Гимназия 1543, математический спецкурс, 8 В

Лекция: квадратные сравнения и символы Лежандра

Решение квадратного уравнения

Напомним, как решаются квадратные уравнения в действительных (или комплексных) числах. Пусть мы имеем дело с уравнением

$$x^2 + ax + b = 0.$$

Путём очевидной замены $y = x + a/2$ мы приходим к эквивалентному уравнению вида

$$y^2 = c, \quad \text{где} \quad c = \frac{a^2}{4} - b.$$

По формуле разности квадратов $(y - \sqrt{c})(y + \sqrt{c}) = 0$, откуда $y = \pm\sqrt{c}$.

Применённая выше замена $y = x + a/2$ называется *выделением полного квадрата*. Она налагает единственное требование на арифметику, в которой решается уравнение: мы должны уметь делить на 2.

Квадратные сравнения по простому модулю

Поговорим о квадратных сравнениях в арифметике остатков. Решать мы их не научимся, зато научимся определять количество их решений. Рассматривать будем лишь сравнения по простому модулю, так как именно этот случай представляет наибольший интерес.[1]

В арифметике по простому модулю p выделение полного квадрата возможно при любом $p > 2$. Если же $p = 2$, то $x^2 \equiv x$ и поэтому сравнение, на самом деле, не является квадратным. Поэтому мы будем считать, что $p > 2$, а полный квадрат уже выделен (т.е. мы имеем дело со сравнением вида $x^2 \equiv c \pmod p$).

Если $p \mid c$, то, очевидно, имеем единственное решение $x \equiv 0$. Если c — точный ненулевой квадрат (или, как его ещё называют, *квадратичный вычет*), то сравнение имеет два решения. В противном случае решений нет.

Малая теорема Ферма приходит на помощь

Число p больше 2, поэтому $p - 1$ чётно. Пусть $2P = p - 1$. Согласно МТФ

$$x^{2P} \equiv 1 \pmod p$$

для любого x, не кратного p. Раскладывая двучлен на множители, получаем

$$(x^P - 1)(x^P + 1) \equiv 0 \pmod p.$$

Отсюда следуют два утверждения:

1) x^P сравнимо с -1, 0 или 1 по модулю p.
2) x^P сравнимо с 0 тогда и только тогда, когда $p \mid x$.

Определение. *Символом Лежандра* $\left(\frac{x}{p}\right)$ (стандартное обозначение) или $\mathfrak{L}_p(x)$ (обозначение на протяжении лекции) называется число, равное -1, 0 или 1 и сравнимое с $x^{(p-1)/2}$ по модулю p.

Обозначим первое (и важнейшее!) следствие:

Следствие. *Для символов Лежандра наблюдается мультипликативность* $\mathfrak{L}_p(x)\mathfrak{L}_p(y) = \mathfrak{L}_p(xy)$.

Также очевидно следующее свойство:

Следствие. *Для любого k выполнено* $\mathfrak{L}_p(x + kp) = \mathfrak{L}_p(x)$.

[1] Если модуль составной, то сравнение по такому модулю, согласно КТО, эквивалентно системе сравнений по модулям степеней простых чисел. Оказывается, что ситуация со степенями простого числа выше первой не существенно сложнее, чем с первой степенью (желающим предлагается разобраться в этом самостоятельно).

Связь с квадратными сравнениями

Казалось бы, причём здесь квадратные сравнения? Для ответа на этот вопрос нам понадобится полезный факт о количестве точных квадратов по модулю p.

Лемма (*о количестве квадратичных вычетов*)**.** *По модулю p есть ровно $(p-1)/2$ квадратичных вычетов.*

Доказательство. Рассмотрим отображение $a \mapsto a^2$ на множестве ненулевых остатков. Докажем, что у каждого остатка есть либо 0, либо 2 прообраза. Пусть $b = a^2$. Тогда $b = (p-a)^2$. Заметим, что третьего быть не может: из $a^2 = A^2$ следует $A = a$ или $A = p - a$.

Мы доказали, что образов ровно в 2 раза меньше, чем прообразов. А прообразов было $p - 1$. □

Теперь мы можем перейти непосредственно к основному факту (называемому иногда *критерием Эйлера*).

Лемма (*о количестве решений*)**.** *Сравнение $x^2 \equiv c \pmod p$ имеет $(\mathfrak{L}_p(c) + 1)$ решений.*

Доказательство. Если $p \mid c$, то у сравнения ровно одно решение $x \equiv 0$, и символ Лежандра $\mathfrak{L}_p(0)$ равен 0.

Пусть c не кратно p. Если c — квадрат некоторого числа b (и, следовательно, сравнение имеет 2 решения), то

$$\mathfrak{L}_p(c) \equiv c^{(p-1)/2} \equiv b^{p-1} \equiv 1.$$

Заметим также, что сравнение $c^{(p-1)/2} \equiv 1$ не может иметь больше решений, чем его степень.[2]

Значит, во всех остальных случаях (т.е. когда c не ноль и не квадратичный вычет) $\mathfrak{L}_p(c) = -1$. □

Теперь мы можем определять, сколько решений имеет квадратное сравнение, вычислив символ Лежандра правой части. Но как его считать эффективно?

Мультипликативность позволяет свести подсчёт к символам Лежандра простых аргументов, но дальше необходимо что-то предпринять. Но перед тем, как мы научимся что-либо предпринимать, потребуется посмотреть с другой стороны на некоторые уже известные вещи.

Лемма о декомпозиции

Сейчас мы сформулируем важнейшее следствие КТО.

Лемма (*декомпозиция арифметики по составному модулю*)**.** *Пусть a и b взаимно просты. Тогда между остатками из $\mathbb{Z}_{ab}$ и парами из $\mathbb{Z}_a \times \mathbb{Z}_b$ есть взаимно однозначное соответствие, заданное соотношением*

$$\pi : \ x \mapsto (x \bmod a, x \bmod b)$$

причём

$$\pi^{-1}(x_1, y_1) \cdot \pi^{-1}(x_2, y_2) \equiv \pi^{-1}(x_1 x_2, y_1 y_2) \pmod{ab}. \tag{1}$$

Доказательство. Взаимная однозначность π выполнена согласно КТО (собственно, КТО и утверждает, что отображение π обратимо). Равенство (1) очевидно (оно следует из устойчивости отношения сравнимости относительно произведения). □

Замечание. В соотношении (1) будем опускать π^{-1}, а также будем явно указывать, какая компонента пары какому остатку соответствует. Т.е. вместо (1) будем записывать

$$(x_1, y_1) \cdot (x_2, y_2) \equiv (x_1 x_2, y_1 y_2) \pmod{(a, b)}$$

Замечание. Вспомним, что если a и b взаимно просты, то m взаимно просто с ab тогда и только тогда, когда m взаимно просто с a и взаимно просто с b. Поэтому остатки по $\bmod ab$, взаимно простые с ab, можно отождествить с парами (x, y) такими, что x взаимно просто с a, а y взаимно просто с b.

Следствие. *Если φ — функция Эйлера, то $\varphi(ab) = \varphi(a)\varphi(b)$ для взаимно простых a и b.*

[2] Многочлен степени n не может иметь больше n различных корней в любой арифметике, в которой обратимо каждое ненулевое число. Это — следствие теоремы Безу, которую можно изучить по любому учебнику высшей алгебры.

Квадратичный закон взаимности

Теперь мы можем доказать красивое и полезное соотношение для символов Лежандра.

Теорема (*квадратичный закон взаимности*)**.** *Для простых p и q, больших 2, выполнено*

$$\mathfrak{L}_p(q)\mathfrak{L}_q(p) = (-1)^{(p-1)(q-1)/4}.$$

Доказательство. Если $p = q$, соотношение очевидно. Поэтому без ограничения общности будем считать $p \neq q$.

Рассмотрим множество остатков по модулю pq, взаимно простых с pq. Выберем половину остатков тремя способами, причём так, чтобы никакой остаток не оказался выбранным вместе со своим противоположным. [3]

Способ первый: выберем первые $(p-1)(q-1)/2$ остатков (это те остатки, которые меньше $pq/2$).

Способ второй: выберем те остатки, которые по модулю p не превышают $P = (p-1)/2$.

Способ третий: выберем те остатки, которые по модулю q не превышают $Q = (q-1)/2$.

Для каждого из этих способов посчитаем произведение выбранных чисел:

$$\begin{aligned}
\Pi_1 &\equiv \left(\frac{(p-1)!^Q P!}{q^P P!}, \frac{(q-1)!^P Q!}{p^Q Q!}\right) && (\mathrm{mod}\ (p,q))\\
\Pi_2 &\equiv \left((P!)^{q-1}, (q-1)!^P\right) && (\mathrm{mod}\ (p,q))\\
\Pi_3 &\equiv \left((p-1)!^Q, (Q!)^{p-1}\right) && (\mathrm{mod}\ (p,q))
\end{aligned}$$

Так как из каждой пары $x, -x$ был выбран только один остаток, произведения Π_1, Π_2, Π_3 могут отличаться друг от друга лишь знаком.

Нетрудно видеть, что $\Pi_2 = \Pi_1\mathfrak{L}_q(p)$ и $\Pi_3 = \Pi_1\mathfrak{L}_p(q)$. Осталось заметить, что

$$(P!)^2 \equiv (P!)(P!) \equiv (p-1)!(-1)^P \pmod{p},$$

так как если у остатков от 1 до P поменять знак по модулю p, получится вторая половина остатков (от $P+1$ до $p-1$). Отсюда следует $\Pi_2 \equiv \Pi_3(-1)^{PQ}$. Имеем цепочку сравнений

$$\Pi_1\mathfrak{L}_q(p) \equiv \Pi_2 \equiv \Pi_3(-1)^{PQ} \equiv \Pi_1\mathfrak{L}_p(q)(-1)^{PQ} \pmod{pq}.$$

Сокращение крайних частей этой цепочки на Π_1 даёт нужное нам равенство. □

При помощи квадратичного закона взаимности можно свести вычисление символа Лежандра простого нечётного числа к вычислению символа меньшего числа. Осталось научиться считать $\mathfrak{L}_p(2)$.

Лемма (*дополнение к квадратичному закону взаимности*)**.** $\mathfrak{L}_p(2) = (-1)^{(p^2-1)/8}$.

Доказательство. Дополнение следует из цепочки сравнений (как и в прошлой теореме, $P = (p-1)/2$)

$$\mathfrak{L}_p(2)P! \equiv 2^P P! \equiv 2 \cdot 4 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Пусть сперва $P = 2k$. Тогда крайняя правая часть имеет вид

$$2 \cdot 4 \cdot \ldots \cdot 2k \cdot \ldots \cdot (p-1) \equiv 2 \cdot 4 \cdot \ldots \cdot 2k \cdot (-1)^k \cdot (2k-1) \cdot \ldots \cdot 3 \cdot 1 \equiv P! \cdot (-1)^{P/2}.$$

Если же $P = 2k+1$, то получаем цепочку

$$2 \cdot 4 \cdot \ldots \cdot 2k \cdot \ldots \cdot (p-1) \equiv 2 \cdot 4 \cdot \ldots \cdot 2k \cdot (-1)^{k+1} \cdot (2k+1) \cdot \ldots \cdot 3 \cdot 1 \equiv P! \cdot (-1)^{(P+1)/2}.$$

Отсюда при чётных $(p-1)/2$ имеем $\mathfrak{L}_p(2) = (-1)^{(p-1)/4}$, при нечётных — $\mathfrak{L}_p(2) = (-1)^{(p+1)/4}$. Нетрудно заметить, что эти два соотношения эквивалентны соотношению $\mathfrak{L}_p(2) = (-1)^{(p^2-1)/8}$. □

Квадратичный закон взаимности в совокупности с дополнением и периодичностью позволяют считать символы Лежандра гораздо эффективнее, чем просто по определению.

Пример. Вычислим символ Лежандра $\mathfrak{L}_{13}(23)$.

$$\mathfrak{L}_{13}(23) = \mathfrak{L}_{13}(10) = \mathfrak{L}_{13}(2)\mathfrak{L}_{13}(5) = -\mathfrak{L}_{13}(5) = -\mathfrak{L}_5(13) = -\mathfrak{L}_5(3) = -\mathfrak{L}_3(5) = -\mathfrak{L}_3(2) = 1.$$

[3] Вообще говоря, трудно придумать какой-либо другой столь же очевидный способ разбиения помимо этих трёх.