Теория чисел, остатки, квадратичные вычеты

Начнём с общих фактов, определений, соображений. Все кольца теперь коммутативны ассоциативны и с единицей. Основной задачей теории чисел условно можно назвать следующее: поиск целочисленных решений полиномиальных уравнений с целыми коэффициентами. Мы с вами обсудили на паре, что не существует алгоритма, который решал бы эту задачу и даже более простую задачу. А именно не существует алгоритма, который по уравнению говорил есть ли у данного уравнения решение в целых числах или нет (перебор может ответить «да», но вообще говоря за конечное время не сможет ответить «нет»).

Однако нас интересуют не все уравнения на свете, а некоторые вполне конкретные. Например первой степени. Или второй. Или от одной переменной. Тут всё не так плохо. Однако стоит иметь приёмы, которые применимы всегда, хотя и не дают полного ответа.

Факт. Пусть имеются два кольца R_1 и R_2 и гомоморфизм $\psi\colon R_1 \to R_2$. Пусть так же есть многочлен $g(x_1, \dots, x_n) \in R_1[x_1, \dots, x_n]$. Тогда определим многочлен $\psi(g)$, как многочлен, на коэффициенты которого подействовали отображением φ. Тогда, если у $\psi(g)$ нет решений в R_2, то их нет и в R_1.

Я буду часто опускать обозначения для переменных в записи многочлена. Если ясно, какой гомоморфизм имеется ввиду, то $\psi(g)$ я буду обозначать как g.

Определение 1. *Пусть $g(x_1, \dots, x_n)$ многочлен в $R[x_1, \dots, x_n]$. Пусть задан некий гомоморфизм из кольца R в кольцо A. Это позволяет нам говорить про решения уравнения $p(x_1, \dots, x_n) = 0$ в A. Введём теперь обозначение для этого множества:*

$$V_g(A) = V_{g(x_1,\dots,x_n)}(A) = \{(a_1, \dots, a_n) \in A^n \mid g(a_1, \dots, a_n) = 0\}.$$

В некоторых ситуациях можно сказать заметно больше про устройство решений.

Факт. Пусть $R = R_1 \times \dots \times R_k$. Пусть так же есть многочлен $g(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$. Тогда корню $g(x_1, \dots, x_n)$ в R однозначно соответствует набор корней $g(x_1, \dots, x_n)$ в R_i по всем i. Иными словами:

$$V_g(R) \cong V_g(R_1) \times \dots \times V_g(R_k).$$

Следствие 1. *Функция Эйлера $\varphi(n)$, как количесто решений уравнения $xy = 1 (\operatorname{mod} n)$, мультипликативна, т.е. $\varphi(mn) = \varphi(n)\varphi(m)$, если $(n, m) = 1$.*

В частности решать уравнения в $\mathbb{Z}/m$, где $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, это тоже самое, что уметь решать уравнения по модулю $p_i^{\alpha_i}$ для всех i. Для того, чтобы восстановить решение по модулю m из решений по модулю $p_i^{\alpha_i}$ надо уметь хорошо пользоваться китайской теоремой об остатках. Или, что эквивалентно, уметь рещать системы линейных сравнений.

Системой сравнений называется следующий набор условий:

$$\begin{cases} a_1 x \equiv b_1 \bmod m_1 \\ \quad\vdots \\ a_k x \equiv b_k \bmod m_k \end{cases}$$

Если a_i взаимнопросто с m_i, то от них легко избавиться поделив по модулю m_i. Напомню, что нахождение обратного к a_i по модулю m_i эквивалентно решению уравнения $a_i x + m_i y = 1$. Пусть $a_i = 1$. Вообще говоря m_i не всегда попарно взаимно просты и решение есть не всегда. Если же модули взаимно просты, то необходимо решить систему сначала для m_1 и m_2 — получится некий $x_1 (\operatorname{mod} m_1 m_2)$. Потом надо решить систему $x \equiv x_1 (\operatorname{mod} m_1 m_2)$ и $x \equiv a_3 (\operatorname{mod} m_3)$. И так далее.

Теперь нам понадобится определение.

Определение 2. *Пусть R кольцо. Элемент $x \in R$ называется корнем степени n из единицы, если $x^n = 1$. Корень степени n из единицы называется первообразным, если $x^l \neq 1$ для любого $0 \leq l < n$.*

Мы занимались решением уравнения $x^m \equiv a (\operatorname{mod} n)$. Сразу заменим число a на его остаток от деления на n. Следующий факт обсуждался нами, но в его предыдущей формулировке была ошибка (подробнее на паре):

Факт. Пусть $b = \text{НОД}(a, n)$ и существует k натуральное, что $\text{НОД}(n, \frac{n}{b}^k) = n$. Тогда, если есть решение $x^m \equiv a (\mathrm{mod}\, n)$, то из b можно извлечь корень степени m.

На паре было объяснено (верно), что если из b можно извлечь корень, то достаточно решать уравнение

$$x^m \equiv \tfrac{a}{b} (\mathrm{mod}\, \tfrac{n}{b}).$$

Теперь a взаимно просто с n, то есть обратимо и весь вопрос свёлся к устройству группы обратимых элементов в $\mathbb{Z}/n$. Мы обсудили следующий факт для $R = \mathbb{Z}/p^\alpha$, хотя то же доказательство работает в общем случае.

Факт. Пусть a обратимый элемент в кольце R. Тогда если x_1 и x_2 — решения $x^m = a$, то их отношение удовлетворяет условия $(x_1 x_2^{-1})^m = 1$, то есть является корнем степени m из единицы. Обратно, пусть x решение $x^m = a$, а y-решение $y^m = 1$, то xy тоже решение $x^m = a$.

Следующее утверждение говорит, что в определённых случаях корень степени m можно легко извлечь:

Лемма 1. *Пусть G — конечная абелева группа, НОД$(|G|, m) = 1$, и z есть решение уравнения $mz + |G|y = 1$. Тогда для любого $a \in G$ элемент a^z удовлетворяет $(a^z)^m = 1$.*

Если $G = (\mathbb{Z}/m)^*$, то это даёт явный способ извлечь корень степени m из любого a, если $\text{НОД}(m, |G|) = 1$. Если же $\text{НОД}(m, |G|) \neq 1$, то требуется особое разбирательство.

Разложим n в произведение $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Будем смотреть, что происходит отдельно по модулю $p_i^{\alpha_i}$. Отметим

Факт. Группа обратимых элементов по модулю p^α при нечётном простом p имеет вид

$$(\mathbb{Z}/p^\alpha)^* \cong \mathbb{Z}/\varphi(p^\alpha) \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{\alpha-1}.$$

При $p = 2$ и $\alpha = 1$ эта группа тривиальна. Для других α верно

$$(\mathbb{Z}/2^\alpha)^* \cong \{\pm 1\} \times \mathbb{Z}/2^{\alpha-2}.$$

Разложим m в произведение $m = AB$, где $(\varphi(p^\alpha), A) = 1$, а любой простой сомножитель B является сомножителем $\varphi(p^\alpha)$. Используя предыдущий факт сведём уравнение $x^m \equiv a (\mathrm{mod}\, p^\alpha)$ к уравнению $x^B \equiv a^z (\mathrm{mod}\, p^\alpha)$, где $zA \equiv 1 (\mathrm{mod}\, \varphi(p^\alpha))$.

Теперь есть три целых числа $\varphi(p^\alpha)$, $\mathrm{ord}\, a$ и B, которые характеризуют ситуацию. Ко всему прочему простые делители $\mathrm{ord}(a)$ и B являются делителями $\varphi(p^\alpha)$.

Факт. Из a можно извлечь корень степени m по модулю p^α тогда и только тогда, когда $\mathrm{ord}(a) \cdot B$ делит $\varphi(p^\alpha)$.

Будем пытаться решать уравнения, когда степень $m = 2$. Заметим, что такое m не взаимно просто ни с каким $\varphi(n)$ кроме $n = 2$. Это исключает автоматическое применение леммы 1.

Рассмотрим уравнение $x^2 \equiv a (\mathrm{mod}\, p)$, где p — простое.

Определение 3. *Пусть p — нечётное простое число, a, такое что НОД$(a, p) = 1$. Символом Лежандра $\left(\frac{a}{p}\right)$ по определению назовём число*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \textit{если уравнение } x^2 \equiv a (\mathrm{mod}\, p) \textit{ разрешимо} \\ -1, & \textit{иначе} \end{cases}$$

Факт. Для символа Лежандра имеет место формула:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p)$$

Факт. Имеют места следующие свойства символа Лежандра:

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

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

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

г) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, иными словами символ Лежандра — гомоморфизм.

Эти свойства позволяют руками считать является число квадратом или нет, однако в процессе приходится раскладывать числа на простые множители, что неудобно. Избежать этих проблем позволяет символ Якоби.

Задачи

Задание 1. Покажите, что уравнение $15x^2 - 7y^2 = 9$ не имеет решений в целых числах.

Задание 2. Найдите $\varphi(40)$ и посчитайте $14^{777} (\operatorname{mod} 40)$.

Задание 3. Найдите обратный к 5 по модулю 29 и решите систему сравнений

$$\begin{cases} 5x \equiv 17 (\operatorname{mod} 29) \\ x \equiv 6 (\operatorname{mod} 35) \end{cases}$$

Задание 4. Вычислите символы Лежандра
а) $\left(\frac{39}{103}\right)$
б) $\left(\frac{470}{991}\right)$
в) $\left(\frac{430}{911}\right)$

Задание 5. Найдите $\varphi(129)$ и решите $x^5 = 16$ в кольце $\mathbb{Z}/129$.

Задание 6. Сколько решений имеет уравнение $x^3 = 1$ в кольце $\mathbb{Z}/2520$?

Задание 7. Пусть p — простое число, а a и b взаимно просты с p. Покажите, что хотя бы одно из трёх чисел a, b, ab является квадратом по модулю p.

Задание 8. Покажите, что $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$ имеет вещественный корень, корень по модулю 8 и корень по модулю p для любого простого нечётного p, но не имеет целых корней.

Задание 9. Покажите, что если число n нечётно, то количество решений уравнения $x^2 \equiv 1 (\operatorname{mod} n)$ определяет число различных простых делителей n. А что происходит при чётном n?

Задание 10. Пусть p — простое число вида $4k + 3$. Пусть a — квадратичный вычет по модулю p. Найдите такое натуральное l, что $(a^l)^2 \equiv a (\operatorname{mod} n)$.

В сторону

Задача 8 может быть доделана до примера многочлена, который имеет корни по любому модулю, но не имеет целых корней. Как видно игра состоит в том, что корень может появиться в разных сомножителях. Вопрос тогда можно поставить следующим образом: существует ли неприводимый многочлен с указанными свойствами. Ответ: для одной переменной — нет. Для большего числа переменных — да. Вот например $x^2 + 23y^2 = 41$. Однако этот многочлен имеет рациональное решение, что сразу даёт решение по модулю почти любого n. Вопрос можно ли потребовать дополнительно, чтобы у уравнения не было не только целых, но и рациональных решений. Ответ — можно, но только для многочленов степени не ниже трёх (и видимо от не менее чем двух переменных).