m} \left(\frac{m}{n}\right)\left(\frac{-4}{n}\right)^{-(r+\frac{1}{2})}(nz+m)^{-(r+\frac{1}{2})}$$

$$F_{r+\frac{1}{2}}(z) := E_{r+\frac{1}{2}}(-1/4z)z^{-(r+\frac{1}{2})}.$$

Тогда $E_{r+\frac{1}{2}}(z), F_{r+\frac{1}{2}}(z) \in M_{r+\frac{1}{2}}(\Gamma_0(4))$ и

$$H_r(z) = 2^{-(2r+1)}\zeta(1-2r)\left((1+i^{2r+1})E_{r+\frac{1}{2}}(z) + i^{2r+1}F_{r+\frac{1}{2}}(z)\right).$$

Лемма 1

Пусть $p > 3$ простое и D нечётный фундаментальный дискриминант взаимнопростой с p для которого $(-1)^{\frac{p-1}{2}} D > 0$. Положим $D_p := (-1)^{\frac{p-1}{2}} Dp$. Тогда $H(\frac{p-1}{2}, (-1)^{\frac{p-1}{2}} D)$ p-целое и

$$H\left(\frac{p-1}{2}, (-1)^{\frac{p-1}{2}} D\right) \equiv \frac{2h(D_p)R_p(D_p)}{\sqrt{D_p}} \pmod{p}.$$

Доказательство: По определению $H\left(\frac{p-1}{2}, (-1)^{\frac{p-1}{2}} D\right) = L(1 - \frac{p-1}{2}, \chi_D) = -\frac{2B_{\frac{p-1}{2}, \chi_D}}{p-1}$. Заметим, что $\chi_D = \chi_{D_p} \cdot \omega^{-\frac{p-1}{2}}$. Так как D_p – положительный фундаментальный дискриминант, то

$$L_p\left(1 - \frac{p-1}{2}, \chi_{D_p}\right) = -\frac{2B_{\frac{p-1}{2}, \chi_{D_p}\omega^{-\frac{p-1}{2}}}}{p-1} = H\left(\frac{p-1}{2}, (-1)^{\frac{p-1}{2}} D\right).$$

$$L_p\left(1 - \frac{p-1}{2}, \chi_{D_p}\right) \overset{p}{\equiv} L(1, \chi_{D_p}) = \frac{2h(D_p)R_p(D_p)}{\sqrt{D_p}}.$$

Лемма 2

Пусть $p > 3$ простое. Тогда существует целое $\alpha(p)$ взаимнопростое с p, такое что

$$\alpha(p)pH_{\frac{p-1}{2}}(z) \in \mathbb{Z}[[q]].$$

Предложение 10 (Карлитс, 1958)

Если f кондуктор χ и f степень простого p, то $B_{\chi,n}/n$ p'-целые для всех простых p' кроме возможно p и для всех простых, когда f имеет хотя бы два различных простых делителя. Если $f = p$, то $B_{\chi,n}/n$ целое если только не $\chi(g)g^n \not\equiv 1 \pmod{p}$, здесь g – первообразный корень по модулю p.

Набросок доказательства Леммы: из теоремы Карлитса следует, что единственные коэффициенты $H_{\frac{p-1}{2}}$, которые не обязательно p-целые, это $H(\frac{p-1}{2}, 0)$ и $H(\frac{p-1}{2}, pn^2)$.

$$H\left(\frac{p-1}{2}, 0\right) = \zeta(1-(p-1)) = -\frac{B_{p-1}}{p-1}$$

Пусть Ψ_p – Кронекеров характер для $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$.

$$H\left(\frac{p-1}{2},p\right)=L\left(1-\frac{p-1}{2},\Psi_p\right)=-\frac{2B_{\frac{p-1}{2},\Psi_p}}{p-1}$$

Утверждение Леммы теперь следует из того, что

$$\frac{H\left(\frac{p-1}{2},p\right)}{H\left(\frac{p-1}{2},0\right)}\equiv 2 \pmod p, \quad \sum_{d|n}\mu(d)\Psi_d(d)d^{\frac{p-3}{2}}\sigma_{p-2}(n/d)\equiv 1 \pmod p.$$

Кроме того видим, что можно подобрать $\alpha(p)$ так, чтобы

$$\alpha(p)pH_{\frac{p-1}{2}}(z)\equiv\theta_0(pz) \pmod p,$$

где $\theta_0(z)=\sum_{n\in\mathbb{Z}}q^{n^2}=1+2q+2q^4+\ldots\in M_{1/2}(\Gamma_0(4))$ $\square$.

Пусть $g(z)=\sum_{n\geq 0}c_nq^n$. Пусть ψ – характер Дирихле. Определим ψ-твист $g(z)$ так: $(g\otimes\psi)(z)=\sum_{n=0}^{\infty}\psi(n)c(n)q^n$.

Положим для $d > 0$

$$\left(\sum_{n\geq n_0} c(n)q^n\right) \mid V(d) := \sum_{n\geq n_0} c(n)q^{dn}$$

$$\left(\sum_{n\geq n_0} c(n)q^n\right) \mid U(d) := \sum_{n\geq n_0} c(dn)q^n$$

Предложение 11

Пусть $f(z) \in M_{\lambda+\frac{1}{2}}(\Gamma_0(4N), \chi)$. *Если* $d > 0$, *то*
$f(z) \mid V(d) \in M_{\lambda+\frac{1}{2}}\left(\Gamma_0(4Nd), \left(\frac{4d}{\cdot}\right)\chi\right)$.
Если $d|N$, *то* $f \mid U(d) \in M_{\lambda+\frac{1}{2}}\left(\Gamma_0(4N), \left(\frac{4d}{\cdot}\right)\chi\right)$.
Если ψ – *характер Дирихле с кондуктором* m, *то*
$(f \otimes \psi)(z) \in M_{\lambda+\frac{1}{2}}\left(\Gamma_0(4Nm^2), \chi\psi^2\right)$.

Нам также понадобится

Предложение 12 (Штурм)

Пусть $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_{\frac{k}{2}}(\Gamma_0(N), \chi)$ *и все коэффициенты* $a(n)$ *лежат в* $\mathcal{O}_K$ *(в кольце целых числового поля* K*). Пусть* $\mathfrak{m} \subset \mathcal{O}_k$ *идеал, такой что*

$$\mathrm{ord}_{\mathfrak{m}}(f) > \frac{k}{24}\left[\Gamma_0(1) : \Gamma_0(N)\right].$$

Тогда $\mathrm{ord}_{\mathfrak{m}}(f) = \infty$. *Здесь* $\mathrm{ord}_{\mathfrak{m}}(f) := \min\{n : a(n) \notin \mathfrak{m}\}$

Теорема 3 (Бён)

Если $p > 3$ *простое, то существует нечетный фундаментальный дискриминант* D_0 *взаимнопростой с* p*, такой что*

$$(-1)^{\frac{p-1}{2}} D_0 > 0, \qquad \left| B_{\frac{p-1}{2}, \chi_{D_0}} \right|_p = 1.$$

Теорема 1 следует из следующей теоремы:

Теорема 4

Если $p > 3$ простое, то существует арифметическая прогрессия $r_p \pmod{t_p}$ с $(r_p, t_p) = 1$ и константа $\kappa(p)$ такая что для любого простого $l \equiv r_p \pmod{t_p}$ существует натуральное $1 \leq d_l \leq \kappa(p)l$ для которого

i) $D_l := d_l lp$ *фундаментальный дискриминант*

ii) $h(D_l) \not\equiv 0 \pmod{p}$

iii) $\left| \frac{R_p(D_l)}{\sqrt{D_l}} \right|_p = 1$

Действительно, для всякого простого $l \equiv r_p \pmod{t_p}$ видим, что $D_l = d_l lp \leq \kappa(p) l^2 p$ – фундаментальный дискриминант с требуемыми свойствами. Осталось воспользоваться теоремой Дирихле о простых в арифметической прогрессии.

Возьмём $\alpha(p)$ как в Лемме 2. Определим $F_p(z) \in M_{\frac{p}{2}}(\Gamma_0(4p^2), \chi_0)$ так:

$$F_p(z) := \alpha(p) H_{\frac{p-1}{2}}(z) - \alpha(p) \left(H_{\frac{p-1}{2}} \mid U(p) \mid V(p) \right) = \alpha(p) \sum_{(n,p)=1} H\left(\frac{p-1}{2}, n\right) q^n.$$

Возьмём D_0 как в Теореме 3. Возьмём простое Q для которого $\left(\frac{D_0}{Q}\right) = -1$ и определим $G_p(z) \in M_{\frac{p}{2}}\left(\Gamma_0(4p^2Q^2), \chi_0\right)$ как

$$G_p(z) := F_p(z) \otimes \left(\frac{\cdot}{Q}\right) = \alpha(p) \sum_{(n,p)=1} \left(\frac{n}{Q}\right) H\left(\frac{p-1}{2}, n\right) q^n.$$

Наконец определим $\mathcal{G}(z) \in M_{\frac{p}{2}}\left(\Gamma_0(4p^2Q^2), \chi_0\right)$ как

$$\mathcal{G}(z) := \frac{G_p(z) \otimes \left(\frac{\cdot}{Q}\right) - G_p(z)}{2} = \alpha(p) \sum_{(n,p)=1,\, \left(\frac{n}{Q}\right)=-1} H\left(\frac{p-1}{2}, n\right) q^n.$$

Ясно, что $0 \not\equiv \mathcal{G}(z) \pmod{p}$, так как коэффциет при q^{D_0} не равен нулю по модулю p (по построению, здесь пользуемся Теоремой Бёна).

Также заметим, что все коэффициенты, которые были не p целые, то есть вида $H(\frac{p-1}{2}, 0), H(\frac{p-1}{2}, n^2), H(\frac{p-1}{2}, np)$ не входят в сумму. Таким образом все коэффициенты целые.
Для простого l рассмотрим $\mathcal{G} \mid U(l), \mathcal{G} \mid V(l) \in M_{\frac{p}{2}} \left(\Gamma_0(4p^2Q^4l), \left(\frac{4l}{\cdot}\right)\right)$

$$\mathcal{G} \mid U(l) = \sum_{n=1}^{\infty} u_{p,l}(n) q^n = \alpha(p) \sum_{(ln,p)=1,\, \left(\frac{ln}{Q}\right)=-1} H\left(\frac{p-1}{2}, ln\right) q^n$$

$$\mathcal{G} \mid V(l) = \sum_{n=1}^{\infty} v_{p,l}(n) q^n = \alpha(p) \sum_{(n,p)=1,\, \left(\frac{n}{Q}\right)=-1} H\left(\frac{p-1}{2}, n\right) q^{ln}$$

Положим $\kappa(p) := p^2Q^3(p+1)(Q+1)/4$. Так как $[\Gamma_0(1) : \Gamma_0(4p^2Q^4l)] = 6pQ^3(p+1)(Q+1)(l+1)$, то для достатоно большого l по Теореме Штурма, если для $g \in M_{\frac{p}{2}} \left(\Gamma_0(4p^2Q^4l), \left(\frac{4l}{\cdot}\right)\right)$ выполнено $\mathrm{ord}_p(g) > \kappa(p)l$, то $g(z) \equiv 0 \pmod{p}$.

Пусть $l \neq p$ простое для которого $\left(\frac{l}{Q}\right) = 1$. Если $\left(\frac{n}{Q}\right) \neq -1$ или $(n,p) \neq 1$, то $u_{pl}(nl) = v_{p,l}(nl) = 0$.
Если $\left(\frac{n}{Q}\right) = -1$, $(n,p) = 1$, то

$$u_{p,l}(nl) = \alpha(p) H\left(\frac{p-1}{2}, nl^2\right), \qquad v_{p,l}(nl) = \alpha(p) H\left(\frac{p-1}{2}, n\right).$$

Для достаточно большого такого l и всех $n \leq \kappa(p)$ находим

$$u_{p,l}(nl) = \alpha(p)(1 - \chi_{D_n}(l) l^{\frac{p-3}{2}} + l^{p-2}) H\left(\frac{p-1}{2}, n\right),$$

где D_n это фундаментальный дискриминант $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} n}\right)$.
Обозначим S_p множество D_n, для которых $n \leq \kappa(p)$, $\left(\frac{n}{Q}\right) = -1$, $(n,p) = 1$. Для остальных D_n для которых $n \leq \kappa(p)$ коэффициенты при $q^{D_n m^2}$ у $\mathcal{G}$ равны 0.

Определим прогрессию $r_p \pmod{t_p}$ условиями:
i) $(r_p, t_p) = 1$ и $p | t_p$
ii) $\chi_{D_n}(l) = 1$ для всякого $l \equiv r_p \pmod{t_p}$ и $D_n \in S_p$
iii) $\left(\frac{l}{Q}\right) = 1$ для всякого $l \equiv r_p \pmod{t_p}$
iv) $\left(\frac{r_p}{p}\right) = -1$.
Для всякого простого $l \equiv r_p \pmod{t_p}$ находим
$u_{p,l}(nl) \equiv (1 - r_p^{\frac{p-3}{2}} + r_p^{p-2}) v_{p,l}(nl) \pmod{p}$ для всех $n \leq \kappa(p)$.
Докажем от противного, что найдется такое $n \leq \kappa(p)l$, взаимнопростое с l для которого $u_{p,l}(n) = \alpha(p) H\left(\frac{p-2}{2}, nl\right) \not\equiv 0 \pmod{p}$. Предположим, что это не так.
Тогда по Теореме Штурма $\mathcal{G} \,|\, U(l) = (1 - r_p^{\frac{p-3}{2}} + r_p^{p-2}) \mathcal{G} \,|\, V(l) \pmod{p}$.
Для простого $l \equiv r_p \pmod{t_p}$ находим

$$u_{p,l}(D_0 l^3) \equiv \alpha(p)(1 - r_p^{\frac{p-3}{2}} - r_p^{\frac{p-5}{2}} + r_p^{p-2} + r_p^{p-3}) H\left(\frac{p-1}{2}, D_0\right) \pmod{p},$$

$$v_{p,l}(D_0 l^3) \equiv \alpha(p)(1 - r_p^{\frac{p-3}{2}} + r_p^{p-2}) H\left(\frac{p-1}{2}, D_0\right) \pmod{p}.$$

Поскольку из условия Теоремы Бёна $\left|\alpha(p) H\left(\frac{p-1}{2}, D_0\right)\right|_p = 1$, получаем $r_p^{p-3} \equiv r_p^{\frac{p-5}{2}} \pmod{p}$. Противоречие с тем, что $\left(\frac{r_p}{p}\right) = -1$.

Значит существует такое $1 \leq n \leq \kappa(p)l$, $(n, l) = 1$, для которого

$$u_{p,l}(n) = \alpha(p)H\left(\frac{p-1}{2}, nl\right) \not\equiv 0 \pmod{p}.$$

Из определения $H(r, N)$ и Леммы 1 видим, что существует фундаментальный дискриминант $D_l := d_l lp$, где $d_l \leq \kappa(p)l$ для которого

$$\frac{2h(D_l)R_p(D_l)}{\sqrt{D_l}} \not\equiv 0 \pmod{p}.$$

Но по Теореме Коутса $\left|\frac{R_p(D_l)}{\sqrt{D_l}}\right|_p \leq 1$. $\square$

Перейдём к доказательству теоремы Бёна. Мы хотим для заданного $p > 3$ найти такое D_0 взаимнопростое с p, что $(-1)^{\frac{p-1}{2}} D_0 > 0$ и $\left| B_{\frac{p-1}{2},\chi_{D_0}} \right|_p = 1$

Оказывается для $p \equiv 1 \pmod 4$ можно взять в качестве D_0 дискриминант $\mathbb{Q}(\sqrt{p-2})$. А если $p \equiv 3 \pmod 4$ дискриминант $\mathbb{Q}(\sqrt{-(p-4)})$. Ясно, что условие $(-1)^{\frac{p-1}{2}} D_0 > 0$ выполнено.

Мы знаем, что если положить $D_{0p} = (-1)^{\frac{p-1}{2}} p D_0$, то

$$-\frac{2B_{\frac{p-1}{2},\chi_{D_0}}}{p-1} \equiv \frac{2h(D_{0p})R_p(D_{0p})}{\sqrt{D_{0p}}} \pmod p.$$

Значит достаточно показать, что 1) $p \nmid h(D_{0p})$, 2) $\left| \frac{R_p(D_{0p})}{\sqrt{D_{0p}}} \right|_p = 1$.

Оценка Хуа говорит, что $L(1,\chi_D) < \frac{\log D}{2} + 1$. Так как $\varepsilon_D > \sqrt{D}/2$ из формулы числа классов $h(D) = \sqrt{D} L(1,\chi_D)/(2\log \varepsilon_D)$ находим $h(D) < \sqrt{D}\frac{(2+\log\sqrt{D})}{2\log(D/4)}$. Получаем $h(D_{0p}) < p$, а значит $p \nmid h(D_{0p})$.

Осталось проверить второе условие.

Пусть $\mathbf{p}$ – простой идеал в $\mathbb{Q}(\sqrt{D_{0p}})$, такой что $\mathbf{p}^2 = p$. Обозначим ε – фундаментальную единицу $\mathbb{Q}(\sqrt{D_{0p}})$.
Пусть $n(p, D_{0p})$ – степень вхождения $\mathbf{p}$ в $\varepsilon^{p-1} - 1$. Ясно, что $n(p, D_{0p}) \geq 1$. Отсюда (мы знаем это для всех чисел $|x|_p < p^{-1/(p-1)}$ из Предложения 2) $|\varepsilon^{p-1} - 1|_p = |\log_p(\varepsilon^{p-1})|_p$. Значит $|R_p(D_{0p})| = p^{-n(p,D_{0p})/2}$. Поскольку $|\sqrt{D_{0p}}| = p^{-1/2}$, нам надо доказать, что $n(p, D_{0p}) = 1$.
Разберём случай $p \equiv 1 \pmod{p}$. Возьмём $\alpha := (p-1) + \sqrt{p(p-2)}$.
Норма $\alpha = 1$, значит $\alpha = \varepsilon^j$ для некоторого целого j.
Заметим, что $\varepsilon^{2j} - 1 \equiv 0 \pmod{\mathbf{p}}$, но $\varepsilon^{2j} - 1 \not\equiv 0 \pmod{\mathbf{p}^2 = p}$.
Предположим, что $\varepsilon^{p-1} - 1 \equiv 0 \pmod{\mathbf{p}^2}$. Тогда если j_0 – порядок ε $\pmod{\mathbf{p}}$, то $j_0 | 2j$, значит $\varepsilon^{j_0} - 1 \not\equiv 0 \pmod{\mathbf{p}^2}$.
Если $(p-1) = j_0 \cdot m$, то $\varepsilon^{p-1} - 1 = (\varepsilon^{j_0} - 1)((\varepsilon^{j_0})^{m-1} + \ldots + 1)$. Так как $(\varepsilon^{j_0})^{m-1} + \ldots + 1 \equiv m \not\equiv 0 \pmod{\mathbf{p}}$, находим, что $\varepsilon^{j_0} - 1 \equiv 0 \pmod{\mathbf{p}^2}$ – противоречие.

Случай $p \equiv 3 \pmod{4}$ разбирается аналогично с $\alpha = \frac{p-2}{2} + \frac{\sqrt{p(p-4)}}{2}$.

Спасибо за внимание!