Деление по модулю

Забродин Денис Александрович

7 сентября 2022 г.

Содержание

1 Деление по модулю

1.1 Отношение эквивалентности

Прежде всего важно понимать, что следующие выражения эквивалентны

- $A \equiv B \ (mod\ C)$
- $A \ mod\ C = B \ mod\ C$
- $C \mid (A - B)$
- $A = B + K \cdot C$

Это поможет нам переключаться между **разными способами** выражения одной и той же мысли.

Убедитесь, что секторы из предыдущего примера обладают следующими свойствами.

- Все значения в одном секторе попарно связаны друг с другом.
- Каждое значение встречается не более чем в одном секторе (секторы взаимно непересекаются).
- Если собрать вместе все секторы, получится «пирог» из всех возможных целых чисел.

Пирог, куски которого обладают этими свойствами, называется **отношением эквивалентности.**
Отношение эквивалентности определяет, как именно следует разрезать наш пирог (то есть как мы разобъём множество всех значений) на куски (классы эквивалентности).

В общем случае, отношение эквивалентности задаётся следующими тремя свойствами.

- Пирог — это все **интересующие нас значения**
- Кусок (или сектор) пирога — **класс эквивалентности**
- Принцип разрезания пирога на куски — **соотношение эквивалентности**

Именно поэтому сравнение по модулю C — это отношение эквивалентности. Оно разделяет множество целых чисел на C различных классов эквивалентности.

Выяснив, что сравнение по модулю C — это отношение эквивалентности, давайте разберём несколько присущих ему свойств. Отношения эквивалентности — это отношения, обладающих следующими свойствами.

- Они **рефлексивны**, то есть A эквивалентно A.
- Они **симметричны**, то есть если A эквивалентно B, то B эквивалентно A.
- Они **транзитивны**, то есть если A эквивалентно B, а B эквивалентно C, то A эквивалентно C.

1.2 Свойства сравнений

Утверждение 1.4.1. *Два числа, сравнимые с третьим, сравнимы между собой.*

Утверждение 1.4.2. *Сравнения можно почленно складывать.*

$$a_1 \equiv b_1 (mod\ m), \ldots, a_k \equiv b_k (mod\ m)$$

$$a_1 - b_1 = mt_1, \ldots, a_k - b_k = mt_k,$$
$$a_1 + \ldots + a_k = b_1 + \ldots + b_k + m(t_1 + \ldots + t_k),$$
$$a_1 + \ldots + a_k \equiv b_1 + \ldots + b_k (mod\ m)$$

(1.4.17) чтд

Утверждение 1.4.3. *Слагаемые, стоящие в какой-либо части сравнения, можно переносить в другую, меняя знак на обратный.*

Действительно, пользуясь утверждением 1.4.2, без ограничения общности, прибавим к сравнению (1.4.17) почленно тривиальное сравнение $-bk \equiv -bk (mod\, m)$. Получим

$$a_1 + \ldots + a_k - b_k \equiv b_1 + \ldots + b_k - b_k (mod\ m)$$

т.е

$$a_1 + \ldots + a_k - b_k \equiv b_1 + \ldots + b_{k-1}$$

Утверждение 1.4.5. *Сравнения можно почленно перемножать*

Действительно, пусть a1 ≡ b1(mod m), a2 ≡ b2(mod m). Это означает, что $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$. Отсюда после перемножения равенств получим $a_1a_2 = b_1b_2 + mT, ..a_1a_2 \equiv b_1b_2 (mod\ m)$.

Утверждение 1.4.6. *Обе части сравнения можно возводить в одну и ту же степень.*

Утверждение 1.4.8. *Обе части сравнения можно разделить на их общий дедитель, если он взаимно прост с модулем.*

Пусть

$$a \equiv b (mod\ m), a = a_1 d, b = b_1 d, (m, d) = 1$$

Тогда

$$a_1 d - b_1 d = mt, (a_1 - b_1)d = mt$$

Так как (m, d) = 1, то

$$a_1 - b_1 = mt', a_1 - b_1 \equiv 0(mod\ m), a_1 \equiv b_1(mod\ m)$$

1.3 Дальнейшие свойства сравнений

Утверждение 1.5.1. *Обе части сравнения и модуль можно умножить на одно и то же число.*

Последовательно имеем

$$a \equiv b(mod\ m), a - b = mt, m_1(a - b) = m_1 mt, m_1 a = m_1 b + m_1 mt$$

Это значит

$$m_1 a \equiv m_1 b(mod\ m_1 m)$$

Утверждение 1.5.2. *Обе части сравнения и модуль можно разделить на их общий делитель.*

Если

$$a \equiv b(mod\ m), a = a_1 d, b = b_1 d, m = m_1 d,$$

то

$$a_1 d = b_1 d + m_1 dt, a_1 = b_1 + m_1 t, a_1 \equiv b_1(mod\ m_1)$$

Утверждение 1.5.3. *Если сравнение имеет место по нескольким модулям $m_1, m_2, \ldots, m_k$, то оно имеет место и по модулю, который равен наименьшему общему кратному модулей: M $(m_1, m_2, \ldots, m_k)$.*

В самом деле, пусть

$$a \equiv b(mod\ m_i), i = 1, 2, \ldots, k; a - b = m_i t.$$

Будучи кратным каждого из модулей, разность a - b, кратна и их наименьшего общего кратного.

Утверждение 1.5.4. *Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.*

Утверждение 1.5.5.*Если одна часть сравнения и модуль делятся на какое-нибудь число, то и другая часть сравнения делится на это число.*

Действительно, пусть

$$a \equiv b(mod\ m); a - b = mt$$

Если

$$a = a_1zm = m_1z, a_1z - m_1zt = b; z(a_1 - m_1t) = b = zb_1$$

Утверждение 1.5.6. Если

$$a \equiv b(mod\ m), (a, m) = (b, m)$$

Д о к а з а т е л ь с т в о. Согласно утверждению 1.5.5 совокупность общих делителей чисел a и m совпадает с совокупностью общих делителей чисел b и m. Значит, совпадают и наибольшие общие делители этих чисел, что и требуется.