РАЗДЕЛ 2. ТЕОРИЯ ДЕЛИМОСТИ

2.1 Отношение делимости нацело на множестве целых чисел и его простейшие свойства. Теорема о делении с остатком

Рассмотрим множество целых чисел Z. Операция деления выполняется не для всех пар чисел из Z.

Определение. Число $a \in Z$ делится на число $b \in Z$ $(b \neq 0)$, если существует такое число $q \in Z$, что $a = bq$.

Вместо выражения «a делится на b» $(a \vdots b)$ очень часто используется фраза «число b делит число a» и при этом применяется запись $b \mid a$. Если «a не делится на b», то говорят, что «число b не делит число a» и записывают $b \nmid a$.

Если a делится на b, то b называется делителем a, само a называется кратным числа a. Число q называется частным от деления a на b.

Число 0 делится на любое $b \neq 0$. Если $a \neq 0$, то, очевидно, что множество всех делителей a конечно.

Докажем простейшие свойства делимости целых чисел.

Лемма 1. Если $c \mid b$ и $b \mid a$, то $c \mid a$.

Доказательство.

Так как $c \mid b$ и $b \mid a$, то $b = q_1 c, a = q_2 b$ при некоторых $q_1, q_2 \in Z$. Отсюда $a = q_2 q_2 c = q\, c$, где $q = q_2 q_1$. Следовательно, $c \mid a$.

Лемма 2. Если $m = a + b, d \mid m$ и $d \mid a$, то $d \mid b$.

Доказательство.

По определению имеем $m = q_1 d, a = q_2 d$ при некоторых $q_1, q_2 \in Z$. Отсюда из равенства $m = a + b$ получаем $b = (q_1 - q_2) \cdot d$, т. е. $d \mid b$.

В любом случае (когда $a \vdots b$ и когда a не делится на b) можно число a разделить на число b с остатком.

Теорема 1 (о делении с остатком). Если $a, b \in Z, b > 0$, то существуют единственные $q, r \in Z$ такие, что $a = b\,q + r, 0 \leq r < b$.

Доказательство.

Существование.

Согласно принципу Архимеда (287 – 212 г. до н.э.) для любого, $a \in Z$ существует такое целое число q, что

$$bq \leq a < b \cdot (q + 1).$$

Отсюда $0 \leq a - bq < b$. Обозначая $a - bq = r$, получим требуемое представление.

Единственность.

Предположим, что кроме найденного выше представления

$$a = bq + r, 0 \leq r < b$$

имеется другое:

$$a = bq_1 + r_1, 0 \leq r_1 < b.$$

Тогда

$$0 = b \cdot (q - q_1) + r - r_1, r - r_1 < b.$$

Из последнего равенства следует, что число b делит разность $r - r_1$. Но

$$r - r_1 < b,$$

следовательно, $r = r_1$, а тогда и $q = q_1$ (подставляя $r - r_1 = 0$ в равенство $0 = b \cdot (q - q_1) + r - r_1$).

2.2 НОД и НОК целых чисел. Алгоритм Евклида. Взаимно простые числа

Определение. Общим делителем чисел $a_1, a_2, \ldots, a_n \in Z$ называется число $d \in Z$, являющееся делителем каждого из этих чисел. Общий делитель данных чисел называется их наибольшим общим делителем, если он делится на всякий общий делитель этих чисел.

Из определения наибольшего общего делителя вытекает важное свойство: если $d = \text{НОД}(a_1, a_2, \ldots, a_n)$, то множество всех общих делителей чисел $a_1, a_2, \ldots, a_n$ состоит из всех делителей числа d.

Если

$$d = \text{НОД}(a_1, a_2, \ldots, a_n),$$

то

$$d = \text{НОД}(a_1, a_2, \ldots, a_n, 0).$$

Обратно, если

$$d = \text{НОД}(a_1, a_2, \dots, a_n, 0),$$

то

$$d = \text{НОД}(a_1, a_2, \dots, a_n)$$

(поэтому при нахождении наибольшего делителя нескольких чисел, не все из которых равны нулю, нули можно не учитывать).

Число 0 является наибольшим общим делителем чисел $a_1, a_2, \dots, a_n$ тогда и только тогда, когда $a_1 = a_2 = \cdots = a_n = 0$.(в этом случае нуль является единственным наибольшим общим делителем данных чисел). В дальнейшем изложении будем ограничиваться случаем, когда все числа отличны от нуля.

Если $d = \text{НОД}(a_1, a_2, \dots, a_n)$, то число $(-d)$ также является наибольшим общим делителем чисел $a_1, a_2, \dots, a_n$. Поэтому в дальнейшем, не ограничивая общности рассуждений, будем называть наибольшим общим делителем положительное число в этой паре чисел.

Если $\text{НОД}(a_1, a_2, \dots, a_n) = 1$, то числа $a_1, a_2, \dots, a_n$ называются взаимно простыми.

Приступим к выяснению вопроса о существовании наибольшего общего делителя. С этой целью для любых двух чисел $a, b \in Z, a \neq 0, b \neq 0$, определим последовательность

$$c_1, c_2, c_3, \dots, c_{n-1}, c_n.$$

Полагаем $c_1 = a$, $c_2 = b$. Если $b \mid a$, то последовательность состоит из двух членов $c_1 = a, c_2 = b$. Тогда $b = \text{НОД}(a, b)$.

Если $b \nmid a$, то c_3 является остатком при делении c_1 на c_2, c_4 – остатком при делении c_2 на c_3 и т.д. Это последовательное деление с остатком, запишем для удобства в виде цепочки равенств:

$$c_1 = c_2 q_2 + c_3,$$

$$c_2 = c_3 q_3 + c_4,$$

$$c_3 = c_4 q_4 + c_5,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$c_{n-2} = c_{n-1}q_{n-1} + c_n ,$$

$$c_{n-1} = c_n q_n .$$

В результате деления с остатком получим: $|c_2| > c_3 > c_4 > \cdots$, причем эти остатки являются неотрицательными целыми числами. Поэтому среди получающихся остатков должен встретиться остаток, равный нулю. В качестве cn берется последний, отличный от нуля остаток, полученный в результате указанного процесса деления. В этом случае c_{n-1} делится на c_n. Построенная последовательность $c_1, c_2, c_3, \ldots, c_{n-1}, c_n$ называется последовательностью Евклида для чисел a и b. Способ построения такой последовательности путем последовательного деления с остатком называется алгоритмом Евклида.

2.3 Простые и составные числа. Бесконечность множества простых чисел

Рассмотрим множество натуральных чисел N. Число 1 имеет единственный натуральный делитель. Любое $n \in N, n > 1$, делится на 1 и n.

Определение. Число $n \in N, n > 1$, называется простым, если оно не имеет других натуральных делителей, кроме 1 и n.

Определение. Число $n \in N$ называется составным, если оно имеет натуральный делитель, отличный от 1 и n.

Из последнего определения следует, что каждое составное число представляется в виде $n = a \cdot b$, где $a, b \in N, 1 < a < n, 1 < b < n$.

Замечание. Число 1 не является ни простым, ни составным.

Лемма 3. Наименьший отличный от 1 натуральный делитель числа $n \in N, n > 1$, есть простое число.

Доказательство.

Число $n > 1$ имеет хотя бы два различных делителя и, следовательно, имеет делитель, отличный от 1 Среди всех делителей n, отличных от 1, имеется наименьший. Пусть это будет q. Число q должно быть простым, так

как иначе оно было бы составным и по определению имело бы делитель q_1 такой, что $1 < q_1 < q$. Итак, $q_1 \mid q$ и $q \mid n$, а тогда по лемме 1 $q_1 \mid n$. Противоречие с тем, что q – наименьший делитель n. Следовательно, q – простое число.

Следствие. Любое число $n \in N, n > 1$, имеет хотя бы один простой делитель.

Лемма 4. Наименьший простой делитель составного числа n не превосходит $\sqrt{n}$.

Доказательство.

Пусть $p, p > 1$, – наименьший делитель n, являющийся по лемме 3 простым числом. Так как n – составное число, то $n = pq$, где $q \geq p$. Поэтому $n \geq p^2$, откуда $p \leq \sqrt{n}$.

Теорема 2. (Евклид (III в. до н.э.)). Множество простых чисел бесконечно.

Доказательство.

Допустим противное, что простые числа $p_1, p_2, \ldots, p_k$ образуют конечное множество и p_k – наибольшее простое число. Рассмотрим число $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. Оно не делится ни на одно из простых чисел $p_1, p_2, \ldots, p_k$ так как при делении N на любое из этих чисел остаток равен 1. Но $N > 1$ и по следствию из леммы 3 N должно иметь простой делитель. Полученное противоречие показывает, что сделанное предположение неверно и теорема справедлива.

Опишем удобный способ выделения простых чисел в данном отрезке натурального ряда, известный еще греческому ученому Эратосфену (276–194 г.г. до н.э.). Он состоит в отсеивании составных чисел, находящихся в данном отрезке, и носит название «решета Эратосфена».

Напишем одно за другим числа $2, 3, 4, \ldots,$. Число 2, являющееся простым, оставляем и зачеркиваем после него все четные числа. Первое следующее за 2 не зачёркнутое число есть 3 Оно не делится на 2 Значит, оно не имеет делителей, отличных от 1 и 3, и поэтому является простым.

Оставляем 3 и зачеркиваем после него все числа, кратные 3 Продолжая этот процесс, найдем все простые числа, не превосходящие некоторого простого числа p_k . При этом будут зачеркнуты все составные числа, кратные $2, 3, \dots, p_k$. Первое не зачеркнутое после p_k число будет простым числом p_{k+1}, так как оно не делится на $2, 3, \dots, p_k$ и поэтому имеет своими делителями только 1 и p_{k+1}. Если найдено $p_k \geq \sqrt{N}$, то все оставшиеся не зачеркнутыми числа будут простыми, поскольку все кратные чисел $2, 3, \dots, p_k$ уже вычеркнуты, а по лемме 4 любое составное число n имеет простой делитель $\leq \sqrt{n}$.

Составление таблицы простых чисел, не превосходящих N, указанным процессом закончено, как только зачеркнуты все числа, кратные простым числам $\leq \sqrt{N}$.

2.4 Основная теорема арифметики и следствия из неё

Теорема 3. (ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ). Любое число $n \in N, n > 1$, представляется в виде произведения простых чисел, причем единственным образом, если не учитывать порядок следования сомножителей.

Доказательство.

По лемме 3 число n имеет наименьший простой делитель p_1. Тогда $n = p_1 \cdot a_1$. Если $a_1 > 1$, то аналогично получим $a_1 = p_2 \cdot a_2$, где p_2 – наименьший простой делитель числа a_1 и т.д. Поскольку числа $a_1, a_2, \dots$ убывают, то на некотором шаге будем иметь, что $a_r = 1$ и $a_{r-1} = p_r$. Перемножая все полученные равенства, получим

$$n \cdot a_1 \cdot a_2 \cdot \dots \cdot a_{r-1} = a_1 \cdot p_1 \cdot a_2 \cdot p_2 \cdot \dots \cdot a_{r-1} \cdot p_{r-1} \cdot p_r .$$

После сокращения на $a_1 \cdot a_2 \cdot \dots \cdot a_{r-1}$ получим разложение числа n на простые сомножители: $n = p_1 \cdot p_2 \cdot \dots \cdot p_{r-1} \cdot p_r$.

Докажем единственность этого разложения. Предположим, что для некоторого n имеются два разложения на простые множители:

$$p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_s .$$

Правая часть этого равенства делится на q_1. Значит, и его левая часть делится на q_1. Тогда хотя бы один из сомножителей левой части делится на q_1. Пусть это будет p_1 . Тогда $p_1 = q_1$, так как p_1 делится только на 1 и p_1 . Сокращая обе части равенства на $p_1 = q_1$, получим, что

$$p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_s.$$

Повторяя рассуждение для последнего равенства, получим

$$p_2 = q_2 \text{ и } p_3 \cdot \ldots \cdot p_k = q_3 \cdot \ldots \cdot q_s$$

и так далее до тех пор, пока в одной из частей получающихся равенств, например, в правой, сократятся все сомножители, так как равенство

$$p_{s+1} \cdot \ldots \cdot p_k = 1$$

невозможно, поскольку все числа $p_{s+1}, \ldots, p_k$ больше единицы. Следовательно, разложения числа n на простые сомножители совпадают.

Пусть $n \in N, n > 1$, и $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ есть разложение n на простые сомножители. Среди чисел $p_1, p_2, \ldots, p_r$ могут быть и одинаковые. Пусть $p_1, p_2, \ldots, p_k$– различные из этих чисел, а $\alpha_1, \alpha_2, \ldots, \alpha_k$ – кратности, с которыми они входят в разложение.

Тогда

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Последнее представление называется каноническим разложением натурального числа n, $n > 1$, на простые сомножители.

2.5 Отношение сравнимости по натуральному модулю на множестве целых чисел и его свойства. Множество классов вычетов Z_m

В ходе дальнейшего изложения будем считать, что число m является натуральным.

Определение. Целые числа a и b сравнимы по модулю m, если они имеют одинаковые остатки от деления на m (при этом используется запись $a \equiv b \ (mod\ m)$).

Замечание. Запись $a \equiv 0 \ (mod\ m)$ означает делимость a на m.

Пример. $-10 \equiv 4\ (mod\ 7)$.

Из определения следует, что все целые числа по модулю m разбиваются на m непересекающихся классов сравнимых между собой чисел (т.е. чисел, имеющих одинаковые остатки при делении на m):

$$K_0, K_1, \dots, K_{m-1}.$$

Каждое число, входящее в какой-либо из классов, называется вычетом этого класса, а сами классы – классами вычетов по модулю m. Беря по одному вычету из каждого класса, получим полную систему вычетов по модулю m.

Пример. Классам чисел по модулю 4 являются:

$$K_0 = \{\dots, -4n, \dots, -8, -4, 0, 4, 8, \dots, 4n, \dots\},$$
$$K_1 = \{\dots, -4n + 1, \dots, -7, -3, 1, 5, 9, \dots, 4n + 1, \dots\},$$
$$K_2 = \{\dots, -4n + 2, \dots, -6, -2, 2, 6, 10, \dots, 4n + 2, \dots\},$$
$$K_3 = \{\dots, -4n + 3, \dots, -5, -1, 3, 7, 11, \dots, 4n + 3, \dots\}.$$

Совокупность $\{8, -11, 2, 23\}$ образует одну из полных систем вычетов по модулю 4. Полной системой наименьших неотрицательных вычетов по модулю 4 является $\{0,1, 2, 3\}$. Полной системой наименьших по абсолютной величине вычетов по модулю 4 является $\{0,1, 2, -1\}$, а также $\{0,1, -2, -1\}$.

Теорема 4. Пусть $a, b \in Z$. Соотношение $a \equiv b\ (mod\ m)$ имеет место тогда и только тогда, когда $m \mid (a - b)$.

Доказательство.

Если $a \equiv b\ (mod\ m)$, то

$$a = mq_1 + r, b = mq_2 + r.$$

Следовательно,

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

Значит, $m \mid (a - b)$.

Если $m \mid (a - b)$, то $a - b = mx$. Если $b = mq + r$, то $a = m \cdot (q + x) + r$. Следовательно, $a \equiv b\ (mod\ m)$?

Замечание. Из теоремы следует, что класс чисел по модулю m, содержащий число $a \in Z$, состоит из всех чисел $x \in Z$ вида $x = a + mq$.

Свойства сравнений.

1 *Рефлексивность*: $a \equiv a\ (mod\ m)$.

Доказательство следует из определения.

2 *Симметричность*: если $a \equiv b\ (mod\ m)$, то $b \equiv a\ (mod\ m)$.

Доказательство следует из определения.

3 *Транзитивность*: если

$a \equiv b\ (mod\ m)$ и $b \equiv c\ (mod\ m)$, то $a \equiv c\ (mod\ m)$.

Доказательство следует из определения.

4 *Если* $a_1 \equiv b_1\ (mod\ m)$, $a_2 \equiv b_2 (mod\ m)$, то

$$a_1 + a_2 \equiv b_1 + b_2 (mod\ m)\ .$$

Доказательство.

По теореме 4 $a_1 - b_1 = mx_1$, $a_2 - b_2 = mx_2$.

Следовательно,

$$a_1 - b_1 + a_2 - b_2 = m(x_1 + x_2).$$

или

$$(a_1 + a_2) - (b_1 + b_2) = m(x_1 + x_2).$$

Таким образом, согласно этой же теореме,

$$(a_1 + a_2) \equiv (b_1 + b_2)\ (mod\ m).$$

5 *Если* $a + \mathrm{c} \equiv b\ (mod\ m)$, *то* $a \equiv (b - \mathrm{c})(mod\ m)$.

Доказательство.

По теореме 4

$$a + \mathrm{c} - b = mx$$

или

$$a - (b - c) = mx\ .$$

Таким образом, согласно этой же теореме,

$$a \equiv (b - \mathrm{c})\ (mod\ m).$$

6 *Если* $a \equiv b\ (mod\ m)$, *то* $a + mk \equiv b\ (mod\ m)$, где $k \in Z$.

Доказательство.

По теореме 4 $a - b = mx$, следовательно,

$$a - b + mk = m \cdot (x + k)\ ,$$

или

$$(a + mk) - b = m \cdot (x + k).$$

Таким образом, согласно этой же теореме, $a + mk \equiv b \pmod m$.

7 *Если* $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, *то*

$$a_1 a_2 \equiv b_1 b_2 \pmod m.$$

Доказательство.

По теореме 4

$$a_1 = b_1 + mx_1,\ a_2 = b_2 + mx_2.$$

Следовательно,

$$a_1 a_2 = b_1 b_2 + m(b_2 x_1 + b_1 x_2 + m x_2 x_1)$$

или

$$a_1 a_2 - b_1 b_2 + mk.$$

Таким образом, согласно этой же теореме,

$$a_1 a_2 \equiv b_1 b_2 \pmod m.$$

8 *Если* $a \equiv b \pmod m$, *то* $a^n \equiv b^n \pmod m$, *где* $n \in N_0$.

Доказательство следует из предыдущего свойства.

9 *Если* $a \equiv b \pmod m$, *то* $ak \equiv bk \pmod m$.

Доказательство.

По теореме 4 $a - b = mx$, значит,

$$ak - bk = m \cdot (xk).$$

Таким образом, согласно этой же теореме,

$$ak \equiv bk \pmod m.$$

10 Если $a \equiv b \pmod m$, *то* $ak \equiv bk \pmod{mk}$, где $k \in N$.

Доказательство.

По теореме 4 $a - b = mx$, значит,

$$ak - bk = (mk) \cdot x.$$

Таким образом, согласно этой же теореме,

$$ak \equiv bk \pmod{mk}.$$

11 *Если* $a \equiv b \pmod m$ *и* $a = ka', b = kb', m = km'$, *то*

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

Доказательство.

Если $a - b = mx$, то $k \cdot (a' - b') = k \cdot (m' x)$, следовательно, $a' - b' = m'x$, или $a' \equiv b' \pmod{m'}$.

12 *Если* $a \equiv b \pmod{m}$ *и* $m = du$, *то* $a \equiv b \pmod{d}$.

Доказательство.

Если $a - b = mx$, то $a - b = d \cdot (ux)$. Таким образом, $a \equiv b \pmod{d}$.

13 *Если* $au \equiv av \pmod{m}$ *и* НОД $(a, m) = 1$, *то* $u \equiv v \pmod{m}$.

Доказательство.

По теореме 4

$$au - av = mx,$$

или

$$a \cdot (u - v) = mx.$$

Согласно свойству делимости $m \mid (u - v)$ (в силу НОД $(a, m) = 1$). Таким образом,

$$u \equiv v \pmod{m}.$$

Следствие. Рассмотрим некоторый многочлен с целыми коэффициентами:

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n.$$

Если $a \equiv b \pmod{m}$, то значения, которые принимает этот многочлен при $x = a$ и $x = b$, также сравнимы между собой по модулю m, т.е.

$$a_0 a^n + a_1 a^{n-1} + a_2 a^{n-2} + \cdots + a_{n-1} a + a_n \equiv (a_0 b^n + a_1 b^{n-1} + a_2 b^{n-2} + \cdots + a_{n-1} b + a_n) \pmod{m}.$$

Рассмотрим простейшее линейное сравнение $ax \equiv b \pmod{m}$.

Теорема 5. Линейное сравнение $ax \equiv b \pmod{m}$, где НОД $(a, m) = 1$, разрешимо. Множество удовлетворяющих ему чисел составляет некоторый класс вычетов по модулю m.

Доказательство.

Так как НОД $(a, m) = 1$, то числа $a, 2a, 3a, \ldots, ma$ имеют разные остатки от деления на m(т.е. $ia \not\equiv ja \pmod{m}$). Действительно, если бы $ia \equiv$

$ja\ (mod\ m)$, то по свойству 13 сравнений выполнялось бы $i \equiv j\ (mod\ m)$, откуда, учитывая $1 \leq i \leq m, 1 \leq j \leq m$, имело бы место равенство $i = j$.

Итак, все числа $a, 2a, 3a, \ldots, ma$ лежат в разных классах вычетов по модулю m. Так как имеется ровно m различных классов вычетов по модулю m, то обязательно одно из чисел $a, 2a, 3a, \ldots, ma$, содержится в классе вычетов, в котором находится число b. Значит, линейное сравнение $ax \equiv b\ (mod\ m)$.разрешимо.

Если $ar \equiv b\ (mod\ m)$, то все числа x из класса вычетов, содержащего r (т.е. числа вида $x = r + my$), удовлетворяют сравнению

$$ax \equiv b\ (mod\ m).$$

Действительно,

$$a \cdot (r + my) = ar + m \cdot (ay),$$

$$ar + m \cdot (ay) \equiv ar\ (modm),$$

отсюда

$$ar + m \cdot (ay) \equiv b\ (modm).$$

Таким образом, любое решение линейного сравнения $ax \equiv b\ (mod\ m)$ НОД $(a, m) = 1$, лежит в классе вычетов, содержащем r.