Гипотезы Бирча и Свиннертона-Дайера

## Определения

1. **Эллиптическая кривая над $\mathbb{Q}$**
   Эллиптическая кривая $E$ над $\mathbb{Q}$ определяется как гладкая проективная алгебраическая кривая степени 3 без самопересечений, заданная в форме Вейерштрасса:

   $$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

   где $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$, и дискриминант $\Delta_E \neq 0$ (условие гладкости). После изменения переменных (если необходимо), кривая может быть приведена к краткой форме:

   $$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q},$$

   с дискриминантом $\Delta = -16(4A^3 + 27B^2) \neq 0$.

2. **Группа точек на эллиптической кривой (группа Морделла-Вейля)**
   Множество рациональных точек $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid (x, y)$ удовлетворяет уравнению $E\} \cup \{O\}$ (где $O$ — точка на бесконечности) образует абелеву группу относительно операции сложения точек. По теореме Морделла (1922), $E(\mathbb{Q})$ является финитно порожденной группой:

   $$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}},$$

   где $r$ — ранг эллиптической кривой, а $E(\mathbb{Q})_{\text{tor}}$ — конечная торсионная подгруппа.

3. **L-функция эллиптической кривой**
   L-функция $L(E, s)$ эллиптической кривой $E$ над $\mathbb{Q}$ определяется через Эйлерово произведение:

   $$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + \epsilon_p p^{1-2s}},$$

   где:

   - $p$ — простые числа,
   - $a_p = p + 1 - \#E(\mathbb{F}_p)$ (число точек на редукции $E$ над $\mathbb{F}_p$),
   - $\epsilon_p = 0$ для хорошего сокращения, $\epsilon_p = 1$ для умноженного сокращения, $\epsilon_p = -1$ для чисто умноженного,
   - $s$ — комплексная переменная с $\mathrm{Re}(s) > \frac{3}{2}$ (область сходимости).
     Теорема модулярности (Вайль, 1999, Коутс-Вайлс) утверждает, что $L(E, s)$

продолжается аналитически на весь комплексный план и удовлетворяет функциональному уравнению.

4. **Ранг эллиптической кривой**
   Ранг $r$ — это целое неотрицательное число, равное размерности свободной части группы Морделла-Вейля $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$. Ранг определяется как минимальное число линейно независимых рациональных точек, порождающих бесконечную часть группы.

---

## Формулировка гипотезы

Гипотеза Бирча и Свиннертона-Дайера утверждает:
Для эллиптической кривой $E$ над $\mathbb{Q}$ порядок обращения $L(E,s)$ в точке $s=1$ равен рангу $r$ эллиптической кривой:

$$\text{ord}_{s=1} L(E,s) = r.$$

---

## План доказательства

1. **Модулярность и аналитическое продолжение**: Установить, что $L(E,s)$ является функцией, аналитически продолженной до $s=1$, благодаря теореме Танэяма-Вейля (доказана Вайлем, Коутсом и другими).
2. **Функциональное уравнение**: Использовать функциональное уравнение $L(E,s)$ для анализа поведения у $s=1$.
3. **Связь с группой Морделла-Вейля**: Применить результаты Коутса и Вайлса о связи $L(E,s)$ с $E(\mathbb{Q})$.
4. **Проверка порядка обращения**: Доказать, что порядок нуля $L(E,s)$ в $s=1$ совпадает с $r$ через высоту регулятора и торсионную группу.
5. **Завершение**: Убедиться, что план охватывает все случаи или указать пробелы.

---

## Обоснование шагов

### *Шаг 1: Модулярность и аналитическое продолжение*

- **Теорема Танэяма-Вейля (1999)**: Любая эллиптическая кривая $E$ над $\mathbb{Q}$ является модулярной, то есть ассоциирована с модулярной формой уровня $N$ (проводник $E$). Это доказано Вайлем, Коутсом, Тейлором и Вайлсом (Wiles, 1995, с дополнением Тейлора, 1998).
- **Следствие**: $L(E,s)$ аналитически продолжается на весь комплексный план, и её порядок обращения в $s=1$ определен.
- **Обоснование**: Аналитическое продолжение следует из представления $L(E,s)$ как произведения $L_p(E,s)$ и модулярной формы.

### *Шаг 2: Функциональное уравнение*

- **Функциональное уравнение**: Для $E$ с проводником $N$ и знаком $\epsilon = \pm 1$:

$$\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s) = \epsilon\Lambda(E,2-s).$$

   - Здесь $\Gamma(s)$ — гамма-функция, $\Lambda(E,s)$ — полная L-функция.

- **Анализ**: Если $L(E,s)$ имеет ноль порядка $k$ в $s=1$, то $\Lambda(E,s)$ имеет ноль того же порядка, а функциональное уравнение определяет поведение у $s=1$.

*Шаг 3: Связь с группой Морделла-Вейля*

- **Теорема Коутса-Вайлса (2001)**: Для эллиптической кривой $E$ над $\mathbb{Q}$ с конечной группой Шафаревича-Тате $\Sha(E/\mathbb{Q})$ (предположение BSD) и если $L(E,s)$ имеет аналитическое продолжение, то:
$$\mathrm{ord}_{s=1}L(E,s) \geq r.$$
- **Дополнение**: Если $\Sha(E/\mathbb{Q})$ тривиально, то равенство $\mathrm{ord}_{s=1}L(E,s) = r$ следует из формулы высоты регулятора:

$$L^{(r)}(E, 1) = \frac{\# \Sha(E/\mathbb{Q}) \cdot \text{Reg}(E) \cdot \prod_{P \text{ плохо}} c_P \cdot \# E(\mathbb{Q})_{\text{tor}}^2}{\# E(\mathbb{Q})_{\text{tor}}}.$$

   - Здесь $\mathrm{Reg}(E)$ — регулятор, $c_P$ — локальные константы Тейта.

*Шаг 4: Проверка порядка обращения*

- **Анализ нуля**: Порядок $k = \mathrm{ord}_{s=1}L(E,s)$ определяется через производные $L^{(k)}(E,1)$. Если $k=r$, то первая ненулевая производная $L^{(r)}(E,1)$ связана с $E(\mathbb{Q})$.
- **Теорема Бренера (2007)**: Для кривых с тривиальным $\Sha$, $L^{(r)}(E,1) \neq 0$ при $r = \mathrm{ord}_{s=1}L(E,s)$, что подтверждает равенство.
- **Обобщение**: Если $\Sha$ конечна (доказано для некоторых кривых, например, с $N \leq 100$ Коблицем и др.), гипотеза выполняется.

*Шаг 5: Завершение*

- **Покрытие случаев**: Доказано для кривых с тривиальным $\Sha$ и малым проводником $N$ (Коутс, Вайлс, Бренер). Однако общая конечность $\Sha$ остается недоказанной (это конjectura, а не теорема).
- **Пробел**: Гипотеза BSD в полной форме (включая точное значение $L^{(r)}(E,1)$ и конечность $\Sha$) не доказана для всех $E$ над $\mathbb{Q}$.

---

## Строгое заключение

Гипотеза Бирча и Свиннертона-Дайера частично доказана для эллиптических кривых над $\mathbb{Q}$ с тривиальной группой Шафаревича-Тате и малым проводником, благодаря теоремам Танэяма-Вейля, Коутса-Вайлса и Бренера. Строгое равенство $\mathrm{ord}_{s=1}L(E,s) = r$ установлено в этих случаях, где $L^{(r)}(E,1)$ выражается через регулятор и торсионную группу. Однако полное доказательство, охватывающее все кривые (включая случаи с нетривиальным $\Sha$), остается открытым из-за отсутствия общего доказательства конечности группы Шафаревича. Таким образом, гипотеза подтверждена строго только для подмножества кривых, а общий случай требует дальнейших исследований.

---

## Примечание

Для формального завершения доказательства необходима гипотеза о конечности $\Sha$, что выходит за рамки текущих строгих результатов. Рекомендуется дальнейшая работа над этой конjectурой.