Лекция «Классы вычетов. Теорема Ферма. Китайская теорема об остатках»

Поздняков Сергей Николаевич

запись конспекта: Кацер Евгений

дата лекции: 21 марта 2018 г.

09:00

Задача (С прошлой лекции)**.** Определить признак делимости на 7 числа, заданного в двоичной системе счисления. Признак представить как в операциях десятичной, так и двоичной систем счисления. Рассмотрим оба варианта:

- Наше число, заданное в двоичной системе счисления, выглядит так:

$$x = b_n 2^n + b_{n-1} 2^{n-1} + \cdots + b_4 2^4 + b_3 2^3 + b_2 2^2 + b_1 2^1 + b_0$$

Свойство делиться на 7 сохранится, если мы уменьшим число на величину, кратную семи, поэтому в этом выражении можно заменить степени двойки их остатками от деления на 7. Заметим, что остаток от деления $2^3 = 8$ на 7 равен 1. Тогда остаток от вдвое большего числа 2^4 на 7 можно найти, умножив предыдущий остаток на 2, аналогично, остаток от деления 2^5 получается умножением предыдущего остатка на 2, что дает 4, дальнейшее умножение на 2 дает 8, но, как уже говорилось, можно вместо 8 взять его остаток от деления на 7, и мы снова получим 1, то есть последовательность остатков от деления степеней 2 на 7 зациклится (в дальнейшем будем использовать символ $\equiv$, означающий, что у чисел одинаковые остатки)

$$x = b_n 2^n + b_{n-1} 2^{n-1} + \underbrace{\cdots + b_4 \underset{\equiv 2}{2^4} + b_3 \underset{\equiv 1}{2^3}}_{} + \underbrace{b_2 \underset{\equiv 4}{2^2} + b_1 \underset{\equiv 2}{2} + b_0 \underset{\equiv 1}{1}}_{\text{цикл}}$$

Тогда, если

$$b_0 + 2b_1 + 4b_2 + b_3 + 2b_4 + 4b_5 + \ldots \ \vdots\ 7 \Rightarrow x \vdots 7 \ (*)$$

— признак делимости на 7 для операций, выполняемых в десятичной системе счисления.

- В двоичной системе полученные на предыдущем шаге коэфициенты $1, 2, 4$ — степени двойки, следовательно, если рассматривать $(*)$ в двоичной системе счисления, коэфициенты $4b_2 + 2b_1 + b_0$ можно записать как $\overline{b_2b_1b_0}$, $4b_5 + 2b_4 + b_3$ можно записать $\overline{b_5b_4b_3}$ и так далее. Получается, что число можно разбить на тройки (если чисел до тройки не хватает, дополнить впереди нулями). А потом сложить эти двоичные числа, и, если сумма будет делиться на 7, то и x будет делиться на 7:

$$\overline{b_0b_1b_2} + \overline{b_3b_4b_5} + \ldots \vdots 7 \Rightarrow x \vdots 7$$

— признак делимости на 7 в двоичной системе счисления.

Пример. Проверим по обоим признакам $35_{10} = 100011_2$:

- Проверим по десятичному признаку: для этого добавим веса и запишем сумму:

$$\underset{4\,2\,1\,4\,2\,1}{100011} \Rightarrow 4 \cdot 1 + 2 \cdot 1 + 1 \cdot 1 = 7 \vdots 7$$

- Проверим по двоичному признаку, для этого разобьем число на тройки и сложим их вместе:

$$\overbrace{100}\,\overbrace{011} \Rightarrow 100 + 011 = 111 = 7 \vdots 7$$

Примечание. При проверке делимости на 7 в двоичной системе счисления не обязательно переводить результат в десятичную систему счисления, так как при многократном применении признака у нас получится число, состоящее из трех двоичных цифр, делящееся на 7. Таких чисел всего два: 000 (ноль) и 111 (семь).

1 Классы вычетов

16:03

Пример. Если к нечетному числу прибавить нечетное — получится четное. Если нечетное число умножить на четное — получится четное. Мы можем оперировать этими понятиями. Мы не складывали конкретные числа 3 и 7, мы работали с классами чисел, то есть мы сразу сложили все нечетные числа со всеми нечетными и заявили, что полученное множество совпадает со множеством четных чисел или является его частью. То, с чем мы сейчас работаем, называется *классами вычетов*. Их можно привязать к остаткам естественным образом, например:

- Все нечетные числа можно обозначить как множество чисел, дающих остаток 1 при делении на 2. Обозначают палочкой над числом $\overline{1}$ и называют классом вычетов.

$$\{2k+1 \mid k \in \mathbb{Z}\} = \overline{1}$$

- Все четные числа можно обозначить, как множество чисел, дающих остаток 0 при делении на 2.

$$\{2k \mid k \in \mathbb{Z}\} = \overline{0}$$

Классы вычетов обозначают $\mathbb{Z}_2$ или $\mathbb{Z}/2\mathbb{Z}$. Последнее обозначение связано с понятием факторизации. То, что стоит под чертой, показывает, что все четные числа рассматриваются, как один объект, и тогда множество всех целых чисел относительно $2\mathbb{Z}$ распадается на две части. Одни попадают в $2\mathbb{Z}$ (четные числа), а другие — нет (нечетные числа). Значок деления выбран не случайно, ведь когда мы записываем дробь $6/3$, мы можем трактовать это как действие «разделить множество из 6 объектов на части по 3 объекта в каждой».

Таблица 1: Арифметика в $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$

(a) Арифметика сложения

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

(b) Арифметика умножения

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

1. (a) Четное+Четное=Четное (как и $0+0=0$)
   Четное+Нечетное=Нечетное (как и $0+1=1$)
   Нечетное+Нечетное=Четное (как и $1+1=0$)

   (b) Четное$*$Четное=Четное (как и $0 \cdot 0 = 0$)
   Четное$*$Нечетное=Четное (как и $0 \cdot 1 = 0$)
   Нечетное$*$Нечетное=Нечетное (как и $1 \cdot 1 = 1$)

Примечание. С помощью такой арифметики мы можем осуществлять арифметические операции сразу над бесконечными количествами чисел.

20:05

Пример. Рассмотрим $\mathbb{Z}_5$ и $\mathbb{Z}_6$.

Таблица 2: Арифметика в $\mathbb{Z}_5$ и $\mathbb{Z}_6$

(a) Умножение в $\mathbb{Z}_5$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(b) Умножение в $\mathbb{Z}_6$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Примечание. Заметим, что классы вычетов $\overline{2}$ и $\overline{3}$ в $\mathbb{Z}_6$ являются делителями нуля. Это означает, что найдутся такие ненулевые классы, которые при умножении на них дадут класс вычетов 0. Например, для $\overline{3}$ это классы $\overline{2}$ и $\overline{4}$.

«Хорошие» строчки или столбцы получаются, если число и модуль класса вычета взаимно просты. В этих строках и столбцах встречаются все варианты классов вычетов.

Структура, образуемая $\mathbb{Z}_5$, называется полем (определены не только сложение, вычитание и умножение, но и деление на любой класс, кроме $\overline{0}$). Например, $\overline{4}/\overline{3} = \overline{3}$ или $\overline{4}/\overline{2} = \overline{2}$. Мы можем это сделать, так как в каждом столбце или строчке есть все числа. Полями также являются множества $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ и др.

Структура, образуемая $\mathbb{Z}_6$ называется — кольцо (все операции, кроме деления определены). Например, мы не можем разделить $\overline{4}$ на $\overline{3}$. Кольцами также являются многочлены (т.к. всегда поделить многочлен на многочлен не получится), множество $\mathbb{Z}$ (т.к. тоже всегда поделить целое число на целое не получится) и др.

Поле вычетов по простому модулю всегда конечное, и в нем справедливы все операции, свойства и формулы, выведенные в математике.

Когда мы работаем с классами вычетов, мы можем записать множество нечетных чисел [1], как:

$$\{2k+1 \mid k \in \mathbb{Z}\} = \{2k+3 \mid k \in \mathbb{Z}\}$$

$\mathbb{Z}$ — бесконечное, поэтому не важно, какое число мы возьмем в качестве базового (от которого будем вести отчет). Таким образом в нашей арифметике мы можем не ограничивать себя выбором конкретного представителя класса вычетов, а выбирать тот, который в данной ситуации

более удобен:

$$\overline{1} = \overline{3} = (\overline{-1})$$

С классами вычетов мы можем работать, как с целыми числами. Иногда при простых вычислениях это очень удобно.

Рассмотрим эффект, возникающий при работе в конечных полях:

Пример. Решить уравнение $x^2 + \overline{2}x + \overline{3} = \overline{0}$ в $\mathbb{Z}_{17}$.

Все операции и свойства, которые работают с вещественными, рациональными числами, переносятся на конечные поля. Если классы вычетов образуют поле, то для работы с ними можно использовать выведенные в школе формулы. Например, проверим применимость к нашей задаче известной формулы квадратного уравнения:

$$x_{1,2} = -\overline{1} \pm \sqrt{\overline{1} - \overline{3}} = -\overline{1} \pm \sqrt{-\overline{2}} = -\overline{1} \pm \sqrt{-\overline{2} + \overline{17}} =$$

$$= -\overline{1} \pm \sqrt{\overline{15}} = -\overline{1} \pm \sqrt{\overline{32}} = -\overline{1} \pm \sqrt{\overline{49}} = -\overline{1} \pm \overline{7}$$

$x_1 = \overline{6}$
$x_1 = -\overline{8} = \overline{9}$
Проверка:

- $6^2 + 2 \cdot 6 + 3 = 36 + 12 + 3 = 51 \equiv 0 \pmod{17}$
- $9^2 + 2 \cdot 9 + 3 = 81 + 18 + 3 = 102 \equiv 0 \pmod{17}$

Примечание 1. В рассмотренном примере [1] всего 17 классов вычетов, поэтому корни можно найти перебором. В этом заключается достоинство арифметики остатков. Не всегда нужно пользоваться формулами, иногда можно использовать подбор.

Примечание 2. $\mathbb{Z}_m$ содержит m классов вычетов: $\overline{0},\ \overline{1},\ \ldots\ ,\ \overline{m-1}$ — *полная система классов вычетов* ($\overline{a}$ — представитель класса вычетов).

39:07

Задача. 1. Доказать, что если добавить ко всем представителям класса вычетов минусы, они все равно будут образовывать полную систему классов вычетов:

$$\overline{0},\ \overline{-1},\ \ldots\ ,\ \overline{1-m}$$

2. Доказать, что если добавить ко всем представителям класса вычетов a, они все равно будут образовывать полную систему классов вычетов:

$$\overline{0+a},\ \overline{1+a},\ \ldots\ ,\ \overline{m-1+a}$$

3. Найти такие a, при которых умножение на a тоже даст полную систему классов вычетов:

$$\overline{0},\ \overline{a},\ \ldots\ ,\ \overline{(m-1)*a}$$

Примечание. Когда мы говорим о классах вычетов, мы имеем в виду множество целых чисел. Иногда удобно использовать свойства, присущие целым числам, делимость, а иногда арифметику классов вычетов и не думать ни о каких целых числах, как в примере [1].

А теперь попробуем наоборот свести свойства классов вычетов к свойствам целых чисел. Для этого введем определение: 42:02

Определение. $a \equiv b \pmod m$ (a сравнимо с b по модулю m), если $\exists\ q_1, q_2 : \begin{cases} a = m \cdot q_1 + r \\ b = m \cdot q_2 + r \end{cases}$ (a и b дают одинаковые остатки от деления на m).

Теорема. $a \equiv b \pmod m \Leftrightarrow (a-b) \vdots m$

Доказательство. $\Rightarrow$ По определению сравнимости a можно записать так: $a = m \cdot q_1 + r$, а b так: $b = m \cdot q_2 + r$, тогда:

$$a - b = m \cdot q_1 + r - (m \cdot q_2 + r) = m \cdot q_1 - m \cdot q_2 = m \cdot (q_1 - q_2)$$

Обозначим $(q_1 - q_2)$ за q, тогда:

$$a - b = m \cdot q$$

У нас получилось в точности определение делимости.
$\Leftarrow$ доказать самостоятельно.

□

1.1 Свойства сравнений:

1. $\begin{cases} a \equiv b \pmod m \\ b \equiv c \pmod m \end{cases} \Rightarrow a \equiv c \pmod m.$

   Доказательство. Числа a и b дают одинаковые остатки при делении на m. Обозначим его r. Числа b и c тоже дают одинаковые остатки при делении на m, но остаток от деления b на m мы уже обозначили r, значит остаток деления c на m тоже $r \Rightarrow a \equiv c \pmod m$. Также это свойство можно доказать с помощью свойств делимости.

   □

2. (a) $a \cdot k \equiv b \cdot k \pmod{m \cdot k} \Leftrightarrow a \equiv b \pmod{m}$.

Доказательство. По теореме (о сведении сравнения к делимости):

$$a \cdot k \equiv b \cdot k \pmod{m \cdot k} \Leftrightarrow a \cdot k - b \cdot k \vdots m \cdot k$$

Разделим на k, чтобы деление было определено в условие в условии надо дописать, что $k \neq 0$. После скоращения получим:

$$a - b \vdots m$$

а это по теореме то же, что и:

$$a \equiv b \pmod{m}$$

□

Свойство после добавления условия:

$$a \cdot k \equiv b \cdot k \pmod{m \cdot k} \text{ и } k \neq 0 \Leftrightarrow a \equiv b \pmod{m}$$

(b) $a \cdot k \equiv b \cdot k \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$. Здесь мы не умножем модуль на k. Возможно ли, что и (a) и (b) справедливы одновременно? Давайте проведем доказательство и выясним.

Доказательство. $\Rightarrow$ По теореме (о сведении сравнения к делимости):

$$a \cdot k \equiv b \cdot k \pmod{m} \Leftrightarrow (a - b) \cdot k \vdots m$$

У нас получилось, что произведение разности и k делится на m. Нужно доказать, что разность делится на m. Это гарантировано только в одном случае, если k взаимно просто с m. При выполнении этого условия:

$$(a - b) \cdot k \vdots m \Rightarrow a - b \vdots m$$

а это по теореме то же, что и:

$$a \equiv b \pmod{m}$$

$\Leftarrow$ Если $a - b \vdots m$, то $(a - b) \cdot k \vdots m$ всегда.

Замечание. Заметим, что для доказательства второго свойства в одну сторону нужно ограничение на k, а в другую — нет.

□

Свойство после добавления условия:

$$a \cdot k \equiv b \cdot k \pmod{m} \text{ и } k \text{ — вз. просто с } m \Rightarrow a \equiv b \pmod{m}$$

$$a \equiv b \pmod{m} \Rightarrow a \cdot k \equiv b \cdot k \pmod{m}$$

Пример. $36x \equiv 24y \pmod{64}$ разделим на 4

$9x \equiv 6y \vdots 3 \pmod{16}$ (3 взаимно просто с 16) $\Rightarrow 3x \equiv 2y \pmod{16}$

54:40

Задача 1. Доказать, что уравнение $x^2 - y^2 = 10^n$ не имеет решений при $n = 1$

$$x^2 - y^2 = (x - y) \cdot (x + y) = 10$$

Произведение этих множителей — четное число $\Rightarrow$ по крайней мере один из множителей должен быть четным. Но если $x - y$ — четный, то и $x + y$ — четный, и наоборот, но 10 не раскладывается на два четных множителя.

Переформулируем на язык сравнений: если $x - y \equiv 0 \pmod{2} \Rightarrow$
$\Rightarrow x + y \equiv 0 \pmod{2}$)

$$x - y = x + (-1) \cdot y,$$

а $(-1) = 1$ по модулю 2 $\Rightarrow (x - y) \equiv (x + y) \equiv 0 \pmod{2}$

Задача 2. Вывести новые свойства сравнений, чтобы перевести рассуждения из задачи 1 полностью на язык сравнений и доказать:

$$x^2 \equiv y^2 \pmod{2} \Rightarrow x^2 \equiv y^2 \pmod{4}$$

58:55

§13 Малая теорема Ферма

Проведем эксперимент: посмотрим, насколько интересными свойствами обладают степени натуральных чисел по простому модулю p. Будем рассматривать выражения вида $n^p \mod p$.

Пример 1. Пусть $n = 3$, $p = 5$.

$$\begin{cases} 3^1 \equiv 3 \pmod 5 \\ 3^2 = 9 \equiv 4 \pmod 5 \\ 3^3 = 4 \cdot 3 = 12 \equiv 2 \pmod 5 \\ 3^4 = 2 \cdot 3 = 6 \equiv 1 \pmod 5 \\ 3^5 = 1 \cdot 3 = 3 \equiv 3 \pmod 5 \end{cases}$$

Мы можем предположить, что $n^p \equiv n \pmod p$ — это и есть малая теорема Ферма. Рассмотрим еще один пример.

Пример 2. Пусть $n = 4$, $p = 5$.

$$\begin{cases} 4^1 \equiv (-1) \equiv 4 \pmod 5 \\ 4^2 \equiv (-1) \cdot (-1) = 1 \pmod 5 \\ 4^3 = 1 \cdot 4 \equiv 4 \pmod 5 \\ 4^4 \equiv (-1) \cdot (-1) = 1 \pmod 5 \\ 4^5 = 1 \cdot 4 \equiv 4 \pmod 5 \end{cases}$$

Примечание. Как видно из примера 2, равенство не обязательно наступает только на p-ом шаге.

Теорема (Малая теорема Ферма)**.** $n^p \equiv n \pmod p$

Доказательство. Рассмотрим полный набор классов вычетов, кроме $\overline{0}$.

$1, 2, \ldots, (p-1)$ — ненулевые остатки. Умножим их на n. ($\diamond$)

$n, 2n, \ldots, n \cdot (p-1)$ — дадут ли эти числа те же самые остатки (будет ли это тот же набор классов вычетов)? ($*$)

65:37

Лемма. *Если p — простое, n не делится на p, то ($*$) — все ненулевые остатки от деления на p.*

Доказательство. От противного: пусть in и jn дают одинаковые остатки ($i \neq j$).

$$in \equiv jn \pmod p \Leftrightarrow [\text{ по теореме }] \Leftrightarrow in - jn \vdots p \Leftrightarrow n \cdot (i-j) \vdots p \Rightarrow$$

$$\Rightarrow [\text{ т.к. } n \text{ не делится на } p\ ] \Rightarrow (i-j) \vdots p$$

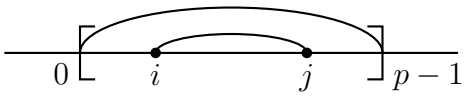

Рис. 1: i и j относительно других остатков

$|i-j|$ не превышает $|p-1-0|$ и поэтому строго меньше p (i и j — остатки от деления на p)

$$\begin{cases} |i-j| < p \\ |i-j| \vdots p \end{cases} \Rightarrow i-j=0 \Rightarrow i=j \text{ — противоречие!!!}$$

□

Таким образом множество остатков при умножении их на n не изменилось, значит, остатки произведений $(*)$ и $(\diamond)$ при делении на p будут одинаковы:

$$n \cdot 2n \cdot \ \ldots \ \cdot (p-1)n \equiv 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1) \pmod{p}$$

Вынесем все n из произведения в левой части.

$$n^{p-1} \cdot (1 \cdot 2 \cdot \ \ldots \ \cdot (p-1)) \equiv 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1) \pmod{p}$$

Разделим обе части на факториал $(p-1)$.

$$n^{p-1} \cdot (1 \cdot 2 \cdot \ \ldots \ \cdot (p-1)) \equiv 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1) \pmod{p} \mid /(p-1)!$$

Домножим на n обе части.

$$n^{p-1} \equiv 1 \pmod{p} \mid \cdot n$$

$$n^p \equiv n \pmod{p}$$

□

Примечание. Мы можем разделить на каждый множитель $(p-1)!$ по свойству сравнений, позволяющему делить обе части на множитель, взаимно простой с модулем, а все остатки от 1 до $p-1$ взаимно просты с p.

73:45

§14 Китайская теорема об остатках

Наименьшее натуральное число, делящееся на $2, 3, 5$ — 30.

Наименьшее натуральное число, дающее остаток 1 при делении на $2, 3, 5$ — 31.

А наименьшее натуральное число, дающее остаток 1 при делении на 2, 2 при делении на 3, 3 при делении на 5, уже так просто не посчитать. На этот вопрос дает ответ китайская теорема об остатках.

Теорема. *Если:*

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ x \equiv r_2 \pmod{m_2} \\ \vdots \\ x \equiv r_n \pmod{m_n} \end{cases} \quad (\forall i, j \ (i \neq j) \ m_i \text{ и } m_j \text{ — взаимно простые}), \text{ то}$$

$$x \equiv c_1 d_1 r_1 + c_2 d_2 r_2 + \ldots + c_n d_n r_n \pmod{m},$$

где $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$, $c_i = \dfrac{m}{m_i} = m_1 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_n$ *(делить никогда не нужно), а* d_i *— такое число, что* $c_i d_i \equiv 1 \pmod{m_i}$

Примечание. Если модули не взаимно простые, то система сведется либо к описанной в теореме, либо не будет иметь решений.

Заметим, что для ответа используется принцип "разделяй и властвуй". Слагаемое с номером i обеспечивает выполнение i-го уравнения, не влияя на выполнение остальных. Это будет видно из следующего доказательства.

Доказательство. Проверим, что построенное решение удовлетворяет каждому из условий. Рассмотрим i-ое условие.

$$x \overset{?}{\equiv} r_i \pmod{m_i}$$

Все слагаемые, кроме i-го будут делиться на m_i, так как в каждом будет присутствовать m_i, следовательно, x будет сравним с i-ым слагаемым, а все остальные слагаемые дадут остаток 0.

$$x = \underbrace{m_2 \cdot \ldots \cdot m_i \cdot \ldots \cdot m_n \cdot d_1 \cdot r_1}_{\vdots m_i} + \ldots \equiv c_i d_i r_i \pmod{m_i}$$

Но c_i и d_i заданы так, что $c_i d_i = 1$, следовательно, останется только r_i.

$$\underbrace{c_i d_i}_{\equiv 1} r_i \equiv r_i \pmod{m_i}$$

□ 84:30

Замечание (как считать обратное).

Лемма. Если m *и* n *— взаимопростые, то существует такое* n'*, что* $n \cdot n' \equiv 1 \pmod{m}$.

Доказательство. Доказательство также является алгоритмом нахождения обратного:

$$n \cdot n' \equiv 1 \pmod{m} \Leftrightarrow [\text{по теореме}] \Leftrightarrow n \cdot n' - 1 \vdots m$$

Обозначим n' за x. Т.к. $(n \cdot n' - 1)$ делится на m, то существует число, обозначим его y, такое, что $my = n \cdot n' - 1$, тогда

$$n \cdot x - 1 = m \cdot y$$

Пренесем $m \cdot y$ в левую часть:

$$n \cdot x - m \cdot y = 1$$

Это диафантово уравнение. Причем при нахождении ответа нас интересует только x.

□