8. Восьмая лекция, 8 ноября 2021 г.

8.1. **Квадратичные вычеты и невычеты.** Наша ближайшая задача будет состоять в том, чтобы научиться искать число решений уравнения $x^2 = a$, где $a \in \mathbb{Z}/p\mathbb{Z}$ — остаток по некоторому фиксированному простому модулю p. Будем считать, что $p > 2$, т.е. p — *нечетное* простое число.

Заметим, что если уравнение $x^2 = a$ при $a \neq 0$ имеет корень, то этих корней обязательно будет ровно два: а именно, если b — корень этого уравнения, то и $-b$ — тоже его корень. При этом, поскольку p нечетно, $b \neq -b$ (т.к. $2b \neq 0 \mod p$, так как b не кратно p).

Поэтому получается, что $x^2 - a = (x-b)(x+b)$. Отсюда следует, что других корней у уравнения $x^2 = a$ нет: если c — корень уравнения, то $(c-b)(c+b) = 0$, откуда $c = b$ или $c = -b$ (здесь мы пользуемся отсутствием делителей нуля в $\mathbb{Z}/p\mathbb{Z}$).

Определение 8.1. Пусть $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$. Будем называть a *квадратичным вычетом*, если уравнение $x^2 = a$ разрешимо, и *квадратичным невычетом* в противном случае.

При этом число 0 мы не будем относить ни к квадратичным вычетам, ни к невычетам (так же, как вещественное число 0 не является ни положительным, ни отрицательным).

Предложение 8.2. *Количество как квадратичных вычетов, так и квадратичных невычетов в $\mathbb{Z}/p\mathbb{Z}$ равно $\frac{p-1}{2}$.*

Доказательство. Каждому квадратичному вычету a соответствуют два решения $\pm b$ уравнения $x^2 = a$. Также ясно, что каждый ненулевой остаток из $\mathbb{Z}/p\mathbb{Z}$ является решением некоторого квадратного уравнения такого вида. Поэтому получается, что квадратичных вычетов оказывается вдвое меньше, чем ненулевых элементов из $\mathbb{Z}/p\mathbb{Z}$, то есть $\frac{p-1}{2}$. Все остальные элементы $\mathbb{Z}/p\mathbb{Z}$ тогда будут квадратичными невычетами, и их $(p-1) - \frac{p-1}{2}$, то есть столько же. □

Упражнение 8.3. Для всех нечетных простых чисел $p < 20$ перечислите все квадратичные вычеты и невычеты по модулю p.

Упражнение 8.4. Докажите, что квадратное уравнение

$$ax^2 + bx + c = 0,$$

где $a, b, c \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$,

- имеет два решения, равные $x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}$, если его дискриминант $D = b^2 - 4ac$ является квадратичным вычетом;
- имеет единственное решение, если $D = 0$;
- неразрешимо над $\mathbb{Z}/p\mathbb{Z}$, если D — квадратичный невычет.

Указание. С помощью выделения полного квадрата сведите данное уравнение к виду $x^2 = D$.

8.2. **Символ Лежандра и его мультипликативность.** Ясно, что произведение двух квадратичных вычетов снова будет квадратичным вычетом. А что будет, если перемножить два квадратичных невычета? А вычет и невычет? Оказывается, верна следующая теорема.

Теорема 8.5. а) *Произведение двух квадратичных вычетов — квадратичный вычет;*

б) *произведение двух квадратичных невычетов — квадратичный вычет;*

в) *произведение квадратичного вычета и квадратичного невычета — квадратичный невычет.*

Доказательство. Пункт а) очевиден: если a и b квадратичные вычеты, то есть существуют такие x и y, для которых $x^2 = a$ и $y^2 = b$, то ab тоже будет квадратичным вычетом, поскольку $(xy)^2 = ab$.

Докажем пункт б). Пусть a — квадратичный вычет, b — квадратичный невычет. Предположим противное: что ab — квадратичный вычет. Поскольку a — квадратичный вычет, найдется такое x, что $x^2 = a$. В таком случае и элемент a^{-1} будет квадратичным вычетом, т.к. $a^{-1} = (x^{-1})^2$. Соответственно, в силу пункта а) элемент b как произведение квадратичных вычетов ab и a^{-1} будет квадратичным вычетом — противоречие.

Пункт в) аналогичными формальными манипуляциями доказать уже не удается. Однако его можно вывести из пункта б) при помощи подсчета числа элементов. А именно, пусть a — фиксированный квадратичный невычет. Рассмотрим все элементы вида $a, 2a, \ldots, (p-1)a$. Как обсуждалось ранее, в этой последовательности все элементы $1, 2, \ldots, (p-1)$ встречаются, причем ровно по одному разу — поэтому среди них $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов. Однако в силу пункта б) при умножении a на квадратичный вычет получается квадратичный невычет, и таких элементов будет $\frac{p-1}{2}$, то есть все квадратичные невычеты будут получаться таким образом. Значит, при умножении a на все остальные элементы (т.е. невычеты) должны получаться квадратичные вычеты, что и требовалось. □

Тем самым квадратичные вычеты и невычеты ведут себя при умножении примерно так же, как положительные и отрицательные числа. Это мотивирует следующее определение.

Определение 8.6. Пусть $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$. *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ — квадратичный вычет;} \\ -1, & a \text{ — квадратичный невычет;} \\ 0, & a = 0. \end{cases}$$

Таким образом, символ Лежандра можно считать аналогом функции знака числа. Тогда предыдущая теорема принимает следующий компактный вид.

Теорема 8.7. *Символ Лежандра мультипликативен:*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Далее мы приведем другое доказательство этой теоремы, которое будет следовать из ещё одного полезного утверждения, позволяющего вычислить символ Лежандра — критерия Эйлера.

8.3. **Критерий Эйлера.** Прежде чем читать дальше, рекомендуем читателю выполнить следующее упражнение.

Упражнение 8.8. Возьмите какое-нибудь нечетное простое число, меньшее 20, и возведите каждый из ненулевых остатков $a \in \mathbb{Z}/p\mathbb{Z}$ в степень $\frac{p-1}{2}$. Убедитесь, что у вас всегда будет получаться ± 1. А когда получается 1, а когда -1?

Тем самым вы «экспериментально» проверите утверждение следующей теоремы.

Теорема 8.9 (критерий Эйлера)**.** *Пусть $p > 2$ — простое число, $a \in \mathbb{Z}/p\mathbb{Z}$. Тогда*

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

Доказательство. При $a = 0$ утверждение теоремы очевидно. Дальше будем считать, что a отлично от 0.

Во-первых, сначала убедимся, что при любом $a \neq 0$ будет иметь место равенство $a^{\frac{p-1}{2}} = \pm 1$. Действительно, $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1$ по малой теореме Ферма. Но число, квадрат которого равен 1, может равняться только 1 или -1.

Далее, ясно, что если $\left(\frac{a}{p}\right) = 1$, то $a^{\frac{p-1}{2}} = 1$. Действительно, если a — квадратичный вычет, то существует такое b, что $b^2 = a$. Тогда $a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} = 1$ опять-таки в силу малой теоремы Ферма.

Осталось доказать, что если a — квадратичный невычет, то $a^{\frac{p-1}{2}} = -1$. Для этого рассмотрим уравнение $x^{\frac{p-1}{2}} - 1 = 0$. Это полиномиальное уравнение степени $\frac{p-1}{2}$ — следовательно, по теореме Безу (которая верна и для многочленов с коэффициентами из $\mathbb{Z}/p\mathbb{Z}$!) у него не может быть более $\frac{p-1}{2}$ корней. Но столько корней нам уже известно: это все квадратичные вычеты. Тем самым получается, что квадратичные невычеты не являются корнями этого уравнения, то есть для них $a^{\frac{p-1}{2}} \neq 1$. Значит, для них $a^{\frac{p-1}{2}} = -1$. □

Из критерия Эйлера очевидно следует мультипликативность символа Лежандра. Действительно,

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

Кроме того, с помощью критерия Эйлера легко понять, когда -1 является квадратичным вычетом, а когда — невычетом:

Следствие 8.10. *Имеет место равенство*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p = 4k+1, \\ -1, & p = 4k+3. \end{cases}$$

8.4. **«Положительные» и «отрицательные» остатки.** Выпишем все элементы из $\mathbb{Z}/p\mathbb{Z}$ в следующем порядке:

$$-\frac{p-1}{2}, \quad \ldots, \quad -2, \quad -1, \quad 0, \quad 1, \quad 2, \quad \ldots, \quad \frac{p-1}{2}.$$

Условимся называть те из них, которые выписаны слева от нуля, «отрицательными», а те, что справа — «положительными».[1]

Рассмотрим произвольный ненулевой элемент $a \in \mathbb{Z}/p\mathbb{Z}$ и умножим его на все «положительные» элементы. Получим элементы $a, 2a, \ldots, \frac{p-1}{2}a$.

Нетрудно доказать следующее

Предложение 8.11. *Множество $\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$ содержит ровно по одному элементу из каждой пары $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$.*

Доказательство. Ранее мы уже видели, что разные элементы из $\mathbb{Z}/p\mathbb{Z}$ при умножении на произвольное ненулевое a не могут переходить в один и тот же элемент: это противоречило бы тому, что в $\mathbb{Z}/p\mathbb{Z}$ нет делителей нуля.

[1] Не надо путать положительные/отрицательные элементы в смысле этого обозначения с квадратичными вычетами/невычетами.

Докажем, что для различных «положительных» элементов $k \neq \ell$ элементы ak и $a\ell$ не могут быть противоположны друг другу. Действительно, это значило бы, что

$$0 = ak + a\ell = a(k + \ell),$$

откуда $k + \ell = 0 \mod p$. Но этого не может быть: поскольку $0 < k, \ell \leq \frac{p-1}{2}$, то $0 < k + \ell < p$, значит, $k + \ell \neq 0 \mod p$.

Поэтому среди элементов $a, 2a, \ldots, \frac{p-1}{2}a$ любое из чисел вида $\pm k$ встречается не более одного раза. Но тех и других по $(p-1)/2$ — стало быть, каждое из чисел вида $\pm k$ войдет ровно однажды. □

Обозначим через $\varepsilon(a)$ количество «отрицательных» элементов, входящих во множество $\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$, то есть число таких «положительных» элементов, которые при умножении на a становятся «отрицательными».

Предложение 8.12 (лемма Гаусса)**.** *Имеет место равенство* $(-1)^{\varepsilon(a)} = \left(\frac{a}{p}\right)$. *Иначе говоря,* $\varepsilon(a)$ *четно, если* a *— квадратичный вычет, и нечетно в противном случае.*

Доказательство. Перемножим все числа $a, 2a, \ldots, \frac{p-1}{2}a$. В силу предыдущего рассуждения мы получим, что это произведение равно

$$a \cdot 2a \cdot \cdots \cdot \frac{p-1}{2}a = (-1)^{\varepsilon(a)} \cdot 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}.$$

Но, с другой стороны, оно же равняется

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

(в последнем равенстве использован критерий Эйлера).

Поделив обе части на отличную от нуля величину $((p-1)/2)!$, получаем требуемое равенство. □

Это предложение позволяет вычислить символ Лежандра для некоторых значений a.

Пример 8.13. Убедимся еще раз, что $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Действительно, при умножении на -1 все «положительные» числа становятся «отрицательными» — а их всего $(p-1)/2$.

Выясним, когда число 2 является квадратичным вычетом по модулю p. Оказывается, что это зависит от остатка от деления p на 8: если он равен 1 или 7, то 2 будет квадратичным вычетом, а если 3 или 5, то невычетом.

Предложение 8.14. *Имеет место равенство*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p = 8k \pm 1, \\ -1, & p = 8k \pm 3. \end{cases}$$

Доказательство. Умножим все «положительные» элементы на 2; получим элементы вида

$$2, \quad 4, \quad \ldots \quad p-3, \quad p-1.$$

«Отрицательными» будут те из них, которые будут заключены между $p/2$ и $p-1$. Их количество, как нетрудно видеть, будет равно $\lceil \frac{p-1}{4} \rceil$ (то есть числу $\frac{p-1}{4}$, округленному до ближайшего целого *вверх*).

Эта величина и будет равна $\varepsilon(2)$; мы хотим найти ее четность. Проще всего сделать это, разобрав четыре возможных случая:

- если $p = 8k + 1$, то $\varepsilon(2) = \lceil \frac{p-1}{4} \rceil = 2k$;

- если $p = 8k + 3$, то $\varepsilon(2) = \lceil 2k + \frac{1}{2} \rceil = 2k + 1$;
- если $p = 8k + 5$, то $\varepsilon(2) = \lceil 2k + 1 \rceil = 2k + 1$;
- наконец, если $p = 8k + 7$, то $\varepsilon(2) = \lceil 2k + \frac{3}{2} \rceil = 2k + 2$.

□

8.5. **Квадратичный закон взаимности Гаусса.** До этого мы имели дело с квадратичными вычетами и невычетами по какому-то конкретному модулю. Следующее замечательное утверждение позволяет устанавливать связь между символами Лежандра по *различным* модулям, что даёт эффективный алгоритм для их вычисления.

Теорема 8.15 (квадратичный закон взаимности)**.** *Для различных нечетных простых чисел имеет место равенство*

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

Сам Гаусс именовал это утверждение «золотой теоремой» (Theorema Aureum); он придумал несколько его различных доказательств. На сегодняшний день известно более ста способов его доказывать. Вкратце приведем доказательство одного из них, принадлежащего ученику Гаусса Эйзенштейну[2].

Доказательство. Начнём со следующего утверждения из тригонометрии (которое, казалось бы, никакого отношения к теории чисел не имеет).

Лемма 8.16 (тригонометрическая лемма)**.** *Пусть m — нечётное целое число. Тогда*

$$\frac{\sin mx}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{(m-1)/2} \left(\sin^2 x - \sin^2\left(\frac{2\pi j}{m}\right)\right).$$

Набросок доказательства. Из формулы синуса суммы углов с помощью индукции нетрудно вывести, что левая часть является многочленом от $\sin^2 x$ степени $\frac{m-1}{2}$. Далее, левая часть обращается в нуль при $x = 2\pi j/m$, то есть при $\sin^2 x = \sin^2\left(\frac{2\pi j}{m}\right)$. Множитель $(-4)^{\frac{m-1}{2}}$ получается сравнением коэффициентов при старшем члене в левой и правой частях. □

Вернемся к доказательству. Пусть p — простое нечетное число, q — произвольный вычет по модулю p. Возьмем вычет a, где $1 \le a \le \frac{p-1}{2}$, и предположим, что $qa = \pm a_q$, где $1 \le a_q \le \frac{p-1}{2}$. Домножим обе части равенства на $\frac{2\pi}{p}$, возьмем от них синус и воспользуемся тем, что синус — нечётная функция:

$$\sin \frac{2\pi}{p} qa = \pm \sin \frac{2\pi}{p} a_q.$$

Теперь перемножим все такие равенства по всем a от 1 до $(p-1)/2$; по лемме Гаусса, количество минусов будет равняться $(-1)^{\varepsilon(q)} = \left(\frac{q}{p}\right)$. Поскольку среди a_q все числа $1, \ldots, \frac{p-1}{2}$ встретятся по одному разу, получим, что

$$\left(\frac{q}{p}\right) = \prod_{a=1}^{(p-1)/2} \left(\sin \frac{2\pi qa}{p} \Big/ \sin \frac{2\pi a}{p}\right).$$

[2]В лекциях доказательство квадратичного закона взаимности не приводилось. В программу экзамена доказательство также не войдёт.

Применим тригонометрическую лемму при $m = q$ и перепишем это равенство следующим образом:

$$\left(\frac{q}{p}\right) = \prod_{a=1}^{(p-1)/2} (-4)^{(p-1)/2} \prod_{b=1}^{(q-1)/2} \left(\sin^2 \frac{2\pi a}{p} - \sin^2 \frac{2\pi b}{q}\right) =$$

$$= (-4)^{(p-1)(q-1)/4} \prod_{a=1}^{(p-1)/2} \prod_{b=1}^{(q-1)/2} \left(\sin^2 \frac{2\pi a}{p} - \sin^2 \frac{2\pi b}{q}\right).$$

Меняя местами роли p и q, аналогично получаем, что

$$\left(\frac{p}{q}\right) = (-4)^{(p-1)(q-1)/4} \prod_{a=1}^{(p-1)/2} \prod_{b=1}^{(q-1)/2} \left(\sin^2 \frac{2\pi b}{q} - \sin^2 \frac{2\pi a}{p}\right).$$

Эти два выражения отличаются переменой знака у $\frac{p-1}{2} \cdot \frac{q-1}{2}$ скобок, т.е. коэффициентом $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. Квадратичный закон взаимности доказан. □

На практике квадратичный закон взаимности удобно использовать в следующей форме.

Следствие 8.17. *Пусть $p, q > 2$ — различные нечетные простые числа. Символы Лежандра $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$ равны, если хотя бы одно из чисел p, q имеет вид $4k + 1$, и различны, если они оба имеют вид $4k + 3$.*

8.6. **Пример использования квадратичного закона взаимности.** В качестве примера выясним с помощью квадратичного закона взаимности, разрешимо ли сравнение

$$x^2 \equiv 57 \mod 179.$$

Для этого нам нужно вычислить $\left(\frac{57}{179}\right) = \left(\frac{3}{179}\right) \cdot \left(\frac{19}{179}\right)$. Вычислим отдельно каждый из этих символов Лежандра.

Оба числа 3 и 179 дают при делении на 4 остаток 3. Поэтому

$$\left(\frac{3}{179}\right) = -\left(\frac{179}{3}\right) = -\left(\frac{-1}{3}\right) = 1,$$

так как -1 является квадратичным невычетом по модулю 3. Значит, 3 — квадратичный вычет по модулю 179.

Далее, по той же причине (19 тоже имеет вид $4k+3$) получаем, что $\left(\frac{19}{179}\right) = -\left(\frac{179}{19}\right) = -\left(\frac{8}{19}\right) = -\left(\frac{2}{19}\right)$ (поскольку $8 = 2 \cdot 4$, а 4 — полный квадрат). Но число 19 имеет вид $8k + 3$, поэтому 2 является квадратичным невычетом по модулю 19. Стало быть, $\left(\frac{19}{179}\right) = 1$, откуда $\left(\frac{57}{179}\right) = 1$, и сравнение $x^2 \equiv 57 \mod 179$ разрешимо.