Лекция №3

7. 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 b. 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 $c \vdots b$ и $b \vdots a$, то $c \vdots a$.

Доказательство.

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

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

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. $b \vdots d$.

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

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

Определение. Общим делителем чисел $a_1, a_2, \dots, a_n \in Z$ 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 $d = \text{НОД}(a_1, a_2, \dots, a_n)$, то множество всех общих делителей чисел $a_1, a_2, \dots, a_n$ состоит из всех делителей числа d.

Если

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

то

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

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 $a \vdots b$, 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 c_n 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.

9.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 $\leq \sqrt{N}$.