# Простые числа

Лекция 8

2 курс

- Определение:

- Простым числом называется такое натуральное число, большее 1, которое имеет только два  делителя – единицу и само это число.

Например:

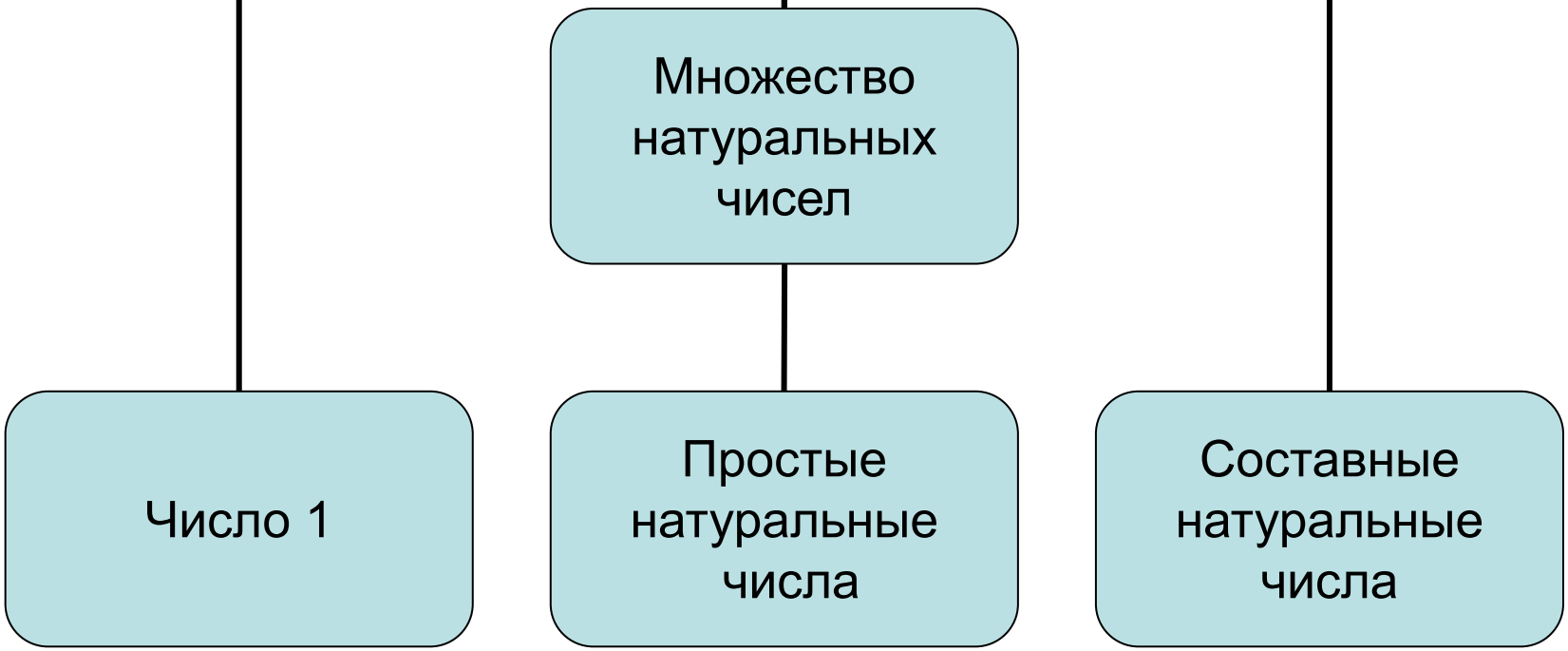
- Число 7 – простое.
- Число 2 – простое.

(единственное простое четное число).

- Числа 3,11,19, 23, 113 ... являются простыми, так как эти числа имеют по два делителя.
- Число 1 ……?

# Классификация натуральных чисел

- Основание классификации - признак: быть простым числом



# Свойства простых чисел

- Свойство1. Если простое число p делится на натуральное число n, отличное от 1, то оно совпадает с n.

Если p- простое, а $n \in N \quad n \neq 1,$

Из того, что $p \vdots n \Rightarrow p \equiv n.$

- Доказательство:
- Предположим, что число p – простое, p≠n, и делится на n. Тогда, по условию число p имеет три делителя: 1,n,p. Следовательно число p не простое. Противоречие.

- Значит наше предположение не верно, а верно то, что требовалось доказать.

- Свойство 2. Если p и g различные простые числа, то p не делится на g.

- Например: 7 и 13. 13 не делится на7

  23 и 5. $23=5\cdot4+3$

Доказательство:

- Если p– простое число, то оно делится на 1 и p.
- По условию g-простое число, $g \neq p$, и $g \neq 1$.
- Поэтому g не является делителем p.
- Что и требовалось доказать.

- Свойство 3. Если натуральное число а не делится на простое число р, то а и р – взаимно простые.

- Например: 25 и 7; но $\overline{25:7}$

- 17 и 13; но $\overline{17:13}$

- Гипотеза : наибольший общий делитель этих чисел равен 1.

- Доказательство:
- Пусть $D(a;p)=d$ – наибольший общий делитель.
- Но p - простое число и не может делится на d, если $d \neq p$ или $d \neq 1$
- Тогда $d=p$ или $d=1$

- Если d=p, то a кратно p. Это противоречит условию.
- Значит, d=1,  тогда числа a и p – взаимно простые числа.
- Что и требовалось доказать.

- Свойство 4. Если произведение двух натуральных чисел (a·b) делится на простое число p, то хотя бы одно из них делится на p.

- Например: (12·5) кратно3, так как 12 кратно 3, хотя 5 не кратно 3.

$$\frac{24 \cdot 14}{7} = \frac{24 \cdot 2}{1} = 24 \cdot 2$$

- Доказательство:
- Пусть a и p взаимно простые числа (a не кратно p).
- Тогда по свойству делимости произведения натуральных чисел, следует, что b кратно p.

$$(a \cdot b) \vdots p;\ \overline{a \not\vdots p}, \Rightarrow b \vdots p$$

- Что и требовалось доказать.

- Свойство 5. Если натуральное число больше 1, то оно имеет хотя бы один простой делитель.

- Например: $2>1$ и $2=2\cdot1$

- $27>1$ и $27=3\cdot9$

- Доказательство:
- Предположим противное: пусть существуют натуральные  числа, большие 1 и не имеющие ни одного простого делителя.

- Множество таких чисел обозначим символом А.

- Если все элементы множества А есть натуральные числа, большие 1.
- Значит во множестве А есть наименьший элемент. Обозначим его символом а.

- А={а, в,с…}

- Число a>1, и оно либо простое, либо составное.
- Если a – простое, то оно не может принадлежать множеству A по условию.
- Если a –составное, то оно имеет натуральный делитель, отличный от 1 и a.
- Назовем этот натуральный делитель b.

- b < a, ( a наименьшее число во множестве A).
- Значит b не принадлежит множеству A, и следовательно, число b имеет простой делитель.
- Пусть этот делитель  - натуральное число p.

- Число a кратно b, а число b кратно p, тогда число a кратно p (свойство транзитивности отношения делимости)

$$a \vdots b,\ b \vdots p \Rightarrow a \vdots p$$

- Следовательно, число a имеет простой делитель.
  Противоречие с выбором множества A.

- Значит, сделанное предположение не верно и чисел, больших 1, но не имеющих простых делителей не существует.

- Свойство 6. Наименьший простой делитель составного числа a не превосходит $\sqrt{a}$.

- Определите, является ли число 137 простым или составным.

- Действительно: Если p наименьший простой делитель числа a, то a=p·g.

- Так как p наименьший простой делитель, то p ≤ g.

- Умножим неравенство p ≤ g на p
- Имеем $p^2 \le p \cdot g,\ íî \quad p \cdot g = a,$

$$çíà \div èò \quad p \le \sqrt{a}.$$

# Способ распознавания простых чисел:

- Если натуральное число а, больше единицы, и не делится ни на одно из простых чисел, квадрат которых не превосходит а, то число а простое.

- Например:
- Определите является ли число 137 простым.
- $121<137<144$

$$11 < \sqrt{137} < 12$$

Выпишем все простые числа, не превышающие 11

Это - 2, 3, 5, 7, 11

- 137  не делится на 2
- 137 не делится на 3
- 137 не делится  на 5
- 137 не делится на 7
- 137 не делится на  11
- Вывод: 137 – простое число

- Определите, какие числа  простые, а какие числа составные?

- 161, 252, 391, 837.

# Историческая справка

- Эратосфен – греческий математик и астроном (III в. до н.э.) – способ определения простых чисел – решето Эратосфена.

- Евклид – греческий математик (около 300г. до н.э.), доказавший теорему : множество простых чисел бесконечно.

# Теорема Эвклида:

- Множество простых чисел бесконечно.
- Доказательство:
- Предположим противное: множество простых чисел конечно.
- Всякое конечное множество содержит наибольшее число.

- Обозначим множество простых чисел символом M.
- M={2,3,5,7,11,13,…p}, где p- самое большое простое число.

- Рассмотрим число a, составленное так:
- $a= 2\cdot3\cdot5\cdot7\cdot11\cdot\ldots\cdot p+1$

- Число a либо простое, либо составное.
- Но число a не может быть простым по предположению, так как оно больше самого большого простого числа.
- И не может быть составным, так как дает остаток 1 при делении на любое простое число.
- Противоречие, которое доказывает, что наше предположение не верно, то есть простых чисел бесконечное множество.

# Основная теорема арифметики.

- Любое составное число можно единственным образом представить в виде произведения простых множителей

- Теорема содержит два утверждения:
- 1. Разложение на простые множители любого составного натурального числа существует.
- 2. Разложение на простые множители любого составного натурального числа единственно.

# Доказательство существования разложения

- Пусть a составное число.

- Тогда (по свойству 5 простых чисел) найдется простой делитель $p_1$, такой что

$$a = p_1 \cdot a_1,$$ где a натуральное число.

- Если $a_1$ -простое число, то составное число а представлено в виде произведения простых множителей $p_1;\ a_1$

Если $a_1$ - составное, то у него найдется простой делитель $p_2$

(Свойство 5 простых чисел)

такой, что $a_1 = p_2 \cdot a_2$ è $a = p_1 \cdot p_2 \cdot a_2$

- заметим, что $1 < a_2 < a_1 < a$

$$a = p_1 \cdot a_1$$

$$a = p_1 \cdot p_2 \cdot a_2$$

$$- - - - - - - - -$$

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

Этот процесс конечен. Значит наступит момент, когда последний множитель в разложении составного числа а будет простым числом и будет получено разложение числа а на простые множители.

- В полученном разложении одинаковые множители могут повторятся.

- Например:
- $900=2\cdot2\cdot3\cdot3\cdot5\cdot5$

# Единственность разложения составного числа на простые множители

- Доказать: разложение составных чисел на простые множители определено однозначно.

- (два разложения составного числа на простые множители могут отличатся друг от друга лишь порядком множителей)

# Доказательство:

- Пусть $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$

  $a = g_1 \cdot g_2 \cdot \ldots \cdot g_l$

Тогда $p_1 \cdot p_2 \cdot \ldots \cdot p_n = g_1 \cdot g_2 \cdot \ldots \cdot g_l$

Правая часть равенства делится на $g_1$

Значит и левая часть делится на $g_1$

- По свойству 4 простых чисел один из множителей в левой части равенства делится $g_1$
- Пусть это будет множитель $p_1$

Так как p и g простые числа, то $p_1 = g_1$

Разделим обе части равенства на $g_1$

Получим: $p_2 \cdot \ldots \cdot p_n = g_2 \cdot \ldots \cdot g_l$

Аналогично устанавливаем, что левая часть делится на $g_2$

- Пусть $p_2 = g_2$

Разделив обе части равенства

Имеем: $p_3 \cdot \ldots \cdot p_n = g_3 \cdot \ldots \cdot g_l$

И так, $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n = g_1 \cdot g_2 \cdot g_3 \cdot \ldots \cdot g_l$

$$p_2 \cdot p_3 \cdot \ldots \cdot p_n = g_2 \cdot g_3 \cdot \ldots \cdot g_l$$

$$p_3 \cdot \ldots \cdot p_n = g_3 \cdot \ldots \cdot g_l$$

- Продолжая рассуждения, придем:
- 1) при n=l к тому, что при делении на

$$g_1, g_2, g_3, \ldots, g_l$$

Все множители в левой части равенства сократятся.

Следовательно, два представления числа a отличаются только порядком следования множителей

- 2) при n<l к неверному равенству

$$1 = g_{n+1} \cdot g_{n+2} \cdot \ldots \cdot g_l$$

Так как произведение простых чисел не может быть равно 1.

3) При n>l так же к неверному равенству

$$p_{l+1} \cdot p_{l+2} \cdot \ldots \cdot p_n = 1$$

Следовательно, два разложения составного числа на простые множители могут отличатся друг от друга лишь порядком множителей.

Теорема доказана.

- Разложение составного числа a на простые множители называется каноническим представлением натурального числа.

- Задание: представьте число n=126 в каноническом виде.

- 126 | 2
  63 | 3
  21 | 3
  7 | 7
  1 |

Значит 126 =2·3·3·7

èëè $126 = 2 \cdot 3^2 \cdot 7$

- НОК(126; 54)
- 126 : 54=2 (ост. 18), тогда
- Представим 126 и 54 в каноническом виде.

$$126 = 2 \cdot 3^2 \cdot 7$$

| | |
|---|---|
| 54 | 2 |
| 27 | 3 |
| 9 | 3 |
| 3 | 3 |
| 1 | |

$$54 = 2 \cdot 3^3$$

- НОК (126;54)= $2 \cdot 3^3 \cdot 7 = 378$

НОД (126;54)= $2 \cdot 3^2 = 18$

Спасибо за внимание!