

2. ВТОРАЯ ЛЕКЦИЯ, 13 СЕНТЯБРЯ 2021 г.

2.1. Сравнения. Пусть m — целое число, не меньшее 2. Будем говорить, что два числа $a, b \in \mathbb{Z}$ *сравнимы по модулю m* , если $a - b$ делится на m . Обозначение:

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

Ясно, что это равносильно тому, что a и b дают при делении на m одинаковые остатки.

Легко проверить следующее предложение (сделайте это сами):

Предложение 2.1. (1) Отношение «быть сравнимыми по модулю m » является отношением эквивалентности на $\mathbb{Z}$;

(2) Если $a \equiv b \pmod{m}$ и $a' \equiv b' \pmod{m}$, то $a + a' \equiv b + b' \pmod{m}$ и $aa' \equiv bb' \pmod{m}$.

Рассмотрим множество *классов эквивалентности* по этому отношению; будем называть их *классами вычетов*. Введем на них операции сложения и умножения так: если $[a] = \{a + km \mid k \in \mathbb{Z}\}$ — класс, содержащий a , и $[b]$ — аналогично определенный класс, содержащий b , то $[a] + [b] = [a + b]$ и $[a] \cdot [b] = [ab]$. Вторая часть предыдущего предложения показывает, что это определение корректно.

Определенные таким образом операции удовлетворяют обычным законам арифметических действий: для них верны переместительный, сочетательный и распределительный законы, существуют нуль и единица (то есть они образуют *кольцо* — этот термин будет объяснён на следующей лекции).

Для примера составим таблицы умножения остатков по модулю 6 и 7. При этом мы опускаем строчку и столбец, отвечающие умножению на нуль: они состоят из одних нулей.

6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Сопоставив эти таблицы, можно сделать некоторые наблюдения. Так, например, в первой из таблиц (по модулю 6) встречаются нули; иначе говоря, существуют такие два ненулевых остатка, произведение которых равно нулю. Такие остатки называются *делителями нуля*. Так, например, по модулю 6 делителями нуля будут числа 2, 3 и 4.

Ясно, что по составному модулю делители нуля всегда будут: так, если m составное, то существуют такие k и ℓ , отличные от единицы, для которых $m = k\ell$. Поэтому числа k и ℓ соответствуют ненулевым остаткам, произведение которых равно нулю по модулю m .

Чуть менее тривиален обратный вопрос: верно ли, что в арифметике остатков по простому модулю делителей нуля нет? (Например, по модулю 7 их нет, что подтверждается второй таблицей). Оказывается, что это тоже верно.

Докажем это. Рассмотрим арифметику остатков по модулю p и предположим противное: пусть нашлись такие k и ℓ , которые дают при делении на p ненулевые остатки — но при этом их произведение делится на p нацело, то есть $k\ell = pm$. Но это противоречило бы основной теореме арифметики: действительно, в разложение числа $k\ell$ на простые множители не может входить число p , т.к. ни k , ни ℓ на p не

делится. Однако это же число равно pt , в разложение которого на простые множители p , очевидно, входит. Это противоречит единственности разложения целого числа на простые множители.

Мы получили следующее

Предложение 2.2. *В арифметике остатков по модулю t нет делителей нуля тогда и только тогда, когда t является простым числом.*

2.2. Остатки по простому модулю. Далее нас будет интересовать в основном тот случай, когда t простое; в этом случае будем обозначать его буквой p , а соответствующее множество остатков (с операциями сложения и умножения) будет обозначаться через $\mathbb{Z}/p\mathbb{Z}$.

Можно сделать еще одно наблюдение: в каждой из строк второй таблицы записаны в каком-то порядке все ненулевые остатки по модулю 7: все числа от 1 до 6 встречаются в ней по одному разу, и ни одно не повторяется. Оказывается, что так обстоит дело и для произвольного простого модуля:

Предложение 2.3. *Пусть p простое, $a \in \mathbb{Z}/p\mathbb{Z}$ — некоторый ненулевой остаток. Тогда среди остатков $0, a, 2a, 3a, \dots, (p-1)a$ нет повторяющихся.*

Доказательство. Пусть два остатка $k, m \in \mathbb{Z}/p\mathbb{Z}$ таковы, что $ak = am$. Тогда $a(k - m)$ равно нулю. Но мы только что доказали, что в $\mathbb{Z}/p\mathbb{Z}$ произведение двух ненулевых остатков отлично от нуля. Поскольку по условию $a \neq 0$, то это значит, что $k - m = 0$, то есть $k = m$, что и требовалось. $\square$

Из этого несложного предложения вытекает несколько интересных следствий.

Следствие 2.4. *В $\mathbb{Z}/p\mathbb{Z}$ линейное уравнение $ax = b$ при $a \neq 0$ имеет единственное решение.*

Доказательство. Действительно, переберем все возможные значения x , то есть рассмотрим все остатки вида $0, a, 2a, \dots$. Согласно предыдущему предложению, среди них будет остаток, равный b , причем ровно один. $\square$

Частным случаем этого следствия является следующее утверждение.

Следствие 2.5. *Для каждого ненулевого числа $a \in \mathbb{Z}/p\mathbb{Z}$ существует и единственно обратное, то есть такое число x , что $ax = 1$.*

Это число обычно обозначается a^{-1} .

Пример 2.6. Например, в $\mathbb{Z}/7\mathbb{Z}$ обратным к остатку 3 будет остаток 5: действительно, $3 \cdot 5 = 15$, что дает остаток 1 по модулю 7.

Замечание 2.7. Отметим, что в арифметике по составному модулю ни то, ни другое следствие не будет выполняться. Так, например, по модулю 6 уравнение $2x = 4$ будет иметь два решения: 2 и 5, а ни один из остатков 2, 3 и 4 не будет обратим.

Упражнение 2.8. Выясните, какие остатки будут обратимы в арифметике остатков по произвольному составному модулю m .

А что будет, если перемножить все остатки $a, 2a, \dots, (p-1)a$? С одной стороны, получится $a^{p-1} \cdot 1 \cdot 2 \cdot \dots \cdot (p-1) = a^{p-1}(p-1)!$. С другой стороны, согласно предложению 2.3, эти остатки — это те же $1, 2, \dots, p-1$, только записанные в другом порядке. То есть их произведение равняется $(p-1)!$. Тем самым мы получаем равенство

$$a^{p-1}(p-1)! = (p-1)!.$$

Поделив это равенство на $(p-1)!$ (контрольный вопрос: почему это можно сделать?), получаем следующую теорему.

Теорема 2.9 (малая теорема Ферма). Пусть p простое. Тогда для любого a , не кратного p , верно, что

$$a^{p-1} \equiv 1 \pmod{p}.$$

Замечание 2.10. Иногда эту теорему формулируют так: для любого $a \in \mathbb{Z}/p\mathbb{Z}$ верно, что

$$a^p \equiv a \pmod{p}.$$

Упражнение 2.11. Покажите, что остатки, обратные к самим себе, то есть такие, для которых $a = a^{-1}$ — это в точности 1 и $p-1$. Выведите отсюда теорему Вильсона:

$$(p-1)! \equiv -1 \pmod{p}.$$

2.3. Китайская теорема об остатках.

Теорема 2.12. Пусть $n_1, \dots, n_k$ — набор попарно взаимно простых чисел, и пусть $r_1, \dots, r_k$ — произвольные целые числа. Тогда существует такое число M , для которого

$$\begin{cases} M \equiv r_1 \pmod{n_1}; \\ \dots \\ M \equiv r_k \pmod{n_k}. \end{cases}$$

Более того, если M и M' — два решения этой системы сравнений, то

$$M \equiv M' \pmod{n_1 \dots n_k}.$$

Доказательство. Пусть $N = n_1 \dots n_k$. Обозначим через N_i произведение всех чисел $n_1, \dots, n_k$, кроме n_i . Пусть M_i — такое число, для которого $M_i N_i \equiv 1 \pmod{n_i}$; такое число существует, т.к. N_i взаимно просто с n_i . Тем самым число $M_i N_i$ даёт остаток 1 по модулю n_i и остаток 0 по всем остальным модулям $n_1, \dots, n_k$, кроме n_i . Найдя такие числа, нетрудно построить и решение исходной системы сравнений: оно равно

$$M = r_1 M_1 N_1 + \dots + r_k M_k N_k.$$

Пусть теперь M, M' — два таких числа; тогда их разность удовлетворяет сравнениям $M - M' \equiv 0 \pmod{n_i}$ при всех $i = 1, \dots, k$. Но т.к. n_i попарно взаимно просты, отсюда следует, что $M - M'$ делится на $N = n_1 \dots n_k$, что и требовалось. $\square$

Вторую часть теоремы можно сформулировать так: число M , удовлетворяющее такой системе сравнений и неравенствам $0 \leq M < N$, единственно.

2.4. Интерполяционный многочлен Лагранжа. Китайская теорема об остатках также справедлива и для многочленов от одной переменной — например, с вещественными (или комплексными) коэффициентами. Доказательство аналогично, т.к. не использует ничего, кроме деления с остатком. Зададимся несколькими попарно различными числами $a_1, \dots, a_k$. По теореме Безу, остаток от деления многочлена $P(x)$ на двучлен $x - a_i$ есть не что иное, как $P(a_i)$, то есть значение многочлена в соответствующей точке. Рассмотрим в качестве модулей в китайской теореме об остатках многочлены $x - a_i$; они все попарно взаимно просты. Тогда мы получаем следствие из китайской теоремы об остатках:

Следствие 2.13. Пусть $a_i \in \mathbb{R}$ попарно различны, b_i произвольны, $1 \leq i \leq k$. Существует единственный многочлен $P(x)$, степень которого не превосходит $k-1$, для которого $P(a_i) = b_i$.

Действительно, последнее условие эквивалентно тому, что $P_i \equiv b_i \pmod{x - a_i}$. Далее, как только такой многочлен построен, его можно поделить с остатком на $(x - a_1) \dots (x - a_k)$, и мы получим многочлен степени не выше $k - 1$; он будет единственным, т.к. разность двух таких многочленов, согласно китайской теореме об остатках, делится на $(x - a_1) \dots (x - a_k)$.

Также китайская теорема об остатках даёт эффективный способ построения такого многочлена. Для этого построим многочлен $P_i(x)$, равный 1 в a_i и 0 в остальных точках a_j . Он должен делиться на $(x - a_1) \dots \widehat{(x - a_i)} \dots (x - a_k)$; далее, сделать его единичным в точке a_i можно, поделив последний многочлен на его значение в a_i :

$$P_i(x) = \frac{(x - a_1) \dots \widehat{(x - a_i)} \dots (x - a_k)}{(a_i - a_1) \dots \widehat{(a_i - a_i)} \dots (a_i - a_k)}$$

Отсюда легко найти многочлен, дающий в $a_1, \dots, a_k$ предписанные значения $b_1, \dots, b_k$:

$$P(x) = \sum_{i=1}^k b_i \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}.$$

Это *интерполяционный многочлен Лагранжа*, знакомый вам по прошлогоднему курсу.