ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Механико-математический факультет МГУ
1 поток 1 курса, осень 2026г.
Лекция 10: Символ Лежандра и его свойства.
Квадратичный закон взаимности.
Символ Якоби и его свойства.

Пусть p – простое нечётное число.

$$ax^2 + bx + c \equiv 0 \pmod{p}, \qquad p \nmid a, \tag{1}$$

Умножив обе части сравнения (1) на число $4a$, не делящееся на p, получим равносильное сравнение

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

или $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$, или

$$y^2 \equiv D \pmod{p}, \tag{2}$$

где использованы обозначения $y = 2ax + b$ и $D = b^2 - 4ac$.
В дальнейшем можно рассматривать лишь сравнения вида

$$x^2 \equiv a \pmod{p}. \tag{3}$$

Целое число a, $p \nmid a$, называется *квадратичным вычетом* по модулю p, если сравнение $x^2 \equiv a \pmod{p}$ имеет решение и *квадратичным невычетом* по модулю p, если это сравнение не имеет решений,

Лемма 1

Любая приведенная система вычетов по модулю p содержит $\frac{p-1}{2}$ *квадратичных вычетов и столько же квадратичных невычетов. Целое число a, не делящееся на p будет квадратичным вычетом в том и только том случае, когда*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{4}$$

и квадратичным невычетом в том и только том случае, когда

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{5}$$

Символ Лежандра $\left(\frac{a}{p}\right)$ есть функция, принимающая три значения: $-1, 0, 1$. Ее аргументами являются простое нечетное число p и целое число a.

Определение 1.

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{если } a\text{-квадратичный невычет по модулю } p \\ 0, & \text{если p}|\text{a} \\ 1, & \text{если } a\text{-квадратичный вычет по модулю } p \end{cases}$$

Свойства символа Лежандра описывает следующая теорема.

Теорема 22

Пусть a, b – произвольные целые числа. Тогда

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
2. *Если* $a \equiv b \pmod{p}$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
4. *Кроме того* $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

• Из определения символа Лежандра и леммы 1 следует, что для каждого квадратичного вычета a выполняется $\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$. Если же a квадратичный невычет, то $\left(\frac{a}{p}\right) = -1 \equiv a^{\frac{p-1}{2}} \pmod{p}$. При $a \equiv 0 \pmod{p}$ обе части нужного сравнения равны нулю и потому совпадают. Первое утверждение теоремы доказано.

Если $a \equiv b \pmod{p}$, то множества решений сравнений $x^2 \equiv a \pmod{p}$ и $x^2 \equiv b \pmod{p}$, очевидно, совпадают. Отсюда следует, что эти сравнения разрешимы или неразрешимы одновременно, что доказывает второе утверждение теоремы.

• С помощью первого утверждения находим следующие сравнения по модулю p

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}.$$

Левая и правая части получившегося сравнения равны ± 1 или 0. Поэтому их разность по модулю не превосходит 2 и делится на $p > 2$. Следовательно их разность равна 0. Третье утверждение доказано.

Сравнение $x^2 \equiv 1 \pmod{p}$ при любом простом нечетном p разрешимо. Решением является класс вычетов $x \equiv 1 \pmod{p}$. Поэтому $\left(\frac{1}{p}\right) = 1$.

- Из первого утверждения теоремы при $a = -1$ следует

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Абсолютная величина разности левой и правой частей этого сравнения не превосходит 2 и делится на нечетное простое число p. Значит, эта разность равна нулю, что доказывает справедливость последнего утверждения теоремы. □

Из последнего утверждения этой теоремы следует, например, что сравнение $x^2 + 1 \equiv 0 \pmod{p}$, где p – простое нечетное число, разрешимо в том и только том случае, когда $p \equiv 1 \pmod{4}$.

Утверждение, называемое *квадратичный закон взаимности* впервые сформулировал Эйлер в 1783г, а в 1796г. Гаусс дал первое его доказательство.

Теорема 23 (Квадратичный закон взаимности)

Если p и q - различные простые нечётные числа, то

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Другими словами,

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right), \quad \text{если } p \equiv 1 \pmod 4 \text{ или } q \equiv 1 \pmod 4, \\ \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right), \quad \text{если } p \equiv 3 \pmod 4 \text{ и } q \equiv 3 \pmod 4. \end{aligned}$$

Можно также сказать, что в первом случае сравнения $x^2 \equiv a \pmod{p}$ и $x^2 \equiv b \pmod{p}$ разрешимы или неразрешимы одновременно, а во втором случае из разрешимости одного из этих сравнений следует неразрешимость другого.

• Квадратичный закон взаимности вместе со свойствами из теоремы 22 позволяют вычислять символ Лежандра и тем устанавливать разрешимость или неразрешимость квадратичных сравнений. Некоторые примеры будут рассмотрены далее.

Перед тем как доказывать теорему 23 установим одно вспомогательное утверждение и выведем следствие из него. В этом утверждении используется тот факт, что совокупность чисел

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}$$

составляет приведённую систему вычетов по модулю p.

Лемма 2 (Лемма Гаусса)

Пусть p – простое нечетное число и a – целое число, не делящееся на p. Для каждого $k = 1, 2 \ldots, \frac{p-1}{2}$, определим $\varepsilon_k = \pm 1$ условиями

$$k \cdot a \equiv \varepsilon_k \cdot r_k \pmod{p}, \qquad 0 < r_k \leq \frac{p-1}{2}. \tag{6}$$

Тогда

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} = (-1)^t,$$

где t - количество отрицательных среди чисел $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{p-1}{2}}$.

Доказательство

Докажем сначала, что все числа r_k, определенные в (6), не сравнимы друг с другом по модулю p. Предположим, что для некоторых индексов $k > \ell$ выполняется сравнение $r_k \equiv r_\ell \pmod{p}$. Тогда

$$\varepsilon_k k \cdot a \equiv r_k \equiv r_\ell \equiv \varepsilon_\ell \ell \cdot a \pmod{p}$$

и, поскольку $p \nmid a$, имеем $p|(k \mp l)$. Но этого быть не может, так как $0 < |k \pm l| \leq p - 1$. Отсюда следует, что набор чисел $\{r_1, \ldots, r_{\frac{p-1}{2}}\}$ лишь перестановкой отличается от набора $\{1, 2 \ldots, \frac{p-1}{2}\}$.

Перемножая все сравнения (6), и пользуясь равенством $r_1 \cdots r_{\frac{p-1}{2}} = \left(\frac{p-1}{2}\right)!$, получим:

$$\left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \cdot \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} \pmod{p}.$$

Сократив это сравнение на не кратное p целое число $\left(\frac{p-1}{2}\right)!$ и пользуясь первым утверждением теоремы 22, находим $\left(\frac{a}{p}\right) \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} \pmod{p}$. Учитывая, что разность левой и правой частей этого сравнения по абсолютной величине не превосходит 2, получаем утверждение леммы. $\square$

Следствие 1

1) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

2) Если a нечётно, то $\left(\frac{a}{p}\right) = (-1)^S$, *где* $S = \sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]$.

Доказательство. Неполное частное от деления числа ak на p равно $\left[\frac{ak}{p}\right]$. Поэтому $0 \leq ak - p\left[\frac{ak}{p}\right] \leq p-1$ и

$$ak - p\left[\frac{ak}{p}\right] \equiv \varepsilon_k r_k \equiv \begin{cases} r_k & , \text{ если } \varepsilon_k = 1 \\ p - r_k & , \text{ если } \varepsilon_k = -1 \end{cases} \pmod{p}.$$

Левая и правая части получившегося сравнения принадлежат отрезку от 0 до $p-1$. Значит, абсолютная величина их разности не превосходит $p-1$ и делится на p. А потому

$$ak - p\left[\frac{ak}{p}\right] = \begin{cases} r_k & , \text{ если } \varepsilon_k = 1 \\ p - r_k & , \text{ если } \varepsilon_k = -1 \end{cases}$$

Суммируем эти равенства при всех $k = 1, 2, \ldots, \frac{p-1}{2}$, учитывая, что $1 + 2 + \ldots + \frac{p-1}{2} = \frac{p^2-1}{8}$ и пользуясь обозначениями леммы 2. В результате получим

$$\frac{p^2-1}{8} \cdot a - p \cdot S = t \cdot p + \sum_{k=1}^{\frac{p-1}{2}} \varepsilon_k \cdot r_k.$$

Перейдем в этом равенстве к сравнению по модулю 2. Заметив, что

$$\sum_{k=1}^{\frac{p-1}{2}} \varepsilon_k \cdot r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} r_k = \sum_{k=1}^{\frac{p-1}{2}} k = \frac{p^2-1}{8} \pmod 2, \qquad p \equiv -1 \pmod 2,$$

получаем $\frac{p^2-1}{8} \cdot a + S \equiv t + \frac{p^2-1}{8} \pmod 2$, то есть

$$t \equiv S + (a-1) \cdot \frac{p^2-1}{8} \pmod 2. \tag{7}$$

Доказательство

При $a = 2$ все слагаемые в сумме, определяющей S равны нулю. Поэтому $S = 0$ и $t \equiv \frac{p^2-1}{8} \pmod 2$. В силу леммы Гаусса это доказывает первый пункт следствия.

Если a - нечётно, то согласно (7) имеем $t \equiv S \pmod 2$, что в силу леммы Гаусса доказывает второй пункт следствия. $\square$

Доказательство теоремы 23. По следствию 1 выполняются равенства $\left(\frac{q}{p}\right) = (-1)^{S_1}$ и $\left(\frac{p}{q}\right) = (-1)^{S_2}$, где

$$S_1 = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right], \qquad S_2 = \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right].$$

Поэтому

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{S_1+S_2},$$

и достаточно доказать равенство

$$S_1 + S_2 = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Доказательство

При фиксированном целом x из интервала $0 < x \leq \frac{p-1}{2}$ величина $\left[\frac{qx}{p}\right]$ есть количество целых точек y на промежутке $0 < y \leq \frac{qx}{p}$ или, учитывая, что $\frac{qx}{p}$ не есть целое число, – на промежутке $0 < y < \frac{qx}{p}$. Отсюда следует, что S_1 равно количеству пар целых чисел x, y, удовлетворяющих неравенствам

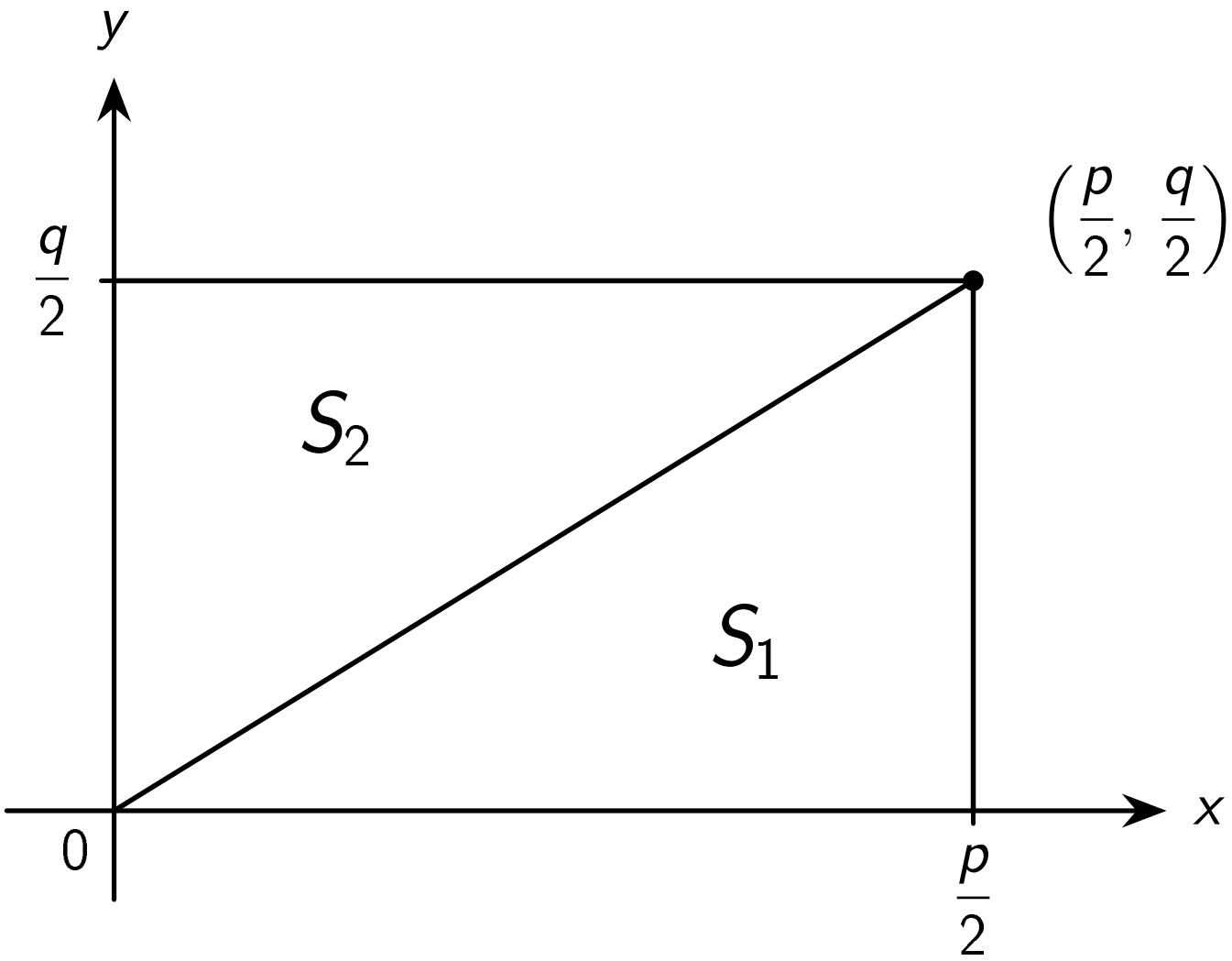
$$0 < x \leq \frac{p-1}{2}, \qquad 0 < y < \frac{qx}{p}.$$

Поскольку $\frac{p}{2}$ не целое число, и $\frac{qx}{p} < \frac{q}{2}$, заключаем, что S_1 есть количество точек $(x, y) \in \mathbb{Z}^2$ с условиями

$$0 < x < \frac{p}{2}, \qquad 0 < y < \frac{q}{2}, \qquad py - qx < 0.$$

S_1 есть количество точек $(x, y) \in \mathbb{Z}^2$ с условиями

$$0 < x < \frac{p}{2}, \qquad 0 < y < \frac{q}{2}, \qquad py - qx < 0.$$



Точно так же, число S_2 равно количеству точек $(x, y) \in \mathbb{Z}^2$ в прямоугольнике

$$T = \{(x, y) \mid 0 < x < \frac{p}{2}, \quad 0 < y < \frac{q}{2}\}$$

с условием $qx - py < 0$. Последнее условие может быть переписано в виде $py - qx > 0$.

Ни одна из точек $(x, y) \in \mathbb{Z}^2$ прямоугольника T не лежит на прямой линии $py - qx = 0$, поэтому сумма $S_1 + S_2$ равна количеству точек с целыми координатами, лежащих в T, т.е. $\frac{p-1}{2} \cdot \frac{q-1}{2}$. □

Рассмотрим несколько примеров.

Пример. Разрешимо ли сравнение $x^2 \equiv 53 \pmod{233}$?
Так как $53 = 1 + 4 \cdot 13$ и $233 = 4 \cdot 53 + 21$, то, применяя квадратичный закон взаимности и второе свойство из теоремы 22, находим

$$\left(\frac{53}{233}\right) = \left(\frac{233}{53}\right) = \left(\frac{21}{53}\right).$$

Пример

Пользуясь третьим свойством из теоремы 22 и опять применяя квадратичный закон взаимности, получаем

$$\left(\frac{21}{53}\right) = \left(\frac{7}{53}\right) \cdot \left(\frac{3}{53}\right) = \left(\frac{53}{7}\right) \cdot \left(\frac{53}{3}\right).$$

Далее, учитывая, что $53 = 7 \cdot 7 + 4$ и $53 = 3 \cdot 18 - 1$, имеем

$$\left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1, \qquad \left(\frac{53}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1,$$

и, наконец,

$$\left(\frac{53}{233}\right) = 1 \cdot (-1) = -1.$$

Таким образом, данное сравнение не имеет решений.

Пример. Для каких простых чисел p разрешимо сравнение

$$x^2 - 5 \equiv 0 \pmod{p} \ ?$$

• При $p = 2$ решение существует $x \equiv 1 \pmod 2$. При $p = 5$ решением сравнения будет класс вычетов $x \equiv 0 \pmod 5$. Далее будем считать, что p – нечётное простое число, отличное от 5.

• Согласно теореме 23 справедливо равенство $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Так как квадратичными вычетами по модулю 5 являются числа $1, -1$, а 2 и -2 есть квадратичные невычеты, заключаем, что простые числа p, отличные от 2 и 5, для которых разрешимо данное сравнение, лежат в классах вычетов $x \equiv \pm 1 \pmod 5$.

• Учитывая, что все эти простые числа должны быть нечётными, т.е. должны удовлетворять сравнению $x \equiv 1 \pmod 2$, с помощью китайской теоремы об остатках находим, что искомые простые числа лежат в классах вычетов $x \equiv \pm 1 \pmod{10}$. Итак, данное сравнение разрешимо лишь при $p = 2, 5$ и всех простых числах вида $\pm 1 + 10n$.

Последний пример может быть обобщен.

Теорема 24

Множество всех простых чисел p, для которых разрешимо сравнение

$$ax^2 + bx + c \equiv 0 \pmod{p}, \qquad p \nmid a, \tag{8}$$

состоит из некоторых делителей числа $2D$, где $D = b^2 - 4ac$, а также из простых, лежащих в нескольких классах вычетов по модулю $4|D|$.

Доказательство

Достаточно рассматривать только простые числа p, не делящие $2D$. Как указывалось выше, существует взаимно однозначное соответствие между решениями сравнения (8) и решениями сравнения $x^2 \equiv D \pmod{p}$. Последнее сравнение разрешимо лишь для тех простых чисел p, для которых выполняется равенство $\left(\frac{D}{p}\right) = 1$.

- Для завершения доказательства теоремы достаточно установить, что множество нечётных простых чисел p, для которых $\left(\frac{D}{p}\right) = 1$, состоит из нескольких классов вычетов по модулю $4|D|$.
- Это равносильно утверждению, что для простых из одного класса вычетов по модулю $4|D|$ сравнение $x^2 \equiv D \pmod{p}$ разрешимо или неразрешимо одновременно, т.е. сравнение $p_1 \equiv p_2 \pmod{4|D|}$ влечет за собой $\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right)$.

Доказательство

Пусть $D = (-1)^{\alpha_1} \cdot 2^{\alpha_2} \cdot \prod\limits_q q^{\alpha_q}$ – разложение числа D в произведение простых сомножителей (с учетом знака). Тогда

$$\left(\frac{D}{p}\right) = \left(\frac{-1}{p}\right)^{\alpha_1} \cdot \left(\frac{2}{p}\right)^{\alpha_2} \cdot \prod_q \left(\frac{q}{p}\right)^{\alpha_q}. \qquad (9)$$

Рассмотрим несколько случаев.

1) Так как $p_1 \equiv p_2 \pmod 4$, то $\frac{p_1-1}{2} \equiv \frac{p_2-1}{2} \pmod 2$ и по четвертому утверждению теоремы 22 выполняется равенство $\left(\frac{-1}{p_1}\right) = \left(\frac{-1}{p_2}\right)$.

2) Допустим, что $\alpha_2 \geq 1$. Тогда D делится на 2, следовательно $p_1 \equiv p_2 \pmod 8$ и

$$\frac{p_1^2-1}{8} - \frac{p_2^2-1}{8} = \frac{p_1-p_2}{8} \cdot (p_1+p_2) \equiv 0 \pmod 2.$$

По первому утверждению следствия 1 получаем $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right)$ и, значит, при любом $\alpha_2 \geq 0$ выполняется равенство $\left(\frac{2}{p_1}\right)^{\alpha_2} = \left(\frac{2}{p_2}\right)^{\alpha_2}$.

3) Пусть теперь $q|D$. Из сравнения $p_1 \equiv p_2 \pmod{4|D|}$ следует $p_1 \equiv p_2 \pmod{q}$, так что $\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right)$. В то же время $p_1 \equiv p_2 \pmod{4}$, поэтому

$$\frac{p_1-1}{2}\cdot\frac{q-1}{2} - \frac{p_2-1}{2}\cdot\frac{q-1}{2} = (q-1)\cdot\frac{p_1-p_2}{4} \equiv 0 \pmod{2}.$$

Теперь с помощью квадратичного закона взаимности находим

$$\left(\frac{q}{p_1}\right) = \left(\frac{p_1}{q}\right)\cdot(-1)^{\frac{p_1-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{p_2}{q}\right)\cdot(-1)^{\frac{p_2-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{q}{p_2}\right),$$

т.е. $\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right)$.

Из равенств, доказанных в пунктах 1)–3) с помощью (9) находим $\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right)$. □

Символ Якоби и его свойства

Символ Лежандра определен только для пар целых чисел a, p, у которых p есть простое нечетное число. Определение можно распространить на большее множество пар целых чисел и построить таким способом функцию, называемую символом Якоби.

Одним из важных свойств символа Якоби является возможность вычислять его значения, не используя весьма трудоемкую операцию разложения чисел на множители. В частности это даёт быстрый способ вычисления значений символа Лежандра.

Символ Якоби и его свойства

Пусть P - положительное нечётное число и $P = p_1 \cdots p_r$ его разложение в произведение простых чисел, не обязательно различных. Определим для каждого целого числа a *символ Якоби* $\left(\frac{a}{P}\right)$ равенством

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right),$$

где справа стоит произведение символов Лежандра.

Следует отметить, что символ Якоби не имеет отношения к разрешимости квадратичных сравнений. Например,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

но сравнение $x^2 \equiv 2 \pmod{15}$ не имеет решений, ведь $\left(\frac{2}{3}\right) = -1$ и, значит, ни при каком целом x число $x^2 - 2$ не делится на 3. Тем более оно не делится на 15.

В дальнейшем буквой P будет обозначаться некоторое положительное нечетное число. Основные свойства символа Якоби описывает

Теорема 25

(1) Если целые числа a, b взаимно просты с P и удовлетворяют сравнению $a \equiv b \pmod{P}$, то $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.
(2) Для любых целых чисел a, b, взаимно простых с P выполняется равенство $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{b}{P}\right)$.
(3) Справедливы равенства

$$\left(\frac{1}{P}\right) = 1, \qquad \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}, \qquad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

(4) Для любых двух положительных нечётных взаимно простых чисел P, Q имеет место равенство $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$.

Заметим, что для каждого нечетного числа u дробь $\frac{u^2-1}{8}$ есть целое число. Действительно $u^2-1=(u-1)(u+1)$ есть произведение двух последовательных целых чисел. Одно из них делится на 4, а другое на 2.

Лемма 3

Для любых нечётных целых чисел $u_1,\ldots,u_m$ справедливы сравнения

(1) $\frac{u_1\cdots u_m-1}{2}\equiv\sum_{i=1}^{m}\frac{u_i-1}{2}\pmod 2$

(2) $\frac{u_1^2\cdots u_m^2-1}{8}\equiv\sum_{i=1}^{m}\frac{u_i^2-1}{8}\pmod 8$.

Доказательство. Рассмотрим сначала случай $m = 2$, обозначая для краткости $u = u_1, v = u_2$. Справедливо сравнение

$$uv - 1 - (u - 1) - (v - 1) = (u - 1)(v - 1) \equiv 0 \pmod 4.$$

Разделив обе части его и модуль на 2, получаем первое утверждение. Для доказательства второго утверждения разделим обе части и модуль сравнения

$$u^2v^2 - 1 - (u^2 - 1) - (v^2 - 1) = (u^2 - 1)(v^2 - 1) \equiv 0 \pmod{64}$$

на 8.

Доказательство

Пользуясь математической индукцией, при любом $m \geq 3$ находим сравнения

$$\frac{u_1 \cdots u_m - 1}{2} \equiv \frac{u_1 \cdots u_{m-1} - 1}{2} + \frac{u_m - 1}{2} \equiv \sum_{i=1}^{m} \frac{u_i - 1}{2} \pmod 2,$$

$$\frac{u_1^2 \cdots u_m^2 - 1}{8} \equiv \frac{u_1^2 \cdots u_{m-1}^2 - 1}{8} + \frac{u_m^2 - 1}{8} \equiv \sum_{i=1}^{m-1} \frac{u_i^2 - 1}{8} \pmod 8,$$

□

Доказательство теоремы 25. Пусть $P = p_1 \cdots p_r$ – разложение в произведение простых чисел. Тогда для любых $a \equiv b \pmod{P}$ имеем $a \equiv b \pmod{p_i}$, $i = 1, \ldots, r$, и согласно определению и теореме 22 получаем

$$\left(\frac{a}{P}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right) = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right) = \left(\frac{b}{P}\right).$$

Это доказывает первое утверждение.

Справедливы равенства

$$\left(\frac{ab}{P}\right) = \prod_{i=1}^{m} \left(\frac{ab}{p_i}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right) \cdot \left(\frac{b}{p_i}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{b}{P}\right),$$

доказывающие второе утверждение.

Пользуясь определением символа Якоби, теоремой 22 и леммой 3, находим

$$\left(\frac{1}{P}\right) = \prod_{i=1}^{r}\left(\frac{1}{p_i}\right) = 1,$$

$$\left(\frac{-1}{P}\right) = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{r}(-1)^{\frac{p_i-1}{2}} = (-1)^{\frac{P-1}{2}},$$

$$\left(\frac{2}{P}\right) = \prod_{i=1}^{r}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{r}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\frac{P^2-1}{8}}.$$

Доказательство

Пусть теперь P, Q – положительные нечетные взаимно простые числа и $P = p_1 \cdots p_r$, $Q = q_1 \cdots q_s$ – их разложения в произведения простых чисел. Пользуясь определением символа Якоби, вторым утверждением теоремы и квадратичным законом взаимности, находим

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}. \quad (10)$$

Согласно лемме 3 имеет место сравнение

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}=\left(\sum_{i=1}^{r}\frac{p_i-1}{2}\right)\cdot\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)\equiv$$

$$\equiv\frac{P-1}{2}\cdot\frac{Q-1}{2}\pmod 2,$$

доказывающее вместе с (10) последнее утверждение теоремы. $\square$

Вычислим с помощью теоремы 25 символ Якоби $\left(\frac{53}{233}\right)$, совпадающий, поскольку 233 – простое число, с соответствующим символом Лежандра. Имеем, пользуясь утверждениями 1), 3) и 4) этой теоремы,

$$\left(\frac{53}{233}\right) = \left(\frac{233}{53}\right) = \left(\frac{21}{53}\right) = \left(\frac{53}{21}\right) = \left(\frac{11}{21}\right) = \\ = \left(\frac{21}{11}\right) = \left(\frac{-1}{11}\right) = -1,$$

что, конечно, совпадает с результатом предыдущих вычислений.

Способ вычисления символа Якоби, применённый в рассмотренном примере, может быть оформлен в виде общего алгоритма полиномиальной сложности.