Лекция №3 (21.09.20)

2. Простые числа и их распределение.

2.1. Основная теорема арифметики.

Будем считать известными понятия простого и составного числа.

Теорема 1. *Если p – простое и $p|ab$, то $p|a$ или $p|b$.*

Следствие 1. *Если p – простое и $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_n)$, то $p|a_k$ для некоторого $k \in [1, \ldots, n]$.*

Следствие 2. *Если $p, q_1, q_2, \ldots, q_n$ – все простые и $p|(q_1 \cdot q_2 \cdot \ldots \cdot q_n)$, то $p = q_k$ для некоторого $k \in [1, \ldots, n]$.*

Теорема 2 (Основная теорема арифметики)**.** *Каждое положительное целое $n > 1$ может быть представлено в виде произведения простых чисел. Данное представление единственно с точностью до порядка следования множителей.*

Доказательство. Доказательство необходимо знать. □

Следствие 3. *Каждое положительное целое $n > 1$ может быть записано единственным образом в виде:*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r},$$

где $i = 1, \ldots, r$, k_i – положительное целое и каждое p_i – простое, причем $p_1 < p_2 < \ldots < p_r$.

2.2. Решето Эратосфена.

Если целое число $a > 1$ – составное, то мы можем записать $a = bc$, где $1 < b < a$ и $1 < c < a$. Предположим, что $b \leq c$, тогда $b^2 \leq bc = a$, следовательно, $b \leq \sqrt{a}$. Так как $b > 1$, то по Основной теореме арифметики b имеет, по крайней мере, один простой множитель p. Тогда $p \leq b \leq \sqrt{a}$. Кроме того, поскольку $p|b$ и $b|a$, то $p|a$. Окончательно, мы можем сделать вывод, что составное число a всегда обладает простым делителем p, удовлетворяющим условию $p \leq \sqrt{a}$.

Чтобы проверить произвольное целое a на простоту, достаточно перебрать простые числа, не превосходящие $\sqrt{a}$, и удостовериться, являются ли они делителями числа a или нет.

Теорема 3 (Евклида). *Существует бесконечно много простых чисел.*

Доказательство. Доказательство необходимо знать. $\square$

Теорема 4. *Если p_n – n-ое простое число, то $p \leq 2^{2n-1}$.*

Следствие 4. *Для любого $n \geq 1$ существуют, по крайней мере, $n+1$ простых чисел, меньших, чем 2^{2^n}.*

2.3. Гипотеза Гольдбаха.

Одна из гипотез Гольдбаха гласит: каждое четное целое число (≥ 6): $4n + 2$ представимо в виде суммы двух чисел, каждое из которых либо является простым вида $4n + 1$, либо равно 1.

При этом Виноградов утверждал: почти все четные числа являются суммой двух простых чисел. "Почти все" в данном контексте означает, что если $A(n)$ – число четных чисел $m < n$, которые нельзя предстваить в виде суммы двух простых чисел, то $\lim_{n\to\infty} A(n)/n = 0$.

Результат Виноградова влечет, что каждое достаточно большое четное целое число явялется суммой не более, чем четырех нечетных чисел. Таким образом, существует четное число, являющееся суммой либо двух, либо четырех нечетных простых чисел.

Лемма 1. *Произведение двух или более целых чисел вида $4n + 1$ имеет аналогичную форму.*

Теорема 5. *Существует бесконечно много простых чисел вида $4n + 3$.*

Теорема 6 (Дирихле). *Если a и b – взаимно простые положительные целые, то арифметическая прогрессия*

$$a, a + b, a + 2b, a + 3b, \ldots$$

содержит бесконечно много простых чисел.