Лекция 2
НОД и НОК. Алгоритм Евклида. Взаимно простые числа

Задача 1

Камин в комнате необходимо выложить отделочной плиткой квадратной формы. Сколько плиток понадобится для камина размером 195×156 см. Каковы наибольшие размеры плитки?

Решение:

1. *195·156=30420 (см²) – S поверхности камина*
2. *НОД (195 и 156)=39 (см) – сторона плитки*
3. *39 ·39=1521 (см²) – S одной плитки*
4. *30420:1521=20 (штук)*

Ответ: 20 плиток размером 39×39 см.

НОД

- ***Определение 1.*** ***Число d называется общим делителем чисел $a_1, a_2, \ldots, a_n$, если $a_1 \vdots d, a_2 \vdots d, \ldots, a_n \vdots d$***
- ***Определение 2.*** ***Наибольшим общим делителем целых чисел $a_1, a_2, \ldots, a_n$ называется такой их общий натуральный делитель, который делится на любой их общих делитель***
- ***Обозначают: $d=(a_1, a_2, \ldots, a_n)$***

$d=(a_1, a_2, \ldots, a_n)$, если

1) $d \in N$

2) d – общий делитель чисел $a_1, a_2, \ldots, a_n$

3) если c – общий делитель чисел $a_1, a_2, \ldots, a_n$, то $d \vdots c$

Примеры

$(16, 30, 12)=2$

$(21, 15, 48)=3$

Задача 2

В портовом городе начинаются три туристических теплоходных рейса, первый из которых длится 15 суток, второй – 20 и третий – 12 суток. Вернувшись в порт, теплоходы в этот же день снова отправляются в рейс. Сегодня из порта вышли теплоходы по всем трем маршрутам. Через сколько суток они впервые снова вместе уйдут в плавание? Какое количество рейсов сделает каждый теплоход?

Решение:

1. ***НОК (15, 20 и 12)=60 (суток) – время встречи***
2. ***60:15=4 (рейса) – 1 теплоход***
3. ***60:20=3 (рейса) – 2 теплоход***
4. ***60:12=5 (рейсов) – 3 теплоход***

НОК

- ***Определение 3.*** ***Число М называется общим кратным целых чисел $a_1, a_2, \ldots, a_n$, если оно делится на каждое из этих чисел***
- ***Определение 4.*** ***Наименьшим общим кратным целых чисел $a_1, a_2, \ldots, a_n$ называется такое их общее натуральное кратное m, которое делит любое их общее кратное***
- ***Обозначают: $m=[a_1, a_2, \ldots, a_n]$***

$m=[a_1, a_2, \ldots, a_n]$, если

1) $m \in N$

2) m – общее кратное чисел $a_1, a_2, \ldots, a_n$

3) если М – общее кратное чисел $a_1, a_2, \ldots, a_n$, то $M \vdots m$

Примеры: $[16, 30, 12]=16\cdot5\cdot3=240$; $[21, 15, 48]=48\cdot5\cdot7$

Лемма

Если a, b ϵ Z, b≠0 и a=bq+r, то (a,b)=(b,r)

Доказательство

- *Пусть (a,b)=d_1, (b,r)=d_2*
- *Так как a⋮d_1, b⋮d_1, то (r=a-bq) ⋮d_1*
- *Следовательно, d_1 – общий делитель чисел b и r, поэтому их наибольший общий делитель d_2=(b,r) ⋮d_1*
- *Так как b⋮d_2, r⋮d_2, то a⋮d_2 и d_2 – общий делитель чисел a и b*
- *Поэтому d_1⋮d_2*
- *Из того, что d_1⋮d_2, d_2⋮d_1 и d_1, d_2 ϵ N, следует, что d_1=d_2*

Алгоритм Евклида

Пусть $a, b \in Z$, $b \neq 0$. По теореме о делении с остатком $a = bq_1 + r_1$, где $0 \leq r_1 < |b|$. Если $r_1 \neq 0$, то

$b = r_1 q_2 + r_2$, где $0 \leq r_2 < r_1$. Если $r_2 \neq 0$, то

$r_1 = r_2 q_3 + r_3$, где $0 \leq r_3 < r_2$. И так далее

……

$r_{n-2} = r_{n-1} q_n + r_n$, где $0 < r_n < r_{n-1}$

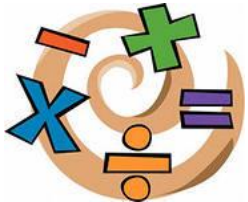
$r_{n-1} = r_n q_{n+1} + r_{n+1}$

Этот процесс не может быть бесконечным, так как не может быть бесконечной убывающей последовательности неотрицательных чисел:

$$|b| > r_1 > r_2 > \ldots > r_n, \qquad r_{n+1} \in [0, |b|]$$

Поэтому после нескольких шагов получим остаток, равный нулю

Пусть $r_{n+1} = 0$



Теорема

Последний не равный нулю остаток в алгоритме Евклида, применённый к целым числам a и b, где $b \neq 0$, есть их наибольший общий делитель (НОД)

Доказательство

Применяя лемму к первому, второму и так далее равенствам алгоритма Евклида, имеем:

$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$, ***так как*** $r_{n-1} \vdots r_n$

Из теоремы следует существование НОД двух чисел, если хотя бы одно из них не равно нулю

Свойства НОД

1. Если $a \vdots b$, то $(a, b) = |b|$
2. Если $(a, b) = d$, то существуют $u, v \in Z$, что $d=au+bv$ (линейная форма НОД)

3) Если $(a, b)=d$, $n \in N$, то $(na, nb)=nd$

4) Если $(a, b)=d$, $a \vdots n$, $b \vdots n$, $n \in N$, то $\left(\frac{a}{n}, \frac{b}{n}\right) = \frac{d}{n}$

В частности, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

5) $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$

Примеры

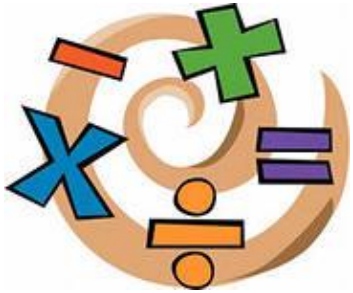
Найдём НОД чисел a и b и выразим его линейно через эти числа

1) $a=1173, b=323;$ $a= 3\cdot b+r_1$, $r_1=204$; $b=1\cdot r_1+r_2$, $r_2=119$; $r_1=r_2+r_3$, $r_3=85$; $r_2=r_3+r_4$, $r_4=34$; $r_3=2\cdot r_4+r_5$, $r_5=17$; $r_4=2\cdot r_5$. Итак, $(a, b)=d=17$. Выразим его линейно через a и b. Из первого равенства $r_1=a-3b$. Подставив в равенство для b, находим $r_2=b-r_1=-a+4b$. Далее: $r_3=r_1-r_2=2a-7b$; $r_4=r_2-r_3=-3a+11b$; $d=r_5=r_3-2r_4=8a-29b$

2) $a=1403, b=1058;$ $1403=1058+345$; $1058=345\cdot3+23$; $345=23\cdot15$. НОД чисел a и b равен 23. $23=1058-345\cdot3=1058-(1403-1058)\cdot3=-3\cdot1403+4\cdot1058=-3a+4b$

Свойства НОК

1) $[a_1, a_2, \ldots, a_n]=[[a_1, a_2, \ldots, a_{n-1}], a_n]$
2) Если к – натуральное, то $[ak, bk]=k[a, b]$
3) Если k = натуральное, $a \vdots k$, $b \vdots k$, то
4) Если $(a, b)=1$, то $[a, b] = ab$



Взаимно простые числа

Числа $a_1, a_2, \ldots, a_n$ называют взаимно простыми, если наибольший общий делитель этих чисел раве

Примеры

1) 15, 21, 14 – взаимно простые числа, однако эти числа не являются попарно взаимно простыми

2) 34, 53, 99, 115 – попарно взаимно простые числа, так как взаимно простые каждые два числа этого ряда

Свойства взаимно простых чисел

1) ***(Признак взаимно простых чисел)***

(a, b)=1 тогда и только тогда, когда найдутся целые u и v, что au+bv=1

2) Если (a, b)=1 и (a, c)=1, то (a, bc)=1

Доказательство. Согласно признаку, существуют целые числа x, y, u, v, что ax+by=1 и au+cv=1. Перемножив эти равенства, получим a(axu+xcv+buy)+bc(yv)=1, то есть $au_1+bcv_1=1$ или (a, bc)=1

Свойства взаимно простых чисел

3) Если $ab \vdots c$ и $(a, c)=1$, то $b \vdots c$

Доказательство. Существуют целые числа u, v, что au+cv=1. Умножим обе части равенства на b: abu+cbv=b. Так как $ab \vdots c$ и $c \vdots c$, то $((ab)u+cbv) \vdots c$, то есть $b \vdots c$

4) Если $a \vdots b$, $a \vdots c$ и $(b, c)=1$, то $a \vdots bc$

Доказательство. Существуют целые u, v, что bu+cv=1. Умножим обе части равенства на a: abu+acv=a. Так как $a \vdots c$, $b \vdots b$, то $ab \vdots bc$. Так как $a \vdots b$, $c \vdots c$, то $ac \vdots bc$. Следовательно, $(abu+acv) \vdots bc$ и $a \vdots bc$