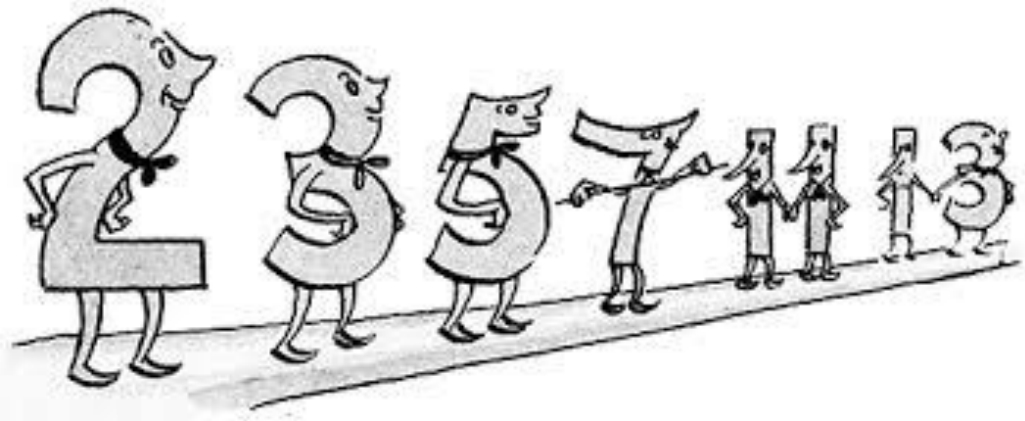
# *Лекция 3*
# *Простые и составные числа. Основная теорема арифметики*



## *Определение 1*

***Натуральное число p называется простым, если p>1 и p не имеет натуральных делителей, отличных от 1 и p***

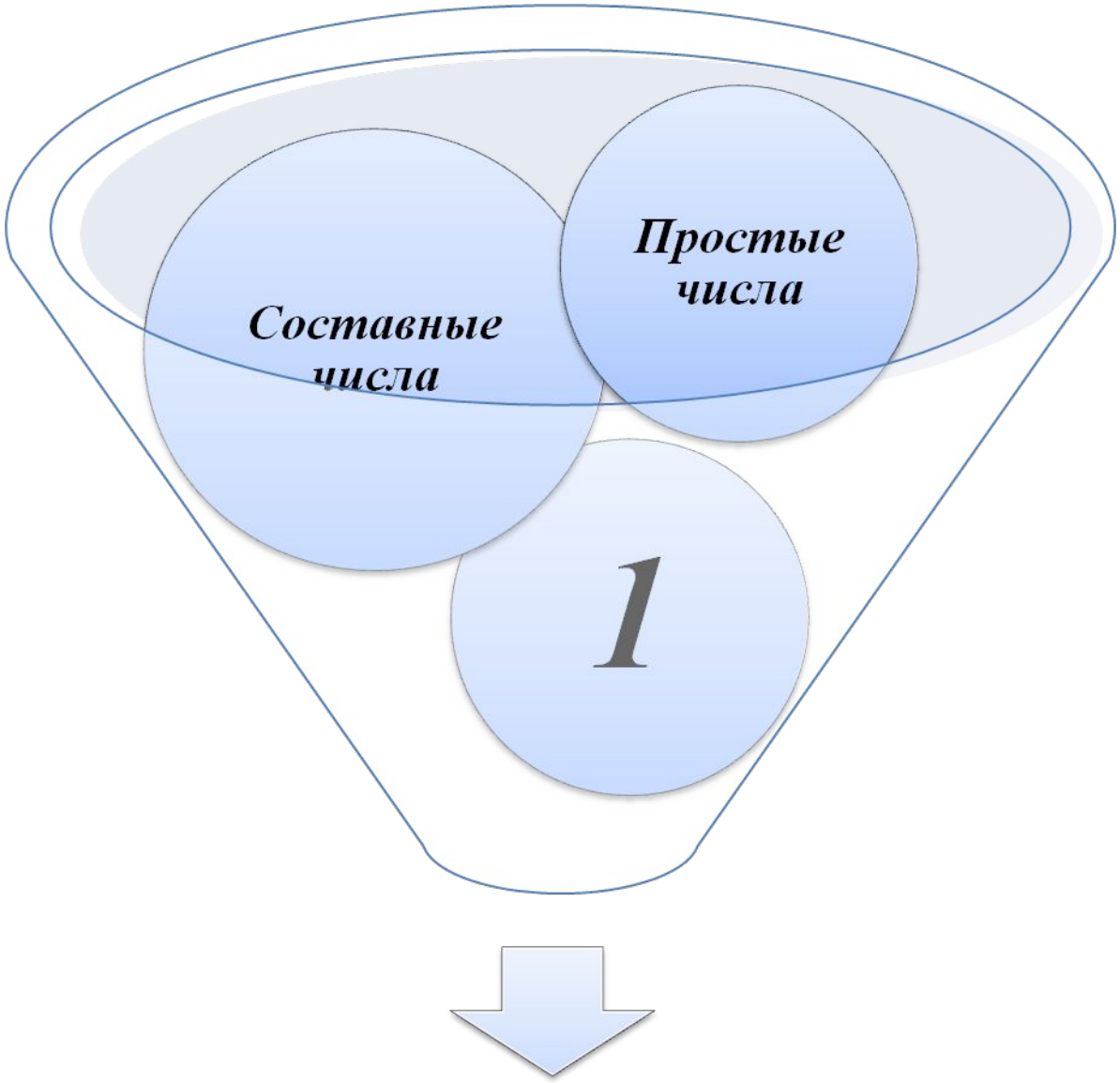
## *Определение 2*

***Натуральное число n>1 называется составным, если n имеет по крайней мере один натуральный делитель, отличный от 1 и n***

## *Примеры*

***2, 3, 5, 7 – простые числа***

***6, 8, 10, 15 – составные***




# Натуральные числа

- ***Если n – составное число, то из определения следует, что оно имеет натуральный делитель, отличный от 1 и n***
- ***Пусть это a ($a \in N$, $a \neq 1$, $a \neq n$)***
- ***Тогда $n=ab$, $b \in N$, $b \neq 1$, $b \neq n$***
- ***Так как $1<a<n$, то и $1<b<n$***

***Итак, если n – составное число, то существуют***

***$a,b \in N$, $n=ab$, $1<a$, $b<n$***

# *Свойства простых чисел*

1. ***Если натуральное число n>1, то наименьший натуральный делитель его, отличный от 1, - простое число***

***Доказательство***

- ***Пусть a – наименьший натуральный делитель n, a≠1 (n имеет натуральные делители, отличные от 1, например, само n)***
- ***Предположим, что a – составное, тогда a⋮b 1<b<a***
- ***Так как n⋮a, a⋮b, то n⋮b и 1<b<a***
- ***Пришли к противоречию с выбором числа a***
- ***Следовательно a – простое***

# *Свойства простых чисел*

## *2. Если a – целое, p – простое, то a⋮p или (a, p)=1*

***Доказательство***

***Так как число p имеет только 2 натуральных делителя: p и 1, то возможны две ситуации:***

***1) (a, p)=p, тогда a⋮p***

***или***

***2) (a, p)=1, тогда a и p – взаимно простые числа***

# *Свойства простых чисел*

***3. (основное свойство простых чисел)***

***Если произведение целых чисел ab делится на простое число p, то хотя бы один из сомножителей делится на p***

***Доказательство***

- ***Пусть ab⋮p***
- ***Предположим, что a не ⋮ p, тогда (a, p)=1 (свойство 2)***
- ***По свойству взаимно простых чисел b⋮p***

***Заметим, что свойство может быть распространено на любое конечное число сомножителей.***

***Теорема (основная теорема арифметики)***
***Любое натуральное число, большее 1, либо является простым, либо может быть представлено в виде произведения простых чисел, причём единственным образом с точностью до порядка сомножителей***

***Доказательство***

- ***Пусть n – составное число и $p_1$ - простой, отличный от 1, наименьший натуральный делитель числа n***

$$n = p_1 n_1,\ n_1 < n$$

- ***Если $n_1 \neq 1$, то $n_1 = p_2 n_2,\ n_2 < n_1$***

$$n = p_1 p_2 n_2$$

- ***Если $n_2 \neq 1$, то $n_2 = p_3 n_3,\ n_3 < n_2$***

$$n = p_1 p_2 p_3 n_3$$

.....

- ***Так как число шагов конечно $n > n_1 > n_2 > \ldots > n_k$, то когда – нибудь $n_{k+1} = 1$***

$$n = p_1 p_2 p_3 \ldots p_k$$

## *Докажем единственность представления*

***Пусть $n=p_1p_2\ldots p_k$ и $n=q_1q_2\ldots q_s$, где $p_i$, $q_j$ – простые числа***

$$p_1p_2\ldots p_k=q_1q_2\ldots q_s$$

- ***Так как $p_1p_2\ldots p_k \vdots q_1$, то (по свойству простых чисел 3) хотя бы один из сомножителей делится на $q_1$***
- ***Пусть, например, $p_1 \vdots q_1$***
- ***Так как оба числа простые, то $p_1 = q_1$***
- ***После сокращения равенства на $p_1 = q_1$ получим:***

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

- ***$p_2\ldots p_k \vdots q_2$, то пусть, например, $p_2 \vdots q_2 \Rightarrow p_2 = q_2$ и т.д.***
- ***Если $k>s$, тогда $p_{s+1}\ldots p_k=1$, что невозможно, т.к. у 1 нет простых делителей, следовательно, $k=s$***

$$p_1 = q_1,\ p_2 = q_2,\ p_k = q_k = q_s$$

## *Всякое составное число n может быть представимо в виде произведения простых чисел*

- *Среди этих простых множителей могут встречаться одинаковые*
- *Пусть, например, $p_1$ встречается $\alpha_1$ раз, $p_2$ - $\alpha_2$ раз, …, $p_s$ - $\alpha_s$ раз*
- *Тогда разложение числа n на простые множители можно записать следующим образом:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

- *Такое представление числа называют каноническим*

***Примеры:***

$60=2^2 \cdot 3 \cdot 5$

$81=3^4$

$666=2 \cdot 3^2 \cdot 37$

## Следствие 1

**Пусть** $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ **- каноническое разложение натурального числа n. Все делители n исчерпываются числами вида** $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$ **, где**

$$0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, \dots, 0 \le \beta_s \le \alpha_s \quad (1)$$

## Доказательство

*Действительно, с одной стороны, всякое число d такого вида делит n. С другой стороны, всякое число, которое делит n, имеет указанный вид, так как по свойствам делимости оно не может иметь других простых сомножителей, кроме* $p_1, p_2, \dots, p_s$, *а их показатели* $\beta_1, \beta_2, \dots, \beta_s$ *не могут противоречить условиям (1)*

- *Заметим, что натуральные числа a и b всегда можно записать в виде*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$$

- *Здесь предполагается, что $\alpha_i$ и $\beta_i$ могут принимать и нулевые значения*
- *Это позволит писать в обоих разложениях одни и те же простые числа $p_1$, $p_2$, …, $p_s$, а именно простые числа, которые входят в разложение хотя бы одного из чисел a и b*

***Пример***

$30 = 2 \cdot 3 \cdot 5 \cdot 7^0$

$42 = 2 \cdot 3 \cdot 5^0 \cdot 7$

## Следствие 2

$$(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_s^{\gamma_s}$$

$$[a,b] = p_1^{\mu_1} p_2^{\mu_2} \dots p_s^{\mu_s}$$

где $\gamma_i = min(\alpha_i, \beta_i)$, $\mu_i = max(\alpha_i, \beta_i)$.

**Справедливость этих равенств следует из того, что наибольший общий делитель чисел a и b делится на любой их общий делитель, а наименьшее общее кратное чисел a и b делит любое их общее кратное**

**Пример**

$30 = 2 \cdot 3 \cdot 5 \cdot 7^o$

$42 = 2 \cdot 3 \cdot 5^o \cdot 7$

$(30, 42) = 2 \cdot 3$

$[30, 42] = 2 \cdot 3 \cdot 5 \cdot 7$

## *Следствие 3*

$$[a, b]\cdot(a, b)=ab$$

*Действительно* $[a,b]\cdot(a,b)=p_1^{\delta_1}p_2^{\delta_2}\dots p_s^{\delta_s}$

*где* $\delta_i=max(\alpha_i, \beta_i)+min(\alpha_i, \beta_i)$

*Но одно из этих слагаемых равно* $\alpha_i$*, а другое –* $\beta_i$

*Следовательно,* $\delta_i=\alpha_i+\beta_i$ *и* $[a, b]\cdot(a, b)=ab$

### *Пример*

$30 = 2\cdot3\cdot5\cdot7^o$

$42= 2\cdot3\cdot5^o\cdot7$

$[30, 42] \cdot(30, 42) = 2\cdot3\cdot5\cdot7\cdot2\cdot3$