Некоторые классические проблемы аналитической теории чисел

Деза Е.И.

5 июня 2007 г.

1 Основные результаты элементарной теории чисел

Элементарная теория чисел имеет дело с *натуральными числами* $1, 2, 3, \ldots$ (множество натуральных чисел обозначается символом $\mathbb{N}$) и *целыми числами* $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$ (множество целых чисел обозначается символом $\mathbb{Z}$).

1.1 Теорема о делении с остатком

Теорема о делении с остатком утверждает, что для любого $a \in \mathbb{Z}$ и любого $b \in \mathbb{N}$ существует единственная пара целых чисел q и r, таких что $a = bq + r$, и $0 \leq r < b$.

Число q называется *неполным частным*, а число r называется *остатком* от деления a на b.

Например, $-10 = 3 \cdot (-4) + 2$, $100 = 20 \cdot 5 + 0$.

1.2 Отношение делимости

Говорят, что целое число a *делится* на целое число b, $b \neq 0$, и пишут $b|a$, если существует целое число c, такое что $a = b \cdot c$. В этом случае b называется *делителем* a.

1 и -1 делят любое целое число, любое целое число (кроме нуля) делит само себя, и любое целое число (кроме нуля) делит 0.

Числа, делящиеся на 2, называются *четными*, числа, не делящиеся на 2, называются *нечетными*.

Делитель числа n, отличный от 1, -1, n или $-n$, называется *нетривиальным делителем*; числа, обладающие нетривиальными делителями, называются *составными*; числа, имеющие только тривиальные делители (и отличные от единицы), называются *простыми*.

Положительный делитель числа n, отличный от n, называется *собственным делителем* числа n.

Свойства отношения делимости

1. Если $a|b$ и $a|c$, то $a|(b+c)$, более того, $a|(mb+nc)$ для любых целых m и n.

2. Если $a|b$ и $b|c$, то $a|c$ (транзитивность).

3. Если $a|b$ и $b|a$, то $a = b$ или $a = -b$.

1.3 Простые и составные числа

Натуральное число p называется *простым*, если оно имеет ровно два натуральных делителя (именно, 1 и p).

Первые 30 простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, и 113.

Натуральное число n называется *составным*, если оно имеет более двух натуральных делителей. Любое составное число n можно представить в виде $n = ab$, где $1 < a \leq b < n$.

Любое натуральное число либо простое, либо составное, либо равно 1.

Любое натуральное число, большее 1, имеет простой делитель.

Фундаментальная теорема арифметики утверждает, что любое натуральное число, большее 1, можно, причем единственным образом (с точностью до порядка сомножителей), представить в виде произведения простых чисел.

1.4 НОД и НОК

Для целых $a_1, ..., a_n$, хотя бы одно из которых не равно нулю, наибольший общий делитель $gcd(a_1, ..., a_n)$ чисел $a_1, ..., a_n$ определяется как наибольшее число, делящее каждое из чисел $a_1, ..., a_n$.

Для целых чисел $a_1, ..., a_n$, каждое из которых не равно нулю, наименьшее общее кратное $lcm(a_1, ..., a_n)$ чисел $a_1, ..., a_n$ определяется как наименьшее натуральное число, делящееся на каждое из чисел $a_1, ..., a_n$.

Свойства НОД и НОК

1. $gcd(\prod_i p_i^{\alpha_i}, \prod_i p_i^{\beta_i}) = \prod_i p_i^{\gamma_i}$, $lcm(\prod_i p_i^{\alpha_i}, \prod_i p_i^{\beta_i}) = \prod_i p_i^{\delta_i}$, где $\alpha_i, \beta_i \geq 0$, $\gamma_i = \min\{\alpha_i, \beta_i\}$, и $\delta_i = \max\{\alpha_i, \beta_i\}$.

2. Каждый общий делитель чисел a и b делит $gcd(a, b)$.

3. Если $gcd(a, b) = d$, то существуют целые числа x и y, такие что $ax + by = d$.

4. Если $a|bc$, и $gcd(a, b) = d$, то $\frac{a}{d}|c$.

5. $gcd(m \cdot a, m \cdot b) = m \cdot gcd(a, b)$ для любого $m \in \mathbb{N}$.

6. $gcd(a + m \cdot b, b) = gcd(a, b)$ для любого $m \in \mathbb{Z}$.

7. Если $m|a$ и $m|b$, где $m \in \mathbb{N}$, то $gcd(a/m, b/m) = gcd(a, b)/m$.

8. $gcd(a, b) \cdot lcm(a, b) = a \cdot b$ для любых натуральных a, b.

Полезно считать, что $gcd(0, 0) = 0$ и $lcm(0, 0) = 0$, так как в этом случае множество натуральных чисел образует дистрибутивную решетку.

Наибольший общий делитель можно определить и для произвольного коммутативного кольца.

1.5 Алгоритм Евклида

Алгоритм Евклида - алгоритм для определения наибольшего общего делителя двух чисел путем последовательного применения теоремы о делении с остатком.

Именно, для любого целого a и любого натурального b, не делящего a, наибольший обший делитель чисел a и b равен последнему ненулевому остатку r_s следующего алгоритма: $a = bq_1 + r_1$, $b = r_1q_2 + r_2$, ..., $r_{s-2} = r_{s-1}q_s + r_s$, $r_{s-1} = r_sq_s + 0$, где $r_1 > r_2 > ... > r_s > 0$.

Например, так как $1071 = 1029 \cdot 1 + 42$, $1029 = 42 \cdot 24 + 21$, и $42 = 21 \cdot 2 + 0$, мы получаем, что $gcd(1071, 1029) = 21$.

Алгоритм Евклида является одним из старейших известных алгоритмов. Он встречается в "Началах"Евклида около 300 года до н.э. Евклид формулировал проблему геометрически, как задачу нахождения общей "меры"для двух отрезков, и его алгоритм состоял в последовательном вычитании меньшего отрезка из большего. Однако вероятно, что алгоритм не был открыт Евклидом, а появился почти на 200 лет раньше. Он был, скорее всего, известен Евдоксу (около 375 года до нашей эры); Аристотель (около 330 года до нашей эры) упоминал о нем в своих трудах.

Этот алгоритм может быть использован на любом множестве, где возможно деление с остатком. Такие множкства включают в себя кольца многочленов над полем, кольцо целых чисел Гаусса, наконец, Евклидовы области.

1.6 Взаимно-простые числа

Два целых числа a и b называются *взаимно-простыми*, если их наибольший общий делитель равен 1, то есть, они не имеют общих делителей, отличных от 1 и -1.

Например, 6 и 35 являются взаимно-простыми, так как $gcd(6, 35) = 1$, но 6 и 27 не взаимно-просты, так как $gcd(6, 27) = 3$.

Число 1 взаимно-просто с любым целым числом; число 0 взаимно-просто только с 1 и -1.

Свойства взаимно-простых чисел

1. a и b являются взаимно-простыми тогда и только тогда, когда существуют целые числа x и y, такие что $ax + by = 1$.
2. Если $b|ac$, и $gcd(b, c) = 1$, то $b|a$.

3. Если $b|a, c|a$, и $gcd(b, c) = 1$, то $bc|a$.

4. $gcd(a, b) = 1$ тогда и только тогда, когда $gcd(a^n, b^m) = 1$ для любых неотрицательных целых чисел m и n.

1.7 Арифметические функции

Комплекснозначная функция $f(n)$ называется *арифметической функцией*, если значение $f(n)$ определено для любого натурального числа n.

Существует много примеров известных арифметических функций, среди них:

- целая часть $\lfloor x \rfloor$, то есть, наибольшее целое число, не превосходящее x;

- Функция Мебиуса $\mu(n)$, определяемая следующим образом: $\mu(1) = 1$, $\mu(p_1...p_k) = (-1)^k$ для бесквадратного числа $n = p_1...p_k$, и $\mu(n) = 0$ в остальных случаях;

- Функция делителей $\sigma_k(n) = \sum_{d|n} d^k$, где сумма берется по всем натуральным делителям d числа n, а k - любое комплексное число;

- Функция Эйлера $\phi(n) = \sharp\{x \in \mathbb{N} : x \leq n, gcd(x, n) = 1\}$;

- Функция $\pi(x) = \sum_{p \leq x} 1$.

Арифметическая функция f называется *мультипликативной*, если $f(1) = 1$, и $f(mn) = f(m)f(n)$ для любых взаимно-простых натуральных чисел n и m.

Мультипликативная функция f называется *вполне мультипликативной*, если $f(mn) = f(m)f(n)$ для любых натуральных чисел m и n.

Например, функция $f(n) = n^\alpha$ является вполне мультипликативной для любого действительного α. Функция делителей, функция Мебиуса, функция Эйлера являются мультипликативными, но не являются вполне мультипликативными. Функция $\pi(x)$ не является мультипликативной функцией.

Свойства мультипликативных функций

1. Произведение мультипликативных функций есть мультипликативная функция.

2. Если f - мультипликативная функция, то, для данного $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, $\sum_{d|n} f(d) = \prod_{i=1}^{k}(1 + f(p_i) + f(p_1^2) + ... + f(p_i^{\alpha_k}))$.

3. Если f - мультипликативная функция, то $h(n) = \sum_{d|n} f(d)$ - мультипликативная функция.

1.8 Отношение сравнимости

Два целых числа a и b называются сравнимыми по модулю n, $n \in \mathbb{N}$, если a и b имеют одинаковые остатки при делении на n, или, что то же, если $n|(a - b)$. В этом случае пишут $a \equiv b(modn)$.

Свойства отношения сравнимости

1. Отношение сравнимости $\equiv$ является отношением эквивалентности.

2. Если $a \equiv b(modn)$, то $f(a) \equiv f(b)(modn)$ для любого многочлена $f(x)$ с целыми коэффициентами.

3. $a \equiv b(modn)$ тогда и только тогда, когда $ka \equiv kb(modkn)$ для любого натурального k.

4. $a \equiv b(modn)$ тогда и только тогда, когда $ka \equiv kb(modn)$ для любого целого k, такого что $gcd(k, n) = 1$.

5. $a \equiv b(modn_i)$, $i = 1, ..., k$, тогда и только тогда, когда $a \equiv b(modM)$, где $M = lcm(n_1, ..., n_k)$.

1.9 Классы вычетов

Множество $[a]_n = \{x \in \mathbb{Z} : x \equiv a(mod n)\} = \{..., a-2n, a-n, a, a+n, a+2n, a+3n, ...\}$ всех целых чисел, сравнимых с данным числом a по модулю n, называется классом вычетов (числа a) по модулю n.

Сложение и умножение на множестве $Z/nZ = \{[0]_n, [1]_n, [2]_n, ..., [n-1]_n\}$ всех классов вычетов определяются следующим образом: $[a]_n + [b]_n = [a+b]_n$, и $[a]_n \cdot [b]_n = [ab]_n$.

В этом случае Z/nZ превращается в коммутативное кольцо, содержащее n элементов. Для простого числа p множество Z/pZ образует поле.

1.10 Функция Эйлера

Для данного натурального n, функция Эйлера $\phi(n)$ определяется как число натуральных чисел, не превосходящмх n и взаимно-простых с n: $\phi(n) = \sharp\{x \in \mathbb{N} : x \leq n, gcd(x, n) = 1\}$.

Например, $\phi(8) = 4$, так как ровно четыре натуральных числа, не превосходящих 8, 1, 3, 5 и 7, являются взаимно-простыми с 8.

Свойства функции Эйлера

1. $\phi(p) = p - 1$ для любого простого p.
2. $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ для любого простого p и любого натурального α.
3. Функция Эйлера мультипликативна, то есть, $\phi(mn) = \phi(m)\phi(n)$ для любых взаимно-простых натуральных чисел m и n.
4. $\sum_{d|n} \phi(d) = n$, где сумма берется по всем положительным делителям d числа n (тождество Гаусса).

Функция Эйлера дает число обратимых элементов кольца Z/nZ.

1.11 Малая теорема Ферма и теорема Эйлера

Малая теорема Ферма утверждает, что, для любого простого p и любого целого a, $a^p \equiv a(mod p)$.

Часто используется и такая формулировка: если p - простое число, и a - целое число, взаимно-простое с p, то $a^{p-1} \equiv 1(mod p)$.

Малая теорема Ферма лежит в основе теста простоты Ферма.

Теорема Эйлера утверждает, что для любого натурального числа n и любого целого a, взаимно-простого с n, $a^{\phi(n)} \equiv 1(mod n)$, где $\phi(n)$ - функция Эйлера.

Теорема Эйлера является обобщением малой теоремы Ферма и, в свою очередь, обобщается теоремой Кармайкла.

Теорема Кармайкла утверждает, что, для взаимно-простых a и n, $a^{\lambda(n)} \equiv 1(mod n)$, где $\lambda(n)$ - функция Кармайкла: для простого $p \geq 3$ и натурального α, $\lambda(p^\alpha) = \phi(p^\alpha)$; для натурального $\alpha \geq 3$, $\lambda(2^\alpha) = 2^{\alpha-2}$, в то время как $\lambda(2) = 1$, и $\lambda(4) = 2$; наконец, $\lambda(p_1^{\alpha_1}...p_k^{\alpha_k}) = lcm(\lambda(p_1^{\alpha_1}), ..., \lambda(p_k^{\alpha_k}))$.

1.12 Решение сравнений

Пусть $f(x) = a_m x^m + ... + a_1 x + a_0$ - многочлен с целыми коэффициентами, и $a_m \neq 0(mod n)$. Если, для некоторого $x_0 \in \mathbb{Z}$, $f(x_0) \equiv 0(mod n)$, то, для любого $y \equiv x_0(mod n)$, $f(y) \equiv 0(mod n)$. В этом случае говорят, что класс вычетов $x \equiv x_0(mod n)$ является *решением* сравнения $f(x) \equiv 0(mod n)$, которое называется *сравнением степени* m *по модулю* n.

Теорема о линейных сравнениях утверждает, что линейное сравнение $ax + b \equiv 0(mod n)$ имеет ровно одно решение, если $gcd(a, n) = 1$, ровно d решений, если $gcd(a, n) = d$, $d|n$, и не имеет решений в остальных случаях.

Китайская теорема об остатках утверждает, что система линейных сравнений

$$\begin{cases} x & \equiv & c_1(mod n_1) \\ ... & & \\ x & \equiv & c_k(mod n_k) \end{cases}$$

с попарно взаимно-простыми модулями n_i имеет ровно одно решение, то есть, класс вычетов по модулю $N = gcd(n_1, ...n_k) = n_1...n_k$, которое имеет вид $x \equiv \frac{N}{n_1} c_1 y_1 + ... + \frac{N}{n_k} c_k y_k(mod M)$, где y_i - решение линейного сравнения $\frac{N}{n_i} y \equiv 1(mod n_i)$.

Заметим, что данная теорема может быть сформулирована также для колец и двусторонних идеалов.

Для данного простого p, сравнение $f(x) \equiv 0(mod p)$ степени m по модулю p эквивалентно сравнению $x^s + ... + b_1 x + b_0 \equiv 0(mod p)$ степени $s \leq p - 1$ по модулю p, и имеет $\leq s$ решений. Их можно найти перебором представителей $0, ..., p - 1$ всех классов вычетов по модулю p.

Для данного простого p и данного натурального $\alpha > 1$ рассмотрим сравнение $f(x) \equiv 0(mod p^\alpha)$ степени m по модулю p^α. Мы можем использовать следующий алгоритм для нахождения всех решений данного сравнения:

- Рассмотрим сравнение $f(x) \equiv 0(mod p)$, найдем все его решения; пусть $x \equiv x_1(mod p)$ - одно из этих решений, то есть, $f(x_1) \equiv 0(mod p)$, и $x = x_1 + pt_1$, $t_1 \in \mathbb{Z}$.

- Рассмотрим линейное сравнение $\frac{f(x_1)}{p} + f'(x_1)t_1 \equiv 0(mod p)$, найдем все его решения; пусть $t_1 \equiv t'(mod p)$ - одно из этих решений, то есть, $t_1 = t' + pt_2$, и $x = x_2 + p^2 t_2$.

- Рассмотрим линейное сравнение $\frac{f(x_2)}{p^2} + f'(x_2)t_2 \equiv 0(mod p)$, найдем все его решения; пусть $t_2 \equiv t''(mod p)$ - одно из этих решений, то есть, $t_2 = t'' + pt_3$, и $x = x_3 + p^3 t_3$.

  ...

- Рассмотрим линейное сравнение $\frac{f(x_{\alpha-1})}{p^{\alpha-1}} + f'(x_{\alpha-1})t_{\alpha-1} \equiv 0(mod p)$, найдем все его решения; пусть $t_{\alpha-1} \equiv t^{''\cdots'}(mod p)$ - одно из этих решений, то есть, $t_{\alpha-1} = t^{''\cdots'} + pt_\alpha$, и $x = x_\alpha + p^\alpha t_\alpha$.

Следовательно, $x \equiv x_\alpha(mod p^\alpha)$ - одно из решений первоначального сравнения, и все его решения могут быть найдены этим способом.

Наконец, для данного составного числа $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ все решения сравнения $f(x) \equiv 0(modn)$ степени m по модулю n могут быть найдены, используя приведенные выше аргументы и следующее свойство: $f(x) \equiv 0(modn)$ тогда и только тогда, когда

$$\begin{cases} f(x) & \equiv & 0(modp^{\alpha_1}) \\ \dots & & \\ f(x) & \equiv & 0(modp_k^{\alpha_k}). \end{cases}$$

1.13 Квадратичные вычеты и символ Лежандра

Для данного нечетного простого числа p, целое число a, взаимно-простое с p, называется *квадратичным вычетом* по модулю p, если $x_0^2 \equiv a(modp)$ для некоторого целого x_0. В противном случае a называется *квадратичным невычетом* по модулю p.

Для любого целого a, взаимно-простого с нечетным простым числом p, *символ Лежандра* $(\frac{a}{p})$ определяется следующим образом: $(\frac{a}{p}) = 1$, если a является квадратичным вычетом по модулю p, и $(\frac{a}{p}) = -1$, если a является квадратичным невычетом по модулю p. Если $p|a$, мы считаем, что $(\frac{a}{p}) = 0$.

Свойства символа Лежандра

1. $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}(modp)$ (критерий Эйлера).
2. Если $a \equiv b(modp)$, то $(\frac{a}{p}) = (\frac{b}{p})$.
3. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
4. $(\frac{a^2}{p}) = 1$; в частности, $(\frac{1}{p}) = 1$.
5. $(\frac{-1}{p}) = 1$, если $p \equiv 1(mod4)$, и $(\frac{-1}{p}) = -1$, если $p \equiv -1(mod4)$.
6. $(\frac{2}{p}) = 1$, если $p \equiv \pm1(mod8)$, и $(\frac{2}{p}) = -1$, если $p \equiv \pm3(mod8)$.
7. Для различных нечетных простых чисел p и q, $(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(\frac{q}{p})$ (квадратичный закон взаимности).

Докажем квадратичный закон взаимности методом Гаусса.

1. Докажем лемму Гаусса: $(\frac{a}{p}) = (-1)^n$, где n - число чисел системы $\{1 \cdot a, 2 \cdot a, ..., \frac{p-1}{2} \cdot a\}$, имеющих отрицательный абсолютно наименьший вычет по модулю p.

Рассмотрев числа $1 \cdot a, ..., \frac{p-1}{2} \cdot a$, мы убедимся, что все они взаимно-просты с числом p ($i \in \{1, ..., \frac{p-1}{2}\}$ взаимно-просто с p, a взаимно-просто с p по условию, тогда и их произведение ia взаимно-просто с p), и принадлежат разным классам вычетов по модулю p ($ia \equiv ka(modp) \Rightarrow i \equiv k(modp) \Rightarrow$ (так как $i, k \in \{1, ..., \frac{p-1}{2}\}$) $i = k$) и, следовательно, каждое из этих чисел сравнимо ровно с одним элементом приведенной системы вычетов $\{\pm1, ..., \pm\frac{p-1}{2}\}$ по модулю p: $ia \equiv (-1)^{n_i} r_i$, $i \in \{1, ..., \frac{p-1}{2}\}$, $r_i \in \{1, ..., \frac{p-1}{2}\}$, $n_i \in \{0, 1\}$. При этом если $i \neq k$, то и $r_i \neq r_k$ (иначе $ia \equiv \pm ka(modp)$, и следовательно $i = k$, противоречие). Таким образом, $1 \cdot ... \cdot \frac{p-1}{2} a^{\frac{p-1}{2}} \equiv (-1)^{n_1 + ... + n_{\frac{p-1}{2}}} r_1 ... r_{\frac{p-1}{2}}$, и, сокращая на одно и то же число $1 \cdot ... \cdot \frac{p-1}{2} = r_1 ... r_{\frac{p-1}{2}}$, получим, что $a^{\frac{p-1}{2}} \equiv (-1)^n$, где $n = n_1 + ... + n_{\frac{p-1}{2}}$

равно числу элементов ia, для которых $n_i = 1$, то есть, которые имеют отрицательные абсолютно наименьшие вычеты.

2. Докажем, что $(\frac{a}{p}) = (-1)^t$, где $t = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{2ia}{p} \rfloor$. Действительно, рассмотрев числа ia из доказательства предыдущего пункта, мы получим, что $ia = pq_i + r_i$, $0 < r_i < p$, при этом ia имеет положительный абсолютно наименьший вычет (равный r_i) тогда и только тогда, когда $0 < r_i \leq \frac{p-1}{2}$.

Таким образом, $n_i = 0$, если $r_i \in \{1, ..., \frac{p-1}{2}\}$, и $n_i = 1$, иначе.

Рассмотрим число $\frac{2ia}{p} = 2q_i + \frac{2r_i}{p}$. Если $r_i \in \{1, ..., \frac{p-1}{2}\}$, то $0 < \frac{2r_i}{p} < 1$, и, так как $2q_i \in \mathbb{Z}$, мы получим, что $\lfloor \frac{2ia}{p} \rfloor = 2q_i + \lfloor \frac{2r_i}{p} \rfloor = 2q_i$. Иначе $\frac{p-1}{2} < r_i \leq p$, $1 < \frac{2r_i}{p} < 2$, и $\lfloor \frac{2ia}{p} \rfloor = 2q_i + \lfloor \frac{2r_i}{p} \rfloor = 2q_i + 1$.

Таким образом, $\lfloor \frac{2ia}{p} \rfloor$ есть число четное тогда и только тогда, когда $n_i = 0$, и число нечетное тогда и только тогда, когда $n_i = 1$, откуда следует, что суммы $t = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{ia}{p} \rfloor$ и $n = \sum_{i=1}^{\frac{p-1}{2}} n_i$ имеют одинаковую четность, то есть, $(-1)^t = (-1)^n$, что и доказывает наше утверждение.

3. Докажем, что для нечетного a мы имеем равенство $(\frac{a}{p}) = (-1)^s$, где $s = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{ia}{p} \rfloor$.

Если a нечетно, то $a + p$ - четно. Рассмотрим $(\frac{2}{p})(\frac{a}{p}) = (\frac{2a}{p}) = (\frac{4\frac{a+p}{2}}{p}) = (\frac{\frac{a+p}{2}}{p}) = (-1)^t$, $t = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{i(a+p)}{p} \rfloor = \sum_{i=1}^{\frac{p-1}{2}} (\lfloor \frac{ia}{p} \rfloor + i) = \frac{p^2-1}{8} + \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{ia}{p} \rfloor$. Беря $a = 1$, получим, что $\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{ia}{p} \rfloor = 0$, и $(\frac{a}{p}) = 1$, то есть $(\frac{a}{p}) = (-1)^{(p^2-1)/8}$. Сокращая теперь обе части равенства на одинаковую величину, получим искомый результат.

4. Пусть $p, q \in P \backslash \{2\}$ и $p \neq q$. По пункту 3., $(\frac{p}{q})(\frac{q}{p}) = (-1)^{s+f}$, где $s = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor$, $f = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$.

Рассмотрим на плоскости прямоугольник с вершинами $(0, 0)$, $(0, \frac{p-1}{2})$, $(\frac{q-1}{2}, 0)$, $(\frac{q-1}{2}, \frac{p-1}{2})$. Число точек с натуральными координатами в этом прямоугольнике равно $\frac{p-1}{2}\frac{q-1}{2}$.

Подсчитаем число данных точек другим способом. Для этого проведем прямую $y = \frac{p}{q}x$. Она не содержит ни одной из рассматриваемых точек (иначе $qy_0 = px_0$, то есть $q|x_0$, и $p|y_0$, что невозможно для точки (x_0, y_0) с натуральными координатами из заданного прямоугольника). Легко видеть, что число точек, лежащих под этой прямой, равно $\sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$. Аналогично, число точек над данной прямой равно $\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p}$ ("переверните"оси координат и расмотрите нашу прямую как прямую $x = \frac{q}{p}y$). Таким образом, $\frac{p-1}{2}\frac{q-1}{2} = s + f$, и $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Символ Лежандра является специальным случаем символа Якоби. Кроме того, символ Лежандра является примером характера Дирихле.

1.14 Показатели, первообразные корни и индексы

Для данного натурального числа n и данного целого числа a, взаимно- простого с n, *показателем* $P_n(a)$ *числа* a *по модулю* n называется наименьшее натуральное число γ, такое что $a^\gamma \equiv 1 (mod n)$.

Свойства показателей

1. $P_n(a)|\phi(n)$; в частности, $0 \le P_n(a) \le \phi(n)$.

2. Если $a^\delta \equiv 1 (mod n)$, то $P_n(a)|\delta$.

3. $a^\delta \equiv a^\eta (mod n)$ тогда и только тогда, когда $\delta \equiv \eta (mod P_n(a))$.

Если $P_n(g) = \phi(n)$, то g называется *первообразным корнем по модулю* n.

В этом случае числа $g^0, ..., g^{\phi(n)-1}$ образуют *приведенную систему вычетов по модулю* n, то есть, дают ровно по одному представителю каждого класса вычетов, взаимно-простого с n.

Первообразные корни существуют только по модулям $n = 2, 4, p^\alpha, 2p^\alpha$, где p - любое нечетное простое число, а α - любое натуральное число.

Если g является первообразным корнем по модулю n, то для любого a, взаимно-простого с n, $a \equiv g^\beta (mod n)$, где $\beta \in [0, \phi(n) - 1]$. Число β называется *индексом числа* a *по модулю* n *с основанием* g. В этом случае мы пишем $\beta = ind a = ind_g a$.

Свойства индексов

1. Если $a \equiv b (mod n)$, то $ind a \equiv ind b (mod \phi(n))$.

2. $ind ab \equiv ind a + ind b (mod \phi(n))$.

3. $ind a^k \equiv k ind a (mod \phi(n))$ для любого целого неотрицательного числа k.

4. $P_n(a) = \frac{\phi(n)}{gcd(ind a, \phi(n))}$.

1.15 Цепные дроби

Цепная дробь $[a_0, ..., a_n, ...]$ определяется как $a_0 + \frac{1}{a_1 + \frac{1}{\cdots \frac{1}{a_n + \cdots}}}$, где a_0 - некоторое целое число, а все a_n, $n \in \mathbb{N}$ - натуральные числа (причем последнее, если оно существует, $\neq 1$).

Рациональные числа $\delta_k = [a_0, ..., a_k] = \frac{P_k}{Q_k}$, $k = 0, ..., n, ...$, называются *подходящими дробями* к цепной дроби $[a_0, ..., a_n, ...]$.

Свойства цепных дробей

1. Если $\delta_k = \frac{P_k}{Q_k}$, то $P_0 = a_0$, $P_1 = a_1 a_0 + 1$, и $P_n = a_n P_{n-1} + P_{n-2}$ для всех $n \ge 2$.

2. Если $\delta_k = \frac{P_k}{Q_k}$, то $Q_0 = 1$, $Q_1 = a_1$, и $Q_n = a_n Q_{n-1} + Q_{n-2}$ для всех $n \ge 2$.

3. $gcd(P_n, Q_n) = 1$.

4. $1 = Q_0 \le Q_1 < Q_2 < ...$.

5. Если $P_0 > 1$, то $P_1 > P_2 > P_3 > ...$.

6. $\delta_n - \delta_{n-1} = \frac{(-1)^{n+1}}{Q_n Q_{n-1}}$.

7. $\delta_0 < \delta_2 < ... < \delta_3 < \delta_1$.

8. Каждая конечная цепная дробь является рациональным числом, и каждое рациональное число представимо, причем единственным образом, в виде конечной цепной дроби.

9. Каждая бесконечная цепная дробь является иррациональным числом, и каждое иррациональное число представимо, причем единственным образом, в виде бесконечной цепной дроби.

10. Бесконечная цепная дробь является периодической тогда и только тогда, когда она представляет некоторую квадратическую иррациональность, то есть, иррациональное число, являющееся корнем квадратного терехчлена с целыми коэффициентами.

11. $[a_0, ..., a_n, ...] = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}}$, где $\alpha_n = [a_n, ...]$.

12. Если $\alpha = [a_0, ..., a_n, ...]$, то $|\alpha - \delta_n| \leq \frac{1}{Q_n Q_{n+1}}$; в частности, для любого $n > 1$, δ_n является *наилучшим приближением* для α.

2 Простые числа

2.1 Предварительные сведения

Натуральное число p, имеющее ровно два натуральных делителя, называется *простым числом.*

Множество простых чисел обозначается символом P. Таким образом, $P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots\}$.

Натуральное число n, имеющее более двух натуральных делителей, называется *составным.*

Множество составных чисел обозначается символом S. Таким образом, $S = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, \dots\}$.

Так как единица имеет ровно один натуральный делитель, то есть не является ни простым, ни составным числом, мы имеем: $\mathbb{N} = P \cup S \cup \{1\}$.

Около двух тысяч лет назад Евелид доказал, что *множество простых чисел бесконечно.* Рассмотрим доказательство Евклида. Предположим, что множество простых чисел конечно, и $P = \{p_1, \dots, p_k\}$ - все простые числа. Пусть $E = p_1 \dots p_k + 1$, и пусть p - простое число, делящее E. Тогда p на может совпадать ни с одним из чисел $p_1, \dots, p_k$, иначе p должно делить разность $E - p_1 ... p_k = 1$, что невозможно. Таким образом, p - простое число, не попавшее в список, то есть, числа $p_1, \dots, p_k$ не могут давать всех простых чисел.

Эйлер дал аналитическое доказательство бесконечности множества простых чисел: предположив, что множество $P = \{p_1, ..., p_k\}$ конечно, рассмотрим рациональное число $X = \prod_{i=1}^{k}(1 - \frac{1}{p_i})^{-1}$. Так как выражение $(1 - \frac{1}{p_i})^{-1}$ равно сумме $1 + \frac{1}{p_i} + \frac{1}{p_i^2} + ...$ бесконечной геометрической прогрессии $1, \frac{1}{p_i}, \frac{1}{p_i^2}, ...$, мы получаем, что $\prod_{i=1}^{k}(1 - \frac{1}{p_i})^{-1} = \prod_{i=1}^{k}(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + ...) = \sum_{\alpha_i \geq 0} \frac{1}{p_1^{\alpha_1} ... p_k^{\alpha_k}} = \sum_{n=1}^{\infty} \frac{1}{n}$. Но $\sum_{n=1}^{\infty} \frac{1}{n}$ - гармонический ряд, являющийся расходящимся. Полученное противоречие показывает, что наше предположение о конечности множества простых чисел неверно.

Эйлер показал также, что сумма $\sum_p \frac{1}{p}$ ряда, составленного из чисел, обратных простым, расходится.

Действительно, для $x \in N$ рассмотрим $\prod_{p_i \le x} \frac{1}{1-p_i^{-1}} = \sum \frac{1}{p_1^{\alpha_1}...p_s^{\alpha_s}} > \sum_{n=1}^{x} \frac{1}{n}$. Легко видеть, что $\sum_{n=1}^{x} \frac{1}{n} \ge 1+\ln x$, и, следовательно, $-\sum_{p_i \le x} \ln(1-\frac{1}{p_i}) > \ln(\ln x+1)$. Так как $\frac{1}{p_i} \le \frac{1}{2}$, то $-\ln(1-\frac{1}{p_i}) = \frac{1}{p_i}+\frac{1}{2}(\frac{1}{p_i})^2+\frac{1}{3}(\frac{1}{p_i})^3... < \frac{1}{p_i}+\frac{1}{p_i}^2+... = \frac{1}{p_i}\frac{1}{1-p_i^{-1}} \le \frac{2}{p_i}$. Следовательно, $2\sum_{p_i \le x} \frac{1}{p_i} \ge -\sum_{p_i \le x} \ln(1-\frac{1}{p_i}) > \ln(\ln x+1)$, и $\sum_{p_i \le x} \frac{1}{p_i} > 0.5\ln(\ln x+1)...$.

Точнее, имеет место асимптотическая формула $\sum_{p \le x} \frac{1}{p} = \ln\ln x + o(\ln\ln x)$.

Упражнения

1. Доказать, что если $n \in S$, то $n = ab$, $1 < a \le b < n$.
2. Доказать, что любое составное число n имеет простой делитель $p \le \sqrt{n}$.
3. Доказать, что $p_n \le 2^{2^n}$ для любого натурального n, где p_n - n-е простое число.
4. Доказать, что $p_n \le 2^{2^{n-1}}$ для $n > 1$.
5. Доказать что для данного $n \ge 3$ между n и $n!$ существует по крайней мере одно простое число; доказать бесконечность множества простых, пользуясь этим соображением.
6. Доказать, что если p - нечетное простое число, то оно имеет вид $4k-1$ или $4k+1$.
7. Доказать, что если p - простое число > 3, то оно имеет вид $6k-1$ или $6k+1$.
8. Доказать, что существует бесконечно много простых чисел вида $4k-1$.
9. Доказать, что существует бесконечно много простых чисел вида $6k-1$.

2.2 Как выяснить, является ли данное натуральное число простым ?

Простейший метод нахождения всех простых чисел на данном интервале был предложен греческим математиком Эратосфеном. Рассмотрим последовательность 2, 3, 4, ... Так как 2 является первым простым числом, p_1, вычеркнем из нашей последовательности все числа, большие p_1 и делящиеся на p_1, то есть, начиная с 2, каждое второе число таблицы. Первое из оставшихся чисел $3 = p_2$. Вычеркнем все числа, большие p_2 и делящиеся на p_2, то есть, начиная с 3, каждое третье число таблицы. Первое из оставшихся чисел $5 = p_3$, и т.д. Таким образом, мы получаем $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $\dots$, $p_{1000} = 7917$, $p_{6000000} = 104395301$, $\dots$. Здесь, напомним, символ p_n обозначает n-е простое число.

Существует много других возможностей определить, является ли данное натуральное число простым.

Простейший такой тест состоит в следующем: для данного натурального n мы проверяем, существует ли число m из промежутка от 2 до $n-1$, которое делит n. Если n делится на некоторое такое m, то n является составным, в противном случае - простым.

Вместо того чтобы проверять все m до $n-1$, можно ограничиться проверкой простых m до $\sqrt{n}$: если n является составным числом, то оно имеет простой делитель $p \leq \sqrt{n}$.

Современные тесты на простоту гораздо эффективнее. Они делятся на две категории: точные и вероятностные. В первом случае мы имеем стопроцентную гарантию того, что прошедшее тест число является простым. Во втором случае существует небольшая, но не равная нулю вероятность того, что прошедшее тест число все-таки является составным.

Простейшим вероятностным тестом является тест Ферма.

Он основан на использовании малой теоремы Ферма.

Theorem 1 *Если p - простое число, и a - целое число, взаимно-простое с p, то $a^{p-1} \equiv 1(mod p)$.*

Докажем теорему по индукции. Для $a = 1$ имеем: $1^p \equiv 1(mod p)$. Переходя от a к $a+1$, получаем $(a+1)^p \equiv a^p + \binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a + 1 \equiv a + 1(mod p)$, так как биномиальные коэффициенты $\binom{p}{k} \equiv 0(mod p)$ для $k = 1, ..., p-1$.

Таким образом, если мы хотим выяснить, является ли данное натуральное число n простым, мы случайным образом выбираем число a из промежутка $[2, n-1]$, и используем малую теорему Ферма. Если сравнение не имеет места для данного a, то n является составным. Если сравнение имеет место для нескольких значений a, мы говорим, что, с большой долей вероятности, n является простым.

Однако всегда имеется вероятность того, что проверенное нами число - только псевдопростое. Составное число x называется *псевдопростым по основанию* a, если a и x взаимно-просты, и $a^{x-1} \equiv 1(mod x)$.

Числа Пуле - это псевдопростые по основанию 2. Наименьшее число Пуле равно 341. Оно составное, так как представимо в виде $11 \cdot 31$, но удовлетворяет условиям малой теоремы Ферма: $2^{340} \equiv 1(mod 341)$. Последовательность чисел Пуле начинается с элементов 341, 561, 645, 1105, 1387, ...

Натуральное число x, которое является псевдопростым для всех допустимых (то есть, взаимно-простых с x) значений a называется *числом Кармайкла.* Натуральное число n является числом Кармайкла тогда и только тогда, когда n бесквадратно, и, для любого простого делителя p числа n, $p-1$ делит $n-1$.

В 1910 Кармайкл нашел первое и наименьшее такое число, 561. (Что 561 является числом Кармайкла, легко видеть из предыдущей теоремы: действительно, $561 = 3 \cdot 11 \cdot 17$ бесквадратно, и $2|560, 10|560, 16|560$.)

Следующие числа Кармайкла: $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, $2821 = 7 \cdot 13 \cdot 31$, $6601 = 7 \cdot 23 \cdot 41$, $8911 = 7 \cdot 19 \cdot 67$, ...

Число $(6k+1)(12k+1)(18k+1)$ является числом Кармайкла, если все три указанных множителя являются простыми.

Существует бесконечно много чисел Кармайкла. Именно, для достаточно большого n существует $n^{2/7}$ чисел Кармайкла между 1 и n.

Однако, при движении вправо по числовой оси, числа Кармайкла становятся очень редки. Например, существует 1401644 чисел Кармайкла между 1 и 10^{18} (приблизительно одно на 700 миллионов чисел).

Тест Соловья-Страссина - еще один вероятностный тест для определения простоты данного натурального числа.

По критерию Эйлера, для любого нечетного простого p и любого $a \in [1, p-1]$, $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}(modp)$, где $(\frac{a}{p})$ - символ Лежандра. Символ Якоби $(\frac{a}{n})$, определяемый как $(\frac{a}{n}) = \prod_i (\frac{a}{p_i})^{\alpha_i}$ для $n = \prod_i p_i^{\alpha_i}$, является обобщением символа Лежандра и может быть использован для любого нечетного n. Используя квадратичный закон взаимности, символ Якоби может быть вычислен за время $O((logn)^2)$.

Таким образом, если мы хотим проверить простоту числа n, мы можем произвольным образом выбрать несколько значений a и убедиться, что указанное выше сравнение выполняется. Если для некоторого a оно нарушается, то n - составное число.

Однако, подобно тесту Ферма, мы можем получить положительный ответ (о простоте) для составного числа. Величина a называется "лгуном Эйлера", если сравнение выполнено, но n является составным. "Свидетелем Эйлера"называется число a, для которого сравнение не будет иметь места при составном n - мы говорим, что a свидетельствует о том, что n - составное.

В отличие от теста Ферма, для каждого n по меньшей мере половина всех $a \in [1, p-1]$ являются свидетелями Эйлера. Следовательно, в данном случае нет чисел, подобных числам Кармайкла в тесте Ферма, которые являются лгунами для всех ситуаций. Тест объявляет составное n как вероятностно-простое с вероятностью не более 2^{-k}, где k - число различных использованных нами a.

Рассмотрим теперь тест Миллера-Рабина.

Для этого используем лемму о квадратных корнях из единицы в конечном поле Z/pZ, где p - некоторое простое число. Очевидно, 1 и -1 при возведении в квадрат по модулю p дают 1; назовем их тривиальными квадратными корнями из 1. Так как p является простым числом, нетривиальных корней из 1 не существует.

Для данного нечетного простого p мы можем записать $p-1$ как $2^k d$, где k - целое, а d - нечетное. Тогда, для всех целых a, $a^d \equiv 1(modp)$, или $a^{2^r d} \equiv -1(modp)$ для некоторого $r \in [0, k-1]$.

Тест Миллера-Рабина использует данные соотношения: для данного нечетного n, если $n - 1 = 2^k d$ и мы можем найти такое a, что $a^d \neq 1(modn)$, и $a^{2^r d} \neq -1(modn)$ для всех $r \in [0, n-1]$, то a свидетельствует о том, что n - составное (иногда его называют "сильным свидетелем"). Иначе (то есть в случае выполнения обоих условий для составного n) a называется "сильным лгуном", и n объявляется "сильным вероятностно-простым"по основанию a.

Наименьшими "сильными вероятностно-простыми числами"($SPRP$) являются: для $a = 2$, $2047 = 23 \cdot 89$ $(2 - SPRP)$, для $a = 3$, $121 = 11 \cdot 11$ $(3 - SPRP)$, для $a = 5$, $781 = 11 \cdot 71$ $(5 - SPRP)$, для $a = 7$, $25 = 5 \cdot 5$ $(7 - SPRP)$.

Для каждого нечетного составного n имеется много свидетелей: по меньшей мере $3/4$ от всех допустимых a. Однако мы не знаем простого способа нахождения таких a. Решением является превращение этого теста в вероятностный: выбирая a случайным образом k раз, мы получим высокую вероятность правильного ответа, так как тест объявит составное n вероятностно-простым с вероятностью не более 4^{-k}.

Несмотря на то, что на практике используются вероятностные тесты простоты, теоретически существует и много критериев простоты. Так, для данного натурального числа n, если, для некоторого $1 < a < n$, $a^{n-1} \equiv 1(modn)$, и, кроме того, $a^{\gamma} \neq 1(modn)$ для всех натуральных $\gamma | n-1$, то n является простым.

Действительно, пользуясь свойствами показателей, из первого условия мы получаем, что $P_n(a)|n-1$, и из второго условия следует теперь равенство $P_n(a) = n - 1$. Так как $P_n(a)|\phi(n)$, то $n-1|\phi(n)$; так как $\phi(n) < n$ для $n \neq 1$, то $\phi(n) = n - 1$, то есть, $n \in P$.

В вычислительной теории чисел этот тест называется тестом Люкаса-Лемера; для его использования необходимо знать все простые делители числа $n - 1$. Данный тест опирается на тот факт, что показатель первообразного корня a по модулю n равен $n-1$ для простого n. Если мы можем показать, что a - первообразный корень по модулю n, мы можем показать, что n - простое число.

Другим критерием простоты данного натурального числа является теорема Вильсона.

Theorem 2 *Натуральное число p является простым тогда и только тогда, когда $(p-1)! \equiv -1 (modp)$.*

Рассмотрим два доказательства этой теоремы. Первое доказательство использует тот факт, что, для нечетного простого числа p, множество $Z/pZ^* = \{1, 2, ...p-1\}$ образует группу относительно умножения по модулю p. Это означает, что, для каждого элемента a, существует обратный ему элемент b, такой что $ab \equiv 1(modp)$. Если $a \equiv b(modp)$, то $a^2 \equiv 1(modp)$, то есть $a^2 - 1 = (a+1)(a-1) \equiv 0(modp)$, и, так как p - простое, $a \equiv 1$ или $\equiv -1(modp)$, то есть $a = 1$ или $a = p - 1$.

Другими словами, 1 и $p-1$ являются обратными сами к себе, а любой другой элемент имеет обратный, отличный от него самого, и все элементы множества Z/pZ^* могут быть разбиты на пары так, что при их перемножении мы получим -1. Например, если $p = 11$, $10! \equiv (1)(10)(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(6 \cdot 8) \equiv -1(mod 11)$. Если p = 2, результат становится тривиальным.

Обратно, предположив, что сравнение имеет место для составного n, и замечая, что составное n имеет собственный делитель d, $1 < d < n$, получим, что d делит $(n-1)!$, и d делит $(n-1)! + 1$, то есть, d делит 1, что дает противоречие.

Рассмотрим второе доказательство. Пусть p - нечетное простое число. Рассмотрим многочлен $g(x) = (x-1)...(x-(p-1))$. Если $f(x)$ - ненулевой многочлен степени d над полем F, то $f(x)$ имеет не более d корней над полем F. Рассмотрим теперь, задавая $g(x)$ по вышеуказанной формуле, многочлен $f(x) = g(x) - (x^{p-1} - 1)$. Так как старшие коэффициенты взаимно уничтожаются, $f(x)$ является многочленом степени не выше $p-2$. Переходя к модулю p, мы видим, что $f(x)$ может иметь не более $p-2$ корней по модулю p. Но, используя малую теорему Ферма, мы видим, что каждый из элементов 1, 2, ..., $p-1$ является корнем многочлена $f(x)$. Это возможно только в случае, когда $f(x)$ превращается в тождественно равный нулю многочлен по модулю p, то есть, все коэффициенты $f(x)$ делятся на p. Поскольку p нечетно, свободный член многочлена $f(x)$ равен $(p-1)! + 1$, что завершает доказателство.

Теорема Вильсона не может быть использована как тест на простоту, так как вычисление $(n-1)!$ - очень долгий процесс при больших n.

Гаусс получпл обобщение теоремы Вильсона: $\prod_{1 \leq a < m, gcd(a,m)=1} a \equiv -1(modm)$ для $m = 4, p^\alpha, 2p^\alpha$, и $\equiv 1(modm)$ в остальных случаях, где p - нечетное простое число.

Упражнения

1. Найти все простые на интервале $[1, 100]$; $[1, 300]$.

2. Доказать, что $n \in P$ тогда и только тогда, когда $\sum_{m=1}^{n} \lfloor \frac{n}{m} \rfloor - \lfloor \frac{n-1}{m} \rfloor = 2$.

3. Доказать, что $p \equiv -1(mod4)$ является простым тогда и только тогда, когда p может быть представлено, причем единственным образом, в виде суммы квадратов двух целых чисел.

4. Проверить, что числа 561, 645, 1105, 1387 являются числами Пуле.

5. Проверить, что числа 1105, 1729, 2465, 6601 являются числами Кармайкла.

6. Доказать, что $(6k+1)(12k+1)(18k+1)$ является числом Кармайкла, если все три указанных множителя являются простыми числами.

7. Доказать представленный выше результат Гаусса.

8. Доказать следующий факт: если p - простое число, и $p-1 = 2^k d$, где d нечетно, то для любого a, взаимно-простого с p, $a^d \equiv 1(modp)$, или $a^{2^r d} \equiv -1(modp)$ для некоторого $r \in [0, ..., k-1]$.

2.3 Формулы простых чисел

Под формулой простых чисел понимают формулу, генерирующую простые числа, причем, в идеальном варианте, только и все простые числа. На сегодняшний день такая "идеальная"формула неизвестна.

На практике для генерирования простых чисел естественным кажется найти формулу, определенную для всех натуралтных n, которая доступна для практических вычислений и генерирует все или хотя бы бесконечно много простых чисел. Например, должно быть выполнено одно из следующих условий:

1. $f(n) = p_n$ для всех $n \geq 1$;

2. $f(n)$ всегда является простым числом, и, если $m \neq n$, то $f(n) \neq f(m)$;

3. Множество простых чисел совпадает с множеством положительных значений функции $f(n)$.

- **Многочлены, генерирующие простые числа**

  Известно (Гольдбах, 1752), что не существует многочлена $f(x)$ положительной степени с целыми коэффициентами, который дает только простые числа для любого целого x.

  Доказательство этого факта достаточно просто. Предоложим, что такой многочлен существует. Тогда значение $f(1)$ должно совпадать с некоторым простым p, в частности, $f(1) \equiv 0(modp)$. Но, для любого k, $f(1+kp) \equiv 0(modp)$, то есть $f(1+kp)$ не может быть простым (так как делится на p), кроме случая совпадения с p, но $f(1+kp) = f(1)$ для всех k только в том случае, когда наш многочлен является константой, то есть многочленом нулевой степени.

  Используя алгебраическую теорию чисел, можно получить более сильный результат: не существует многочлена $f(n)$ ненулевой степени, который дает простые числа для почти всех целых n.

Лежандр показал, что не существует рациональной функции, дающей только простые числа.

Можно показать, что если f_i, g_i, $i = 1, ..., n$, являются многочленами с положительными коэффициентами, то функция $\sum_{i=1}^{n} f_i(x)^{g_i(x)}$ не может давать только простые значения для $x \in \mathbb{N}$.

Однако существуют многочлены, которые могут давать много простых значений. Так, многочлен Эйлера (Эйлер, 1772) $f(x) = x^2 + x + 41$ дает простые значения для всех неотрицательных x меньших 40. Простые для $x = 0$, 1, 2, 3... равны, соответственно, 41, 43, 47, 53, 61, 71... Разности между их значениями равны 2, 4, 6, 8, 10... Для $n = 40$ многочлен дает число 1681, равное 41^2 - наименьшее составное число, получаемое по этой формуле. Более того, если 41 делит n, то оно делит и $f(n)$.

Квадратичный трехчлен $x^2 - x + 41$ (Лежандр, 1798) дает те же самые простые числа для $x = 1, ..., 40$, и дает составные числа для 41 и 42.

Многочлен $g(x) = x^2 - 79x + 1601$ дает простые для $x = 0, ..., 79$, соответствующие 40 простым, получаемым по предыдущей формуле, взятым каждое по два раза.

Более того, любой многочлен $x^2 + x + q$, $q = 2, 3, 5, 11, 17$, дает простые для всех $x = 0, ..., q - 2$.

В силу теоремы Дирихле о бесконечности простых чисел в арифметических прогрессиях (Дирихле, 1837) мы можем утверждать, что линейный многочлен $f(x) = ax + b$ продуцирует бесконечно много простых чисел при взаимно-простых a и b (хотя ни одна такая функция не дает простые значения для всех значений n). В частности, существует бесконечно много простых чисел видов $4x - 1$, $4x + 1$, $6x - 1$, $6x + 1$.

Неизвестно, существует ли многочлен степени выше первой, котоый продуцирует бесконечно много простых чисел. В частности, неизвестно, существует ли бесконечно много простых чисел вида $ax^2 + bx + c$, и, особенно, простых вида $x^2 + 1$.

Однако Дирихле доказал, что для целых a, b, c, удовлетворяющих условиям $gcd(a, 2b, c) = 1$ и $b^2 = ac$, многочлен от двух переменных $ax^2 + bxy + cy^2$ представляет бесконечно много простых чисел. В частности, существует бесконечно много простых вида $x^2 + y^2$, и простых вида $x^2 + y^2 + 1$.

- **Формулы простых чисел первого рода**

В этом разделе мы рассмотрим формулы, которые дают n-е простое число как функцию натурального аргумента n. Эти формулы не имеют практического значения, так как большинство тестов на простоту значительно эффективнее. Более того, обычно такие формулы содержат константы, точное значение которых может быть определено только при использовании информации обо всем множестве простых чисел в целом.

Серпинский (1952) предложил определить константу A следуюшим образом:

$$A = \sum_{n=1}^{\infty} p_n 10^{-2^n} = 0.02030005000000070\ldots.$$

Тогда, используя функцию $\lfloor x \rfloor$ (ннаибольшее целое, не превосходящее x), мы получим точную формулу для n-го простого числа:

$$p_n = \lfloor 10^{2^n} \cdot A \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \cdot A \rfloor.$$

Действительно, $10^{2^n} A = \sum_{k=1}^{n-1} p_k 10^{2^n - 2^k} + p_n + \sum_{k>n} p_k 10^{2^n - 2^k}$, и $\lfloor 10^{2^n} A \rfloor = \sum_{k=1}^{n-1} p_k 10^{2^n - 2^k} + p_n + \lfloor \sum_{k>n} p_k 10^{2^n - 2^k} \rfloor$. Так как $p_n \le 2^{2^{n-1}}$ для $n > 1$, мы имеем, что $p_{n+1} 10^{2^n - 2^{n+1}} \le (0.2)^{2^n}$, и $p_{n+t} 10^{2^n - 2^{n+t}} \le (0.2)^{2^{n+(t-1)}}$, то есть, $\sum_{k>n} p_k 10^{2^n - 2^k} \le \sum_{t \ge 1} (0.2)^{2^{n+(t-1)}} \le \sum_{t \ge 1} (0.2)^{2^n + (t-1)} = (0.2)^{2^n + 1} < 1$, и $\lfloor \sum_{k>n} p_k 10^{2^n - 2^k} \rfloor = 0$, следовательно, $\lfloor 10^{2^n} A \rfloor = \sum_{k=1}^{n-1} p_k 10^{2^n - 2^k} + p_n$.

Аналогичным образом мы получим, что $\lfloor 10^{2^{n-1}} A \rfloor = \sum_{k=1}^{n-2} p_k 10^{2^{n-1} - 2^k} + p_{n-1}$, и, следовательно, $10^{2^{n-1}} \lfloor 10^{2^{n-1}} \cdot A \rfloor = \sum_{k=1}^{n-2} p_k 10^{2^n - 2^k} + 10^{2^{n-1}} p_{n-1}$.

Так как $10^{2^n - 2^{n-1}} = 10^{2^{n-1}}$, мы получаем теперь искомую формулу.

Харди и Райт (1979) предложили вариант формулы Серпинского. Пусть r - целое число, большее единицы. Определим константу B следующим образом:

$$B = \sum_{n=1}^{\infty} p_n r^{-n^2}.$$

Тогда мы получим n-е простое число из формулы

$$p_n = \lfloor r^{n^2} B \rfloor - r^{2n-1} \lfloor r^{(n-1)^2} B \rfloor.$$

Используя теорему Вильсона, Уинстон (1964) предложил следующую формулу для проверки простоты числа x:

$$f(x) = \lfloor \cos^2 \pi \frac{(x-1)! + 1}{x} \rfloor.$$

Данная функция дает значение 1, если x - простое, и 0, если x - составное; $f(1) = 1$.

Функция $\pi(x)$, то есть, число простых, не превосходящих x, может быть записана в виде $\pi(x) = -1 + \sum_{j=1}^{x} f(j)$.

Тогда n-е простое число p_n можно получить как

$$p_n = 1 + \sum_{m=1}^{2^n} \lfloor (\frac{n}{1 + \pi(m)})^{\frac{1}{n}} \rfloor$$

или, эквивалентно, как

$$p_n = 1 + \sum_{m=1}^{2^n} \lfloor (\frac{1}{n} \sum_{x=1}^{m} \lfloor \cos^2 \pi \frac{(x-1)! + 1}{x} \rfloor)^{-\frac{1}{n}} \rfloor.$$

Мы можем записать так же, что $\pi(m) = \sum_{j=2}^{m} \lfloor \frac{(j-1)!+1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor$, и тогда

$$p_n = 1 + \sum_{m=1}^{2^n} \lfloor (\frac{n}{1 + \pi(m)})^{\frac{1}{n}} \rfloor.$$

Рассмотрим конструкцию последней формулы. Известно, что $p_n \leq 2^n$ для любого $n \in \mathbb{N}$. Так как $\pi(p_n) = n$, мы получаем, что $\pi(m) \geq n$ для любого $m \geq p_n$, и, следовательно, $\frac{n}{1+\pi(m)} \leq \frac{n}{n+1} < 1$, то есть $\lfloor(\frac{n}{1+\pi(m)})^{1/n}\rfloor = 0$. С другой стороны, $\pi(m) < n$ для любого $1 \leq m < p_n$, и, следовательно, $1 \leq \frac{n}{1+\pi(m)} \leq n < p_n \leq 2^n$, то есть, $1 \leq (\frac{n}{1+\pi(m)})^{1/n} < 2$, и $\lfloor(\frac{n}{1+\pi(m)})^{1/n}\rfloor = 1$. Тогда $1 + \sum_{m=1}^{2^n}\lfloor(\frac{n}{1+\pi(m)})^{\frac{1}{n}}\rfloor = 1 + \sum_{m=1}^{p_n-1} 1 = 1 + (p_n - 1) = p_n$.

Другой подход (Ruiz, 2000) не использует факториалы и теорему Вильсона, но по-прежнему опирается на функцию "целая часть x": сначала определим $\pi(k) = k - 1 + \sum_{j=2}^{k}\lfloor\frac{2}{j}(1 + \sum_{s=1}^{\lfloor\sqrt{j}\rfloor}(\lfloor\frac{j-1}{s}\rfloor - \lfloor\frac{j}{s}\rfloor))\rfloor$, а затем получим формулу

$$p_n = 1 + \sum_{k=1}^{2(\lfloor n\log n+1)\rfloor}(1 - \lfloor\frac{\pi(k)}{n}\rfloor).$$

Еще одна формула такого рода (Gandi, 1971) имеет вид

$$p_n = \lfloor 1 - \frac{1}{\log 2}\log(-\frac{1}{2} + \sum_{d|P_{n-1}}\frac{\mu(d)}{2^d - 1})\rfloor,$$

где $\mu(n)$ - функция Мебиуса, и $P_{n-1} = p_1 ... p_{n-1}$.

Рассмотрим доказательство последней формулы. Достаточно показать, что p_n - единственное целое число, такое что $1 < 2^{p_n}(-\frac{1}{2}+\sum_{d|P_{n-1}}\frac{\mu(d)}{2^d-1}) \leq 2$. Действительно, $p_n \leq \alpha < p_{n+1}$, и $2^{p_n} \leq 2^{\alpha} < 2^{p_{n+1}}$, то есть, $2^{p_n} \cdot 2^{\log_2(-\frac{1}{2}+\sum_{d|P_{n-1}}\frac{\mu(d)}{2^d-1})} \leq 2$, и $2^{p_n} \cdot 2^{\log_2(-\frac{1}{2}+\sum_{d|P_{n-1}}\frac{\mu(d)}{2^d-1})} > 1$, то есть, $1 < 2^{p_n}(-\frac{1}{2} + \sum_{d|P_{n-1}}\frac{\mu(d)}{2^d-1}) \leq 2$.

Пусть $S = \sum_{d|P_{n-1}}\frac{\mu(d)}{2^d-1}$.

Тогда (используя свойство $\sum_{d|n}\mu(d) = 1$ для $n = 1$, и $= 0$, иначе) мы имеем:

$$(2^{P_{n-1}} - 1)S = \sum_{d|P_{n-1}}\mu(d)\frac{2^{P_{n-1}} - 1}{2^d - 1} =$$

$$= \sum_{d|P_{n-1}}\mu(d)(1 + 2^d + ... + 2^{P_{n-1}-d}) = \sum_{0\leq t\leq P_{n-1}}(\sum_{d|gcd(t,P_{n-1})}\mu(d))2^t$$

$$= \sum_{0<t<P_{n-1},gcd(t,P_{n-1})=1} 2^t == 2^{P_{n-1}} + \sum_{0<t<P_{n-1}-1,gcd(t,P_{n-1})=1} 2^t.$$

Тогда

$$2(2^{P_{n-1}} - 1)(-\frac{1}{2} + S) = 2^{P_{n-1}} + \sum_{0<t<P_{n-1}-1,gcd(t,P_{n-1})=1} 2^{t+1} - 2^{P_{n-1}} + 1 =$$

$$= 1 + \sum_{0<t<P_{n-1}-1,gcd(t,P_{n-1})=1} 2^{t+1} = 1 + \sum_{0<t\leq P_{n-1}-p_n,gcd(t,P_{n-1})=1} 2^{t+1}.$$

Действительно, если $2 \leq j < p_n$, то существует $q \in P$, такое что $q|j$. Но тогда $q < p_n$, то есть, $q|P_{n-1}$, и, следовательно, $q|P_{n-1} - j$. Таким образом, если $0 < t < P_n - 1$, и $gcd(t, P_{n-1}) = 1$, то $0 < t \leq P_{n-1} - p_n$.

Пусть $\sum_{0<t\leq P_{n-1}-p_n, gcd(t,P_{n-1})=1} 2^{t+1} = \sum$. Тогда

1. $1 + \sum \leq 1 + 2 + 2^2 + \cdots + 2^{P_{n-1}-p_n+1} = 2^{P_{n-1}-p_n+1}$;

2. $1 + \sum \geq 2^{P_{n-1}-p_n+1}$, так как для $t = P_{n-1} - p_n$ мы имеем $gcd(t, P_{n-1}) = 1$ (если $q|t$, $q|P_{n-1}$, то $q|p_n$ - противоречие).

Следовательно, $\frac{2^{P_{n-1}-p_n+1}}{2^{P_{n-1}+1}} < -\frac{1}{2} + S = \frac{1+\sum}{2(2^{P_{n-1}}-1)} < \frac{2^{P_{n-1}+2}-1}{2^{P_{n-1}+1}-2} < \frac{2^{P_{n-1}-p_n+2}}{2^{P_{n-1}+1}}$, и

$1 < 2^{p_n}(-\frac{1}{2} + S) < 2$.

- **Формулы простых чисел второго рода**

  В этом разделе мы рассмотрим формулы, дающие различные простые числа при различных значениях аргумента.

  Первая такая формула была получена в 1947 Миллсом, который доказал, что существует дейсвительное число θ, такое что $\lfloor \theta^{3^n} \rfloor$ является простым числом для любого натурального n. Наименьшее такое θ равно 1.3063... и известно как *константа Миллса*.

  Аналогично (Wright, 1951), $g(n) = \lfloor 2^{2^{\cdot^{\cdot^{\cdot^{\omega}}}}} \rfloor$ (цепочка из n показателей) является простым для любого $n \geq 1$. Здесь ω равно 1.9287800... . Именно, $g(1) = 3$, $g(2) = 13$, $g(3) = 16381$, а $g(4)$ имеет более 5000 десятичных знаков.

  Тот факт, что константы θ и ω известны только приблизительно, и что значения представленных функций растут очень быстро, делает эти формулы бесполезными с практической точки зрения.

  Следующая функция, $f(n) = 2 + (2n! mod(n + 1))$, дает простые числа, и только простые числа, для любого натурального n: число два появляется много раз, а любое другое простое число появляется ровно однажды. Эта формула основана на теореме Вильсона: именно, мы получаем простое число p для $n = p - 1$, и мы получаем число 2 во всех остальных случаях; это значит, 2 появляется, если $n + 1$ является составным.

- **Формулы простых чисел третьего рода**

  В этом разделе мы рассмотрим формулы, которые генерируют множество простых чисел как множество своих положительных значений.

  Как было показано Матиясевичем (1971), существует многочлен от нескольких переменных, который дает множество простых чисел как множество своих положительных значений, если переменные пробегают все неотрицательные целые числа.

  Первым из полученных многочленов такого рода был многочлен от 26 переменных степени 25 (Sato, Wada, Wiens, 1976):

$$(k+2)\{1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1)(h + j) + h - z]^2 - [2n + p + q + z - e]^2 -$$

$$[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-$$
$$[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-u^2]^2-$$
$$[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2-$$
$$[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2-$$
$$[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}.$$

Заметим, что этот многочден разложен на множители. Второй множитель имеет специальную форму - единица минус сумма квадратов - так что единственная возможность получить положительное значение состоит в приравнивании всех квадратов к нулю.

Многочлен такого рода наименьшей известной степени имеет степень 5 (и 42 переменных), многочлен такого рода с наименьшим известным числом переменных имеет 10 переменных (и степень приблизительно $1,6 \cdot 10^{45}$).

В свете представленного выше многочлена, мы можем сказать, что для получения простых чисел может быть использована система Диофантовых уравнений с 26 переменными. Именно, данное число $k+2$ является простым тогда и только тогда, когда следующая система Диофантовых уравнений имеет решения в натуральных числах:

$0 = wz + h + j - q;$

$0 = (gk + 2g + k + 1)(h + j) + h - z;$

$0 = 16(k+1)^3(k+2)(n+1)^2 + 1 - f^2;$

$0 = 2n + p + q + z - e;$

$0 = e^3(e+2)(a+1)^2 + 1 - o^2;$

$0 = (a^2-1)y^2 + 1 - x^2;$

$0 = 16r^2y^4(a^2-1) + 1 - u^2;$

$0 = n + l + v - y;$

$0 = (a^2-1)l^2 + 1 - m^2;$

$0 = ai + k + 1 - l - i;$

$0 = ((a + u^2(u^2-a))^2 - 1)(n+4dy)^2 + 1 - (x+cu)^2;$

$0 = p + l(a-n-1) + b(2an + 2a - n^2 - 2n - 2) - m;$

$0 = q + y(a-p-1) + s(2ap + 2p - p^2 - 2p - 2) - x;$

$0 = z + pl(a-p) + t(2ap - p^2 - 1) - pm.$

Общая теорема Матиясевича утверждает, что множество значений любой рекурсивно перечислимой функции может быть получено как множество решений системы Диофантовых уравнений от 9 переменных, но, в общем случае, очень высокой степени. Отсюда следует существование системы Диофантовых уравнений от 9 переменных, имеющей представленное выше свойство. Джонс показал, что существует система уравнений степени 4, но от 58 переменных, удовлетворяющая тому же свойству.

Упражнения

1. Доказать, что любой многочлен $x^2 + x + q$, $q = 2, 3, 5, 11, 17$, дает простые числа для всех $x = 0, ..., q - 2$.

2. Доказать, что существует бесконечно много простых вида $x^2 - y^2$.

3. Доказать, что существует бесконечно много простых вида $x^2 + y^2$.

4. Доказать, что функция $f(x) = \lfloor \cos^2 \pi \frac{(x-1)!+1}{x} \rfloor$ принимает значение 1, если x - простое, и 0, если x - составное; кроме того, $f(1) = 1$.

5. Проверить формулы для p_n, представленные выше.

6. Проверить, что $f(n) = 2 + (2n! mod(n + 1))$ дает простое число p для $n = p - 1$, и 2, иначе.

3 Числа Мерсенна и Ферма

3.1 Предварительные сведения

Потерпев неудачу с использованием простейших функций, многочленов, для построения формулы простых чисел, попробуем получать простые числа, используя показательную функцию $f(n) = k^n$, точнее, так как k^n не может давать бесконечно много простых, более общую функцию $f(n) = k^n \pm b^n$. Так как, для любого натурального n, $k^n - b^n = (k - b)(k^{n-1} + k^{n-2}b + ... + k^2b^{n-2} + b^{n-1})$, то $k^n - b^n$ может быть простым только в случае $k - b = 1$, или $k = b + 1$. В простейшем случае мы имеем $b = 1$, то есть, $f(n) = k^n - 1$. Тот же выбор b дает нам в случае $k^n + b^n$ функцию $f(n) = k^n + 1$.

Для простоты числа $k^m + 1$ необходимо, чтобы k было четным, а m представляло собой степень 2. Простейший случай, $k = 2$, дает нам *числа Ферма*

$$F_n = 2^{2^n} + 1.$$

В общем случае мы получаем *обобщенные числа Ферма*

$$F_{b,n} = b^{2^n} + 1, 2|b.$$

Если $k^m - 1$ является простым, то $k = 2$, и m - простое число, так что проблема сводится к *числам Мерсенна*

$$M_p = 2^p - 1.$$

Упражнения

1. Доказать, что функция $(-1)^n + 4$ дает простые числа для любого натурального n.

2. Доказать, что, если $a^n + 1$ - простое, то $n = 2^k$.

3. Доказать, что, если $a^n - 1$ - простое, то $a = 2$, и $n \in P$.

4. Доказать, что любое число вида $4n^4 + 1$, $n > 1$, является составным.

Простые	n = 0, 1, 2, 3, 4
Полностью факторизованные	n = 5, 6, 7, 8 (два простых мн. в каждом), 9 (3 мн.), 10 (4 мн.), 11 (5 мн.)
известно пять простых мн.	n = 12
известно четыре простых мн.	n = 13
известно три простых мн.	n = 15, 25
известно два простых мн.	n = 16, 18, 19, 27, 30, 36, 38, 52, 77, 147, 150, 284, 416
известен один простой мн.	n = 17, 21, 23, 26, 28, 29, 31, 32, 37, 39, 42, 43 и 187 значений n с 43 < n < 2478782
составное, но не известно ни одного простого множителя	n = 14, 20, 22, 24
характер неизвестен	n = 33, 34, 35, 40, 41, 44, 45, 46, 47, 49, 50, . . .

3.2 Числа Ферма

Числа Ферма $F_n = 2^{2^n} + 1$, $n \geq 0$, были введены французским математиком 17-го века Пьером Ферма, который предположил (1640), что они являются простыми числами для всех $n = 0, 1, \ldots$. Первые пять чисел Ферма действительно являются простыми: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Но в 1732 Эйлер доказал, что F_5 является составным:

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Для того, чтобы это доказать, рассмотрим $2^{32} + 1 = 2^4 \cdot 2^{28} + 1$, и запишем $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$. Следовательно, $5^4 \equiv -2^4 (mod 641)$, и $5 \cdot 2^7 \equiv -1 (mod 641)$. Тогда мы получим, что $5^4 \cdot 2^{28} \equiv 1 (mod 641)$, или $-2^4 \cdot 2^{28} \equiv 1 (mod 641)$, или $2^{32} + 1 \equiv 0 (mod 641)$.

Другое доказательство еще более элементарно. Обозначим $a = 2^7$, и $b = 5$. Тогда, замечая что $a - b^3 = 3$, мы получим, что $2^{2^5} + 1 = 2^4 (2^7)^4 + 1 = 2^4 a^4 + 1 = (1 + 3b) a^4 + 1 = (1 + (a - b^3) b) a^4 + 1 = (1 + ab - b^4) a^4 + 1 = (1 + ab) a^4 + (1 - a^4 b^4) = (1 + ab) a^4 + (1 - a^2 b^2)(1 + a^2 b^2) = (1 + ab) a^4 + (1 + ab)(1 - ab)(1 + a^2 b^2) = (1 + ab)(a^4 + (1 + ab)(1 + a^2 b^2))$.

Следовательно, $1 + ab = 1 + 5 \times 2^7 = 641$ делит $2^{2^5} + 1$.

Сведения о разложимости на простые множители чисел F_n

Таким образом, гипотеза Ферма о простоте чисел F_n была опровергнута. Более того, не найдено ни одного простого числа Ферма, большего F_4. Доказано, что F_n является составным для всех n от 5 до 32, и для многих других значений n, хотя не для всех составных чисел Ферма найдены простые делители. На сегодняшний день известно 227 составных чисел Ферма. Наибольшее известное составное число Ферма (Cosgrave, Jobling, Woltman, Gallotis, 2003) - $F_{2478782}$, оно имеет простой делитель $p = 3 \cdot 2^{2478765} + 1$.

Можно заключить, что F_4 - наибольшее известное простое число Ферма; F_{11} - наибольшее из полностью факторизованных составных чисел Ферма; $F_{2478782}$ - наибольшее известное составное число Ферма, и F_{33} - наименьшее число Ферма, характер которого неизвестен.

Простейшие свойства чисел Ферма

1. $F_n \neq p+q$ для любых простых p и q, и любого $n \neq 1$.

2. $F_n = F_0 \ldots F_{n-1} + 2$.

3. $(F_n, F_m) = 1$, если $n \neq m$.

4. $F_n \neq k^s$, в частности, $F_n \neq k^2$, то есть, не является квадратным числом.

5. $F_n \neq \frac{k(k+1)}{2}$, то есть, не является треугольным числом.

6. Если $F_n \in P$, то $F_n \neq k^p - l^p$ $(k, l, p \in \mathbb{N})$.

7. $F_n \equiv 2(mod 3)$, то есть, 3 не делит F_n.

8. $F_n \equiv 3; 5(mod 7)$, то есть, 7 не делит F_n.

9. $F_n \equiv 2(mod 5)$, то есть, 5 не делит F_n.

10. $F_n | 2^{F_n} - 2$, то есть, составные числа Ферма являются псевдопростыми числами с основанием 2. (Можно доказать, что, если для некоторого натурального k число $m = 2^k + 1$ удовлетворяет условию $m | 2^m - 2$, то m - число Ферма.)

11. Среди чисел вида $2^{2^n} + 3$ существует бесконечно много составных.

12. Каждое число вида $2^{2^n} + 5$ - составное.

Рассмотрим доказательства некоторых из этих свойств.

1. Если $F_n = p + q$, то $q = 2$, то есть, $p = 2^{2^n} - 1 = (2^2 - 1)K$, $K \in \mathbb{Z}$.

2. Имеем, что $F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = ... = F_{n-1} ... F_0$.

3. Если $p | F_n$, $p | F_m$, $n > m$, то $p | 2$, противоречие.

4. Любое целое k имеет остаток $0, 1$ или 2 при делении на 3, то есть, $k^2 \equiv 0(mod 3)$, или $k^2 \equiv 1(mod 3)$ для любого целого k. Но, для любого $n \geq 1$, $F_n \equiv 2^{2m} + 1 \equiv (-1)^{2m} + 1 \equiv 2(mod 3)$, следовательно, $F_n \neq k^2$. Для $n = 0$, $F_0 = 3$ также не является квадратом целого числа. Если мы рассмотрим делимость на 7, мы сможем аналогичным образом доказать, что $F_n \neq k^3$.

7. Имеем: $2^{2^n} + 1 \equiv (-1)^{2l} + 2 \equiv 2(mod 3)$.

10. Имеем: $2^{n+1} | 2^{2^n} \Rightarrow 2^{2^{n+1}} - 1 | 2^{2^{2^n}} - 1$, но $F_n = 2^{2^n} + 1 | 2^{2^{n+1}} - 1$, следовательно, $F_n | 2^{F_n} - 2 = 2(2^{2^{2^n}} - 1)$.

11. Рассмотрим $n = 2^{k+1}$. Для $k \in \mathbb{N}$, $2^{2^k} = 3l + 1$, следовательно, $2^{2^{2^{k+1}}} + 3 \equiv 2^{6l} + 2 + 3 \equiv 4(2^3)^{2l} + 3 \equiv 4 + 3 \equiv 0(mod 7)$.

12. Любое такое число делится на 3.

Более интересны для нас свойства простых делителей чисел Ферма, которые имеют специальную форму.

Theorem 3 *Любой простой делитель p числа $F_n, n \geq 1$, имеет вид $p = 2^{n+1}k + 1$. Кроме того, если $n > 1$, любой простой делитель числа F_nимеет вид $p = 2^{n+2}k + 1$.*

Доказательство.

$p|F_n$, следовательно, $2^{2^n} \equiv -1(modp)$, то есть $(2^{2^n})^2 \equiv 1(modp)$, и $2^{2^{n+1}} \equiv 1(modp)$. Следовательно, $P_p(2) = 2^{n+1}$, то есть, $2^{n+1}|(p-1)$, и мы получаем, что $p = 2^{n+1}k + 1$.

Для $n \geq 2$ мы имеем, что $p = 2^{n+1}k + 1 \equiv 1(mod8)$, следовательно, $(\frac{2}{p}) = 1$, то есть, $2^{\frac{p-1}{2}} \equiv 1(modp)$, и $2^{n+1} = P_p(2)|\frac{p-1}{2}$.

Это свойство чисел F_n используется для проверки простоты данного числа Ферма. Например, любой простой делитель числа F_5 должен иметь вид $2^7k + 1$. Мы получаем простые числа только для $k = 2$ и $k = 5$: 257 и 641, соответственно. Простое 641 делит F_5, и F_5 представляет собой произведение двух различных простых чисел.

Landry (1880) доказал, что $2741|F_6$, $2741 = 256k + 1$, $k = 1071$. Именно, $F_6 = 274177 \cdot 67280421310721$ есть произведение двух простых.

Morrison и Brillhart (1975) показали, что $a|F_7$, $a = 512k + 1$, $k = 116503103764643$, и F_7 есть произведение двух простых.

В связи со сказанным возникает естественный вопрос: какие из чисел вида $k \cdot 2^m + 1$, $k = 1, 2, ...$, являются простыми?

Для $k = 4$ мы имеем только три простых вида $4 \cdot 2^m + 1$. Для $k = 5$ известны 17 простых вида $5 \cdot 2^m + 1$. Для любого $k < 3061$ мы знаем по меньшей мере одно m, такое что $k \cdot 2^m + 1$ - простое. Для $k = 3061$, $k \cdot 2^m + 1 \in P$ для любого $m < 17008$.

Серпинский показал, что существует бесконечно много $k \in \mathbb{N}$, таких что $k \cdot 2^m + 1$ является составным для любого $m \in \mathbb{N}$.

Если для $k \cdot 2^m + 1$ мы положим $k = m = n$, мы получим число Куллена $C_n = n \cdot 2^n + 1$. Известно, что $C_n \in P$, если $n = 1, 141, 4713, ...$. Доказано, что почти все числа Куллена являются составными.

Другим методом проверки простоты чисел Ферма является *критерий Пепина.*

Theorem 4 *Число Ферма F_n, $n \geq 1$, является простым тогда и только тогда, когда $F_n|3^{\frac{F_n-1}{2}} + 1$.*

Доказательство.

Прежде всего заметим, что для $n \geq 1$ мы имеем $F_n = 12k + 5$, так как $4^k \equiv 4(mod12)$.

Докажем первую часть теоремы. Пусть $F_n \in P$. Тогда $(\frac{3}{F_n}) = (\frac{F_n}{3}) = (\frac{-1}{3}) = -1$. Следовательно, $3^{\frac{F_n-1}{2}} \equiv -1(modF_n)$.

Докажем вторую часть теоремы. Если $3^{\frac{F_n-1}{2}} \equiv -1(modF_n)$, то $3^{F_n-1} \equiv 1(modF_n)$. Пусть $p|F_n$, тогда $3^{\frac{F_n-1}{2}} \equiv -1(modp)$, и $3^{F_n-1} \equiv 1(modp)$. Если $P_p(3) = \gamma$, то $\gamma|F_n - 1 = 2^{2^n}$, и γ не делит 2^{2^n-1}, следовательно, $\gamma = 2^{2^n}$, и $\gamma = 2^{2^n}|p-1$. Таким образом, $F_n - 1|p-1$, и $p|F_n$, то есть, $p = F_n$ (иначе мы имеем: $p = 2^{2^n}X + 1$, $X > 1$, $p|2^{2^n} + 1$, то есть, $p|2^{2^n}(X-1)$, или $p|X - 1$, и $X - 1 \leq 2^{2^n}X + 1$, противоречие).

Заметим, что вместо числа 3 можно взять любое число k, для которого символ Якоби $(\frac{k}{F_n}) = -1$, в частности, k может быть равно 5 или 10.

Если мы обозначим через $\overline{t}$ остаток от деления t на F_n, и положим $r_1 = 3$, $r_{k+1} = \overline{r_k^2}$, мы получим, что $F_n | 3^{2^{k-1}} - r_k$ для любого $k = 1, 2, \ldots$. Именно, $F_n | 3^{2^0} - r_1 = 0$, и $F_n | 3^{2^k} - r_{k+1} = (3^{2^{k-1}})^2 - \overline{r_k^2} = (3^{2^{k-1}} - r_k)(3^{2^{k-1}} + r_k)$, так как F_n делит первый множитель. Следовательно, для $k = 2^n$ мы получаем $F_n | 3^{\frac{F_n - 1}{2}} - r_{2^n}$. Таким образом, $3^{\frac{F_n-1}{2}} \equiv r_{2^n} (mod F_n)$, и мы можем использовать для теста Пепина числа r_{2^n}.

Именно этим методом было доказано, что числа F_7, F_8, F_{13} и F_{14} являются составными.

Заметим, что этот метод не дает информации о простых множителях тестируемого числа; именно поэтому мы не имеем информации ни об одном простом делителе составного числа F_{14}.

В 1878 было получено обобщение критерия Пепина - теорема Плота: число $n = h \cdot 2^k + 1, 2^k > h$ является простым, если существует целое a, такое что $a^{\frac{n-1}{2}} \equiv -1 (mod n)$. Мы получаем одно из утверждений теоремы Пепина при $h = 1$ и $a = 3$.

Числа Ферма имеют непосредственное отношение к известной проблеме построения правильного многоугольника с помощью циркуля и линейки. В 1796 году 19-летний Гаусс решил проблему, занимавшую умы математиков более 2000 лет. Он доказал, что правильный n-угольник может быть построен циркулем и линейкой (или, что то же, окружность может быть разделена циркулем и линейкой на n равных частей) для $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, \ldots$, но не для $n = 7, 9, 11, 13, 14, 18, \ldots$. Именно, правильный n-угольник может быть построен циркулем и линейкой тогда и только тогда, когда

$$n = 2^r p_1 \cdot \cdots \cdot p_k,$$

где p_i - различные простые числа Ферма.

Нерешенные проблемы

1. Существует ли бесконечно много составных чисел Ферма?

2. Существует ли бесконечно много простых чисел Ферма?

3. Существует ли по крайней мере одно простое число Ферма $> F_4$?

Эвристические рассуждения позволяют предполагать, что имеется только конечное число простых чисел Ферма: пользуясь утверждением асимптотического закона распределения простых чисел, мы получаем, что вероятность случайного числа быть простым не превосходит $\frac{A}{\log n}$ для некоторого действительного числа A; таким образом, проводя суммирование выражения $\frac{A}{\log F_n} < \frac{A}{2^n \log 2}$ по всем неотрицательным числам, мы получам, что мы можем рассчитывать не более чем на $\frac{A}{\log 2}$ простых чисел Ферма, что дает конечное число. Но в этих рассуждениях мы предполагаем, что числа Ферма ведут себя как случайные числа, что на самом деле не так: по крайней мере, они имеют простые делители специальной формы.

Отметим, что простота чисел вида $2 + 1$, $2^2 + 1$, $2^{2^2} + 1$, $2^{2^{\cdot^{\cdot^{2}}}} + 1$ была опровергнута, когда было доказано, что F_{16} (имеющее 19729 десятичных знаков) является составным.

Упражнения.

1. Доказать, что $(F_n, F_m) = 1$.

2. Доказать, что $F_n \neq p + q$.

3. Доказать, что $F_n | F_{n+k} - 2$.

4. Доказать бесконечность множества простых чисел, используя числа Ферма.

   Доказательство. Пусть q_n - наименьший простой делитель числа F_n. Так как $gcd(F_m, F_n) = 1$ для $n \neq m$, то $q_n \neq q_m$, и мы получаем бесконечно много простых чисел $q_0, ..., q_k, ...$.

5. Доказать бесконечность простых чисел в арифметической прогрессии $4k + 1$. (Заметим, что любой простой делитель числа F_n, $n \geq 1$, имеет вид $4k + 1$, и используем предыдущие рассуждения.)

6. Для данного $t \in \mathbb{N}$ доказать бесконечность простых чисел в арифметической прогрессии $2^t k + 1$. (Для $t > 2$ рассмотрим числа $F_t, F_{t+1}, ..., F_{t+l}, \ldots$, и заметим, что каждое число F_{n+l} имеет простой делитель вида $2^{t+l+2} + 1 = 2^t s + 1$.)

7. Для данного $p \in P, t \in \mathbb{N}$, доказать бесконечность простых чисел в арифметической прогрессии $2p^t k + 1$.

8. Доказать, что $p_n \leq 2^{2^{n-5}} + 1$. (Заметим, что $q_0 = 3 = p_2$, $q_1 = 5 = p_3$, $q_3 = 17 = p_7$, где q_n - наименьшее простое, делящее F_n, и получим, что $p_n \leq q_{n-5}$ для $n \geq 7$.)

9. Доказать, что $\pi(x) \geq \log_2 \log_2 x + 4$ для любого $x \geq 17$.

   Доказательство. Пусть $x \in [p_n, p_{n+1})$. Тогда $\pi(x) = \pi(p_n) = n$. Кроме того, $x \leq p_{n+1} \leq 2^{2^{n-4}} + 1$, то есть, $x \leq 2^{2^{n-4}}$, или $\log_2 \log_2 x \leq n - 4$. Теперь мы получаем, что $\pi(x) = n \geq \log_2 \log_2 x + 4$.

10. Найти все правильные n-угольники ($n \leq 1000$), которые могут быть получены с помощью циркуля и линейки.

11. Доказать, что $F_n \neq p^2 + q^2$.

12. Доказать, что $F_n \neq p^2 + q^2 + 1$.

13. Доказать, что $F_n = p^2 + q^2 + z^2$ тогда и только тогда, когда $n = 2$.

14. Доказать, что $F_n + 8, F_n^2 + 8, F_n^3 + 8 \in S$.

3.3 Числа Мерсенна

Числами Мерсенна называются натуральные числа вида $M_n = 2^n - 1$ (некоторые авторы требуют, чтобы n было простым). Последовательность чисел Мерсенна начинается с чисел 1, 3, 15, 31, 63, 127, 255, 511, 1023, 2047....

Хотя числа вида $2^n - 1$ изучались и до 17-го столетия (в 1536 Regius показал, что $2^{11} - 1 = 2047$ не является простым, оно равно $23 \cdot 89$; в 1588 Катальди доказал, что $2^{17} - 1$ и $2^{19} - 1$ являются простыми), они были названы именем французского монаха и математика Марина Мерсенна, рассмотревшего их в своей книге "Cogita physico mathematics", и высказавшего несколько гипотез о их поведении. Одна из его наиболее известных гипотез (так называемая *гипотеза Мерсенна*) утверждает, что $2^n - 1$ является простым для $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, и является составным для всех остальных чисел $2 \leq n \leq 257$.

Очевидно, что Мерсенн не мог полностью проверить высказанную им гипотезу. Понадобилось три столетия и несколько серьезных математических открытий (таких, как тест Лукаса-Лемера) для полной проверки всех показателей списка. Оказалось, что Мерсенн сделал 5 ошибок (три простых пропущены, и два составных объявлены как простые), и правильный список индексов простых чисел Мерсенна в указанных пределах имеет вид: $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ и 127.

Как Мерсенн получил этот список? Возможно, Мерсенн считал, что необходимым и достаточным условием простоты числа $2^p - 1$ является требование, чтобы число p было простым одного из указанных видов: $2^{2n} + 1$, $2^{2n} \pm 3$, $2^{2n+1} - 1$.

Надо отметить пропущенное условие на величину показателя: $2^3 - 1$ простое, но 3 не имеет не одного из указанных видов.

Если проверить все числа до 257, мы получим список Мерсенна без тройки, но с дополнительным числом 61.

К несчастью, гипотеза Мерсенна не дает ни необходимого, ни достаточного условия простоты. Числа Мерсенна M_p являются составными для следующих p: $257 = 2^8 + 1$, $1021 = 2^{10} - 3$, $67 = 2^6 + 3$, и $8191 = 2^{13} - 1$ (то есть ни одно из "достаточных"условий не выполняется). Кроме того, M_p является простым для $p = 89$, но 89 нельзя записать ни в одной из указанных форм.

Новая гипотеза Мерсенна (Bateman, Selfridge, Wagstaff) состоит в следующем. Пусть p - нечетное натуральное число. Если два из указанных ниже условий выполнены, то выполнено и третье:

1. $p = 2^k \pm 1$ или $p = 4^k \pm 3$;

2. $2^p - 1$ является простым (простым Мерсенна);

3. $\frac{(2p+1)}{3}$ является простым (простым Вагстаффа).

Эта гипотеза проверена для всех p, меньших 100000, и для всех известных простых чисел Мерсенна.

Числа Мерсенна дают нам почти все известные рекорды простых чисел. Так, в 1999 (Hajratwala, Woltman, Kurowski и др.), было найдено первое простое число, имеющее более 1000000 десятичных знаков (на самом деле, более 2000000). Оно является 38-м простым числом Мерсенна, $M_{6972593}$, и имеет 2098960 десятичных знаков. В 2006 (Cooper, Boone, Woltman, Kurowski и др.), было получено новое (именно, 44-е известное) простое число Мерсенна, $M_{32582657}$. Оно имеет 9808358 десятичных знаков.

Элементарные свойства чисел Мерсенна

1. Если M_n является простым, то и n является простым.

2. $M_n | M_{mn}$.

3. $M_{m-n} | M_m - M_n$ для $m > n$.

4. Если $m = nq + r$, $d|M_m$, $d|M_n$, то $d|M_r$.

5. $gcd(M_m, M_n) = M_{gcd(m,n)}$, в частности, $M_n|M_m$ тогда и только тогда, когда $n|m$.

6. $gcd(M_n, M_m) = 1$, если $gcd(m, n) = 1$.

7. $M_n \neq k^2$, кроме того, $M_n \neq k^s$ для целого k и натурального $s > 1$.

8. $M_n = \frac{k(k+1)}{2}$ только для $n = 1, 2, 4, 12$.

Рассмотрим доказательства нескольких из перечисленных свойств.

1. $M_1 = 2^1 - 1$ не является простым. С другой стороны, $M_{ab} = 2^{ab} - 1 = (2^a - 1)X$, $X \in \mathbb{Z}$, и для составного числа $n = ab$ (с нетривиальным делителем a), число M_n является составным.

2. $2^{mn} - 1 = (2^n - 1)K$, $K \in \mathbb{Z}$.

3. $M_m - M_n = 2^m - 2^n = 2^n(2^{m-n} - 1)$.

4. Если $d|M_n$, то $d|M_{nq}$. Так как $d|M_m$, то $d|M_{m-nq} = M_r$.

5. По алгоритму Евклида, для $m > n$ мы имеем $m = nq_1 + r_1$, $n = r_1q_2 + r_2$, ..., $r_{s-2} = r_{s-1}q_s + r_s$, и $r_{s-1} = r_sq_s$. Тогда $gcd(m, n) = r_s$.

Так как $r_s|m$, $r_s|n$, то $M_{r_s}|M_n$, и $M_{r_s}|M_m$, то есть, M_{r_s} является общим делителем M_n и M_m. С другой стороны, пусть $d|M_n$ и $d|M_m$. Тогда $d|M_{r_1}$, и $d|M_{r_2}$, ..., $d|M_{r_s}$. Следовательно, M_{r_s} является наибольшим общим делителем.

7. Если $2^n - 1 = k^s$, то k должно быть нечетным. Если s четно, то $k^s \equiv 1(mod 8)$, и $2^n = k^s + 1 = 2(4t + 1)$, противоречие. Если s нечетно, то $2^n = k^s + 1 = (k + 1)T$, где T нечетно, и, следовательно, равно 1. Тогда $2^n = k + 1$, то есть, $s = 1$, противоречие.

8. Легко проверить, что $M_1 = S_3(1)$, $M_2 = S_3(2)$, $M_4 = S_3(4)$, $M_{12} = S_3(90)$, где $S_3(k)$ - k-е треугольное число.

Рассмотрим теперь несколько важных свойств делимости чисел Мерсенна.

Свойства делимости чисел Мерсенна

1. Если $q \in P$, $q \equiv \pm 1(mod 8)$, то $q|M_{\frac{q-1}{2}}$.

2. Если $q|M_p$, то $q = 2pk + 1$.

3. Если $q|M_p$, то $q \equiv \pm 1(mod 8)$.

4. Если $q|M_p$, и $p = 4t \mp 1$, то $q \in \{8pk + 1, 8pk + 1 \pm 2p\}$.

Рассмотрим доказательства этих свойств.

1. $q \equiv \pm 1(mod 8)$, то есть, $(\frac{2}{q}) = 1$, и $2^{\frac{q-1}{2}} \equiv 1(mod q)$, или $q|M_{\frac{q-1}{2}}$. Например, для $n = 11$, $q = 2n + 1 = 23$, и $23|M_{11}$.

Таким образом, если существует бесконечно много простых чисел p, для которых $q = 2p + 1$ также является простым, то существует бесконечно много простых чисел p, таких, что $M_p \in S$. (Простое число p называется *простым числом Софи Жермен*, если $2p+1$ также является простым. Например, 23 является простым числом Софи Жермен, так как оно простое, и $2 \cdot 23 + 1 = 47$ - также простое.)

2. $q|M_p$, следовательно, $2^p \equiv 1(mod q)$, то есть, $P_q(2)|p$, то есть, $P_q(2) = p$. Следовательно, $p|q-1$, и q нечетно, то есть, $q \equiv 1(mod p)$, $q \equiv 1(mod 2)$, откуда следует, что $q \equiv 1(mod 2p)$, то есть, $q = 2pt + 1$.

3. $q|M_p$, следовательно, $q|2^{2k+1} - 1 = 2(2^k)^2 - 1$, то есть, $q|2(2^k x)^2 - x^2$ для любого целого x. Так как $gcd(2^k, q) = 1$, то $2^k x_0 - qy_0 = 1$, и $2^k x_0 = 1 + qy_0$. Следовательно, $q|2(1+qy_0)^2 - x_0^2$, то есть, $q|2 - x_0^2$.

Рассмотрим разложение числа $\frac{x_0}{q}$ в цепную дробь $[a_0, ... a_s]= a_0 + \frac{1}{a_1 + \frac{1}{... + \frac{1}{a_s}}}$. Тогда $1 = Q_0 \leq Q_1 < Q_2 < ... < Q_s = q$. Так как $q > 1$, то найдется натуральное n, такое что $Q_n^2 < q < Q_{n+1}^2$. Тогда $|\frac{x_0}{q} - \frac{P_n}{Q_n}| \leq \frac{q^2}{Q_{n+1}^2} < q$. Следовательно, $0 \leq (x_0 Q_n - qP_n)^2 \leq \frac{q^2}{Q_{n+1}^2} < q$, и $-2q < -2Q_n^2 \leq (x_0 Q_n - qP_n)^2 - 2Q_n^2 = (x_0^2 - 2)Q_n^2 + qM < q - 2Q_n^2 < q$. Так как $(x_0^2 - 2)Q_n^2 + qM$ делится на q, $(x_0 Q_n - qP_n)^2 - 2Q_n^2$ может принимать только значения 0 или $-q$. В первом случае мы получим противоречие, именно, представление $2 = t^2$, где $t = \frac{x_0 Q_n - qP_n}{Q_n}$ - рациональное число. Во втором случае $q = 2x^2 - y^2$ (где $x = Q_n$, и $y = x_0 Q_n = qP_n$), то есть y нечетно ($y = 2k + 1$), и, следовательно, $y^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 \equiv 1(mod 8)$. Если x нечетно, то $2x^2 \equiv 2(mod 8)$, и $q \equiv 1(mod 8)$. Если x четно, то $2x^2 \equiv 0(mod 8)$, и $q \equiv -1(mod 8)$.

4. a). $q = 2pt + 1$, и $q \equiv 1(mod 8)$, то есть, $2pt \equiv 0(mod 8)$, $pt \equiv 0(mod 4)$, $t \equiv 0(mod 4)$, и $q = 8pk + 1$.

b). $q = 2pt + 1$, и $q \equiv -1(mod 8)$, то есть $2pt \equiv -2(mod 8)$, $pt \equiv -1(mod 4)$. Если $p \equiv 1(mod 4)$, то $t \equiv -1(mod 4)$, и $q = 8pk + 1 - 2p$. Иначе, $t \equiv 1(mod 4)$, и $q = 8pk + 1 + 2p$.

Эйлер (1771) доказал, что M_{31} является простым, проверяя числа вида $248n + 1$ и $248n + 63$ до 46339 как возможные делители M_{31} (имеется только 84 таких простых), но даже урезанное множество возможных делителей становится слишком большим с ростом M_n.

Другим методом проверки простоты чисел Мерсенна является *тест Люкаса-Лемера.*

Theorem 5 *Число M_p, где p - нечетное простое, является простым числом тогда и только тогда, когда оно является делителем $(p-1)$-го элемента последовательности $S_1, S_2, ...$, где $S_1 = 4$, и $S_{k+1} = S_k^2 - 2$.*

Основы этого теста были заложены Люкасом в 1870. Исследуя числа Фибоначчи u_n, он открыл следующий факт: если $n \equiv \pm 3(mod 10)$ и n - собственный делитель числа u_{n+1}, то n - простое; если $n \equiv \pm 1(mod 10)$ и n - собственный делитель числа u_{n-1}, то n - простое.

Люкас доказал простоту числа M_{127} в 1876. Он писал: "Я доказал, что число $A = 2^{127} - 1$ - простое. Именно, число A имеет вид $10k - 3$, и я проверил, что u_k не делится на A для $k = 2^n$, кроме случая $n = 127$".

В 1930 Лемер упростил тест Люкаса. Тест Люкаса-Лемера идеально подходит для бинарных компьюьеров, так как вычисление S_k обходится без деления, и может быть выполнено только при использовании умножения и сложения, которые бинарные компьютеры выполняют быстро. Для экономии времени S_n вычисляют по модулю 2^p-1. Рассматривать S_k по модулю M_n также удобно в двоичной системе, так как здесь M_n представляет собой конечную последовательность единиц.

После Люкаса, следующее простое число Мерсенна было найдено в 1952 с помощью компьютера.

Доказательство.
Пусть $a = 1 + \sqrt{3}$ и $b = 1 - \sqrt{3}$, то есть, $a + b = 2$, и $ab = -2$.
Пусть $u_r = \frac{a^r - b^r}{a-b}$, и $v_r = a^r + b^r$.

Лемма 1. Имеют место следующие тождества:

1. $2u_{r+s} = u_r v_s + v_r u_s$;
2. $u_s v_r - u_r v_s = (-2)^{s+1} u_{r-s}$;
3. $v_r v_s + 12 u_r u_s = 2 v_{r+s}$;
4. $u_r v_r = u_{2r}$;
5. $v_r^2 + (-2)^{r+1} = n_{2r}$;
6. $v_r^2 - 12u_r^2 = (-2)^{r+2}$.

Например,
$u_r v_s + v_r u_s = \frac{a^r-b^r}{a-b}(a^s + b^s) + \frac{a^s-b^s}{a-b}(a^r + b^r) = \frac{2a^{r+s}-2b^{r+s}+a^r b^s - b^r a^s + a^s b^r - a^r b^s}{a-b} =$
$2\frac{a^{r+s}-b^{r+s}}{a-b} = 2u_{r+s}$.

Лемма 2. Для данного простого $p > 3$, $u_p \equiv (\frac{3}{p})(mod p)$, и $v_p \equiv 2(mod p)$.

Легко видеть, что $u_p = \frac{(1+\sqrt{3})^p - (1-\sqrt{3})^p}{2\sqrt{3}} = \frac{1}{2\sqrt{2}}(2\binom{p}{1}\sqrt{3} + 2\binom{p}{2}(\sqrt{3})^3 + ...$
$+2\binom{p}{p}(\sqrt{3})^p) = \binom{p}{1} + 3\binom{p}{3} + ... + \binom{p}{p}3^{\frac{p-1}{2}} \equiv 3^{\frac{p-1}{2}} = (\frac{3}{p})(mod p)$, так как биномиальные коэффициенты $\binom{p}{k} \equiv 0(mod p)$ для $k \in [1, p-1]$.

Аналогично, $v_p = (1+\sqrt{3})^p + (1-\sqrt{3})^p = 2 + 2\binom{p}{2}(\sqrt{3})^2 + ... + 2\binom{p}{p-1}\sqrt{3}^{\frac{p-1}{2}} \equiv 2(mod p)$.

Пусть p - простое > 3. Пусть $p|u_w$, но p не делит u_r для $r < w$. Тогда $w = w(p)$ называется *рангом* числа p.

Лемма 3. $p|u_r$ тогда и только тогда, когда $w|r$, где p - простое > 3, и w - ранг p.

Пусть $X_p = \{r : u_r \equiv 0(mod p)\}$. Используя тождества 1 и 2 леммы 1, мы получим следующий факт: если $u_r \equiv 0(mod p)$, и $u_s \equiv 0(mod p)$, то $u_{r\pm s} \equiv 0(mod p)$. Если w - наименьший элемент множества X_p, и $r \in X_p$, то последовательные вычитания дают $r - kw = 0$, то есть, $w|r$.

Лемма 4. $w \leq p + 1$, где p - простое > 3, и w - ранг p.

Достаточно показать, что $p|u_{p-1}u_{p+1}$. Возьмем в тождествах 1 и 2 леммы 1 значения $r = p$ и $s = 1$. Тогда, так как $u_1 = 1$, и $v_1 = 2$, мы получим, что $2u_{p+1} = v_p + 2u_p$, и $4u_{p-1} = v_p - 2u_p$. Следовательно, по лемме 2, $8u_{p+1}u_{p-1} = v_p^2 - 4u_p^2 = 4 - 4(\pm 1)^2 \equiv 0(mod p)$.

Лемма 5. $v_{2^k} = 2^{2^{k-1}} S_k$, то есть, $M_p | S_k$ тогда и только тогда, когда $M_p | v_{2^k}$.

Для $k = 1$, $v_2 = 8 = 2S_1$. Переходя от k к $k+1$, мы получим, используя тождество 5 леммы 1 с $r = 2^k$, что $v_{2^{k+1}} = v_{2^k}^2 - 2^{2^k+1} = (2^{2^{k-1}} S_k)^2 - 2^{2^k+1} = 2^{2^k}(S_k^2 - 2) = 2^{2^k} S_{k+1}$.

Доказательство первой части теоремы: если $M_p \in P$, то $M_p | S_{p-1}$.

Пусть $M_p \in P$. Достаточно показать, что $M_p | v_{2^{p-1}} = v_{\frac{M_p+1}{2}}$. Используя тождество 5 леммы 1 с $r = \frac{M_p+1}{2}$, мы получим, что $v_{M_p+1} = v_{\frac{M_p+1}{2}}^2 - 4 \cdot 2^{\frac{M_p-1}{2}}$. Так как $M_p \in P$, и для простого $p > 3$ мы имеем $M_p = 2^p - 1 \equiv -1 (mod 8)$, то $(\frac{2}{M_p}) = 1$, то есть, $2^{\frac{M_p-1}{2}} \equiv 1 (mod p)$. Следовательно, $v_{M_p+1} \equiv v_{\frac{M_p+1}{2}}^2 - 4 (mod p)$.

С другой стороны, используя тождество 3 леммы 1 с $r = M_p$ и $s = 1$, мы получим, что $2v_{M_p+1} = 2v_{M_p} + 12u_{M_p}$ (так как $v_1 = 2$, и $u_1 = 1$). Теперь, замечая, что $M_p \equiv -1 (mod 4)$ и $M_p \equiv 1 (mod 3)$, то есть, что $(\frac{3}{M_p}) = -(\frac{M_p}{3}) = -(\frac{1}{3}) = -1$, мы получим по лемме 2, что $v_{M_p+1} \equiv v_{M_p} + 6u_{M_p} \equiv 2 + 6(\frac{3}{M_p}) \equiv 2 - 6 \equiv -4 (mod M_p)$.

Следовательно, $v_{\frac{M_p+1}{2}}^2 \equiv 0 (mod M_p)$.

Доказательство второй части теоремы: если $M_n | S_{n-1}$, то M_n является простым числом.

Пусть $M_n | S_{n-1}$, то есть, $M_n | v_{2^{n-1}}$. Пусть $p | M_n$. Так как для $k > 1$ любое $S_k \equiv -1 (mod 3)$, то $p > 3$. Пусть w - ранг p. Используя тождество 4 леммы 1 с $r = 2^{n-1}$, мы получим, что $M_n | u_{2^n} = u_{2^{n-1}} v_{2^{n-1}}$. Следовательно, $p | u_{2^n}$, то есть, по лемме 3, $w | 2^n$. Легко видеть, что $w = 2^n$. Именно, если $w < 2^n$, то $p | u_{2^{n-1}}$, и, используя тождество 6 леммы 1 с $r = 2^{n-1}$, мы получим, что $p | v_{2^{n-1}}^2 - 12u_{2^{n-1}}^2 = (-2)^{2^{n-1}+2}$, противоречие.

Но, по лемме 4, мы имеем, что $w \leq p + 1$. Следовательно, $p \geq w - 1 = 2^n - 1 = M_n$, где p - простое, делящее M_n, то есть, $p = M_n$.

Подобно числам Ферма, числа Мерсенна также связяны с очень старой и известной математической проблемой. Рассмотрим так называемые *совершенные числа* - натуральные числа, равные сумме их собсьвенных делителей (то есть, натуральных делителей, отличных от самого числа). Первыми совершенными числами являются числа 6, 28, 496, 8128, ... По теореме Евклида-Эйлера, каждое четное совершенное число имеет вид

$$n = 2^{k-1}(2^k - 1),$$

где $2^k - 1$ - простое число Мерсенна. Таким образом, мы получим новое четное совершенное число тогда и только тогда, когда мы получим новое простое число Мерсенна. Что касается нечетных совершенных чисел, пока не найдено ни одного такого числа. Если нечетные совершеные числа существуют, они должны быть очень большими и очень специальными.

Theorem 6 *Четное натуральное число является совершенным тогда и только тогда, когда $n = 2^{k-1}(2^k - 1)$, где $2^k - 1 \in P$.*

Доказательство.

Рассмотрим Евклидову часть теоремы: каждое число $2^{k-1}(2^k - 1)$ с простым $2^k - 1$ является совершенным.

Именно, для такого n мы имеем: $\sigma(n) = (2^k - 1)2^k = 2\sigma(n)$, то есть, n является совершенным.

Рассмотрим Эйлерову часть теоремы: если n - четное совершенное число, то оно имеет указанную выше форму.

Пусть $\sigma(n) = 2n$. Пусть $n = 2^{t-1}m$, где m нечетно. Тогда $\sigma(n) = (2^t - 1)\sigma(m) = 2^t m$. Теперь мы имеем, что $\sigma(m)|2^t$, и $2^t - 1|m$, то есть, $2^t = \sigma(m)d$, и $m = (2^t - 1)d$. Если $d \neq 1$, то $\sigma(m) > d + (2^t - 1)d = d2^t$, противоречие. Следовательно, $d = 1$, и $m = 2^t - 1$. Так как $\sigma(m) = m + 1 = 2^t$, мы получаем, что $m \in P$.

Гипотезы и нерешенные проблемы

1. Существуют ли нечетные совершенные числа? Если да, то такое число должно быть произведением полного квадрата на нечетную степень одного единственного простого числа; оно делится не менее чем на 9 различных простых, и имеет не менее 75 (не обязятельно различных) простых делителей; оно имеет не менее 300 десятичных знаков; оно имеет простой делитель, больший 1200.

2. Существует ли бесконечно много простых чисел Мерсенна? Эквивалентный вопрос: существует ли бесконечно много четных совершенных чисел? Ответ, возможно, должен быть "да"(так как гармонический ряд расходится): используя асимптотический закон распределения простых чисел, мы можем утверждать, что вероятность "случайного"числа n быть простым не превосходит $A/\log n$ для некоторого действительного числа A. Суммируя выражение $\frac{A}{\log M_n} > \frac{A}{\log(2^n)} = \frac{A}{n \log 2}$, по всем n, мы получаем расходящийся ряд $\sum \frac{1}{n}$.

3. Существует ли бесконечно много составных чисел Мерсенна с простыми индексами?

   Эйлер показал: если $k > 1$, и $p = 4k + 3$ является простым, то $2p + 1$ является простым тогда и только тогда, когда $2^p = 1(mod 2p + 1)$.

   Таким образом, если $p = 4k + 3$ и $2p + 1$ являются простыми, то число Мерсенна $2^p - 1$ является составным (существует гипотеза о бесконечности пар простых чисел p, $2p + 1$).

4. Верна ли новая гипотеза Мерсенна?

5. Является ли число Мерсенна M_p бесквадратным? Легко показать, что если квадрат простого числа p делит число Мерсенна, то p является простым числом Вифериша, а они очень редки. Только два таких простых известны (1093 и 3511) в интервале до 4,000,000,000,000, и квадрат ни одного из них не делит числа Мерсенна.

6. Пусть $C_0 = 2$, $C_1 = 2^{C_0} - 1$, $C_2 = 2^{C_1} - 1$, $C_3 = 2^{C_2} - 1$, ... Являются ли все такие числа простыми?

   Эти числа растут очень быстро:

   $C_0 = 2$ (простое);

   $C_1 = 3$ (простое);

$C_2 = 7$ (простое);

$C_3 = 127$ (простое);

$C_4 = 170141183460469231731687303715884105727$ (простое);

$C_5 > 10512175997193696818750060546250516163 49$ (простое?).

Маловероятно, что C_5 (или большие члены) являются простыми. Заметим, что если один из членов последовательности окажется составным, то составными будут и все последующие члены.

7. Существуют ли новые простые двойные числа Мерсенна?

   Этот вопрос связан еще с одной ошибочной гипотезой: если $n = M_p$ - простое, то простым является и число M_n; обозначим это число MM_p и назовем *двойным числом Мерсенна*.

   Первые четыре таких числа действительно являются простыми:

   $MM_2 = 2^3 - 1 = 7$, $MM_3 = 2^7 - 1 = 127$, $MM_5 = 2^{31} - 1 = 2147483647$, $MM_7 = 2^{127} - 1 = 170141183460469231731687303715884105727$.

   Однако следующие четыре ($MM_{13}, MM_{17}, MM_{19}$ и MM_{31}) являются составными. Сущкствуют ли другие простые числа в этой прогрессии? Возможно, нет, но это остается открытым вопросом.

   Заметим, что последовательность чисел Каталана, рассмотренная выше, является подпоследовательностью последовательности двойных чисел Мерсенна.

Упражнения

1. Доказать, что $M_n|M_{nm}$.

2. Доказать, что $M_{n-m}|M_n - M_m$.

3. Доказать, что $gcd(M_n, M_m) = M_{gcd(n,m)}$.

4. Доказать, что $3|M_n \Leftrightarrow 2|n$, $5|M_n \Leftrightarrow 4|n$, $7|M_n \Leftrightarrow 3|n$, $11|M_n \Leftrightarrow 10|n$, $13|M_n \Leftrightarrow 12|n$, $17|M_n \Leftrightarrow 8|n$, $23|M_n \Leftrightarrow 11|n$.

5. Доказать, что если $n \equiv a(mod 4)$, то $M_n \equiv k(mod 10)$, где $a = 0, 1, 2, 3$, и $k = 5, 1, 3, 7$, соответственно.

   Доказательство. Так как $2^1 \equiv 2(mod 10)$, $2^2 \equiv 4(mod 10)$, $2^3 \equiv 8(mod 10)$, $2^4 \equiv 6(mod 10)$, $2^5 \equiv 2(mod 10)$,..., то $2^{4k} \equiv 6(mod 10)$, $2^{4k+1} \equiv 2(mod 10)$, $2^{4k+2} \equiv 4(mod 10)$, и $2^{4k+3} \equiv 8(mod 10)$.

6. Доказать бесконечность множества простых чисел, используя числа Мерсенна.

   Доказательство. Пусть $q_i|M_{p_i}$; так как $gcd(M_{p_i}, M_{p_j}) = 1$, то $q_i \neq q_j$; если множество $P = \{p_1, ..., p_k\}$ простых чисел конечно, то $P = \{q_1, ..., q_k\}$, но $p_1 = 2$, в то время как все q_i нечетны.

7. Доказать, что $M_n \neq x^2 + y^2 + z^2$ для $n \geq 3$.

8. Доказать, что производящая функция последовательности $M_1, M_2, ...$ имеет вид $\frac{1}{(1-x)(1-2x)}$ (и соответствующий ряд сходится при $|x| \leq 0.5$).

   Доказательство.

   $M_1 + M_2x + ... = ((2^1 - 1) + (2^2 - 1)x + ... = -(1 + x + x^2 + ...) + 2(1 + 2x + (2x)^2 + ...) = -\frac{1}{1-x} + \frac{2}{1-2x} = \frac{1}{(1-x)(1-2x)}$.

9. Доказать, что любое нечетное натуральное число n делит бесконечно много чисел Мерсенна. (Рассмотрите числа $M_{k\phi(n)}$.)

10. Найти наименьшее число Мерсенна, содержащее квадрат простого числа.

11. Найти наименьшее число Мерсенна M_n, содержащее квадрат простого числа, с нечетным n. (Это M_{21}; следуюшими такими числами являются M_{63} и M_{105}, но это тривиальный результат, так как $M_{21}|M_{63}$, и $M_{21}|M_{105}$.)

12. Доказать, что для любого натурального числа m существует число Мерсенна M_n, такое что первые знаки числа M_n совпадают с десятичным представлением числа m.

13. Доказать, что, для любого натурального числа s, последние s знаков числа M_n, $n = 1, 2, ...$, образуют бесконечную периодическую последовательность из $4 \cdot 5^{s-1}$ элементов.

4 Распределение простых чисел

Простые числа расположены пе числовой оси крайне неравномерно.

- Для данного натурального N, существует промежуток длины N, который не содержит простых чисел: число $(N+1)! + 2$ делится на 2, $(N+2)! + 3$ делится на 3, ..., $(N+1)! + (N+1)$ делится на $(N+1)$.

  С другой стороны, в списке простых чисел достаточно часто можно встретить два последовательных нечетных числа: 3 и 5, 5 и 7, 11 и 13, 17 и 19, ... Эти пары простых чисел $\{p, p+2\}$ называются *простыми-близнецами* (Stackel, 1916). Первыми парами простых-близнецов являются: (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241), (269, 271), (281, 283), (311, 313), (347, 349), (419, 421), (431, 433), (461, 463), (521, 523), (569, 571), (599, 601), (617, 619), (641, 643), (659, 661), (809, 811), (821, 823), (827, 829), (857, 859), (881, 883).

  Неизвестно, существует ли бесконечно много простых-близнецов. Брун в 1919 доказал, что ряд, составленный из чисел, обратных простым-близнецам, сходится. Этот известный результат показывает, что простых-близнецов в натуральном ряду достаточно мало, даже если их количество бесконечно. Сумма B_2 ряда $(\frac{1}{3} + \frac{1}{5}) + (\frac{1}{5} + \frac{1}{7}) + (\frac{1}{11} + \frac{1}{13}) + \ldots$ была вычислена Бруном с точностью до шести десятичных знаков, и называется сегодня *постоянной Бруна*:

  $$B_2 = 1.902160577783278\ldots$$

Используя простые-близнецы до 10^{16}, было получено (Sebah и Demichel, 2002) значение $B_2 = 1.902160583104\ldots$

Точнее, пусть $\pi_2(x)$ означает число простых $p \le x$, для которых $p+2$ также является простым. Брун (1919) предположил, что, для $x \ge x_0$, $\pi_2(x) < \frac{100x}{(\log x)^2}$. Доказательство появилось в 1920.

Bunt (1976) показал, что существует 152892 пар простых-близнецов, не превосходящих 10^{11}.

Наибольшая из известных пар простых-близнев: $100314512544015 \cdot 2^{171960} - 1$ и $100314512544015 \cdot 2^{171960} + 1$ (Járai, Farkas, Csajbok, Kasza, Járai, 2006). Эти числа имеют по 51780 десятичных знаков.

Неизвестно также, существует ли бесконечно много простых чисел p, для которых $p, p+2, p+6$ и $p+8$ - также простые (числа $p, p+2, p+4$ не могут быть одновременно простыми, так как одно из них делится на 3). Наборы простых такого вида называются *простыми квадруплетами*. Первые шесть таких квадруплетов получаются при $p = 5, 11, 101, 191, 821, 1481$.

Наименьший простой квадруплет, состоящий из 50-значных чисел (Stevens, 1995) имеет вид $1000\ldots058537891, 93, 97, 99$.

Наибольший известный простой квадруплет получается при $p = 4104082046 \cdot 4799\# + 5651$ (Norman Luhn, 2005), где $4799\#$ - произведение всех простых чисел, меньших ≤ 4799.

Константа, получающаяся при суммировании чисел, обратных простым квадруплетам (*константа Бруна для простых квадруплетов*) равна 0.87058....

Существуют и другие простые числа продобного рода. Так, *простыми-кузинами* называются пары простых, отличающиеся на 4. До 1000 такими парами являются: (3, 7), (7, 11), (13, 17), (19, 23), (37, 41), (43, 47), (67, 71), (79, 83), (97, 101), (103, 107), (109, 113), (127, 131), (163, 167), (193, 197), (223, 227), (229, 233), (277, 281), (307, 311), (313, 317), (349, 353), (379, 383), (397, 401), (439, 441), (457, 461), (487, 491), (499, 503), (613, 617), (643, 647), (673, 677), (739, 743), (757, 761), (769, 773), (823, 827), (853, 857), (859, 863), (877, 881), (883, 887), (907, 911), (937, 941), (967, 971). Наибольщая известная такая пара $(p, p+4)$ получается при $p = (9771919142 \cdot ((53238 \cdot 7879\#)2-1)+2310) \cdot 53238 \cdot 7879\#/385+1$ (Alm, Fleuren, Andersen, 2005). Каждое из чисел имеет здесь 10154 знаков. Выражение $n\#$ является *примориалом*, то есть, произведением всех простых чисел $\le n$.

Простые-кузины имеют в натуральном ряду ту же плотность, что и простые-близнецы. Аналог константы Бруна для них (с пропущенной парой $(3,7)$) определяется как $B_4 = \left(\frac{1}{7} + \frac{1}{11}\right) + \ldots$. Используя простые-кузины до 2^{42}, мы получим (Wolf, 1996) $B_4 = 1.1970449\ldots$

Рассмотрим пары простых, отличающихся на 6 ("sexy primes"). Первыми такими парами (до 500) являются: (5,11), (7,13), (11,17), (13,19), (17,23), (23,29), (31,37), (37,43), (41,47), (47,53), (53,59), (61,67), (67,73), (73,79), (83,89), (97,103), (101,107), (103,109), (107,113), (131,137), (151,157), (157,163), (167,173), (173,179), (191,197), (193,199), (223,229), (227,233), (233,239), (251,257), (263,269), (271,277), (277,283), (307,313), (311,317), (331,337), (347,353), (353,359), (367,373), (373,379), (383,389), (433,439), (443,449), (457,463), (461,467).

Наибольшая известная такая пара $(p, p+6)$ получается при $p = (48011837012 \cdot ((53238 \cdot 7879\#)2 - 1) + 2310) \cdot 53238 \cdot 7879\#/385 + 1$ (Alm, Fleuren, Andersen, 2005). Каждое число данной пары имеет 10154 знаков.

Рассматриваются также тройки простых $(p, p+6, p+12)$, такие что $p+18$ является составным ("sexy prime triplets"); первыми такими тройками (до 1000) являются: (7,13,19), (17,23,29), (31,37,43), (47,53,59), (67,73,79), (97,103,109), (151,157,163), (167,173,179), (227,233,239), (257,263,269), (271,277,283), (347,353,359), (367,373,379), (557,563,569), (587,593,599), (607,613,619), (647,653,659), (727,733,739), (941,947,953), (971,977,983).

Наибольшая известная такая тройка (Davis, 2006) имеет 5132 знаков: в ней $p = (84055657369 \cdot 205881 \cdot 4001\#(205881 \cdot 4001\#+1)+210) \cdot (205881 \cdot 4001\#-1)/35+1$.

Так как каждое пятое число вида $6n-1$ $(6n+1)$ делится на 5, существует только одна пятерка простых чисел такого вида: (5,11,17,23,29).

- Для любого положительного действительного числа x определим функцию $\pi(x)$ как число простых, не превосходящих x. Мы имеем: $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = \pi(6) = 3$, $\ldots$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10000) = 1229$, $\pi(10^5) = 9592$, $\pi(10^6) = 78498$, $\pi(10^7) = 664579$, $\pi(10^8) = 5761455$, $\pi(10^9) = 50847534$.

  В 1972 было получено (Bohman) значение $\pi(10^{10}) = 455052511$. Недавно (Lagarias, Miller, Oleyzko) было доказано, что $\pi(10^{16}) = 27923834033925$.

  Очевидно, что $\pi(p_n) = n$.

  Из теоремы Евклида (о бесконечности простых чисел) следует, что $\pi(x) \to \infty$ при $x \to \infty$.

  Эйлер (1737) дал аналитическое доказательство теоремы Евклида. При этом он рассмотрел ряд $\zeta(s) = 1 + \frac{1}{2^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s}$ для $s \in \mathbb{R}, s > 1$. Он оценил суммы $\zeta(2k)$ для всех $k \geq 1$; в частности, были получены значения $\zeta(2) = \frac{\pi^2}{6}$ и $\zeta(4) = \frac{\pi^4}{90}$. Эйлер заметил, что $\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in P}(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots) = \prod_{p \in P}(1 - \frac{1}{p^s})^{-1}$. На этом и основано его аналитическое доказательство бесконечности простых чисел.

  Эйлер доказал также, что $\pi(x) = o(x)$, то есть, что $\lim_{x \to \infty} \frac{\pi(x)}{x} = 0$. ($g(x) = o(f(x))$ означает, что $\lim_{x \to \infty} \frac{g(x)}{f(x)} = 0$.)

  Позже Гаусс (1792) предположил, что существует следующая асимптотическая формула для $\pi(x)$:

$$\pi(x) \sim \frac{x}{\log x}$$

при $x \to \infty$. Позднее он уточнил результат:

$$\pi(x) \sim \int_2^x \frac{du}{\log u}.$$

(Заметим, что *логарифмический интеграл* $Li(n) = \int_2^n \frac{dx}{\ln x}$ может быть представлен как $Li(n) = \sum_{k=0}^{\infty} \frac{k!n}{(\ln n)^{k+1}} = \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2n}{(\ln n)^3} + \ldots$, и использование первых трех членов дает лучшую оценку по сравнению с первоначальной формулой, соответствующей только первому члену разложения.)

Гаусс не опубликовал данный результат, о котором он впервые упомянул в 1849 в письме к Encke. Он был опубликован только в 1863.

Лежандр (1808) предположил, что

$$\pi(x) \sim \frac{x}{\log x - 1.08366}.$$

Первый существенный успех в этой области был получен Чебышевым в 1850. Он нашел для функции $\pi(x)$ следующие границы:

$$a \cdot \frac{x}{\log x} < \pi(x) < b\frac{x}{\log x},$$

где $x \geq 2$, $a = \frac{2^{1/2}3^{1/3}5^{1/5}}{30^{1/30}}$, и $b = \frac{6}{5}a$; следовательно, были получены и новые границы для n-го простого числа p_n:

$$0.91 \cdot n \log n < p_n < 1.7 \cdot n \log n.$$

Докажем этот результат, пользуясь элементарными методами. Именно, докажем, что существуют постоянные a и b, $0 < a < 1 < b$, такие что для всех $x \geq 6$ $a\frac{x}{\ln x} \leq \pi(x) \leq b\frac{x}{\ln x}$.

1. Предварительные оценки.

Пусть $T(x) = \ln(\lfloor x \rfloor !)$, то есть $T(n) = \ln n! = \ln 1 + \ln 2 + \ldots + \ln n$. Тогда

а) при $n \geq 3$, $T(2n) - 2T(n) \geq (n+1)\ln 2$. Действительно, $T(2n) - 2T(n) = \ln \frac{2n)!}{(n!)^2} = \ln \frac{n+1}{1} \cdot \ldots \cdot \frac{n+n}{n} = \ln \frac{n+1}{1} + \ldots + \ln \frac{n+n}{n}$. При $2 \leq s \leq n$, $\ln \frac{n+s}{s} = \ln(1 + \frac{n}{s}) \geq \ln(1+1) = \ln 2$; при $s = 1$ и $n \geq 3$, $\ln \frac{n+1}{1} \geq \ln(3+1) = 2\ln 2$. Таким образом, неравенство доказано.

б) при $n \geq 1$, $T(2n) - 2T(n) < 2n \ln 2$. Действительно, $\frac{(2n)!}{(n!)^2} = \binom{2n}{n} < \binom{2n}{0} + \binom{2n}{1} + \ldots + \binom{2n}{2n} = 2^{2n}$, и $T(2n) - 2T(n) = \ln \frac{(2n)!}{(n!)^2} < \ln 2^{2n} = 2n \ln 2$.

в) при $x \geq 6$, $\frac{\ln 2}{2} x \leq T(x) - 2T(\frac{x}{2}) \leq x \ln 2 + \ln(x+1)$. Действительно, пусть $n = \lfloor \frac{x}{2} \rfloor$. Тогда $n \geq 3$ (так как $x \geq 6$), $n \leq \frac{x}{2} < n+1$, или $2n \leq x < 2n+2$. Тогда $T(\frac{x}{2}) = T(n)$, а $T(x) = T(2n)$, если $2n \leq x < 2n+1$, и $T(x) = T(2n+1)$, если $2n+1 \leq x < 2n+2$. Так как $T(2n+1) = \ln(2n)! + \ln(2n+1) = T(2n) + \ln(2n+1)$, то $T(2n) \leq T(x) \leq T(2n) + \ln(2n+1)$. Тогда (так как $2n \leq x$) $T(x) - 2T(\frac{x}{2}) \leq T(2n) - 2T(n) + \ln(2n+1) \leq 2n\ln 2 + \ln(2n+1) \leq x \ln 2 + \ln(x+1)$.

С другой стороны (так как $n \geq 3$, и $n+1 > \frac{x}{2}$) $T(x) - 2T(\frac{x}{2}) \geq T(2n) - 2T(n) \geq (n+1)\ln 2 \geq \frac{x}{2}\ln 2$.

2. Оценка $\pi(x)$ снизу.

а) $T(x) = \ln\lfloor x\rfloor! = \ln p_1^{\alpha_1}...p_s^{\alpha_s}$, где $p_1 < ... < p_s \leq \lfloor x\rfloor < p_{s+1}$, $\alpha_i = \lfloor\frac{\lfloor x\rfloor}{p_i}\rfloor + \lfloor\frac{\lfloor x\rfloor}{p_i^2}\rfloor + ...$ Так как $p \leq \lfloor x\rfloor \Leftrightarrow p \leq x$, и $\lfloor\frac{\lfloor x\rfloor}{a}\rfloor = \lfloor\frac{x}{a}\rfloor$, то $T(x) = \ln\prod_{p\leq x} p^{\lfloor\frac{x}{p}\rfloor+...} = \sum_{p\leq x}\ln p(\lfloor\frac{x}{p}\rfloor + \lfloor\frac{x}{p^2}\rfloor + ...)$. Тогда $T(x) - 2T(\frac{x}{2}) = \sum_{p\leq x}\ln p((\lfloor\frac{x}{p}\rfloor - 2\lfloor\frac{x}{2p}\rfloor) + (\lfloor\frac{x}{p^2}\rfloor - 2\lfloor\frac{x}{2p^2}\rfloor) + ...) = \sum_{p\leq x}\alpha_p \ln p$, где $\alpha_p = \sum_{k=1}^{s}(\lfloor\frac{x}{p^k}\rfloor - 2\lfloor\frac{x}{2p^k}\rfloor)$, а $s = \frac{\ln x}{\ln p}$ (при $k > \frac{\ln x}{\ln p}$, $\ln p^k > \ln x$, $p^k > x$, и соответствующая скобка равне нулю). Так как $0 \leq \lfloor x\rfloor - 2\lfloor\frac{x}{2}\rfloor \leq 1$, то каждое слагаемое в α_p не превосходит 1, число таких слагаемых $\leq \frac{\ln x}{\ln p}$, и $\alpha_p \leq \frac{\ln x}{\ln p}$. Тогда, с одной стороны, $T(x) - 2T(\frac{x}{2}) \leq \sum_{p\leq x}\ln p\frac{\ln x}{\ln p} = \ln x\pi(x)$. С другой стороны, $T(x) - 2T(\frac{x}{2}) \geq \frac{\ln x}{2}$. Таким образом, $\pi(x)\ln x \geq \frac{\ln 2}{2}x$, или $\pi(x) \geq a\frac{x}{\ln x}$, где $a = \frac{\ln 2}{2}$.

3. Оценка $\pi(x)$ сверху.

$T(x) - 2T(\frac{x}{2}) = \sum_{p\leq x}\ln p((\lfloor\frac{x}{p}\rfloor - 2\lfloor\frac{x}{2p}\rfloor) + ...) \geq \sum_{\frac{x}{2}<p\leq x}\ln p((\lfloor\frac{x}{p}\rfloor - 2\lfloor\frac{x}{2p}\rfloor) + ...)$. При $\frac{x}{2} < p \leq x$, $1 \leq \frac{x}{p} < 2$, и $\lfloor\frac{x}{p}\rfloor = 1$. С другой стороны, $2p > x$, $p^2 > x$, ..., то есть $\lfloor\frac{x}{2p}\rfloor = \lfloor\frac{x}{p^2}\rfloor = ... = 0$. Тогда $T(x) - 2T(\frac{x}{2}) \leq \sum_{\frac{x}{2}<p\leq x}\ln p \leq \sum_{\frac{x}{2}<p\leq x}\ln\frac{x}{2} = \ln\frac{x}{2}(\pi(x) - \pi(\frac{x}{2})) = \pi(x)\ln x - \pi(\frac{x}{2})\ln\frac{x}{2}$ $-\pi(x)\ln 2$. Таким образом, $\pi(x)\ln x - \pi(\frac{x}{2})\ln\frac{x}{2} \leq T(x) - 2T(\frac{x}{2}) + \pi(x)\ln 2 \leq 2x\ln 2 + \ln(x+1) = x(2\ln 2 + \frac{\ln(x+1)}{x}) \leq Cx$, где $C > 1$ - абсолютная постоянная, или $\pi(x)\ln x \leq Cx + \pi(\frac{x}{2})\ln\frac{x}{2}$.

Тогда, заменяя x последовательно на $\frac{x}{2}$, $\frac{x}{4}$, ..., получим $\pi(x)\ln x \leq Cx + C\frac{x}{2} + C\frac{x}{4} + ... \leq Cx(1 + \frac{1}{2} + \frac{1}{4} + ...) = 2Cx = bx$, где $b > 1$ - абсолютная постоянная.

Получим теперь точные границы для n-го простого числа: существуют постоянные c и d, такие что $cn\ln n \leq p_n \leq dn\ln n$.

Действительно, по предыдущему утверждению, $a\frac{p_n}{\ln p_n} \leq \pi(p_n) = n \leq b\frac{p_n}{\ln p_n}$. Отсюда $\frac{1}{b}n\ln p_n \leq p_n \leq \frac{1}{a}n\ln p_n$.

а). Так как $p_n \geq n$, то $p_n \geq \frac{1}{b}n\ln p_n \geq \frac{1}{b}n\ln n$.

б). Так как $\lim\frac{\ln z}{\sqrt{z}} = \lim\frac{1/z}{(1/2)\sqrt{z}} = \lim\frac{2}{\sqrt{z}} = 0$ при $z \to \infty$, то $\ln p_n < a\sqrt{p_n}$ при достаточно больших n. Тогда $p_n \leq \frac{1}{a}n\ln p_n < n\sqrt{p_n}$, $\sqrt{p_n} < n$, и $\ln\sqrt{p_n} < \ln n$, то есть $\ln p_n < 2\ln n$, и $p_n \leq \frac{2}{a}n\ln n$.

Утверждение о расходимости ряда чисел, обратных простым, является теперь следствием полученной оценки.

Заметим, что Чебышев доказал также (1852 г.) *постулат Бертрана* (1845 г.): если n - натуральное число > 1, то между n и $2n$ существует по крайней мере одно простое число.

Докажем это утверждение.

1. Покажем, что при $n > 1$ $\binom{2n}{n} > \frac{4}{2\sqrt{n}}$. Проведем доказательство по индукции. При $n = 2$, $\binom{4}{2} = 6 > 4\sqrt{2} = \frac{4^2}{2\sqrt{2}}$. Переходя от n к $n+1$, получим:

$\binom{2(n+1)}{n+1} = \frac{(2n+2)!}{(n+1)!(n+1)!} = \frac{(2n)!(2n+1)2(n+1)}{n!n!(n+1)(n+1)} = \binom{2n}{n}\frac{2(2n+1)}{n+1} > \frac{4^n \cdot 2(2n+1)}{2\sqrt{n}(n+1)} = \frac{2\cdot 4^n(2n+1)}{\sqrt{n+1}\sqrt{4n(n+1)}} < \frac{4^{n+1}}{\sqrt{n+1}}$, так как $\frac{2n+1}{\sqrt{4n(n+1)}} > 1$ $((2n+1)^2 = 4n^2+4n+1 > 4n^2+4n = 4n(n+1))$.

2. Покажем, что $\prod_{p\leq x} p \leq 4^x$.

Не ограничивая общности, можно считать, что $x \in \mathbb{N}$ (если для натурального x утверждение доказано, то $\prod_{p\leq x} p = \prod_{p\leq \lfloor x\rfloor} p < 4^{\lfloor x\rfloor} \leq 4^x$). Проведем доказательство индукцией по x. Для $x = 1$ и $x = 2$ утверждение верно: $\prod_{p\leq 1} p = 1 < 4^1$, $\prod_{p\leq 2} p = 2 < 4^2$. Пусть утверждение верно для всех $x < n$ $(n \geq 3)$. Докажем его для n.

а). если n четное, то $n \in S$, и, пользуясь предположением индукции, $\prod_{p\leq n} p = \prod_{p\leq n-1} p < 4^{n-1} < 4^n$.

б). если n - нечетное, то $n = 2k+1$, $k \in \mathbb{N}$.

Рассмотрим $p \in P$, $k+2 \leq p \leq 2k+1$. Каждое такое p является делителем $\binom{2k+1}{k} = \frac{(2k+1)!}{k!(k+1)!} = \frac{(k+2)...(2k+1)}{1\cdot 2...k}$, так как входит в числитель, и не входит в знаменатель. Тогда $\prod_{k+2\leq p\leq 2k+1} p \leq \binom{2k+1}{k}$.

При этом $\binom{2k+1}{k} < 4^k$, так как $\binom{2k+1}{0} + ... + \binom{2k+1}{2k+1} = 2^{2k+1}$, и $\binom{2k+1}{k} = \binom{2k+1}{k}$, то есть $2\binom{2k+1}{k} < 2^{2k+1}$, и $\binom{2k+1}{k} < 2^{2k} = 4^k$.

Тогда, используя это утверждение и предположение индукции, получим $\prod_{p\leq n} p = \prod_{p\leq 2k+1} p = \prod_{p\leq k+1} p \prod_{k+2\leq p\leq 2k+1} p < 4^{k+1}\cdot 4^k = 4^n$.

3. Покажем, что $\binom{2n}{n} \leq (2n)^{\pi(2n)}$.

$\binom{2n}{n} = \frac{(2n)!}{n!n!} = p_1^{\alpha_1}...p_s^{\alpha_s}$, где $2 = p_1 < ... < p_s \leq 2n < p_{s+1}$, а $\alpha_i = \sum_{k=1}^{\infty}(\lfloor\frac{2n}{p_i^k}\rfloor - 2\lfloor\frac{n}{p_i^k}\rfloor)$.

Отсюда немедленно следует, что $s = \pi(2n)$.

Кроме того, $p_i^{\lfloor alpha_i} \leq 2n$. Действительно, если $p_i^{\alpha_i} > 2n$, то $\lfloor\frac{2n}{p_i^{\alpha_i}}\rfloor = 0$, $\lfloor\frac{n}{p_i^{\alpha_i}}\rfloor = 0$, ..., то есть (так как $0 \leq \lfloor 2x\rfloor - 2\lfloor x\rfloor \leq 1$) $\alpha_i = \sum_{k=1}^{\alpha_i-1}$ $(\lfloor\frac{2n}{p_i^k}\rfloor - 2\lfloor\frac{n}{p_i^k}\rfloor \leq \alpha_i - 1$, противоречие.

Тогда получаем, что $\binom{2n}{n} \leq (2n)^s = (2n)^{\pi(n)}$.

Заметим, что мы доказали более общее утверждение: если $\binom{2n}{n} = p_1^{\alpha_1}...p_t^{\alpha_t}...p_s^{\alpha_s}$, то $p_1^{\alpha_1}...p_t^{\alpha_t} \leq (2n)^t = (2n)^{\pi(p_t)}$.

4. Покажем, что для $p \in P$, $\sqrt{2n} \leq p \leq 2n$, p входит в разложение числа $\binom{2n}{n}$ с показателем, ≤ 1.

$\binom{2n}{n} = \frac{(2n)!}{n!n!} = p_1^{\alpha_1}...p_s^{\alpha_s}$, где $2 = p_1 < p_2 < ... < p_s \leq 2n < p_{s+1}$ - все простые, $\leq 2n$, а $\alpha_i = \sum_{k=1}^{\infty}(\lfloor\frac{2n}{p_i^k}\rfloor - 2\lfloor\frac{n}{p_1^k}\rfloor)$.

Рассмотрим $p_i \geq \sqrt{2n}$. Для вырожденного случая $p_i = \sqrt{2n}$ имеем $p_i^2 = 2n$, то есть $p = 2$, $n = 2$. В этом случае $\binom{2n}{n} = 6 = 2\cdot 3$, и условие леммы выполнено. В общем случае $p_i^2 > 2n$, и $\lfloor\frac{2n}{p_i^2}\rfloor = 0$, $\lfloor\frac{n}{p_i^2}\rfloor = 0$, $\lfloor\frac{2n}{p_i^3}\rfloor = 0$, $\lfloor\frac{n}{p_i^3}\rfloor = 0$, ..., то есть $\alpha_i = \lfloor\frac{2n}{p_i}\rfloor - 2\lfloor\frac{n}{p_i}\rfloor$.

Так как $0 \leq \lfloor 2x\rfloor - 2\lfloor x\rfloor \leq 1$, то $0 \leq \alpha_i \leq 1$.

5. Покажем, что при $p \in P$, $\frac{2}{3}n < p \leq n$, $n \geq 3$, p не входит в разложение числа $\binom{2n}{n}$.

Для $n = 3$ и $n = 4$ утверждение проверяется непосредственно. При $n = 3$, $\binom{6}{3} = 20 = 2^2 \cdot 5$. Если $\frac{2}{3} \cdot 3 < p \leq 3$, то $p = 3$, а 3 не входит в разложение числа 20. Для $n = 4$, $\binom{8}{4} = 70 = 2 \cdot 5 \cdot 7$. Если $\frac{2}{3} \cdot 4 < p \leq 4$, то $p = 3$, а 3 не входит в разложение числа 70.

Рассмотрим случай $n \geq 5$. Записав разложение $\binom{2n}{n} = \frac{(2n)!}{n!n!} = p_1^{\alpha_1}...p_s^{\alpha_s}$, где $2 = p_1 < p_2 < ... < p_s \leq 2n < p_{s+1}$ - все простые, $\leq 2n$, а $\alpha_i = \sum_{k=1}^{\infty}(\lfloor\frac{2n}{p_i^k}\rfloor - 2\lfloor\frac{n}{p_1^k}\rfloor)$, положим, что $\frac{2}{3}n < p \leq n$. Тогда

а). $\frac{2n}{p} < 3$, $\frac{n}{p} \geq 1$, то есть $\lfloor\frac{2n}{p}\rfloor \leq 2$, а $\lfloor\frac{n}{p}\rfloor \geq 1$, то есть $0 \leq \lfloor\frac{2n}{p}\rfloor - 2\lfloor\frac{n}{p}\rfloor \leq 2 - 2 \cdot 1 = 0$, или $= 0$.

б). При $k \geq 2$, $p^k \geq p^2 > \frac{4}{9}n^2$, и $(n \geq 5)$ $\frac{2n}{p^k} < \frac{9}{2n} < 1$, то есть $\lfloor\frac{2n}{p^k}\rfloor = 0$, и $\lfloor\frac{n}{p^k}\rfloor = 0$.

Таким образом, $\alpha_i = 0$, и утверждение доказано.

6. Покажем, что для $p \in P$, $n < p \leq 2n$, p входит в разложение числа $\binom{2n}{n}$ с показателем 1.

а). Если $p = 2n$, то $p = 2$, $n = 1$, и утверждение очевидно: $\binom{2}{1} = 2$, и $2|2$.

б). Пусть $p \in P$, $n < p < 2n$. Проведем рассуждения индукцией по n.

Для $n = 1$ таких p не существует, и утверждение доказано.

Пусть $n \geq 2$. Рассмотрим разложение $\binom{2n}{n} = \frac{(2n)!}{n!n!} = p_1^{\alpha_1}...p^{\alpha}...p_s^{\alpha_s}$, где $2 = p_1 < p_2 < ... < p_s \leq 2n < p_{s+1}$ - все простые, $\leq 2n$, а $\alpha_i = \sum_{k=1}^{\infty}(\lfloor\frac{2n}{p_i^k}\rfloor - 2\lfloor\frac{n}{p_1^k}\rfloor)$. При $n < p < 2n$ имеем $\frac{n}{p} < 1$, $1 < \frac{2n}{p} < 2$, и $\lfloor\frac{2n}{p}\rfloor = 1 <$ $\lfloor\frac{n}{p}\rfloor = 0$, то есть $\lfloor\frac{2n}{p}\rfloor - 2\lfloor\frac{n}{p}\rfloor = 1$.

Для $k \geq 2$ имеем $(p > n$, $n \geq 2)$: $\frac{2n}{p^k} \leq \frac{2n}{p^2} < \frac{2}{n} \leq 1$. таким образом, $\lfloor\frac{2n}{p^k}\rfloor = 0$, $\lfloor\frac{n}{p^k}\rfloor = 0$, и $\lfloor\frac{2n}{p^k}\rfloor - 2\lfloor\frac{n}{p^k}\rfloor = 0$.

Мы получили, что $\alpha = 1$ для рассматриваемого простого p.

7. Покажем, что при $n \geq 14$ $\pi(n) \leq \frac{n}{2} - 1$.

Для $n = 14$ имеем $\pi(14) = 6 = \frac{14}{2} - 1$.

Для $n \geq 15$ среди чисел $1, 2, ..., n$ четные числа $4, 6, ..., 2\lfloor\frac{n}{2}\rfloor \in S$. Их число равно $\lfloor\frac{n}{2}\rfloor - 1$ (2 не учитываем). Кроме того, при $n \geq 15$ в последовательность $1, 2, ..., n$ входят составные числа $9, 15$ и число $1 \notin P$. Тогда $\pi(n) \leq n - (\lfloor\frac{n}{2}\rfloor - 1) - 3 < \frac{n}{2} - 1$, так как $0 \leq \frac{n}{2} - \lfloor\frac{n}{2}\rfloor < 1$.

8. Покажем, что при $n \geq 98$ $R_n = \prod_{n<p\leq 2n} p > \frac{4^{4/3}}{2\sqrt{n}(2n)^{\sqrt{n/2}}}$.

Рассмотрим $\binom{2n}{n} = p_1^{\alpha_1}...p_s^{\alpha_s}$, $2 = p_1 < ... < p_s \leq 2n < p_{s+1}$. По 6., $\binom{2n}{n} = Q_n R_n$, где $Q_n = p_1^{\alpha_1}...p_m^{\alpha_m}$, $2 = p_1 < ... < p_m \leq n$.

Оценим Q_n. По 5., $p_m \leq \frac{2}{3}n$. По 4., если $\alpha_i > 1$, то $p_i < \sqrt{2n}$. Таким образом, $Q_n \leq p_1^{\alpha_1}...p_t^{\alpha_t}p_{t+1}...p_m$, где $2 = p_1 < ... < p_t < \sqrt{2n} \leq p_{t+1} < ... < p_m \leq \frac{2}{3}n$, и $\alpha_i \geq 1$. Запишем $Q_n = \prod_1 \prod_2$, где $\prod_1 = \prod_{2\leq p_j \leq \frac{2}{3}n}$, $\prod_2 = \prod_{2\leq p\leq\sqrt{2n}} p_i^{\alpha_i - 1}$. Оценим $\prod_1$ и $\prod_2$ сверху.

а). По 3. (точнее, по замечанию к 3.): $\prod_2 < p_1^{\alpha_1}...p_t^{\alpha_t} \leq (2n)^t = (2n)^{\pi(p_t)}$, где $p_t \leq \sqrt{2n}$. При $n \geq 98$ $\sqrt{2n} \geq \sqrt{196} = 14$, $\lfloor\sqrt{2n}\rfloor \geq 14$, и по 7.

$\pi(p_t) \le \pi(\lfloor\sqrt{2n}\rfloor) \le \frac{1}{2}\lfloor\sqrt{2n}\rfloor - 1 \le \frac{\sqrt{2n}}{2} - 1 = \sqrt{\frac{n}{2}} - 1 < \sqrt{\frac{n}{2}}$. Следовательно, $\prod_2 \le (2n)^{\sqrt{n/2}}$.

б). По 2., $\prod_1 = \prod_{p \le \frac{2n}{3}} < 4^{\frac{2n}{3}}$.

Тогда $Q_n < 4^{\frac{2n}{3}}(2n)^{\sqrt{n/2}}$.

Вернемся к $\binom{2n}{n} = Q_n R_n$. По 1., $\binom{2n}{n} > \frac{4^n}{2\sqrt{n}}$. Тогда $R_n = \frac{\binom{2n}{n}}{Q_n} < \frac{4^n}{2\sqrt{n}4^{2n/3}(2n)^{n/2}} = \frac{4^{n/3}}{2\sqrt{n}(2n)^{\sqrt{n/2}}}$.

9. Покажем, что при $k \ge 8$, $k \in \mathbb{N}$, $2^k > 18(k+1)$.

Проведем рассуждения индукцией по k. При $k = 8$, $2^8 = 256 > 18 \cdot 9 = 162$. Переходя от k к $k+1$, имеем $2^{k+1} = 2^k + 2^k > 18k+18+18k+18 > 18k+36 = 18(k+2)$.

10. Покажем, что при $x \ge 8$, $x \in \mathbb{R}$, $2^x \ge 18x$.

$x \ge 8$, то есть $\lfloor x \rfloor \ge 8$, и по 9. $2^x \ge 2^{\lfloor x \rfloor} > 18(\lfloor x \rfloor + 1) > 18x$.

11. Покажем, что, при $k \ge 6$, $2^k > 6(k+1)$.

При $k = 6$, $2^6 = 64 > 42 = 6 \cdot 7$. При $k = 7$, $2^7 = 128 > 48 = 6 \cdot 8$. При $k \ge 8$ по 9. $2^k > 18(k+1) > 6(k+1)$.

12. Покажем, что, при $x \ge 6$, $x \in \mathbb{R}$, $2^x > 6x$.

По 11., $2^x \ge 2^{\lfloor x \rfloor} > 6(\lfloor x \rfloor + 1) > 6x$.

13. Покажем, что, при $n \ge 648$, $R_n > 2n$.

По 8., при $n \ge 98$, $R_n > \frac{4^{n/3}}{2\sqrt{n}(2n)^{\sqrt{n/2}}}$. Для доказательства утверждения достаточно показать, что $4^{n/3} > 4n\sqrt{n}(2n)^{\sqrt{n/2}}$.

а). При $n \ge 648$, $\frac{\sqrt{2n}}{6} \ge \frac{36}{6} = 6$. Тогда по 12. $2^{\sqrt{2n}/6} > 6(\frac{\sqrt{2n}}{6}) = \sqrt{2n}$. Возводя данное неравенство в степень $\sqrt{2n}$, получим $2^{2n/6} = 2^{n/3} > (2n)^{\frac{1}{2}\sqrt{2n}} = (2n)^{\sqrt{n/2}}$. Таким образом, $2^{n/3} > (2n)^{\sqrt{n/2}}$.

б). При $n \ge 648$, $\frac{2n}{9} \ge \frac{2^4 \cdot 3^4}{9} = 16 \cdot 9 > 8$, и по 10. $2^{\frac{2n}{9}} > 18(\frac{2n}{9}) = 4n$. Возводя в степень $3/2$, получим $2^{n/3} > (4n)^{3/2} = 4n\sqrt{4n} > 4n\sqrt{n}$, то есть, $2^{n/3} > 4n\sqrt{n}$.

в). Теперь $2^{n/3} \cdot 2^{n/3} = 4^{n/3} > 4n\sqrt{n}(2n)^{\sqrt{n/2}}$.

14. Покажем, что при $n \ge 648$ между n и $2n$ существует по крайней мере 2 простых числа: $\pi(2n) - \pi(n) \ge 2$.

Рассмотрим $R_n = \prod_{n<p\le 2n} p$. Так как, при $n \ge 648$, $R_n > 2n$, то на промежутке $(n, 2n]$ существует по крайней мере одно простое число. При этом если оно ровно одно, то $R_n = p \le 2n$, противоречие.

15. Покажем что, уже при $n \ge 6$, $\pi(2n) - \pi(n) \ge 2$.

Для $n = 6$, на $(6, 12]$ имеется 2 простых 7 и 11. Для $n \ge 648$ утверждение уже доказано. Рассмотрим $7 \le n \le 647$. Для доказательства утверждения при таких n достаточно построить последовательность $\{q_0, ..., q_m\}$ простых чисел, удовлетворяющих условиям: $q_0 = 7$, $q_1 = 11$, $q_k < 2q_{k-2}$ при $k = 2, ..., m$, $q_{m-1} > 647$.

Действительно, пусть $7 \le n \le 647$, и такая последовательность $\{q_0, ..., q_m\}$ построена. Тогда $q_0 = 7 \le n \le 647 < q_{m-1}$, то есть существует $k, 0 \le k \le m-2$, такое что $q_k \le n < q_{k+1}$. Так как $k \le m-2$, то $k+2 \le m$, и $q_{k+2} \le q_m$. Кроме того (так как $q_k \le n$) $q_{k+2} < 2q_k \le 2n$. Таким образом ($n < q_{k+1}$) $n < q_{k+1} < q_{k+2} \le 2n$, то есть на $(n, 2n]$ существует два простых числа.

Легко видеть, что последовательность 7, 11, 13, 19, 23, 37, 43, 73, 83, 139, 163, 277, 317, 547, 631, 653, 1259 является искомой.

16. Покажем, что $\pi(2n-3) - \pi(n) \ge 1$ при $n \ge 4$.

Для $n = 4, 5$ утверждение проверяется непосредственно: $5 \in (4,5]$, $7 \in (5,7]$. Для $n \ge 6$ на $(n, 2n]$ найдется 2 простых числа: $n < p < q \le 2n$. Так как $n \ge 6$, то $q \le 2n-1$, и p и q нечетны, то есть $p \le q-2$. Отсюда $p \le 2n-3$, что завершает рассуждения.

17. Покажем, что $\pi(2n) - \pi(n) \ge 1$ для $n \ge 1$.

Для этого достаточно использовать 15. и проверить все $1 \le n \le 5$ (соответствующие простые равны 2, 3, 5, 7, 7) или использовать 16. и проверить все $1 \le n \le 3$.

Фундаментальный вклад в проблему исследования распределения простых чисел был сделан Риманом в 1859. Он вернулся к Эйлерову доказательству бесконечности простых чисел, и ввел в рассмотрение функцию

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{n^s} + \dots$$

как функцию комплексного переменного $s = \sigma + it$, $\sigma > 1$. Эта сумма абсолютно сходится при $Res = \sigma > 1$ и дает аналитическую функцию в этой области. Риман показал, что $\zeta(s)$ аналитически продолжаема не всю комплексную плоскость, и имеет единственный полюс с вычетом 1 в точке $s = 1$.

Кроме того, Риман показал, что дзета-функция удовлетворяет функциональному уравнению, из которого следует, что она имеет нули $s = -2, -4, \dots, -2n, \dots$ (так называемые *тривиальные нули*), и что все остальные нули (так называемые *нетривиальные нули*) принадлежат полосе $0 \le Res \le 1$, которая была названа *критической полосой*. *Гипотеза Римана* утверждает, что все нетривиальные нули лежат на прямой $Res = \frac{1}{2}$, которая называется *критической прямой.* Это предположение остается открытым до сих пор и, может быть, является, после доказательства Великой Теоремы Ферма, наиболее известной нерешенной математической проблемой.

Вычисления показывают, что первые $1.5 \cdot 10^9$ нетривиальных нулей дзета-функции действительно лежат на критической прямой.

Исследования Римана послужили основой доказательства в 1896, независимо Адамаром и Валле Пуссеном, *асимптотического закона распределения простых чисел*:

$$\pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x}),$$

то есть,

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Основную часть рассуждений составляет доказательство того факта, что $\zeta(1+it) \neq 1$ для любого $t \in \mathbb{R}$.

Точнее, Валле Пуссен (1899) показал, что

$$\pi(x) = Li(x) + O\left(\frac{x}{\ln x} e^{-a\sqrt{\ln x}}\right)$$

для некоторой константы a. (Здесь $g(x) = O(f(x))$, если найдется такое число x_0, что, для любого $x \geq x_0$, $|f(x)| \leq Cg(x)$ для некоторой положительной константы C.)

В 1901 Кох показал, что, при условии выполнимости гипотезы Римана,

$$\pi(x) = Li(x) + O(\sqrt{x} \ln x),$$

что можно записать в несколько более слабой форме как $\pi(x) = Li(x) + O(x^{1/2+\epsilon})$.

Таким образом, из гипотезы Римана следует очень хорошая оценка остаточного члена в асимптотической формуле для $\pi(x)$ с остаточным членом порядка $\sqrt{x}$. Лучшие из имеющихся безусловных оценок пока очень далеки от этого результата.

Логарифмический интеграл $Li(x)$ больше чем $\pi(x)$ для "малых"значений x. Однако в 1914 Литтлвуд доказал, что ситуация может меняться при больших x. Первое значение x, для которого $\pi(x)$ превышает $Li(x)$, приблизительно равно $x = 10^{316}$.

Как следствие асимптотического закона распределения простых чисел, мы можем получить информацию об асимптотическом поведении n-го простого числа:

$$p_n \sim n \ln n.$$

Еще более точная аппроксимация имеет вид: $p_n = n \ln n + n \ln \ln n + O(\frac{n}{\ln n} \ln \ln n)$.

Упражнения

1. Найти $\pi(100)$, $\pi(\sqrt{50})$, $\pi(\log_8 121)$.
2. Доказать, что $\pi(x) \geq \log_2 \log_2 x$.
3. Доказать, что одно из чисел $n, n+2, n+4$ делится на 3.
4. Найти все пары простых-близнецов, в которых одно число является числом Мерсенна, а другое - числом Ферма.

5 Асимптотический закон распределения простых чисел

В этом разделе мы рассматриваем доказательство асимптотического закона распределения простых чисел. Именно, мы докажем, что $\pi(x) \sim \frac{x}{\ln x}$.

5.1 Дзета-функция Римана

Дзета-функция Римана $\zeta(s)$ определена для любого комплексного числа s с действительной частью > 1 с помощью следующего ряда Дирихле:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Для $Re(s) > 1$ данный ряд сходится и определяет функцию, аналитическую в этой области.

Лемма 1. $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ является аналитической в области $Re(s) = \sigma > 1$.

Доказательство.

Мы знаем, что $e^{i\phi} = \cos\phi + i\sin\phi$, то есть, $|e^{i\phi}| = \sqrt{\cos^2\phi + \sin^2\phi} = 1$. Тогда $|\frac{1}{n^s}| = |\frac{1}{n^\sigma} e^{it\ln n}| = \frac{1}{n^\sigma}$. Так как ряд $\sum_{n=1}^{\infty} \frac{1}{n^\sigma}$ сходится для $\sigma > 1$, то первый ряд равномерно сходится в любой области $\sigma > 1 + \delta$, $\delta > 0$, следовательно, в этой области сумма ряда представляет собой аналитическую функцию. Так как δ - любое положительное число, то последнее утверждение верно и в области $\sigma > 1$.

Следствие. Для $Re(s) = \sigma > 1$, $\zeta^{'}(s) = -\sum_{n=2}^{\infty} \frac{\ln n}{n^s}$.

Доказательство. $\zeta^{'}(s) = \sum_{n=1}^{\infty} (n^{-s})^{'} = \sum_{n=1}^{\infty} -n^{-s}\ln n = -\sum_{n=2}^{\infty} \frac{\ln n}{n^s}$.

Лемма 2 (формула Эйлера). Для $Re(s) = \sigma > 1$, $\zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1}$.

Доказательство.

Каждый множитель (для данного простого p) в нашем произведении может быть заменен суммой бесконечной геометрической прогрессии: $\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots$. Если $Re(s) > 1$, данный ряд абсолютно сходится. Следовательно,

$$\prod_{p\le X} (1 - p^{-s})^{-1} = \prod_{p\le X} (1 + p^{-s} + p^{-2s} + \ldots) = \sum{}^{*} \frac{1}{n^s} = \sum_{n\le X} \frac{1}{n^s} + \sum_{n>X}{}^{''} \frac{1}{n^s}.$$

(Сумма $\sum^{*}$ содержит члены $\frac{1}{n^s}$, где n - произведение некоторых простых, не превосходящих X.)

Так как $X \to \infty$, и $\sum_{n=1}^{\infty} \frac{1}{n^s}$ абсолютно сходится, то $\sum_{n>X} \frac{1}{n^s} \to 0$, и $\sum^{''} \to 0$.

Следуюхая схема рассуждений соответствует идее оригинального доказательства Эйлера: $\zeta(s) = 1 + \frac{1}{2^s} + \ldots$, и $\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \ldots$; вычитая второе равенство из первого, получим: $(1 - \frac{1}{2^s})\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \ldots$.

Далее: $\frac{1}{3^s}(1 - \frac{1}{2^s})\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \ldots$. Еще раз вычитая, получим: $(1 - \frac{1}{3^s})(1 - \frac{1}{2^s})\zeta(s) = \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \ldots$.

Повторяя операцию бесконечное число раз, получим: $\ldots(1 - \frac{1}{11^s})\ldots(1 - \frac{1}{2^s})\zeta(s) = 1$.

Отсюда следует равенство: $\zeta(s) = \frac{1}{(1-\frac{1}{2^s})(1-\frac{1}{3^s})\ldots}$.

Для обоснования этого доказательства достаточно заметить, что при $Re(s) > 1$ правая часть стремится к 1, что немедленно следует из сходимости ряда для $\zeta(s)$.

Результат Эйлера является специальным случаем одной общей формулы: пусть f - вполне мультипликативная функция, и ряд $\sum_{n=1}^{\infty} f(n)$ абсолютно сходится для $Re(s) > 1$; тогда $\sum_{n=1}^{\infty} f(n) = \prod_p (1 - f(p))^{-1}$.

Имеют место следующие результаты:
$\zeta(1)=\infty$ - это гармонический ряд;
$\zeta(2)=\frac{\pi}{6}=1.645...$;
$\zeta(3)=1.202...$;
$\zeta(4)=\frac{\pi^2}{90}=1.0823...$.

Перейдем к рассмотрению функции Мангольдта.

Функция Мангольдта, обозначаемая символом $\Lambda(n)$, определяется как $\Lambda(n)=\ln p$, если $n=p^k$ для простого p и натурального k, и как $\Lambda(n)=0$, иначе.

Имеет место формула $\ln n=\sum_{d|n}\Lambda(n)$, где сумма берется по всем натуральным делителям d числа n. Действительно, для $n=1$ мы получаем тождество $0=\ln 1$. Для $n\neq 1$ мы получаем, что $\sum_{d|n}\Lambda(d)=\ln p_1^{\alpha_1}...p_k^{\alpha_k}=\ln n$.

Функция Чебышева $\psi(x)$ определяется как $\psi(x)=\sum_{n\leq x}\Lambda(n)$.

Лемма 3. Для $Re(s)>1$, $\frac{\zeta'(s)}{\zeta(s)}=-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}$.

Доказательство. $\ln\zeta(s)=\sum_p\ln(1-p^{-s})^{-1}$, следовательно,

$$\frac{\zeta'(s)}{\zeta(s)}=-\sum_p\frac{p^{-s}\ln p}{1-p^{-s}}=-\sum_p\sum_{k=1}^{\infty}\frac{\ln p}{p^{ks}}=-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

В теории чисел имеется много аналогичных соотношений.

Так, например,

$$\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}, Re(s)>1.$$

Квадрат дзета-фунуции связян с функцией делителей $\tau(n)=\sum_{d|n}1$, дающей число натуральных делителей натурального числа n:

$$\zeta^2(s)=\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s},\ Re(s)>1.$$

Действительно, $\zeta^2(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{m=1}^{\infty}\frac{1}{m^s}=\sum\sum_{n,m=1}^{\infty}\frac{1}{(nm)^s}=\sum_{k=1}^{\infty}\frac{\tau(k)}{k^s}$, где $k=nm$.

В общем случае,

$$\zeta^k(s)=\sum_{n=1}^{\infty}\frac{\tau_k(n)}{n^s},\ Re(s)>1,$$

где $\tau_k(n)=\sum_{n=n_1...n_k}1$ дает число представлений натурального числа n в виде произведения k натуральных множителей.

Лемма 4 (частное суммирование). Пусть $a_n\in\mathbb{C}$, $A(x)=\sum_{n\leq x}a_n$, $g(t)$-комплекснозначная функция, непрерывно-диффекенцируемая на $[1,\infty)$. Тогда

$$\sum_{n\leq x}a_ng(n)=A(x)g(x)-\int_1^x A(t)g'(t)dt.$$

Кроме того, если $\lim_{x\to\infty} A(x)g(x) = 0$, то

$$\sum_{n=1}^{\infty} a_n g(n) = -\int_1^{\infty} A(t)g'(t)dt,$$

если соответствующий ряд абсолютно сходится.

Доказательство.

Пусть $\phi_n(t) = 0$, если $t < n$, и $\phi_n(t) = a_n$, если $t \geq n$. Тогда, для любого $t \in [1, x]$,

$$\sum_{n\leq x} \phi_n(t) = \sum_{n\leq t} \phi_n(t) = \sum_{n\leq t} a_n = A(t),$$

и

$$\int_1^x A(t)g'(t)dt = \int_1^x (\sum_{n\leq x} \phi_n(t))g'(t)dt = \int_1^x \sum_{n\leq x} \phi_n(t)g'(t)dt =$$

$$= \sum_{n\leq x} \int_1^x \phi_n(t)g'(t)dt = \sum_{n\leq x} \int_n^x a_n g'(t)dt = \sum_{n\leq x} a_n \int_n^x g'(t)dt =$$

$$= \sum_{n\leq x} a_n(g(x) - g(n)) = A(x)g(x) - \sum_{n\leq x} a_n g(n).$$

Лемма 5. $\zeta(s)$ является аналитической функцией при $Re(s) > 0$, где она имеет единственный полюс с вычетом 1 в точке $s = 1$:

$$\zeta(s) = 1 + \frac{1}{s-1} - s\int_1^{\infty} \frac{\{x\}}{x^{s+1}}dx.$$

Доказательство.

Пусть $\sigma > 1$, $N \in \mathbb{N}$, $a_n = 1$, $g(x) = (x+N)^{-s}$. Тогда $A(x) = \lfloor x \rfloor$, $\lim_{x\to\infty} |A(x)g(x)| \leq \lim \frac{x}{(x+N)^{\sigma}} = 0$, и

$$\sum_{x=1}^{\infty} (x+N)^{-s} = -\int_1^{\infty} \lfloor t \rfloor ((t+N)^{-s})'dt = s\int_0^{\infty} (t - \{t\})(t+N)^{-s-1}dt =$$

$$= s\int_N^{\infty} (x - N - \{x - N\})x^{-s-1}dx = s(\int_N^{\infty} \frac{dx}{x^s} - N\int_N^{\infty} \frac{dx}{x^{s+1}} - \int_N^{\infty} \frac{\{x\}dx}{x^{s+1}}) =$$

$$= s(\frac{N^{1-s}}{s-1} - \frac{N^{1-s}}{s} - \int_N^{\infty} \frac{\{x\}dx}{x^{s+1}}) = \frac{N^{1-s}}{s-1} - s\int_N^{\infty} \frac{\{x\}dx}{x^{s+1}}.$$

Следовательно, для $\sigma > 1$ получаем, что $\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} + \frac{N^{1-s}}{s-1} - s\int_N^{\infty} \frac{\{x\}dx}{x^{s+1}}$.

Для $N = 1$, $\zeta(s) = 1 + \frac{1}{s-1} - s\int_1^{\infty} \frac{\{x\}dx}{x^{s+1}}$. Но $\int_1^{\infty} \frac{\{x\}dx}{x^{s+1}}$ - аналитическая функция для $\sigma > 0$. Действительно, $\int_1^{\infty} \frac{\{x\}dx}{x^{s+1}} = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{\{x\}dx}{x^{s+1}}$, $|\int_n^{n+1} \frac{\{x\}dx}{x^{s+1}}| \leq \int_n^{n+1} \frac{dx}{x_{\sigma+1}} \leq \frac{1}{n^{\sigma+1}}$, и ряд $\sum_{n=1}^{\infty} \frac{1}{n^{\sigma+1}}$ сходится для $\sigma > 0$, то есть, первый ряд абсолютно сходится для $\sigma > 0$, и равномерно сходится для $\sigma > \delta > 0$.

Следствие. Для $Re(s) = \sigma > 0$,

$$\zeta(s) = \sum_{n=1}^{N} n^{-s} + \frac{N^{1-s}}{s-1} - s\int_N^{\infty} \frac{\{x\}dx}{x^{s+1}}.$$

Более того, дзета-функция удовлетворяет следующему функциональному уравнению:

$$\zeta(s) = 2^s \pi^{s-1} \sin(\frac{\pi s}{2}) \Gamma(1-s)\zeta(1-s),$$

верному для всех s из $C \backslash \{0, 1\}$. Здесь Γ обозначает *гамма-функцию Эйлера*. Это функциональное уравнение используется для аналитического продолжения $\zeta(s)$ на всю комплексную плоскость.

Более симметричная версия функционального уравнения получится, если мы определим функцию $\varepsilon(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$. Тогда мы сможем записать функциональное уравнение в виде

$$\varepsilon(s) = \varepsilon(1-s).$$

Лемма 6. Пусть $s = \sigma + it$, $|t| \geq 3$, $1 \leq \sigma \leq 2$. Тогда

$$|\zeta(s)| \leq 6|\ln t|, \quad \text{и} \quad |\zeta'(s)| \leq 8 \ln^2 |t|.$$

Доказательство.

Пусть $N = \lfloor |t| \rfloor$. Тогда $|s-1| \geq 3$, и $N \leq |t| < N+1$, или, что то же, $N \leq |t|$, $N > |t| - 1$. Кроме того, $|s| = \sqrt{t^2 + \sigma^2} \leq |t| + \sigma \leq |t| + 2$.

I. Оценим каждый член в приведенной формуле для $\zeta(s)$. Прежде всего,

$$\sum_{n=1}^{N} n^{-s} \leq \sum_{n=1}^{N} n^{-\sigma} \leq \sum_{n=1}^{N} n^{-1} \leq 1 + \int_1^N \frac{dx}{x} = 1 + \ln N \leq 1 + \ln |t|.$$

Во-вторых,

$$|\frac{N^{1-s}}{s-1}| = \frac{N^{1-\sigma}}{|s-1|} \leq \frac{N^0}{3} = \frac{1}{3}.$$

Наконец,

$$|-s\int_N^\infty \frac{\{x\}dx}{x^{s+1}}| \leq |s| \int_N^\infty \frac{dx}{x^{\sigma+1}} \leq (|t|+2)\int_N^\infty \frac{dx}{x^2} = (|t|+2)\frac{1}{x}|_\infty^N =$$

$$= (|t|+2)\frac{1}{N} \leq \frac{|t|+2}{|t|-1} \leq 1 + \frac{3}{|t|-1} \leq 1 + \frac{3}{2} = 2.5.$$

Следовательно, $|\zeta(s)| \leq 4 + \ln |t| < 6 \ln |t|$.

II. Так как $(n^{-s})' = -\frac{\ln n}{n^s}$, $(\frac{N^{1-s}}{s-1})' = -\frac{N^{1-s}\ln N}{s-1} - \frac{N^{1-s}}{(s-1)^2}$, и $s\int_N^\infty \frac{\{x\}dx}{x^{s+1}})' = \int_N^\infty \frac{\{x\}dx}{x^{s+1}} - s\int_N^\infty \frac{\{x\}\ln x dx}{x^{s+1}}$, мы имеем:

$$\zeta'(s) = \sum_{n=1}^{N} \frac{\ln n}{n^s} - \frac{N^{1-s}\ln N}{s-1} - \frac{N^{1-s}}{(s-1)^2} - \int_N^\infty \frac{\{x\}dx}{x^{s+1}} + s\int_N^\infty \frac{\{x\}\ln x dx}{x^{s+1}}.$$

Оценим каждый член данной формулы.

1. $|-\sum_{n=1}^N \frac{\ln N}{n^s}| \leq \sum_{n=1}^N \frac{\ln n}{n^\sigma} < \sum_{n=1}^N \frac{\ln n}{n} = = \frac{\ln 2}{2} + \frac{\ln 3}{3} + \frac{\ln^2 x}{2}|_3^N < \frac{\ln 3}{3} + \frac{1}{2}\ln^2|t|$,
   так как $\frac{\ln 2}{2} - \frac{\ln^2 3}{2} < 0$.

2. $|-\frac{N^{1-s}\ln N}{s-1}| = \frac{N^{1-\sigma}\ln N}{|s-1|} \le \frac{\ln|t|}{3}$.

3. $|-\frac{N^{1-s}\ln N}{(s-1)^2}| \le \frac{1}{9}$.

4. $|-\int_N^\infty \frac{\{x\}dx}{x^{s+1}}| \le \int_N^\infty \frac{dx}{x^2} = \frac{1}{x}|_\infty^N = \frac{1}{N} \le \frac{1}{|t|-1} \le \frac{1}{2}$.

5. $|s\int_N^\infty \frac{\{x\}\ln x dx}{x^{s+1}}| \le |s|\int_N^\infty \frac{\ln x dx}{x^2} = |s|(\frac{\ln x}{x} + \frac{1}{x})|_\infty^N \le (|t|+2)(\frac{1}{|t|-1})(\ln|t|+1)$
   $\le 2.5(\ln|t|+1)$.

Следовательно,

$$|\zeta'(s)| \le \frac{1}{2}\ln^2|t| + (\frac{\ln 3}{3} + \frac{1}{9}) + \frac{1}{2q} + 2.5|t| + 2.5 \le$$

$$\le \frac{1}{2}\ln^2|t| + 4 + 3\ln|t| \le 8\ln^2|t|.$$

5.2 Нули дзета-функции Римана

Известно, что все четные отрицательные числа являются (тривиальными) нулями дзета-функции, и что все остальные (нетривиальные) нули дзета-функции принадлежат (критической) полосе $0 < Re(s) < 1$. Гипотеза Римана утверждает, что каждый нетривиальный нуль s имеет $Re(s) = 1/2$. В теории дзета-функции прямая $Re(s) = 1/2$ называется критической прямой.

Нули $\zeta(s)$ важны в аналитической теории чисел потому, что некоторые интегралы, содержащие функцию $ln(1/\zeta(s))$, могут быть использованы для приближения функции $\pi(x)$. Вычисление таких интегралов с помощью теоремы Коши о вычетах требует информации об особенностях подинтегральной функции.

Лемма 7. $\zeta(s) \ne 0$ для $\sigma > 1$.

Доказательство.
$|\frac{1}{\zeta(s)}| = |\prod_p(1-p^{-s})| = \prod_p|1-p^{-s}| \le \prod_p(1+|p^{-s}|) = \prod_p(1+p^\sigma) = \sum_{n|p_1\dots p_s\dots} n^{-\sigma}$
$< \sum_{n=1}^\infty n^{-\sigma} \le 1+\int_1^\infty \frac{du}{u^\sigma} = 1+\frac{u^{1-\sigma}}{1-\sigma}|_1^\infty = 1+\frac{1}{\sigma-1} = \frac{\sigma}{\sigma-1}$. Таким образом, $|\zeta(s)| \ge \frac{\sigma-1}{\sigma} > 0$.

Лемма 8. Для $0 \le r < 1$, $\phi \in \mathbb{R}$, мы имеем

$$|(1-r)^3(1-re^{i\phi})^4(1-re^{2i\phi})|^{-1} \ge 1.$$

Доказательство.
Известно, что, для $z \in \mathbb{C}$, $|z| < 1$, мы имеем $-\ln(1-z) = \sum_{n=1}^\infty \frac{z^n}{n}$.

Кроме того, если $z \in \mathbb{C}$, то $\ln|z| = Re(\ln z)$. Действительно, $z = |z|e^{i\phi}$, $\ln z = \ln|z| + i\phi$, и $Re(\ lnz) = \ln|z|$.

Теперь мы имеем:

$$\ln|(1-r)^3(1-re^{i\phi})^4(1-re^{2i\phi})|^{-1} =$$

$$= -3\ln|1-r| - 4\ln|1-re^{i\phi}| - \ln|1-re^{2i\phi}| =$$

$$= -3Re(\ln(1-r)) - 4Re(\ln(1-re^{i\phi})) - Re(\ln(1-re^{2i\phi})) =$$

$$= Re(3\sum_{n=1}^{\infty}\frac{r^n}{n} + 4\sum_{n=1}^{\infty}\frac{r^n e^{in\phi}}{n} + \sum_{n=1}^{\infty}\frac{r^n e^{2i\phi}}{n}) = Re(\sum_{n+1}^{\infty}\frac{r^n}{n}(3 + 4e^{in\phi} + e^{2in\phi})) =$$

$$= \sum_{n=1}^{\infty}\frac{r^n}{n}(3 + 4\cos n\phi + \cos 2n\phi) = \sum_{n+1}^{\infty}\frac{2r^n}{n}(1 + \cos n\phi)^2 \geq 0.$$

Следовательно, $|(1-r)^3(1-re^{i\phi})^4(1-re^{2i\phi})|^{-1} \geq 1$.

Лемма 9. $\zeta(1+it) \neq 0$.

Доказательство.

Достаточно рассмотреть $t \neq 0$. Пусть $\sigma > 1$. Тогда

$$|\zeta(\sigma)\zeta(\sigma+it)\zeta(\sigma+2it)| = \prod_p |(1-p^{-\sigma})(1-p^{-\sigma}p^{-it})(1-p^{\sigma}p^{-2it})|^{-1} \geq 1,$$

так как для $r = p^{-\sigma}$ и $e^{i\phi} = p^{-it\ln p}$ каждый множитель ≥ 1.

Рассмотрим фиксированное $t_0 \neq 0$. Пусть $\zeta(1+t_0) = 0$. Дзета-функция является аналитической в области $1+it_0$, следовательно, она разложима в ряд в некоторой окрестности точки $1+it_0$:

$$\zeta(\sigma+it_0) = a_0 + a_1(\sigma-1) + a_2(\sigma-1)^2 + ... = a_1(\sigma-1) + o(\sigma-1) = O(\sigma-1).$$

Следовательно, $\zeta(\sigma+it_0) = O(\sigma-1)$, если $\sigma \to 1$, для фиксированного t_0.

Мы знаем, что $\zeta(\sigma+2it_0)$ непрерывна, и, следовательно, ограничена.

Наконец, $|\zeta(\sigma)| \leq \sum_{n=1}^{\infty} n^{-\sigma} \leq 1 + \int_1^{\infty}\frac{dx}{x^{\sigma}} = 1 + \frac{x^{1-\sigma}}{1-\sigma}|_1^{\infty} = O(\frac{1}{\sigma-1})$.

Следовательно, $\zeta^3(\sigma)\zeta^4(\sigma+it_0)\zeta(\sigma+2it_0) = O(\frac{(\sigma-1)^4}{(\sigma-1)^3}) = O(\sigma-1)$, то есть, $\to 0$ для $\sigma \to 1$. Полученное противоречие завершает доказательство.

Лемма 10. Для $s = \sigma + it$, $|t| \geq 3$, $1 \leq \sigma \leq 2$, мы имеем:

$$|\frac{\zeta'(s)}{\zeta(s)}| \leq c\ln^9|t|, \text{ где } c = 2^{23}.$$

Доказательство.

I. Пусть $\sigma_1 = 1 + \frac{1}{c\ln^9|t|}$, и $\sigma_1 \leq \sigma \leq 2$. Здесь $|\zeta(\sigma)| \leq \frac{2}{\sigma-1} \leq 2c\ln^9|t|$.

Кроме того, $|\zeta(\sigma+2it)| \leq 6\ln 2|t| \leq 12\ln|t| < 16\ln|t|$. Тогда

$$|\zeta(\sigma+it)| \geq |\zeta(\sigma)|^{-3/4}|\zeta(\sigma+2it)|^{-1/4} \geq (2c\ln^9|t|)^{-3/4}(16\ln|t|)^{-1/4} =$$

$$= 2^{-7/4}c^{1/4}c^{-1}\ln^{-7}|t| \leq 16c^{-1}\ln^{-7}|t|.$$

II. Пусть $1 \leq \sigma \leq \sigma_1$. В этом случае

$$|\zeta(\sigma_1+it) - \zeta(\sigma+it)| = |\int_{\sigma}^{\sigma_1}\zeta'(u+it)du| \leq 8(\sigma_1-\sigma)\ln^2|t| \leq 8c^{-1}\ln^{-7}|t|.$$

Тогда

$$|\zeta(\sigma+it) \geq |\zeta(\sigma_1+it)| - |\zeta(\sigma_1+it) - \zeta(\sigma+it)| \geq 16c^{-1}\ln^{-7}|t| - 8c^{-1}\ln^{-7}|t|,$$

и мы получаем утверждение леммы.

5.3 Утверждения, эквивалентные асимптотическому закону распределения простых чисел

Рассмотрим три утверждения.

1. $\pi(x) = \frac{x}{\ln x} + o(\frac{x}{\ln x})$, где $\pi(x) = \sum_{p \le x} 1$.

2. $\psi(x) = x + o(x)$, где $\psi(x) = \sum_{n \le x} \Lambda(n) = \sum_{p^k \le x} \ln p$.

3. $\omega(x) = x + o(x)$, где $\omega(x) = \int_1^x \frac{\psi(t)}{t} dt = \sum_{n \le x} \Lambda(n) \ln \frac{x}{n}$.

Лемма 11. Все три приведенных утверждения эквивалентны.

Доказательство.

I. Покажем, что $3 \Rightarrow 2$.

a). Для $\epsilon > 0$ мы имеем $\omega((1+\epsilon)x) - \omega(x) = \int_x^{(1+\epsilon)x} \frac{\psi(t)}{t} dt \ge \psi(x)(\ln((1+\epsilon)x) - \ln x)$, и $\frac{\psi(x)}{x} \le \frac{\frac{\omega((1+\epsilon)x)-\omega(x)}{x}}{\ln(1+\epsilon)}$, следовательно, $\overline{\lim \frac{\psi(x)}{x}} \le \frac{\epsilon}{\ln(1+\epsilon)}$, то есть, $\overline{\lim \frac{\psi(x)}{x}} \le 1$.

b). Для $\epsilon > 0$ мы имеем $\omega(x)\omega((1-\epsilon)x) = \int_{(1-\epsilon)x}^x \frac{\psi(t)}{t} dt \le \psi(x)(\ln x \ln((1-\epsilon)x))$, и $\underline{\lim \frac{\psi(x)}{x}} \ge \frac{\epsilon}{\ln(1+\epsilon)}$, то есть, $\underline{\lim \frac{\psi(x)}{x}} \ge 1$.

Теперь мы получаем, что $\underline{\lim \frac{\psi(x)}{x}} = \overline{\lim \frac{\psi(x)}{x}} = 1$.

2. Покажем, что $2 \Rightarrow 1$.

a). $\psi(x) = \sum_{p \le x} \ln p + \sum_{p^2 \le x} \ln p + ... \le \pi(x) \ln x + \pi(\sqrt{x}) \ln \sqrt{x} + ... = \ln \pi(x) + o(x)$, то есть, $\frac{\pi(x)}{x/\ln x} \ge \frac{\psi(x)}{x} + o(1)$, и $\underline{\lim \frac{\pi(x)}{x/\ln x}} \ge 1$.

b). Для $0 < \lambda < 1$ мы имеем $\overline{\psi(x)} \ge \sum_{p \le x} \ln p \ge \sum_{x^\alpha < p \le x} \ln p \ge \ln x^\alpha (\pi(x) - \pi(x^\alpha))$, то есть, $\frac{\pi(x)}{x/\ln x} \le \frac{1}{\alpha} \frac{\psi(x)}{x} + \frac{\ln x}{x^{1-\alpha}}$, и $\overline{\lim \frac{\pi(x)}{x/\ln x}} \le \frac{1}{\alpha}$, то есть, ≤ 1.

Утверждение получается теперь аналогичным образом.

5.4 Формулы для $\omega(x)$

Лемма. Для $a > 0, b > 0$, мы имеем

$$I = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \frac{b^s}{s^2} ds = \begin{cases} \ln b, & b \ge 1, \\ 0, & 0 < b < 1. \end{cases}$$

Доказательство. Пусть $s = a + it$. Так как $|\frac{b^s}{s^2}| = \frac{b^a}{a^2+t^2}$, и $\int_{\infty}^{+\infty} \frac{dt}{a^2+b^2} = \frac{1}{a} arctg \frac{t}{a}|_{-\infty}^{+\infty} = \frac{\pi}{a^2}$, то $|I| \le \frac{b^a}{2a^2} = const$, то есть, интеграл I абсолютно сходится.

1. Рассмотрим случай $b \ge 1$. Пусть u - фиксированное число. Построим контур Γ из части C_1 окружности $|s| = \sqrt{a^2+u^2}$ с условием $Re(s) \le a$, и соответствующей части прямой $Re(s) = a$. Функция $\frac{b^2}{s^2} = \frac{e^s \ln b}{s^2} = \frac{1}{s^2} + \frac{\ln b}{s} + \frac{\ln^2 b}{2} + ...$ имеет в точке $s = 0$ полюс второго порядка с вычетом $\ln b$ (напомним, что $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} ...$). Тогда $\frac{1}{2\pi i} \int_\Gamma \frac{b^s}{s^2} ds = \ln b$, то есть, $\frac{1}{2\pi i} \int_{a-iu}^{a+iu} \frac{b^s}{s^2} ds = \ln b - \frac{1}{2\pi i} \int_{C_1} \frac{b^s}{s^2} ds$.

Обозначим $J = \frac{1}{2\pi i} \int_{C_1} \frac{b^s}{s^2} ds$. Здесь $|b^s| = b^{Re(s)} \le b^a$; $|s|^2 = a^2 + u^2$. Так как $\int_{C_1} ds \le \int_{circle} ds = 2\pi\sqrt{a^2+u^2}$, то $|J| \le \frac{b^a}{\sqrt{a^2+u^2}} \le \frac{b^a}{u} \to 0$ при $u \to \infty$. Следовательно, $\frac{1}{2\pi i} \int_{a-i\infty}^{a+ß\infty} \frac{b^s}{s^2} ds = \ln b$.

2. Рассмотрим случай $0 < b < 1$. Пусть C_2 определена как часть окружности $|s| = \sqrt{a^2+u^2}$ с $Re(s) \geq a$. Мы получим утверждение леммы аналогичным образом, используя тот факт, что для C_2 мы имеем $|b^s| = b^{Re(s)} \leq b^a$, так как $b < 1$.

Лемма 12. $\omega(x) = \sum_{n\leq x} \Lambda(n) \ln \frac{x}{n}$.

Доказательство. Используя частное суммирование, имеем: $\sum_{n\leq x} \Lambda(n) \ln \frac{x}{n} = \psi(x) \ln \frac{x}{x} - \int_1^x \psi(t)(\ln \frac{x}{t})' dt = \int_1^x \frac{\psi(t)}{t} dt = \omega(x)$, так как $(\ln \frac{x}{t})'_t = -\frac{1}{t}$.

Лемма 13. Для $a > 1$, $x \geq 2$, имеем:

$$\omega(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} (-\frac{\zeta'(s)}{\zeta(s)}) \frac{x^s}{s^2} ds.$$

Доказательство. Обозначим данный интеграл через I. Пусть $s = a + it$. Для $a > 1$, $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$, и $|-\frac{\zeta'(s)}{\zeta(s)}| \leq \sum_{n=1}^{\infty} \frac{\ln n}{n^a} = const$; $|x^s| = a^2 + t^2$; и $\int_{-\infty}^{+\infty} \frac{dt}{a^2+t^2} = \frac{1}{a} arctg \frac{t}{a}|_{-\infty}^{+\infty} = \frac{\pi}{a^2}$. Следовательно, $|I| \leq C \frac{x^a}{2a^2} + const$, то есть, I абсолютно сходится.

Кроме того, если $a > 1$, то
$\frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \sum_{n=1}^{\infty} \Lambda(n) \frac{(x/a)^s}{s^2} ds = \sum_{n=1}^{\infty} \Lambda(n) (\frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \frac{(x/n)^s}{s^2} ds) = \sum_{n=1}^{x} \Lambda(n) \ln \frac{x}{n} = \omega(x)$, так как последний интеграл равен $\ln \frac{x}{n}$ для $\frac{x}{n} \geq 1$, то есть, для $n \leq x$, и $= 0$, иначе.

Можно показать, что, для $a > 1$ и $x > 1$, мы имеем $\psi(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} (-\frac{\zeta'(s)}{\zeta(s)}) \frac{x^s}{s} ds$, но данный интеграл не является абсолюьно сходящимся, что затрудняет рассуждения.

5.5 Доказательство асимптотического закона распределения простых чисел

Лемма 14. Пусть $\zeta(s) \neq 0$ в некотором прямоугольнике $\eta \leq \sigma \leq 1$, $-T \leq t \leq T$, где $0 < \eta < 1$, и $T > 0$. Тогда

$$\omega(x) = x(1 + R(x)),$$

где

$R(x) = \frac{1}{2\pi i} \int_{\Gamma(\eta,T)} (-\frac{\zeta'(s)}{\zeta(s)}) \frac{x^{s-1}}{s^2} ds$, и $\Gamma(\eta, T)$ - ломаная, состоящая из отрезков прямых $s = 1 + it$, $s = \sigma + iT$, $s = \eta + it$, $s = \sigma - iT$, $s = 1 - it$, соответственно.

Доказательство. Рассмотрим контур Γ многоугольника $ABCDEFGHA$, где AB - отрезок прямой $s = 2 + it$, BC и HA - отрезки прямых $s = \sigma \pm iU$, $U > T$, соответственно, CD и GH - верхняя и нижняя части отрезка прямой $s = 1 + it$, ED и FG - отрезки прямых $s = \sigma \pm iT$, соответественно, и EF - отрезок прямой $s = \eta + it$.

Легко видеть, что $\frac{1}{2\pi i} \int_{\Gamma} (-\frac{\zeta'(s)}{\zeta(s)}) \frac{x^s}{s^2} ds = x$. Действительно, внутри контура Γ имеется только одна специальная точка $s = 1$. Так как $\zeta(s) = \frac{1}{s-1} + f(s)$, мы имеем, что $\zeta'(s) = -\frac{1}{(s-1)^2} + f'(s)$, и $-\frac{\zeta'(s)}{\zeta(s)} = \frac{1-f'(s)(s-1)^2}{1+f(s)(s-1)} \cdot \frac{1}{s-1}$. Следовательно, вычет подинтегральной функции равен

$$Res_{s=1} (-\frac{\zeta'(s)}{\zeta(s)}) \frac{x^s}{s^2} = \lim_{s\to 1} (s-1) (\frac{1 - f'(s)(s-1)^2}{1 + f(s)(s-1)} \cdot \frac{1}{s-1} \cdot \frac{x^s}{s^2}) = x.$$

Оценим теперь интегралы J_1 и J_2 по сторонам CB и AH. Именно,

$$\max\{|J_1|, |J_2|\} \leq \int_1^2 |-\frac{\zeta(\sigma \pm iU)}{\zeta(\sigma \pm iU)}| \frac{x^\sigma}{\sigma^2 + U^2} d\sigma \leq c\ln^9 U \cdot \frac{x^2}{U^2},$$

и $c\ln^9 U \cdot \frac{x^2}{U^2} \to 0$ при $U \to +\infty$.

Кроме того, $\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}(-\frac{\zeta'(s)}{\zeta(s)})\frac{x^s}{s^2}ds = \omega(x)$.

Следовательно,

$$-\frac{1}{2\pi i}\int_\Gamma(-\frac{\zeta'(s)}{\zeta(s)})\frac{x^s}{s^2}ds + \omega(x) = x,$$

и

$$\omega(x) = x + \frac{1}{2\pi i}\int_\Gamma(-\frac{\zeta'(s)}{\zeta(s)})\frac{x^s}{s^2}ds = x(1 + R(x)).$$

Theorem 7 $\omega(x) = x + o(x)$.

Доказательство. В свете предыдущего результата, мы должны показать только, что $R(x) = o(1)$.

1. Пусть $s = 1 + it$. Тогда $|\frac{\zeta(1+it)}{\zeta(1+it)} \cdot \frac{x^{it}}{(1+it)^2}| \leq \frac{c\ln^9|t|}{1+t^2}$, и существует $T = T(\epsilon)$, такое что

$$\max\{|J_1|, |J_2|\} \leq \int_T^\infty \frac{c\ln^9 t}{1+t^2}dt < \frac{\epsilon}{5}$$

(так как последний интеграл стремится к 0 с ростом T), где J_1 и J_2 - интегралы по сторонам $s = 1 \pm it$, $t \geq T$.

2. Функция $|\frac{\zeta'(s)}{\zeta(s)} \cdot \frac{1}{s^2}|$ является непрерывной на линии интегрирования, так как здесь $\zeta(s) \neq 0$, и $s \neq 0$, таким образом, существует $M = M(T, \eta)$, такое что $|\frac{\zeta'(s)}{\zeta(s)} \cdot \frac{1}{s^2}| \leq M$, и

$$\max\{|J_3|, |J_4|\} \leq M\int_\eta^1 x^{\sigma-1}d\sigma \leq M\int_\infty^1 x^{\sigma-1}d\sigma = M\frac{x^{\sigma-1}}{\ln x}|_{-\infty}^1 = \frac{M}{\ln x},$$

где J_3 и J_4 - интергалы по сторонам $s = \sigma \pm iT$, соответственно. Таким образом, существует $x_0 = x_0(M, T, \eta)$, такое что для любого $x > x_0$ мы имеем $|J_3| < \frac{\epsilon}{5}$, и $|J_4| < \frac{\epsilon}{5}$.

3. Наконец,

$$|J_5| \leq M\int_{-T}^T x^{\eta-1}dt \leq Mx^{\eta-1} \cdot 2T,$$

и $Mx^{\eta-1} \cdot 2T \to 0$ при $x \to \infty$ для фиксированного T, где J_5 - интеграл по строне EF. Тогда существует $x_1 = x_1(M, T, \eta)$, такое что, для любого $x > x_1$, мы имеем $|J_5| < \frac{\epsilon}{5}$.

Следовательно, мы получаем, что $|R(x)| < \epsilon$, то есть, утверждение теоремы доказано.

Упражнения

1. Доказать, что если f является вполне мультиплкативной функцией, и $\sum_{n=1}^\infty f(n)$ абсолютно сходится для $Re(s) > 1$, то $\sum_{n=1}^\infty f(n) = \prod_p(1 - f(p))^{-1}$.

2. Доказать, что, для $Re(s) > 1$, $\frac{1}{\zeta(s)} = \sum_{n=1}^\infty \frac{\mu(n)}{n^s}$.

3. Доказать, что, для $Re(s) > 1$, $\zeta^k(s) = \sum_{n=1}^\infty \frac{\tau_k(n)}{n^s}$, где $\tau_k(n) = \sum_{n=n_1\dots n_k} 1$ дает число представлений натурального n в виде произведения k натуральных множителей.

6 Теорема Дирихле о бесконечности простых чисел в арифметических прогрессиях

Теорема Дирихле утверждает, что, для любых взаимно-простых натуральных чисел a и b, существует бесконечно много простых чисел вида $a + bx$, где $x > 0$, или, другими словами, существует бесконечно много простых чисел, сравнимых с a по модулю b.

Эйлер утверждал, что любая арифметическая прогрессия, начинающаяся с 1, содержит бесконечно много простых чисел. В общем виде теорема была сформулирована Гауссом, и доказана Дирихле (1837) с использованием L-рядов Дирихле.

6.1 Характеры Дирихле

.

Характер Дирихле по модулю n представляет собой комплекснозначную функцию χ целого аргумента, удовлетворяюшую следующим свойствам:

1. $\chi(a) = \chi(a + n)$ для всех целых a.
2. $\chi(a) = 0$ для любого a с $gcd(a, n) > 1$.
3. $\chi(ab) = \chi(a)\chi(b)$ для всех целых a и b.
4. $\chi(1) = 1$.

Условие 1 утверждает, что характер Дирихле - периодическая функция с периодом n. Условия 3 и 4 утверждают, что характер Дирихле - вполне мультипликативная функция.

Единственный характер по модулю 1 называется *тривиальным*. Любой характер, кроме тривиального, равен 0 в точке 0, в то время как тривиальный характер равен 1 для всех целых чисел. Характер называется *главным*, если он имеет значение 1 для всех значений аргумента, взаимно-простых с модулем, и равен 0, иначе. Характер называется *действительным*, если он принимает только действительные значения. В противном случае характер называется *комплексным*.

Можно показать, что $\chi(a)$ является $\phi(n)$-ым корнем из единицы, если a и n взаимно-просты, где $\phi(n)$ - функция Эйлера.

Если $n > 1$ - натуральное число, то числа, взаимно-простые с n, формируют группу по умножению по модулю n; она обозначается символом $(Z/nZ)^*$. Эта группа является циклической если и только если n равно $1, 2, 4, p^k$ или $2p^k$ для некоторого простого $p \geq 3$ и некоторого натурального $k \geq 1$. Образующим элементом этой группы является первообразный корень по модулю n, который называется также примитивным элементом группы Z_n^*.

Не существует простых формул для вычисления первообразных корней по модулю n. Однако существуют некоторые методы определения первообразных корней, более продуктивные, чем простой перебор кандидатов. Число m является первообразным корнем по модулю n, если его показатель по данному модулю равен $\phi(n)$ (порядку $(Z/nZ)^*$), что можно использовать для определения примитивных корней.

Во-первых, вычислим $\phi(n)$. Во-вторых, определим простые делители $\phi(n)$, скажем $p_1, ..., p_k$. Теперь, для любого элемента m множества $(Z/nZ)^*$, вычислим $m^{\phi(n)/p_i}$,

$i = 1, ..., k$. Число m, для которого эти k результатов отличны от 1, является примитивным корнем.

Число примитивных корней по модулю n, если они существуют, равно $\phi(\phi(n))$, так как циклическая группа из r элементов имеет $\phi(r)$ образующих.

Таким образом, если g является первообразным корнем по модулю n, $n \in \{2, 4, p^\alpha, 2p^\alpha\}$, то любое $a \in (Z/nZ)^*$ равно g^γ, где $\gamma \in \{0, ..., \phi(n) - 1\}$. Число γ называется *индексом a по модулю n с основанием g*.

Легко показать, что, для $n = 2^\alpha$, $\alpha \geq 3$, числа $\pm 5^0, ..., \pm 5^{2^{\alpha-2}-1}$ представляют все классы вычетов по модулю 2^α, взаимно-простые с модулем 2^α, то есть, любое нечетное a можно представить как $a \equiv (-1)^\gamma 5^{\gamma_0} (mod 2^\alpha)$; в этом случае пара (γ, γ_0) называется *индексом числа a по модулю 2^α*.

Если $n = 2^\alpha p_1^{\alpha_1} ... p_k^{\alpha_k}$, мы получим систему индексов $(\gamma, \gamma_0, \gamma_1, ..., \gamma_k)$ данного числа a, взаимно-простого с n, вычисляя индексы (γ, γ_0) по модулю 2^α, γ_1 по модулю $p_1^{\alpha_1}$ (с первообразным корнем g_1), ..., γ_k по модулю $p_k^{\alpha_k}$ (с первообразным корнем g_k).

Пусть $c = 1$, $c_0 = 1$, если $\alpha = 0$ или $\alpha = 1$; пусть $c = 2$, $c_0 = 2^{\alpha-2}$, если $\alpha \geq 2$. Пусть $c_i = \phi(p_i^{\alpha_1})$ для $i = 1, ..., k$.

Рассмотрим систему $(R, R_0, R_1, ..., R_k)$ некоторых корней уравнений $R^c = 1$, $R_0^{c_0} = 1$, $R_1^{c_1} = 1$,..., $R_k^{c_k} = 1$.

Теперь, если мы определим $\chi(a) = R^\gamma R_0^{\gamma_0} R_1^{\gamma_1} ... R_k^{\gamma_k}$ для любого a, взаимно-простого с n (и $\chi(a) = 0$, в остальных случаях), то функция $\chi(a)$ будет характером Дирихле по модулю n, и все характеры Дирихле по модулю n могут быть получены этим способом.

Напомним, что главный характер по модулю n, обозначаемый χ_0, определяется как $\chi_0(a) = 1$, если $gcd(a, n) = 1$, и как $\chi_0(a) = 0$, если $gcd(a, n) > 1$.

Мы имеем ровно один $(1 = \phi(2))$ характер Дирихле по модулю 2, который является главным характером: $\chi_0(a) = 1$ для нечетного a, и $\chi_0(a) = 0$ для четного a.

Мы имеем ровно два $(2 = \phi(3))$ характера Дирихле по модулю 3.

Главный характер $\chi_0(a) = 1$ для $a \equiv 1, 2 (mod 3)$, и $\chi_0(a) = 0$ для $a \equiv 0 (mod 3)$.

Неглавный характер $\chi_1(a) = 1$ для $a \equiv 1 (mod 3)$, $\chi_1(a) = -1$ для $a \equiv -1 (mod 3)$, и $\chi_1(a) = 0$ для $a \equiv 0 (mod 3)$.

Для получения этого результата мы рассмотрим $n = 3$ как $n = p_1$, возьмем первообразный корень $g_1 = 2$ по модулю p_1, и найдем систему индексов (γ_1) для любого a, взаимно-простого с p_1. Легко видеть, что $\gamma_1(a) = 0$ для $a \equiv 1 (mod 3)$ (так как $2^0 \equiv a (mod 3)$), и $\gamma_1(a) = 1$ для $a \equiv -1 (mod 3)$ (так как $2^1 \equiv a (mod 3)$). Беря $c_1 = \phi(p_1) = 2$, мы найдем $R_1 \in \{1, -1\}$, где R_1 - решение уравнения $R_1^{c_1} = 1$. Выбирая $R_1 = 1$, мы получим χ_0. Выбирая $R_1 = -1$, мы получим χ_1: для $a \equiv 1 (mod 3)$, $\chi_1(a) = (-1)^{\gamma_1(a)} = (-1)^0 = 1$, и для $a \equiv -1 (mod 3)$, $\chi_1(a) = (-1)^{\gamma_1(a)} = (-1)^1 = -1$.

Мы имеем ровно два $(2 = \phi(4))$ характера Дирихле по модулю 4.

Главный характер $\chi_0(a) = 1$ для $a \equiv 1, -1 (mod 4)$, то есть, для a нечетного, и $\chi_0(a) = 0$ для $a \equiv 0, 2 (mod 4)$, то есть, для a четного.

Неглавный характер $\chi_1(a) = 1$ для $a \equiv 1 (mod 4)$, $\chi_1(a) = -1$ для $a \equiv -1 (mod 4)$, и $\chi_1(a) = 0$ для $a \equiv 0, 2 (mod 4)$.

Для получения этого результата рассмотрим $n = 4$ как $n = 2^2$, и найдем систему индексов (γ, γ_0) для любого a, взаимно-простого с 2^2. Легко видеть, что $(\gamma(a), \gamma_0(a)) = (0, 0)$ для $a \equiv 1 (mod 4)$ (так как $a = (-1)^0 5^0 (mod 4)$), и $(\gamma(a), \gamma_0(a)) = (1, 0)$

для $a \equiv -1(mod4)$ (так как $a \equiv (-1)^1 5^0 (mod4)$). Беря $c = 2$, $c_0 = 2^{2-2} = 1$, мы найдем системы $(R, R_0) \in \{(1,1), (-1,1)\}$, где R - решение уравнения $R^c = 1$, и R_0 - решение уравнения $R_0^{c_0} = 1$. Выбирая $(R, R_0) = (1,1)$, мы получим χ_0. Выбирая $(R, R_0) = (-1,1)$, мы получим χ_1: для $a \equiv 1(mod4)$, $\chi_1(a) = R^{\gamma(a)} R_0^{\gamma_0(a)} = (-1)^0 = 1$, и для $a \equiv -1(mod4)$, $\chi_1(a) = R^{\gamma(a)} R_0^{\gamma_0(a)} = (-1)^1 = -1$.

Мы имеем ровно $(4 = \phi(5))$ характера Дирихле по модулю 5.

Главный характер $\chi_0(a) = 1$ для $a \neq 0(mod5)$, и $\chi_0(a) = 0$ для $a \equiv 0(mod5)$.

Первый неглавный характер $\chi_1(a) = 1$ для $a \equiv 1, 4(mod5)$, и $\chi_1(a) = -1$ для $a \equiv 2, 3(mod5)$.

Второй неглавный характер $\chi_2(a) = 1$ для $a \equiv 1(mod5)$, $\chi_1(a) = i$ для $a \equiv 2(mod5)$, $\chi_2(a) = -i$ для $a \equiv 3(mod5)$, и $\chi_2(a) = -1$ для $a \equiv 4(mod5)$.

Третий неглавный характер $\chi_3(a) = 1$ для $a \equiv 1(mod5)$, $\chi_3(a) = -i$ для $a \equiv 2(mod5)$, $\chi_1(a) = i$ для $a \equiv 3(mod5)$, и $\chi_1(a) = -1$ для $a \equiv 4(mod5)$.

Для получения этого результата запишем $n = 5$ как $n = p_1$, возьмем первообразный корень $g_1 = 2$ по модулю p_1, и найдем системы индексов (γ_1) для всех a, взаимно-простых с p_1. Легко видеть, что $\gamma_1(a) = 0$ для $a \equiv 1(mod5)$ (так как $2^0 \equiv a(mod5)$), $\gamma_1(a) = 1$ для $a \equiv 2(mod5)$ (так как $2^1 \equiv a(mod5)$), $\gamma_1(a) = 3$ для $a \equiv 3(mod5)$ (так как $2^3 \equiv a(mod5)$), и $\gamma_1(a) = 2$ для $a \equiv 4(mod5)$ (так как $2^2 \equiv a(mod5)$). Беря $c_1 = \phi(p_1) = 4$, мы найдем $R_1 \in \{1, -1, i, -i\}$, где R_1 - решение уравнения $R_1^{c_1} = 1$. Теперь, выбирая $R_1 = 1$, мы получим χ_0. Выбирая $R_1 = -1$, мы получим χ_1: для $a \equiv 1(mod5)$, $\chi_1(a) = (-1)^{\gamma_1(a)} = (-1)^0 = 1$, для $a \equiv 2(mod5)$, $\chi_1(a) = (-1)^{\gamma_1(a)} = (-1)^1 = -1$, для $a \equiv 3(mod5)$, $\chi_1(a) = (-1)^{\gamma_1(a)} = (-1)^3 = -1$, для $a \equiv 4(mod5)$, $\chi_1(a) = (-1)^{\gamma_1(a)} = (-1)^2 = 1$. Выбирая $R_1 = i$, мы получим χ_2: для $a \equiv 1(mod5)$, $\chi_2(a) = i^{\gamma_1(a)} = i^0 = 1$, для $a \equiv 2(mod5)$, $\chi_2(a) = i^{\gamma_1(a)} = i^1 = i$, для $a \equiv 3(mod5)$, $\chi_2(a) = i^{\gamma_1(a)} = i^3 = -i$, для $a \equiv 4(mod5)$, $\chi_2(a) = i^{\gamma_1(a)} = i^2 = -1$. Выбирая $R_1 = -i$, мы получим χ_3: для $a \equiv 1(mod5)$, $\chi_3(a) = (-i)^{\gamma_1(a)} = (-i)^0 = 1$, для $a \equiv 2(mod5)$, $\chi_3(a) = (-i)^{\gamma_1(a)} = (-i)^1 = -i$, для $a \equiv 3(mod5)$, $\chi_3(a) = (-i)^{\gamma_1(a)} = (-i)^3 = i$, для $a \equiv 4(mod5)$, $\chi_3(a) = (-i)^{\gamma_1(a)} = (-i)^2 = -1$.

Свойства характеров Дирихле

1. Число характеров Дирихле по модулю n равно $\phi(n)$.
2. $\chi(a)$ является корнем степени $\phi(n)$ из единицы.
3. $|\chi(a)| \leq 1$.
4. $\sum_{\chi} \chi(a) = \phi(n)$, если $a \equiv 1(modn)$, и $= 0$, иначе.
5. $\sum_{o \leq a < m} \chi(a) = \phi(n)$, если $\chi = \chi_0$, и $= 0$, иначе.
6. $|\sum_{a \leq x} \chi(a)| \leq n$ для $\chi \neq \chi_0$.

Упражнения

1. Доказать, что два определения характеров Дирихле, рассмотренные выше, являются эквивалентными.

2. Доказать, что, для данного простого p, символ Лежандра $(\frac{a}{p})$ является характером Дирихле.

3. Построить все характеры Дирихле по модулю 6, модулю 7, модулю 8.

4. Доказать представленные выше свойства характеров Дирихле.

6.2 L-функции Дирихле

Для данного натурального n и данного характера Дирихле $\chi(n)$ по модулю n, рассмотрим так называемую *L-функцию Дирихле*, которая определяется, для $Res > 1$, как следующий ряд Дирихле:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Свойства L-функций Дирихле

1. $L(s,\chi_0)$ является аналитической функцией в области $Re(s) > 1$, и имеет единственный полюс в точке $s = 1$.

2. $L(s,\chi)$ для $\chi \neq \chi_0$ является аналитической в области $Re(s) > 0$.

3. Для $Re(s) > 1$, $L(s,\chi) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}$.

4. Для $Re(s) > 1$, $-L'(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n^s}$.

5. Для $Re(s) > 1$, $-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n-1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}$.

6. $L(s,\chi_0) = \zeta(s)\prod_{p|n}(1-\frac{1}{p^s})$. (Это показывает, что $L(s,\chi_0)$ имеет полюс в точке $s = 1$ с вычетом $\prod_{p|n}(1 - \frac{1}{p})$.)

7. $L(s,\chi) \neq 0$ для $Re(s) > 1$.

8. $L(1,\chi) \neq 0$ для $\chi \neq \chi_0$.

Упражнения

1. Доказать указанные выше свойства L-функций.

2. Построить все L-функции Дирихле по модулю 4, по модулю 5, по модулю 6.

6.3 Доказательство теоремы Дирихле для простейшего случая

В этом разделе мы рассмотрим доказательство теоремы Дирихле для простейших арифметических прогрессий $4x + 1$ и $4x - 1$.

Для $n = 4$, мы имеем ровно два характера. Именно, $\chi_0(n) = 1$ для нечетного n, и $\chi_0(n) = 0$, иначе; $\chi_1(n) = 1$ для $n \equiv 1(mod4)$, $\chi_1(n) = -1$ для $n \equiv -1(mod4)$, и $\chi_1(n) = 0$, иначе.

Theorem 8 *Множество простых вида $4k-1$ бесконечно; множество простых чисел вида $4k+1$ бесконечно.*

Доказательство.

I. Элементарное доказательство.

Для случая простых чисел вида $4k-1$, мы можем применить метод Евклида. Именно, любое натуральное число вида $4k-1$ имеет простой делитель того же вида: такое число $\neq 1$ и является нечетным, следовательно, имеет простой делитель, не равный 2, то есть, простой делитель вида $4k-1$, или вида $4k+1$. Если все простые делители числа n имеют вид $4k+1$, то и само число n должно иметь вид $4k+1$, противоречие.

Предполагая, что множество простых чисел вида $4k-1$ конечно, и что $p_1, ..., p_k$ - все такие простые, рассмотрим число $E = 4p_1...p_k - 1$. Это число имеет вид $4m-1$ и, следовательно, имеет простой делитель p того же вида. Тогда $p = p_i$ для некоторого p_i, и, следовательно, $p|p_1...p_k$, то есть, $p|1$, противоречие.

Для простых чисел вида $4k+1$ метод Евклида неприменим, так как некоторые числа вида $4k+1$ имеют только простые делители вида $4k-1$, например, число 25. В этом случае, предполагая, что множество простых чисел вида $4k+1$ конечно, и что $q_1, ...q_s$ - все такие числа, рассмотрим число $E = 4(q_1...q_k)^2 + 1$. Пусть $p|E$. Тогда $p \neq 2$, и $(2q_1...q_s)^2 \equiv -1(mod p)$, то есть, -1 является квадратичным вычетом по модулю p, следовательно, $p \equiv 1(mod 4)$. Тогда $p = q_i$ для некоторого $i = 1, .., s$, и $p|q_1...q_s$, то есть, $p|1$, противоречие.

II. Аналитическое доказательство.

Рассмотрим функции $L_i(s) = \sum_{n=1}^{\infty} \frac{\chi_i(n)}{n^s}$ для $i = 0$ и 1, то есть,

$$L_0(s) = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^s}, \quad \text{и} \quad L_1(s) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s}.$$

Легко видеть, что оба ряда абсолютно сходятся для $Re(s) > 1$, а второй сходится и для $Re(s) > 0$.

Кроме того, $L_1(1) = 1 - \frac{1}{3} + \frac{1}{5}... > 1 - \frac{1}{3} = \frac{2}{3}$, то есть, $L_1(1) = const \neq 0$.

С другой стороны, $L_0(s) \geq \frac{1}{2}\int_0^{\infty} \frac{d(2x+1)}{(2x+1)^s} = \frac{1}{2}\frac{(2x+1)^{1-s}}{1-s}|_0^{\infty} = \frac{1}{2(s-1)}$, и $\frac{1}{2(s-1)} \to \infty$ при $s \to 1+$, то есть, $L_0(s) \to \infty$ при $s \to 1+$.

Так как $\sum_{n=1}^{\infty} \frac{\chi_i(n)}{n^s} = \prod_p (1 - \frac{\chi_i(p)}{p^s})^{-1}$, то $\ln L_i(s) = -\sum_p \ln(1 - \frac{\chi(p)}{p^s}) = \sum_p \sum_{k=1}^{\infty} \frac{(\chi(p))^k}{kp^{ks}}$, и $-\frac{L_i'(s)}{L_i(s)} = \sum_{n=2}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}$. Следовательно, $-\frac{L_i'(s)}{L_i(s)} = \sum_p \frac{\ln p\chi(p^k)}{p^{ks}} = \sum_p \frac{\ln p\chi(p)}{p^s} + \sum_p \sum_{k=2}^{\infty} \frac{\ln p\chi(p^k)}{p^{ks}}$. Модуль второй суммы (для всех $k \geq 2$) $\leq \sum_p \sum_{k=2}^{\infty} \frac{\ln p}{p^{k\sigma}} = \sum_p \ln p(\frac{1}{p^{2\sigma}} + \frac{1}{p^{3\sigma}} + ...) = \sum_p \ln p \frac{p^{-2\sigma}}{1-p^{-\sigma}}$ $\leq 2\sum_p \ln p \frac{1}{p^{2\sigma}} = O(1)$.

Следовательно, $\sum_p \ln p \frac{\chi_i(p)}{p^s} = \frac{L_i'(s)}{L_i(s)} + O(1)$, или

$$\sum_{p\equiv 1(mod 4)} \frac{\ln p}{p^s} + \sum_{p\equiv -1(mod 4)} \frac{\ln p}{p^s} = \frac{L_0'(s)}{L_0(s)} + O(1),$$

и

$$\sum_{p\equiv 1(mod 4)} \frac{\ln p}{p^s} - \sum_{p\equiv -1(mod 4)} \frac{\ln p}{p^s} = \frac{L_1'(s)}{L_1(s)} + O(1).$$

Следовательно,

$$\sum_{p\equiv 1(mod4)}\frac{\ln p}{p^s}=\frac{1}{2}(\frac{L_0^{'}(s)}{L_0(s)}+\frac{L_1^{'}(s)}{L_1(s)})+O(1),\ \text{ и }\ \sum_{p\equiv 3(mod4)}\frac{\ln p}{p^s}=\frac{1}{2}(\frac{L_0^{'}(s)}{L_0(s)}-\frac{L_1^{'}(s)}{L_1(s)})+O(1).$$

Так как $L_1(s) = O(1)$ для $s \to 1+$, и $L_1(s) \to \infty$ для $s \to 1+$, то правые части каждого из вышеприведенных равенств $\to \infty$ при $s \to 1+$, и оба ряда, $\sum_{p\equiv 1(mod4)} \frac{\ln p}{p}$ и $\sum_{p\equiv -1(mod4)} \frac{\ln p}{p}$, расходятся, то есть, существует бесконечно много простых чисел вида $4k+1$, и существует бесконечно много простых чисел вида $4k-1$.

Упражнения

1. Доказать, что существует бесконечно много простых чисел вида $6k-1$.

2. Доказать, что существует бесконечно много простых чисел вида $6k+1$.

6.4 Общее доказательство теоремы Дирихле

Рассмотрим арифметическую прогрессию $nx+l$ с взаимно-простыми n и l. Рассмотрим произвольный характер Дирихле по модулю n, и произвольную L-функцию Дирихле, заданную, для $Re(s) > 1$, рядом $L(s,\chi) = \sum_n^\infty \frac{\chi(n)}{n^s}$.

Аналогично доказательству, приведенному выше, заметим, для $Re(s) > 1$, что $-\frac{L^{'}(s,\chi)}{L(s,\chi)} = \sum_{n=2}^\infty \frac{\Lambda(n)\chi(n)}{n^s} = \sum_p \frac{\ln p\chi(p)}{p^s} + \sum_1$, где $\sum_1 = \sum_p \sum_{k=2}^\infty \frac{\ln p\chi(p^k)}{p^{ks}} = O(1)$. Следовательно, для любого характера χ по модулю n,

$$\sum_p \frac{\ln p\chi(p)}{p^s} = \frac{L^{'}(s,\chi)}{L(s,\chi)} + O(1).$$

Мы хотим получить простые числа p, такие что $p \equiv l(modn)$. Для этого найдем v, такое что $lv \equiv 1(modn)$. Это возможно, так как l и n взаимно-просты. Для данного χ, умножим равенство на $\chi(v)$, и просуммируем полученные равенства по всем характерам по модулю n:

$$\sum_p \frac{\ln p}{p^s}\sum_\chi \chi(v)\chi(p) = -\sum_\chi \chi(v)\frac{L^{'}(s,\chi)}{L(s,\chi)} + O(\sum_\chi \chi(v)).$$

Так как $p \equiv l(modn)$, и $vl \equiv 1(modn)$, то $pv \equiv 1(modn)$, то есть, $\sum_\chi \chi(v)\chi(p) = \sum_\chi \chi(pv) = \phi(n)$ для таких p, и $\sum_\chi \chi(v)\chi(p) = \sum_\chi \chi(pv) = 0$, иначе, то есть, для всех других p. С другой стороны, $O(\sum_\chi \chi(v)) = O(1)$, $\sum_{\chi\neq\chi_0} \chi(v)\frac{L^{'}(s,\chi)}{L(s,\chi)} = O(1)$, и $\chi_0(v)\frac{L^{'}(s,\chi_0)}{L(s,\chi_0)} = \chi_0(v)(\frac{A}{s-1} + O(1)) = \frac{A}{s-1} + O(1)$. Таким образом,

$$\sum_{p\equiv l(modn)} \frac{\ln p}{p^s} = \frac{A}{\phi(n)}\cdot\frac{1}{s-1} + O(1),$$

где A - абсолютная постоянная. Это означает, что ряд $\sum_{p\equiv l(modn)} \frac{\ln p}{p}$ расходится, и множество простых чисел вида $nx+l$ бесконечно.

Упражнения

1. Доказать, что существует бесконечно много простых чисел вида $2x + 1$.
2. Доказать, что существует бесконечно много простых чисел вида $2x - 1$.
3. Доказать, что существует бесконечно много простых чисел вида $5x - 1$.
4. Доказать, что существует бесконечно много простых чисел вида $5x + 1$.
5. Доказать, что существует бесконечно много простых чисел вида $kx + 1$.

7 Другие результаты

В общем случае, мы планируем рассмотреть доказательство асимптотического закона распределения простых чисел в форме

$$\pi(x) = Li(x) + O(xe^{-a\sqrt{\ln x}}),$$

и рассмотреть схему доказательства асимптотического закона распределения простых чисел в арифметических прогрессиях:

для числа $\pi_{a,b}(x)$ простых чисел, не превосходящих x, в арифметической прогрессии $ax + b$ со взаимно-простыми a и b имеет место асимптотическая формула

$$\pi_{a,b}(x) \sim \tfrac{Li(x)}{\phi(a)}.$$

Рассмотрим доказательство первого утверждения.

7.1 Доказательство асимптотического закона

Теорема.

$$\psi(x) = x + O(xe^{c_1\sqrt{\log x}})$$

для некоторой абсолютной положительной константы c_1.

Доказательство.

Известно, что $\psi(x) = x - \sum_{|\gamma|<T} \frac{x^{\beta+i\gamma}}{\beta+i\gamma} + O(\frac{x\log^2 x}{T})$, где T - параметр, для которого $2 \le T \le x$, и $\rho = \beta + i\gamma$ - нетривиальный нуль $\zeta(s)$.

Тогда $|\sum_{|\gamma|<T} \frac{x^{\beta+i\gamma}}{\beta+i\gamma}| \le \sum_{|\gamma|\le T} \frac{x^\beta}{\sqrt{\beta^2+\gamma^2}}$.

Рассмотрим вместо интервала $|\gamma| \le T$ интервалы $\frac{T}{2} < |\gamma| \le T$, $\frac{T}{4} < |\gamma| \le \frac{T}{2}$,..., $\frac{T}{2^{n-1}} < |\gamma| \le \frac{T}{2^n}$,... . Так как $\frac{T}{2^n} \le 1$ если и только если $n \ge \log_2 T$, то существует $\ll \log T$ таких интервалов. По теореме Валле Пуссена,

$$\sum_{\frac{T}{2}<|\gamma|\le T} \frac{x^\beta}{\sqrt{\beta^2+\gamma^2}} \le \sum_{\frac{T}{2}<|\gamma|\le T} \frac{x^{1-\frac{c}{\log(|\gamma|+2)}}}{|\gamma|} \le \frac{x^{1-\frac{c}{\log(T+2)}}}{0.5T} \sum_{\frac{T}{2}<|\gamma|\le T} 1 =$$

$$= O(x^{1-\frac{c}{\log(T+2)}} \log T)$$

(так как число нулей во второй сумме равно $O(T\log T)$). Тогда $|\sum_{|\gamma|\le T} \frac{x^{\beta+i\gamma}}{\beta+i\gamma}| = O(x^{1-\frac{c}{\log(T+2)}} \log^2 T)$, и $\psi(x) = x + O(x^{1-\frac{c}{\log(T+2)}} \log^2 x) + O(\frac{x\log^2 x}{T})$.

Выберем значение T таким образом, чтобы два остаточных члена в вышепривеленной формуле совпадали. Тогда $x^{1-\frac{c}{\log(T+2)}} = \frac{x}{T+2}$, $T+2 = x^{\frac{c}{\log(T+2)}}$, $\log^2(T+2) = c\log x$, $T+2 = e^{\sqrt{c\log x}}$, и $T < x$ для $x \geq x_0 > 0$.

Теорема.

$$\pi(x) = \int_2^x \frac{du}{\log u} + O(xe^{-c_2\sqrt{\log x}}).$$

Доказательство.

$\sum_{2\leq n\leq x} \frac{\Lambda(n)}{\log n} = \sum_{1\leq k\leq \log_2 x} \sum_{n=p^k\leq x} \frac{\log p}{k\log p} =$

$\sum_{n=p\leq x} 1 + \sum_{2\leq k\leq \log_2 x} \frac{1}{k} \sum_{p\leq x^{1/k}} 1 = \pi(x) + O(\sqrt{x}\log x)$.

Легко видеть, что $\sum_{p\leq x^{1/k}} 1 \leq x^{1/k} \leq \sqrt{x}$ для $k \geq 2$, и что $\sum_{k\leq \log_2 x} \frac{1}{k} \leq \sum_{k\leq \log_2 x} 1 \ll \log x$.

Используя частное суммирование, получим:

$\sum_{2<n\leq x} \frac{\Lambda(n)}{\log n} = -\int_2^x C(u) d\frac{1}{\log u} + C(x)\frac{1}{\log x}$, где $C(u) = \sum_{n\leq u} \Lambda(n) = \psi(u)$.

Следовательно,

$\sum_{2<n\leq x} \frac{\Lambda(n)}{\log n} = -\int_2^x (u + O(ue^{-\sqrt{c\log u}}))d\frac{1}{\log u} + (x + O(xe^{-\sqrt{c\log x}}))\frac{1}{\log x} =$

$-u\frac{1}{\log u}|_2^x + \int_2^x \frac{du}{\log u} + O(\int_2^x ue^{-\sqrt{c\log u}} \frac{du}{u\log^2 u}) + \frac{x}{\log x} + O(xe^{-\sqrt{c\log x}}) =$

$\frac{2}{\log 2} + \int_2^x \frac{du}{\log u} + O(\int_2^x ue^{-\sqrt{c\log u}} \frac{du}{u\log^2 u}) + O(xe^{-\sqrt{c\log x}})$.

Так как константа $\frac{2}{\log 2}$ есть $O(xe^{-\sqrt{c\log x}})$, мы получим, что $\pi(x) = \int_2^x \frac{du}{\log u} + O(\int_2^x ue^{-\sqrt{c\log x}} \frac{du}{u\log^2 u}) + O(xe^{-\sqrt{c\log x}}) + O(\sqrt{x}\log x)$.

Здесь

$O(\int_2^x ue^{-\sqrt{c\log u}} \frac{du}{u\log^2 u}) \ll \int_2^x e^{-\sqrt{c\log u}} du = \int_2^{\sqrt{x}} e^{-\sqrt{c\log u}} du + \int_{\sqrt{x}}^x e^{-\sqrt{c\log u}} du$

$\ll \sqrt{x} + xe^{-\sqrt{c\log\sqrt{x}}} \ll xe^{-\sqrt{\frac{c}{2}\log x}}$, так как 1. $|e^{-\sqrt{\cdots}}| < 1$, то есть $|\int_2^{\sqrt{x}} e^{\cdots}| < \int_2^{\sqrt{x}} du = \sqrt{x}$, 2. $|\int_{\sqrt{x}}^x| <$ длина промежутка умноженная на махимум подинтегральной функции.

Замечая, что $O(xe^{-\sqrt{c\log x}}) \ll xe^{-\sqrt{\frac{c}{2}\log x}}$, и что $O(\sqrt{x}\log x) \ll xe^{-\sqrt{\frac{c}{2}\log x}}$, мы получим результат теоремы.

Заметим, что $(\log x)^A \ll e^{c\sqrt{\log x}} \ll x^\delta$, так как $A\log\log x \ll c\sqrt{\log x} \ll \delta\log x$.

7.2 Сведения о нулях дзета-функции

Мы уже показали, что дзета-функция является аналитической в области $Res > 0$, где имеет единственный полюс первого порядка в точке $s = 1$ с вычетом 1.

Задача. Доказать, что при $Res > 0$

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + s\int_1^\infty \frac{\rho(u)du}{u^{s+1}},$$

где $\rho(u) = \frac{1}{2} - \{u\}$.

Действительно, $\int_1^\infty \frac{\rho(u)du}{u^{s+1}} = \sum_{k=1}^\infty \int_k^{k+1} \frac{0.5-\{u\}}{u^{s+1}}du$, $\int_k^{k+1} \frac{0.5-\{u\}}{u^{s+1}}du = \frac{1}{2}\int_k^{k+1} \frac{du}{u^{s+1}} - \int_k^{k+1} \frac{\{u\}}{u^{s+1}}du$. $\int_k^{k+1} \frac{\{u\}}{u^{s+1}}du = \int_0^1 \frac{\{u+k\}}{(u+k)^{s+1}}du = \int_0^1 \frac{\{u\}}{(u+k)^{s+1}}du = \int_0^1 \frac{u}{(u+k)^{s+1}}du = \int_0^1 \frac{u+k-k}{(u+k)^{s+1}}du = (u+k)^{1-s}|_0^1 - k(u+k)^{-s}|_0^1 = (k+1)^{1-s} - k^{1-s} - k(1+k)^{-s} + k(k^{-s})$. Преобразования дают $\sum_{n=1}^\infty \frac{1}{n^s}$. Так как $|\rho(u)| < 1$, то интеграл определен при $Res > 0$.

Более того, имеется функциональное уравнение (см. [Кара83])

$$\pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s).$$

Замечая, что точки s и $1-s$ симметричны относительно прямой $Res = \frac{1}{2}$, и учитывая, что при $Res > 0$ дзета-функция Римана аналитична, получаем аналитическое продолжение дзета-функции на всю комплексную плоскость.

Здесь $\Gamma(s)$ - гамма-функция Эйлера, одно из определений которой имеет вид

$$\frac{1}{\Gamma(s)} = se^{\gamma s}\prod_{n=1}^{\infty}(1+\frac{s}{n})e^{-\frac{s}{n}},$$

где γ - постоянная Эйлера. (Заметим, что часто для определения используется и интегральная формула $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$. Следует знать также, что имеет место следующее функциональное уравнение для $\Gamma(s)$: $\Gamma(s+1) = s\Gamma(s)$, откуда следует, что $\Gamma(n+1) = n!$ при $n \in \mathbb{N}$. Полезна также формула Стирлинга: при $\delta > 0$ И $-\pi+\delta \leq args \leq \pi-\delta$ имеет место формула $\log\Gamma(s) = (s-\frac{1}{2})\log s - s + \log\sqrt{2\pi} + O(\frac{1}{|s|}).$) Из задания гамма-функции видно, что она имеет пристые полюсы при $s = 0, -1, -2, \ldots$. Отсюда следует, что дзета-функция имеет нули в точках $-2, -4, \ldots$ - так называемы триви альные нули. Полюс гамма-функции в 0 гасится полюсом функции $\zeta(1-s)$ в единице.

Продолжим исследование нулей дзета-функции.

Умножив обе части на $\frac{1}{2}s(1-s)$, получим

$$\frac{1}{2}s(1-s)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \frac{1}{2}s(1-s)\pi^{-\frac{1-s}{2}\Gamma(1-s}2)\zeta(1-s),$$

или, обозначая $\xi(s) = \frac{1}{2}s(1-s)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$,

$$\xi(s) = \xi(1-s).$$

Из определения гамма-функции следует, что она имеет простые полюсы при $s = 0$ и $s = -n$, $n \in \mathbb{N}$. При $Res \geq \frac{1}{2}$ эта функция аналитична. Полюс функции $\zeta(s)$ в точке $s = 1$ гасится скобкой $1-s$, так что функция $\xi(s)$ является аналитической в области $Res \geq \frac{1}{2}$ а, следовательно, и во всей комплексной плоскости. Таким образом, $\xi(s)$ - целая функция. (Напомним, что целой называется функция $G(s)$, аналитичная в любой конечной части комплексной плоскости. Если $M(r) = M_G(r) = \max_{|s|=r}|G(s)|$ И существует $a > 0$ такое что $M(r) < e^{r^a}$ при $r > r_0(a) > 0$, то $G(s)$ называется целой функцией конечного порядка, а $\alpha = \inf a$ называется порядком $G(s)$. Имеет место следующая теорема: если $G(s)$ - уелая функция конечого порядка α, и $G(0) \neq 0$, s_n - последовательность всех нулей $G(s)$, причем $0 < |s_1| \geq |s_2| \geq \ldots \geq |s_n| \geq \ldots$, то последовательность s_n имеет конечный показатель сходимости $\beta \leq \alpha$, $G(s) = e^{g(s)}\prod_{n=1}^{\infty}(1-\frac{s}{s_n})e^{\frac{s}{s_n}+\frac{1}{2}(\frac{s}{s_n})^2+\ldots+\frac{1}{p}(\frac{s}{s_n})^p}$, где $p \geq 0$ - наименьшее целое число, для которого $\sum_{n=1}^{\infty}|s_n|^{-(p+1)} < +\infty$, $g(s)$ - многочоен степени $g \leq \alpha$, и $\alpha = \max\{g, \beta\}$. Если, кроме того, для любого $c > 0$ найдется бесконечная последовательность $r_1, r_2, \ldots, r_n \to +\infty$ такая что $\max|G(s)| > e^{cr_n^\alpha}$, $|s| = r_n$, $n = 1, 2, \ldots$, то $\alpha = \beta$ и ряд $\sum_{n=1}^{\infty}|s_n|^{-\beta}$ расходится.)

Ее порядок равен 1. Для доказательства оценим $\xi(s)$ при $|s| \to \infty$, причем достаточно это сделать при $Res > 0.5$. Из формулы аналитического продолжения дзета-функции на $Res > 0$ следует, что при $Res > 0.5$ мы имеем $\zeta(s) = O(|s|)$. Так как $|\Gamma(s)| \leq e^{c|s|\ln|s|}$, то порядок $\xi(s)$ не выше первого, но при $s \to \infty$ $\ln\Gamma(s) \sim s\ln s$, поэтому порядок $\xi(s)$ равен 1. Из общей теоремы о целых функциях конечного порядка мы получаем, что ряд $\sum|\rho_n|$ расходится, откуда следует, что функция $\xi(s)$ имеет бесконечно много нулей, а ряд $\sum_{n=1}^{\infty}|rho_n|^{-1-\epsilon}$ схходится пмри любом ϵ.

Используем теорему о представлении целой функции в виде произведения по нулям:

$$\xi(s) = e^{A+Bs}\prod_{n=1}^{\infty}(1-\frac{s}{\rho_n})e^{\frac{s}{\rho_n}}$$

- бесконечное произведение Вейерштрасса. Заметим, что нулей бесконечно много, и $\sum_{n=1}^{\infty}\frac{1}{|\rho_n|}$ расходится, а $\sum_{n=1}^{\infty}\frac{1}{|\rho_n|^{1+\epsilon}}$ сходится для любого $\epsilon > 0$. Тогда получим

$$e^{A+Bs}\prod_{n=1}^{\infty}(1-\frac{s}{\rho_n})e^{\frac{s}{\rho_n}} = \frac{1}{2}s(1-s)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s).$$

При $Res > 1$ множитель $\frac{1}{2}s(1-s)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2}) \neq 0$, $\zeta(s) \neq 0$, и, следовательно, $\xi(s) \neq 0$. Так как $\xi(s) = \xi(1-s)$, то $\xi(s) \neq 0$ и при $Res < 0$. Таким образом, все нули $\xi(s)$ лежат в полосе $0 \leq Res \leq 1$. При $s = 1$ функция $\xi(1) \neq 0$, так как нуль $1-s$ гасится полюсом $\zeta(1)$. Таким образом, в критической полосе нули функции $\xi(s)$ совпадают с нулями функции $\zeta(s)$.

Из сделанных замечаний немедленно следует, что нетривиальные нули дзета-функции симметричны относительно прямой $Res = \frac{1}{2}$ и относительно прямой $Ims = 0$ (возьмите сопряженное!).

В дальнейшем нетривиальные нули будем нумеровать в порядке возрастания абсолютной величины их мнимой части, а при одинваковых абсолютных величинах мнимых частей - в произвольном порядке.

Теорема.

$$\frac{\zeta'(s)}{\zeta(s)} = -\frac{1}{s-1} + \sum_{n=1}^{\infty}(\frac{1}{s-\rho_n}+\frac{1}{\rho_n}) + \sum_{n=1}^{\infty}(\frac{1}{s+2n}-\frac{1}{2n}) + B_0.$$

Доказательство.

Заменив в последней формуле выражение для $\Gamma(\frac{s}{2})$ его представлением в виде бесконечного произведения, получим

$$\frac{s}{2}e^{\frac{\gamma s}{2}}\prod_{n=1}^{\infty}(1+\frac{s}{2n})e^{-\frac{s}{2n}}e^{A+Bs}\prod_{n=1}^{\infty}(1-\frac{s}{\rho_n})e^{\frac{s}{\rho_n}} = \frac{s}{2}(1-s)\pi^{-\frac{s}{2}}\zeta(s),$$

или

$$e^{\frac{\gamma s}{2}}\prod_{n=1}^{\infty}(1+\frac{s}{2n})e^{-\frac{s}{2n}}e^{A+Bs}\prod_{n=1}^{\infty}(1-\frac{s}{\rho_n})e^{\frac{s}{\rho_n}} = (1-s)\pi^{-\frac{s}{2}}\zeta(s).$$

Возьмем логарифмическую производную от правой и левой частей равенства, получим

$$\frac{\gamma}{2} + \sum_{n=1}^{\infty}(\frac{1}{s+2n}-\frac{1}{2n}) + B + \sum_{n=1}^{\infty}(\frac{1}{s-\rho_n}+\frac{1}{\rho_n}) = \frac{1}{s-1} - \frac{\ln\pi}{2} + \frac{\zeta'(s)}{\zeta(s)}.$$

Отсюда имеем

$$\frac{\zeta'(s)}{\zeta(s)} = -\frac{1}{s-1} + \sum_{n=1}^{\infty}(\frac{1}{s-\rho_n} + \frac{1}{\rho_n}) + \sum_{n=1}^{\infty}(\frac{1}{s+2n} - \frac{1}{2n}) + B_0,$$

$B_0 = \frac{\gamma}{2} + B + \frac{\ln \pi}{2}$.

Теорема.

Пусть $\rho_n = \beta_n + i\gamma_n$ - все нетривиальные нули $\zeta(s)$. Пусть $t \geq 2$. Тогда

$$\sum_{n=1}^{\infty} \frac{1}{1+(t-\gamma_n)^2} << \ln t.$$

Доказательство.

Пусть $\rho_n = \beta_n + i\gamma_n$. Пусть для $t \geq 2$ имеем $s = 2+it$. В этом случае $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$, и мы имеем

$$\sum_{n=1}^{\infty}(\frac{1}{s-\rho_n} + \frac{1}{\rho_n}) = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} + \frac{1}{s-1} - \sum_{n=1}^{\infty}(\frac{1}{s+2n} - \frac{1}{2n}) - B_0,$$

$$Re(\sum_{n=1}^{\infty}(\frac{1}{s-\rho_n} + \frac{1}{\rho_n})) = Re(-\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} + \frac{1}{s-1} - \sum_{n=1}^{\infty}(\frac{1}{s+2n} - \frac{1}{2n}) - B_0) \leq$$

$$\leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^2} + \frac{1}{|1+it|} + \sum_{n=1}^{\infty} |\frac{1}{s+2n} - \frac{1}{2n}| + B_0 = O(\ln t),$$

так как $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^2} = O(1)$ (ряд сходится), $\frac{1}{|1+it|} = O(1)$, $B_0 = O(1)$, $\sum_{n\leq t} |\frac{1}{s+2n} - \frac{1}{2n}| + \sum_{n>t} |\frac{1}{s+2n} - \frac{1}{2n}| \leq \sum_{n\leq t} \frac{1}{n} + \sum_{n>t} \frac{|s|}{4n^2} = O(\ln t) + O(1) = O(\ln t)$.

Следовательно, $Re(\sum_{n=1}^{\infty}(\frac{1}{s-\rho_n} + \frac{1}{\rho_n})) = \sum_{n=1}^{\infty}(Re\frac{1}{s-\rho_n} + Re\frac{1}{\rho_n}) = O(\ln t)$. При этом $Re\frac{1}{\rho_n} = Re\frac{1}{\beta_n+i\gamma_n} = \frac{\beta_n}{\beta_n^2+\gamma_n^2} \geq 0$, $Re\frac{1}{s-\rho_n} = Re\frac{1}{(2-\beta_n)+i(t-\gamma_n)} = \frac{2-\beta_n}{(2-\beta_n)^2+(t-\gamma_n)^2} \geq \frac{1}{4+4(t-\gamma_n)^2} = \frac{0.25}{1+(t-\gamma_n)^2}$, то есть $\sum_{n=1}^{\infty}(Re\frac{1}{s-\rho_n} + Re\frac{1}{\rho_n}) \leq 0.25\sum_{n=1}^{\infty} \frac{1}{1+(t-\gamma_n)^2}$. Теперь мы имеем

$$\sum_{n=1}^{\infty} \frac{1}{1+(t-\gamma_n)^2} = O(\ln t).$$

Отсюда получаем несколько следствий.

Следствие 1.

$$\sum_{T\leq\gamma_n\leq T+1} = O(\ln T).$$

- число нулей в указанном прямоугольнике есть $O(\ln T)$.

Доказательство.

Действительно, $\sum_{T\leq\gamma_n\leq T+1} \leq 2\sum_{T\leq\gamma_n\leq T+1} \frac{1}{1+(T-\gamma_n)^2} = O(\sum_{n=1}^{\infty} \frac{1}{1+(T+\gamma_n)^2}) = O(\ln T)$, так как $|T-\gamma_n| \leq 1$, $(T-\gamma_n)^2 \leq 1$, $1+(T-\gamma_n)^2 \leq 2$, $\frac{1}{1+(T-\gamma_n)^2} \leq \frac{1}{2}$, $2\frac{1}{1+(T-\gamma_n)^2} \leq 1$.

Следствие 2.

$$\sum_{|T-\gamma_n|>1} \frac{1}{(T-\gamma_n)^2} = O(\ln T).$$

Доказательство.

Действительно, $\sum_{|T-\gamma_n|>1}\frac{1}{(T-\gamma_n)^2}\le 2\sum_{|T-\gamma_n|>1}\frac{1}{1+(T-\gamma_n)^2}$.

Следствие 3.

$$\frac{\zeta'(s)}{\zeta(s)}=\sum_{|t-\gamma_n|\le 1}\frac{1}{s-\rho_n}+O(\ln|t|)$$

при $-1\le\sigma\le 2$, $|t|\ge 2$, $s=\sigma+it$.

Доказательство.

Действительно, пусть $s=\sigma+it$, $\rho_n=\beta_n+i\gamma_n$ и, дополнительно, $s=2+it$. При двух этих s сумма второго ряда в представлении для $\frac{\zeta'(s)}{\zeta(s)}$ оценивается как $O(\ln t)$: $\sum_{n=1}^{\infty}(\frac{1}{s+\rho_n}-\frac{1}{2n})=\sum_{1\le n\le|t|}+\sum_{n>|t|}\le\sum_{1\le n\le|t|}\frac{1}{n}+\sum_{n>|t|}\frac{|s|}{2n(2n-1)}=O(\ln t)+O(1)=O(\ln t)$. Здесь a) $|\frac{1}{s+2n}-\frac{1}{2n}|\le\frac{1}{|s+2n|}+\frac{1}{2n}\le\frac{1}{|\sigma+2n+it|}+\frac{1}{2n}\le\frac{1}{2n+\sigma}+\frac{1}{2n}\le\frac{1}{2n-1}+\frac{1}{2n}<<\frac{1}{n}$, b) $\sum_{n\ge|t|}\frac{|s|}{2n(2n-1)}=O(\frac{|t|}{|t|})=O(1)$. Следовательно, при $s=\sigma+it$ $\frac{\zeta'(s)}{\zeta(s)}=O(\ln t)$, при $s=2+it$ -тоже (взяли $\sigma=2$). Вычтем формулы друг из друга при разных s: $\frac{\zeta'(s)}{\zeta(s)}=\sum_{n=1}^{\infty}(\frac{1}{s-\rho_n}-\frac{1}{2-\rho_n+it})+O(\ln|t|)$ ($\frac{\zeta'(2+it)}{\zeta(2+it)}=const=O(1)=O(\ln|t|)$ вошло в остаточный член). Отсюда 1) $\sum_{|t-\gamma_n|\le 1}(\frac{1}{s-\rho_n}-\frac{1}{2+it-\rho_n})=\sum_{|t-\gamma_n|\le 1}\frac{1}{s-\rho_n}+O(\ln t)$ ($\frac{1}{|2-\beta_n+i(t-\gamma_n)|}\le\frac{1}{2-\beta_n}\le 1$). 2) $|\sum_{|t-\gamma_n|>1}(\frac{1}{s-\rho_n}-\frac{1}{2+it-\rho_n})|=|\sum_{|t-\gamma_n|>1}\frac{(2+it-\rho_n-s+\rho_n)}{(\sigma+it-\beta_n-i\gamma_n)(2+it-\beta_n-i\gamma_n)}|\le\sum_{|t-\gamma_n|>1}\frac{(2-\sigma)}{(t-\gamma_n)(t-\gamma_n)}\le\sum_{|t-\gamma_n|>1}\frac{3}{(t-\gamma_n)^2}=O(\ln|t|)$. Здесь $2-\sigma\le 3$ по заданию σ; $|\sigma+it-\beta_n-i\gamma_n|\ge|Im(\sigma+it-\beta_n-i\gamma_n)|=|t-\gamma_n|$.

Теорема Валле Пуссена.

Существует абсолютная положительная постоянная c, такая что

$$Re\rho=\beta<1-\frac{c}{\log(|\gamma|+2)},$$

где ρ - нетривиальный нуль дзета-функции, то есть, $\zeta(\rho)=0$, и $\rho=\beta+i\gamma$.

Доказательство. Функция $\zeta(s)$ имеет полюс в точке $s=1$, следовательно, в некоторой окрестности этой точки $\zeta(s)\ne 0$, например, она не равна нулю в области $|s-1|\le\gamma_0$ для достаточно малого $\gamma_0>0$. Тогда для $\rho_n=\beta_n+i\gamma_n$ мы имеем $|\gamma_n|>\gamma_0>0$.

Для $Re(s)>1$, $-\frac{\zeta'(s)}{\zeta(s)}=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^s}=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^\sigma}e^{-it\log n}$, то есть, $Re(-\frac{\zeta'(s)}{\zeta(s)})=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^\sigma}\cos(t\log n)$.

Легко показать, что

$$3+4\cos\phi+\cos 2\phi=2(1+\cos\phi)^2\ge 0.$$

Беря в формуле для действительной части логарифмической производной дзета-функции вместо t значения 0, t и $2t$, соответственно, мы получим

$$Re(-\frac{\zeta'(\sigma)}{\zeta(\sigma)})=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^\sigma},$$

$$Re(-\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)})=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^\sigma}\cos(t\log n),$$

$$Re(-\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}) = \sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^{\sigma}}\cos(2t\log n).$$

Тогда мы получим, что

$$3Re(-\frac{\zeta'(\sigma)}{\zeta(\sigma)}) + 4Re(-\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}) + Re(-\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}) =$$

$$= \sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^{\sigma}}(3 + 4\cos t\log n + \cos 2t\log n) \geq 0.$$

Оценим эту сумму сверху.

Известно, что $-\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{s-1} - \sum_{n=1}^{\infty}(\frac{1}{s-\rho_n}+\frac{1}{\rho_n}) - \sum_{n=1}^{\infty}(\frac{1}{s+2n}-\frac{1}{2n}) - B_0$, где B_0 - абсолютная постоянная.

1. $-\frac{\zeta'(\sigma)}{\zeta(\sigma)} = \frac{1}{\sigma-1} + A_1$, где A_1 - абсолютная постоянная, так как для $s = \sigma$ мы получим $\frac{1}{s-\rho_n} + \frac{1}{\rho_n} = \frac{1}{\sigma-\rho_n} + \frac{1}{\rho_n} = \frac{\sigma}{(\sigma-\rho_n)\rho_n} \ll \frac{1}{|\gamma_n|^2}$ $(1 < \sigma < 2)$, и ряд $\sum\frac{1}{|\gamma_n|^2}$ сходится: $\sum\frac{1}{|\gamma_n|^2} = \sum_m\sum_{m<|\gamma_n|\leq m+1}\frac{1}{|\gamma_n|^2} \ll \sum_m\frac{1}{m^2}\log m$, так как число нулей дзета-функции с мнимой частью между m и $m+1$ равно $\ll \log m$. Кроме того, $\sum(\frac{1}{\sigma+2n} - \frac{1}{2n}) \ll \sum\frac{\sigma}{n^2} \ll \sum\frac{1}{n^2}$ также сходится. Следовательно, $Re(-\frac{\zeta'(\sigma)}{\zeta(\sigma)}) \leq \frac{1}{\sigma-1} + A_1$.

2. $Re(-\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}) \leq A_2 + c\log(|t|+2) - \frac{\sigma-\beta_n}{(\sigma-\beta_n)^2+(t-\gamma_n)^2}$. Именно, $\frac{1}{|s-1|} \leq \frac{1}{|t|} \leq \gamma_0$, так как $|t| \geq \gamma_0 > 0$; кроме того, можно показать, что $\sum(\frac{1}{\sigma+it+2n} - \frac{1}{2n}) = O(\log|t|) = O(\log(|t|+2))$ (см. доказательство следствия 3). Наконец, $Re(\frac{1}{s-\rho_n}) = Re(\frac{1}{\sigma-\beta_n+i(t-\gamma_n)}) = \frac{\sigma-\beta_n}{(\sigma-\beta_n)^2+(t-\gamma_n)^2}$ - положительно, и все соответствующие отрицательные слагаемые в сумме можно отбросить; мы отбрасываем все, кроме одного. То же относится и к $Re(\frac{1}{\rho_n})$, где мы отбрасываем все слагаемые.

3. Аналогично, мы можем получить, что $Re(-\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}) \leq A_3 + c\log(|t|+2)$ - проведя соответствующие рассуждения, отбросим все отрицательные слагаемые.

Следовательно, мы имеем, что $\frac{3}{\sigma-1} - 4\frac{\sigma-\beta_n}{(\sigma-\beta_n)^2+(t-\gamma_n)^2} + c_1\log(|t|+2) \geq 0$.

Пусть $\sigma \in (1,2)$, пусть t - параметр. Если мы выберем $t = \gamma_n$, мы получим неравенство $\frac{3}{\sigma-1} - \frac{4}{\sigma-\beta_n} + c_1\log(|\gamma_n|+2) \geq 0$.

Беря $\sigma = 1 + \frac{1}{2c_1\log(|\gamma_n|+2)}$, мы получим: $\frac{4}{\sigma-\beta_n} \leq 7c_1\log(|\gamma_n|+2)$, или $\frac{4}{7c_1\log(|\gamma_n|+2)} \leq \sigma-\beta_n$. Это значит, что $\beta_n \leq \sigma - \frac{4}{7c_1\log(|\gamma_n|+2)} = 1 + \frac{7}{14c_1\log(|\gamma_n|+2)} - \frac{8}{14c_1\log(|\gamma_n|+2)} = 1 - \frac{1}{14c_1\log(|\gamma_n|+2)}$.

7.3 Ряды Дирихле

Лемма.

$$\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{a^s}{s}ds = \begin{cases} 1 + \frac{\theta a^b}{T\ln a}, & a > 1 \\ \frac{\theta a^b}{T|\ln a|}, & 0 < a < 1, \end{cases}$$

где $|\theta| \leq 1$, $T \geq 1$, $b > 0$, $\theta = \theta(a,T,b)$.

Доказательство.

Действительно, пусть $a > 1$. Рассмотрим прямоугольный контур Γ с вершинами $b \pm iT$, $-U \pm iT$, где $U > 0$ - произвольный параметр. Подинтегральная функция имеет единственную особенность внутри контура Γ в точке $s = 0$, причем так как $a^s = e^{s\ln a} = 1 + s\ln a + \frac{1}{2!}s^2\ln^2 a + ...$, $\frac{a^s}{s} = \frac{1}{s} + \ln a + ...$, то вычет подинтегральной функции в данной точке равен 1. Тогда $\frac{1}{2\pi i}\int_\Gamma \frac{a^s}{s}ds = 1$, или $\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{a^s}{s}ds = 1 + J_1 + J_2 + J_3$, где J_1, J_2, J_3 - интегралы по верхней, нижней и левой стронам контура, соответственно. Оценим три последних интеграла. Имеем $\max\{|J_1|,|J_2|\} \le \frac{1}{2\pi}\int_{-U}^{b}\frac{a^\sigma}{\sigma^2+T^2} \le \frac{1}{2\pi}\int_{-U}^{b}\frac{a^\sigma}{T} = \frac{1}{2\pi T}\frac{a^\sigma}{\ln a}\Big|_{-U}^{b} < \frac{a^b}{2\pi T\ln a}$; $|J_3| \le \frac{1}{2\pi}\int_{-T}^{T}\frac{a^{-U}}{U}dt = \frac{T}{\pi}\frac{a^{-U}}{U}$. Так как $\frac{Ta^{-U}}{\pi U} \to 0$ при $U \to \infty$, то можно найти такое U, что $\frac{Ta^{-U}}{\pi U} < \frac{a^b}{2\pi T\ln a}$. Тогда сумма модулей последних трех интегралов не превосходит $\frac{3a^b}{2\pi T\ln a} < \frac{a^b}{T\ln a}$, откуда следует первое утверждение леммы.

При $0 < a < 1$ рассмотрим контур Γ с вершинами $b \pm iT$, $U \pm iT$. Поскольку подинтегральная функция не имеет особенностей внутри данного контура, то $\int_{b-iT}^{b+iT}\frac{a^s}{s}ds = 0 + J_1 + J_2 + J_3$, где J_1, J_2, J_3 - интегралы по верхней, нижней и правой сторонам контура, соответственно. При этом $\max\{|J_1|,|J_2|\} \le \frac{1}{2\pi}\int_{b}^{U}\frac{a^\sigma}{T}d\sigma = \frac{1}{2\pi}\frac{a^\sigma}{\ln a}\Big|_{b}^{U} = \frac{a^U}{2\pi T\ln a} - \frac{a^b}{2\pi T\ln a} < \frac{a^b}{2\pi T|\ln a|}$ (так как $\ln a < 0$), $|J_3| \le \frac{1}{2\pi}\int_{-T}^{T}\frac{a^U}{U}dt = \frac{a^U T}{\pi U}$, что $\to 0$ при $U \to \infty$. Выбрав U так, чтобы $\frac{a^U T}{\pi U} < \frac{a^b}{2\pi T|\ln a|}$, мы завершим доказательство леммы.

Определение.

Рядом Дирихле называется выражение вида

$$f(s) = \sum_{n=1}^{\infty}\frac{a(n)}{n^s},$$

$a(n) \in \mathbb{C}$, $s = \sigma + it$.

При $x \ge 1$ функция $\Phi(x) = \sum_{n\le x} a(n)$ называется сумматорной функцией коэффициентов ряда Дирихле $f(s)$.

Теорема (формула суммирования).

Пусть

1. ряд $f(s)$ абсолютно сходится при $Res = \sigma > 1$;
2. пусть $|a(n)| \le A(n)$, причем $A(n)$ монотонно возрастает с ростом n;
3. при $\sigma \to 1 + 0$ имеет место оценка $\sum_{n=1}^{\infty}\frac{|a(n)|}{n^\sigma} = O(\frac{1}{(\sigma-1)^\alpha})$, $\alpha > 0$.

Тогда при любых b, $b_0 \ge b > 1$, $T \ge 1$, $x = N + 0.5$, $N \in \mathbb{N}$, $N \ge 4$ справедлива формула

$$\Phi(x) = \sum_{n\le x} a(n)\frac{1}{2\pi i}\int_{b-iT}^{b+iT} f(s)\frac{x^s}{s}ds + O(\frac{x^b}{T(b-1)^\alpha}) + O(\frac{xA(2x)\ln x}{T}),$$

причем постоянные в знаках $O(...)$ зависят только от b_0.

Доказательство. Рассмотрим

$$\frac{1}{2\pi i}\int_{b-iT}^{b+iT} f(s)\frac{x^s}{s}ds = \frac{1}{2\pi i}\int_{b-iT}^{b+iT}\sum_{n=1}^{\infty}\frac{a(n)}{n^s}\frac{x^s}{s}ds$$

$(b > 1)$. Поскольку ряд абсолютно сходится, то можно почленно интегрировать: $\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\sum_{n=1}^{\infty}\frac{a(n)}{n^s}\frac{x^s}{s}ds = \frac{1}{2\pi i}\sum_{n=1}^{\infty}a(n)\int_{b-iT}^{b+iT}(\frac{x}{n})^s\frac{ds}{s} = \sum_{n<x}a(n)(1 + \frac{\theta(x/n)^b}{T\ln(x/n)}) + \sum_{n>x}a(n)\frac{\theta(x/n)^b}{T|ln(x/n)|} = \sum_{n\le x}a(n) + R$ $(a = x/n$, $x = N + 0.5$

$\Rightarrow a \neq 1)$, $|R| \leq \sum_{n=1}^{\infty} \frac{|a(n)|(x/n)^b}{T|\ln(x/n)} = \frac{x^b}{T}\sum_{n=1}^{\infty} \frac{|a(n)|}{n^b|\ln(x/n)|} = \frac{x^b}{T}A$, $A = \sum_{n\leq x/2} + (\sum_{x/2<n\leq 2x} + \sum_{n>2x}) = A_1 + A_2$.

Таким образом, $\Phi(x) = \frac{1}{2\pi i}\int_{b-iT}^{b+iT} f(s)\frac{x}{s}ds + O(R)$.

Для оценки R оценим A_1 и A_2. Начнем с A_2: при $n \leq x/2$, $x/n \geq 2$, при $n > 2x$, $x/n < 1/2$, откуда $|\ln(x/n)| \geq 2$, и $A_2 \leq \frac{1}{\ln 2}\sum_{n\leq x/2} \frac{|a(n)|}{n^b} + \frac{1}{\ln 2}\sum_{n\geq 2x}\frac{|a(n)|}{n^b} < \frac{1}{\ln 2}\sum_{n=1}^{\infty}\frac{|a(n)|}{n^b} = O(\frac{1}{(b-1)^\alpha})$. Таким образом, $A_2 = O(\frac{1}{(b-1)^\alpha})$.

Оценим A_1. Прежде всего, $A_1 \leq \frac{A(2x)}{(x/2)^b}\sum_{x/2<n\leq 2x}\frac{1}{|\ln(x/n)|}$, так как $|a(n)| \leq A(n) \leq A(2x)$. Рассмотрим последнюю сумму. $\sum_{x/2<n\leq 2x}\frac{1}{|\ln(x/n)|} = \sum_{x/2<n\leq N-2} + \sum_{n=N-1}^{N+1} + \sum_{N+2\leq n\leq 2x}$, где N - натуральное число из равенства $x = N + 0.5$.

1. Оценим вторую сумму. В ней всего три члена. При $n = N$, $\ln(x/N) = \ln\frac{N+0.5}{N} = \ln(1+\frac{1}{2N}) = \frac{1}{2N} - \frac{1}{2(2N)^2} + ... \geq \frac{1}{2N} - \frac{1}{2(2N)^2} \geq \frac{1}{4N}$. Тогда вся вторая сумма $= O(4N) = O(x)$.

2. Оценим третью сумму. $\sum_{N+2\leq n\leq 2x}\frac{1}{|\ln(x/n)|} = \sum_{N+2\leq n\leq 2x}\frac{1}{\ln(x/n)} = \sum_{r=1}^{N}\frac{1}{\ln\frac{N+1+r}{N+0.5}}$. При этом $\ln\frac{N+1+r}{N+0.5} = \ln(1+\frac{r+0.5}{N+0.5}) \geq \frac{r+0.5}{N+0.5} - \frac{1}{2}(\frac{r+0.5}{N+0.5}) \geq \frac{1}{2}(\frac{r+0.5}{N+0.5}) = \frac{r+0.5}{2N+1}$. Тогда $\sum_{N+2\leq n\leq 2x}\frac{1}{\ln(x/n)} = \sum_{r=1}^{N}\frac{1}{\ln\frac{N+1+r}{N+0.5}} \leq \sum_{r=1}^{N}\frac{2N+1}{r+0.5} < (2N+1)\int_0^N\frac{du}{u+0.5} = (2N+1)\ln(u+0.5)|_0^N$ $= (2N+1)\ln(2N+1) = O(x\ln x)$, постоянная в знаке $O()$ - абсолютная.

3. Первая сумма оценивается также. как третья и дает $O(x\ln x)$. Таким образом, $\sum_{x/2<n\leq 2x}\frac{1}{|\ln(x/n)|} = O(x\ln x)$, и $A_1 = O(\frac{A(2x)x\ln x}{x^b})$. Тогда $|R| \leq \frac{x^b}{T}(A_1 + A_2) = O(\frac{A(2x)x\ln x}{T}) + O(\frac{x^b}{T(b-1)^\alpha})$.

Теорема.

При $2 \leq T \leq x$, $b = 1 + \frac{1}{\ln x}$,

$$\psi(x) = \sum_{n\leq x}\Lambda(n) = \frac{1}{2\pi i}\int_{b-iT}^{b+iT}(-\frac{\zeta'(s)}{\zeta(s)})\frac{x^s}{s}ds + O(\frac{x\ln^2 x}{T}).$$

Доказательство. Применим предыдущую теорему для ряда Дирихле $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}$, $Res > 1$, $b > 1$, $T \geq 1$. Тогда $\psi(x) = \sum_{n\leq x}\Lambda(n) = \frac{1}{2\pi i}\int_{b-iT}^{b+iT}(-\frac{\zeta'(s)}{\zeta(s)})\frac{x^s}{s}ds + O(\frac{x\ln^2 x}{T}) + O(\frac{x^b}{T(b-1)^\alpha})$. Здесь $\Lambda(n) \leq \ln n$, то есть $A(x) = \ln x$. При $b = 1 + \frac{1}{\ln x}$ имеем $x^b = O(x)$, $(b-1)^\alpha = (\ln x)^{-\alpha}$. Найдем α. Так как $\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^\sigma} \leq \sum_{n=1}^{\infty}\frac{\ln n}{n^\sigma} = \sum_{n=2}^{\infty}\frac{\ln n}{n^\sigma} = \frac{\ln 2}{2^\sigma} + \frac{\ln 3}{3^\sigma} + \sum_{n=4}^{\infty}\frac{\ln n}{n^\sigma} \leq \frac{\ln 2}{2^\sigma} + \frac{\ln 3}{3^\sigma} + \int_3^{\infty}\frac{\ln u}{u^\sigma}du = \frac{\ln 2}{2^\sigma} + \frac{\ln 3}{3^\sigma} + \frac{1}{1-\sigma}(\ln u)u^{1-\sigma}|_3^{\infty} - \frac{1}{(1-\sigma)^2}u^{1-\sigma}|_3^{\infty} = O(\frac{1}{(\sigma-1)^2})$, то есть $\alpha = 2$. Теперь оба остаточных члена совпадают и равны $O(\frac{x\ln^2 x}{T})$.

Теорема. Пусть $x \geq T \geq 2$. тогда

$$\psi(x) = x - \sum_{|Im\rho|\leq T}\frac{x^\rho}{\rho} + O(\frac{x\ln^2 x}{T}).$$

Доказательство. Воспользуемся предыдущей теоремой: $\psi(x) = \sum_{n\leq x}\Lambda(n) = \frac{1}{2\pi i}\int_{b-iT}^{b+iT}(-\frac{\zeta'(s)}{\zeta(s)})\frac{x^s}{s}ds + O(\frac{x\ln^2 x}{T})$. Выберем T_1: $T \leq T_1 \leq T+1$. Напомним, что $b = 1 + \frac{1}{\ln x}$. Рассмотрим все нули дзета-функции, мнимые части которых принадлежат отрезку $[T, T+1]$. Поскольку их не больше $O(\ln T)$, то найдутся два таких нуля, что расстояние между их мнимыми частями $> \frac{c}{\ln T}$. Возьмем две такие точки. Середина отрезка между ними и будет T_1. Таким образом, любой ноль отстоит от T_1 не меньше, чем на $\frac{c}{2\ln T}$, то есть, все нули расположены "далеко"от T_1. Рассмотрим прямоугольный контур Γ с вершинами $b \pm iT_1$, $-0.5 \pm iT_1$. Рассмотрим интеграл $\frac{1}{2\pi i}\int_\Gamma(-\frac{\zeta'(s)}{\zeta(s)})\frac{x^s}{s}ds$. Особенностями подинтегральной функции являются нули дзета-функции, лежащие внутри контура, и точки $s = 0$, $s = 1$. При этом вычет в точке 0 равен $-\frac{\zeta'(0)}{\zeta(0)} = const$, вычет в точке 1 равен x, а вычет в точке ρ_n равен $\frac{x^{\rho_n}}{\rho_n}$. таким образом, $\psi(x) = x - \sum_{|Im\rho_n|\le T_1}\frac{x^{\rho_n}}{\rho_n} + O(\frac{x\ln^2 x}{T}) + J_1 + J_2 + J_3$, где интегралы J_1, J_2, J_3 берутся по верхней, нижней и левой сторонам контура, соответственно ($\frac{\zeta'(0)}{\zeta(0)}$ ушло в $O(...)$).

Оценим указанные интегралы.

1. $|J_1| \le \frac{1}{2\pi}\int_{-0.5}^{b}|\frac{\zeta'(\sigma+iT_1)}{\zeta(\sigma+iT_1)})\frac{|x^{\sigma+iT_1}|}{|\sigma+iT_1|}d\sigma \le \frac{1}{2\pi}\int_{-0.5}^{b}|\frac{\zeta'(\sigma+iT_1)}{\zeta(\sigma+iT_1)})\frac{x^\sigma}{T}d\sigma$. Так как по выбору T_1 имеем что $|\beta_n + \sigma + i(T_1 - \gamma_n)| \ge \frac{c}{2\ln T}$, то $\frac{\zeta'(\sigma+iT_1)}{\zeta(\sigma+iT_1)} = \sum_{|T_1-\gamma_n|\le 1}\frac{1}{\sigma+iT_1-\rho_n} + O(\ln T_1) = O(\ln^2 T) + O(\ln T) = O(\ln^2 T) = O(\ln^2 x)$. Таким образом, $J_1 = O(\frac{x\ln^2 x}{T})$. 2. $|J_2| \le \frac{1}{2\pi}\int_{-T_1}^{T_1}|\frac{\zeta'(-0.5+it)}{\zeta(-0.5+it)}||\frac{x^{-0.5+it}}{-0.5+it}|dt \le \frac{1}{2\pi}2\int_0^{T_1} \le \frac{1}{\pi}\int_0^2|\frac{\zeta'(-0.5+it)}{\zeta(-0.5+it)}|\frac{x^{-0.5}}{0.5}dt + \int_2^{T_1}|\frac{\zeta'(-0.5+it)}{\zeta(-0.5+it)}|\frac{x^{-0.5}}{t}dt \le \frac{1}{\pi}(O(x^{-0.5}) + O(x^{-0.5}\ln^2 T_1)) = O(1)$. Здесь для первого интеграла все остальное дает константу, а для второго имеем $\frac{\zeta'(-0.5+it)}{\zeta(-0.5+it)} = \sum_{|t-\gamma_n|\le 1}\frac{1}{-0.5+it-\rho_n} + O(\ln t) = O(1) + O(\ln t) = O(\ln t)$, так как $|Re(-0.5 - \rho_n + it)| = |-0.5 - \beta_n| = O(1)$, то есть вся первая сумма есть $O(1)$. Таким образом, все три интеграла попадают в остаточный член.

Осталось оценить $\sum_{T<|Im\rho_n|\le T_1}\frac{x^{\rho_n}}{\rho_n} = O(\frac{x^{\beta_n}}{T}\ln T) = O(\frac{x}{T}\ln T) = O(\frac{x\ln x}{T})$, так как 1. $\beta_n \le 1 \Rightarrow O(x^{\rho_n}) = O(x)$, 2. $T \le |\gamma_n| \Rightarrow \frac{1}{|\rho_n}| = O(\frac{1}{T})$, 3. $\sum_{T<|Im\rho_n|\le T_1} \le \sum_{T<|Im\rho_n|<T+1}$ - число слагаемых $O(\ln T)$.

8 Арифметические функции и их средние значения

8.1 Функции "целая часть"и "дробная часть"

Функция "целая часть x", обозначаемая $\lfloor x\rfloor$, есть наибольшее целое число, не превосходящее x. Например, $\lfloor 2.9\rfloor = 2$, $\lfloor -2\rfloor = -2$, и $\lfloor -2.3\rfloor = -3$.

Функция "дробная часть x"определяется как $\{x\} = x - \lfloor x\rfloor$.

Функция $\lceil x\rceil$ определяется как наименьшее целое число, большее или равное x. Например, $\lceil 2.3\rceil = 3$, $\lceil 2\rceil = 2$, и $\lceil -2.3\rceil = -2$.

Свойства функций $\lfloor x\rfloor$ и $\lfloor x\rfloor$

1. $\lfloor x\rfloor \le x < \lfloor x\rfloor + 1$ с равенством слева если и только если x - целое.

2. $\lfloor\lfloor x\rfloor\rfloor = \lfloor x\rfloor$ (идемпотентность).

3. Для любого целого k и любого действительного x, $\lfloor k + x\rfloor = k + \lfloor x\rfloor$.

4. Расстояние от x до ближайшего целого можно записать как $\lfloor x + 0.5\rfloor$.

5. Если x - действительное число, и n - целое число, то $n \leq x$ если и только если $n \leq \lfloor x \rfloor$.

6. Для действительного нецелого x мы имеем разложение в ряд Фурье $\lfloor x \rfloor = x - \frac{1}{2} + \frac{1}{\pi}\sum_{k=1}^{\infty}\frac{\sin(2\pi kx)}{k}$.

7. Если m и n - взаимно-простые натуральные числа, то $\sum_{i=1}^{n-1}\lfloor\frac{im}{n}\rfloor = \frac{(m-1)(n-1)}{2}$.

8. $\sharp\{n \in \mathbb{N} : n \leq x, d|N\} = \lfloor\frac{x}{d}\rfloor$.

9. $\lfloor x \rfloor - 2\lfloor\frac{x}{2}\rfloor = 0$ или 1.

10. $n! = p_1^{\alpha_1}...p_k^{\alpha_k}$, где p_i пробегает все простые, не превосходящие n, и $\alpha_i = \lfloor\frac{n}{p_i}\rfloor + \lfloor\frac{n}{p_i^2}\rfloor + ...$

11. $\lceil x \rceil = -\lfloor -x \rfloor$.

12. $x \leq \lceil x \rceil < x + 1$.

13. Для любого целого k, $\lfloor\frac{k}{2}\rfloor + \lceil\frac{k}{2}\rceil = k$.

Рассмотрим, например, доказательство свойства 9. Пусть d, $2d$, ..., $kd \leq x < (k+1)d$. Тогда $\sharp\{n \in \mathbb{N} : n \leq x, d|n\} = k$. С другой стороны, $k \leq \frac{x}{d} < k + 1$, то есть, $k = \lfloor\frac{x}{d}\rfloor$.

Упражнения

1. Построить графики всех упомянутых функций.

2. Доказать вышеприведенные свойства.

8.2 Мультипликативные функции

Мультипликативная функция - это комплекснозначная функция $f(n)$ натурального аргумента n, удовлетворяющая условиям $f(1) = 1$, и, для взаимно-простых a и b, $f(ab) = f(a)f(b)$.

Мультипликативная функция $f(n)$ называется вполне мультипликативной, если $f(ab) = f(a)f(b)$ для любых натуральных a и b.

Примеры мультипликативных функций:

1. $\phi(n)$: функция Эйлера, дающая число натуральных чисел, не превосходяших n и взаимно-простых с ним;

2. $\mu(n)$: функция Мебиуса, связянная с простыми делителями бесквадратных чисел;

3. $gcd(n, k)$: наибольший общий делитель n и k, где k фиксированно;

4. $\tau(n)$: число натуральных делителей n;

5. $\sigma(n)$: сумма натуральных делителей n;

6. $\sigma_k(n)$: k-функция делителей, представляющая собой сумму k-ых степеней натуральных делителей n (где k - любое комплексное число); в специальных случаях мы имеем $\sigma_0(n) = \tau(n)$, и $\sigma_1(n) = \sigma(n)$;

7. $1(n)$: функция, определяемая как $1(n) \equiv 1$ (вполне мультипликативна);

8. $1_C(n)$: характеристическая функция множества C (квадратов, кубов, и т.д.), $1_C(n) = 1$ для $n \in C$, и $1_C(n) = 0$, иначе;

9. $Id(n)$: функция $Id(n) = n$ (вполне мультипликативна);

10. $Id_k(n)$: функция, определенная как $Id_k(n) = n^k$ для любого комплексного числа k (вполне мультипликативна); как специальные случаи мы имеем $Id_0(n) = 1(n)$, и $Id_1(n) = Id(n)$;

11. $\varepsilon(n)$: функция, определяемая как $\varepsilon(n) = 1$, если $n = 1$ и $\varepsilon(n) = 0$, если $n > 1$, иногда называемая мультипликативной единицей для конволюции Дирихле (вполне мультипликативна);

12. $(\frac{n}{p})$: символ Лежандра, где p - фиксированное нечетное простое число (вполне мультипликативна);

13. $\lambda(n)$: функция Лиувилля, определяемая как $\lambda(n) = (-1)^{\Omega(n)}$, где $\Omega(n)$ - число простых делителей n, считаемых с повторениями (вполне мультипликативна);

14. $\gamma(n)$: функция, определяемая как $\gamma(n) = (-1)^{\omega(n)}$, где аддитивная функция $\omega(n)$ дает число различных простых делителей n;

15. $\chi(n)$: любой характер Дирихле является вполне мультипликативной функцией.

Примерами функций, которые не являются мультипликативными, являются функция $\pi(x)$, функция Мангольдта $\Lambda(n)$, функция $r_2(n)$ - число представлений n в виде суммы двух квадратов целых чисел. Например: $1 = 1^2 + 0^2 = (-1)^2 + 0^2 = 0^2 + 1^2 = 0^2 + (-1)^2$ и, следовательно, $r_2(1) = 4 \neq 1$. Это показывает, что данная функция не является мультипликативной. Однако функция $r_2(n)/4$ мультипликативна.

Свойства мультипликативных функций

1. Если f и g мультипликативны, то и fg мультипликативна.

2. Если f мультипликативна, то, для данного $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, $\sum_{d|n} f(d) = \prod_{i=1}^{k}(1 + f(p_i) + f(p_1^2) + ... + f(p_i^{\alpha_k}))$.

3. Если f мультипликативна, то $h(n) = \sum_{d|n} f(d)$ мультипликативна.

4. Мультипликативная функция f полностью определяется ее значениями на степенях простых чисел: $f(p_1^{\alpha_1}...p_k^{\alpha_k}) = f(p_1^{\alpha_1})...f(p_k^{\alpha_k})$.

5. Если f мультипликативна, и a, b - произвольные натуральные числа, то $f(a)f(b) = f(gd(a,b))f(lcm(a,b))$.

Рассмотрим, например, доказательство третьего свойства. Если a и b взаимно-просты, то, для любого делителя d числа ab, мы можем записать его как $d = d_1 d_2$, где d_1 и d_2 взаимно-просты, и $d_1|a$, $d_2|b$. Тогда $h(ab) = \sum_{d|ab} f(d) = \sum_{d_1|a, d_2|b} f(d_1 d_2) = \sum_{d_1|a} f(d_1) \sum_{d_2|b} f(d_2) = h(a)h(b)$.

Если f и g мультипликативны, мы можем определить новую мультипликативную функцию $f*g$, называемую *конволюцией Дирихле функций f и g*, следующим образом: $(f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$, где сумма берется по всем натуральным делителям d числа n. Множество всех мультипликативных функций, снабженное этой операцией, превращается в абелеву группу; ε является единичным элементом.

Упражнения

1. Проверить, что функции, представленные выше, мультипликативны.

2. Доказать свойства мультипликативных функций.

8.3 Формула обращения Мебиуса

Рассмотрим функцию Мебиуса $\mu(n)$, определенную для всех натуральных n, и принимающую значения из множества $\{-1, 0, 1\}$ в зависимости от разложения n на простые множители: $\mu(n) = 1$, если n - бесквадратное число с четным числом простых делителей; $\mu(n) = -1$, если n - бесквадратное число с нечетным числом простых делителей; $\mu(n) = 0$, если n не является бесквадратным.

Функция Мебиуса мультипликативна. Кроме того, имеет место следующее свойство: $\sum_{d|n} \mu(d) = 1$ для $n = 1$, и $\sum_{d|n} \mu(d) = 0$, иначе. Действительно, для $n = 1$ доказательство очевидно. Если $n \neq 1$, то $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, и $\sum_{d|n} \mu(d) = \prod_{i=1}^{k}(1 + \mu(p_1) + \mu(p_1^2) + ...) = \prod_{i=1}^{k}(1 - 1 + 0...) = 0$.

Theorem 9 *$F(n) = \sum_{d|n} f(d)$ если и только если $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d})$.*

Доказательство. $\sum_{d|n} \mu(d)F(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) =$
$\sum_{cd|n} \mu(d)f(c) = \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d) = f(n)$.

С другой стороны, $\sum_{d|n} f(d) = \sum_{d|n} \sum_{c|d} \mu(c)F(\frac{d}{c}) = \sum_{k|n} F(k) \sum_{c} \frac{n}{k}\mu(c) = F(n)$.

В терминах конволюции Дирихле, первая формула может быть записана как $F = f*1$, где 1 - это функция $1(n) \equiv 1$. Вторая формула примет вид $f = F*\mu$.

Упражнения

1. Показать, что $\sum_{d|n} \mu(d)\tau(\frac{n}{d}) = 1$.

2. Показать, что $\sum_{d|n} \mu(d)\frac{n}{d} = \phi(n)$.

3. Показать, что $\sum_{d|n} \mu(d)\sigma(\frac{n}{d}) = n$.

8.4 Средние значения некоторых арифметических функций

В теории чисел имеется много арифметических функций, играющих важную роль при решении различных проблем. Однако, как правило, поведение таких функций крайне нерегулярно, и исследовать его очень нелегко.

Но часто оказывается возможным получить полезную информацию о поведении функции f "в среднем", то есть, рассмотреть функцию

$$F(x) = \sum_{1 \leq n \leq x} f(n),$$

которая называется *средним значением функции f на интервале* $[1, x]$. Обычно данная функция ведет себя значительно лучше.

Напомним, что $f(x) = O(g(x))$, если для некоторого x_0 мы имеем: для любого $x \geq x_0$ функция $g(x) > 0$, и $|f(x)| \leq Cg(x)$ для некоторой положительной константы C.

- **Средние значения функции** $\sigma(n)$

Theorem 10 *Для данного натурального* N,

$$\sum_{n=1}^{N} \sigma(n) = \frac{\pi^2}{12} N^2 + O(N \ln N).$$

Доказательство. Мы имеем:

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} \sum_{d|n} d = \sum_{n=1}^{N} \sum_{d|n} \frac{n}{d} = \sum_{d=1}^{N} \sum_{n \leq N, d|n} \frac{n}{d}.$$

Так как $\sum_{n \leq N, d|n} \frac{n}{d} = \sum_{s=1}^{\lfloor \frac{N}{d} \rfloor} s = \frac{1}{2} \lfloor \frac{N}{d} \rfloor (\lfloor \frac{N}{d} \rfloor + 1)$, мы получим что

$$\sum_{n=1}^{N} \sigma(n) = \frac{1}{2} \sum_{d=1}^{N} (\frac{N}{d} - \{\frac{N}{d}\})(\frac{N}{d} + 1 - \{\frac{N}{d}\}) = \frac{N^2}{2} \sum_{d=1}^{\infty} \frac{1}{d^2} - \frac{N^2}{2} \sum_{d=N+1}^{\infty} \frac{1}{d^2} + O(N \sum_{d=1}^{N} \frac{1}{d}).$$

Так как $\sum_{1}^{\infty} \frac{1}{d^2} = \zeta(2) = \frac{\pi^2}{6}$, и $\sum_{N+1}^{\infty} \frac{1}{d^2} < \sum_{n+1}^{\infty} (\frac{1}{d-1} - \frac{1}{d}) = \frac{1}{N} = O(\frac{1}{N})$, мы получим, что

$$\sum_{n=1}^{N} \sigma(n) = \frac{N^2 \pi}{12} + O(N \ln N).$$

- **Средние значения функции Эйлера** $\phi(n)$

Theorem 11 *Для любого натурального* N,

$$\sum_{d=1}^{N} \phi(n) = \frac{3N^2}{\pi^2} + O(N \ln N).$$

Доказательство. Мы имеем, что

$$\sum_{n=1}^{N} \phi(n) = \sum_{n=1}^{N} n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d=1}^{N} \frac{\mu(d)}{d} \sum_{n \leq N, d|n} n.$$

Используя аргументы доказательства предыдущей теоремы и замечая, что $\sum \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$, мы получим результат теоремы аналогичным образом.

- **Средние значения функции** $\tau(n)$

Для получения информации о средних значениях функции $\tau(n)$, нам нужно получить дополнительную информацию о средних значениях арифметической функции $f(n) = \frac{1}{n}$.

Theorem 12 *Для любого натурального N,*

$$\sum_{k=1}^{N} \frac{1}{k} = \ln N + O(1).$$

Доказательство. Мы имеем:

$$\frac{1}{k} \leq \int_{k}^{k+1} \frac{dx}{x} \leq \frac{1}{k+1},$$

то есть, $0 \leq \frac{1}{k} - \int_k^{k+1} \frac{dx}{x} \leq \frac{1}{k} - \frac{1}{k+1}$, и $0 \leq \sum_{k=1}^{N} \frac{1}{k} - \int_1^N \frac{dx}{x} \leq 1\frac{1}{N+1} + \int_N^{N+1} \frac{dx}{x} = 1 + O(\frac{1}{N+1} = O(1)$. Таким образом,

$$\sum_{k=1}^{N} \frac{1}{k} = \ln N + O(1).$$

Theorem 13 *Для любого натурального N,*

$$\sum_{n=1}^{N} \tau(n) = N \ln N + O(N).$$

Доказательство. Мы имеем:

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \sum_{d|N} 1 = \sum_{nm \leq N} 1 = \sum_{1 \leq k \leq N} \lfloor \frac{N}{k} \rfloor =$$

$$= N \sum_{k=1}^{N} \frac{1}{k} + O(N) = N \ln N + O(N).$$

Заметим, что, пользуясь теми же методами, мы можем получить более точные результаты для $\frac{1}{n}$ и $\tau(n)$, но доказательства будут неоправданно громоздкими. В следуюшем разделе мы получим эти результаты, пользуясь специальными теоретико-числовыми методами.

Theorem 14 *Для любого натурального числа N,*

$$\sum_{k=1}^{N} \frac{1}{k} = \ln N + \gamma + O(\frac{1}{N}),$$

где $\gamma = \lim_{N\to\infty}(\sum_{n=1}^{N} \frac{1}{n} - \int_1^N \frac{dx}{x}) = 0.57721...$ *- постоянная Эйлера.*

Доказательство. Легко видеть, что

$$\frac{1}{k} \leq \int_k^{k+1} \frac{dx}{x} \leq \frac{1}{k+1},$$

то есть, $0 \leq \frac{1}{k} - \int_k^{k+1} \frac{dx}{x} \leq \frac{1}{k} - \frac{1}{k+1}$, и $0 \leq \sum_{k=1}^{N} \frac{1}{k} - \int_1^N \frac{dx}{x} \leq 1 + O(\frac{1}{N})$. Таким образом, при $N \to \infty$ величина $\sum_{k=1}^{N} \frac{1}{k} - \int_1^N \frac{dx}{x} = \sum_{k=1}^{N} \frac{1}{k} - \ln N$ сходится к некоторой константе γ. Теперь мы можем записать, что

$$\sum_{k=1}^{N} \frac{1}{k} = \ln N + \gamma + O(\sum_{k=N+1}^{\infty} \frac{1}{k} - \int_{N+1}^{\infty} \frac{dx}{x}),$$

где последний остаточный член, в свете последних рассуждений, равен $O(\frac{1}{N+1})$, то есть, $O(\frac{1}{N})$.

Theorem 15 *Для любого натурального N,*

$$\sum_{n=1}^{N} \tau(n) = N \ln N + (2\gamma - 1) + O(\sqrt{N}).$$

Доказательство. Мы имеем:

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \sum_{d|N} 1 = \sum_{nm \leq N} 1 = 2 \sum_{1 \leq k \leq \sqrt{N}} \lfloor \frac{N}{k} \rfloor - \lfloor \sqrt{N} \rfloor^2 =$$

$$= 2N \sum_{k=1}^{\sqrt{N}} \frac{1}{k} + O(\sqrt{N}) - N = 2N(\ln \sqrt{n} + \gamma + O(\frac{1}{\sqrt{N}})) - N + O(\sqrt{N})$$

$$= N \ln N + (2\gamma - 1) + O(\sqrt{N}).$$

Заметим, что среднее значение функции $\tau(n)$ дает нам число точек с натуральными координатами под гиперболой $xy = N$: $\sum_{n=1}^{N} \tau(n) = \sum_{nm \leq N} 1$ (*проблема делителей Дирихле*). Аналогичные аргументы позволяют получить число целых точек в круге (*проблема Гаусса о числе целых точек в круге*).

Theorem 16 *Число целых точек в круге $x^2 + y^2 = R^2$ равно*

$$\pi R^2 + O(R).$$

- Таким образом, "в среднем"функция $\tau(n)$ ведет себя как $\log n$, сумма делителей - как константа $\frac{\pi^2}{12} \approx 0.82246...$, умноженная на n, и функция Эйлера - как константа $\frac{3}{\pi^2} \approx 0,3096...$, умноженная на n:

$$\tau(n) \sim logn;$$

$$\sigma(n) \sim 0,82246... \cdot n;$$

$$\varphi(n) \sim 0.3069... \cdot n.$$

Упражнения

1. Доказать, что $\tau(1)+...+\tau(n) = \lfloor \frac{n}{1} \rfloor + ... + \lfloor \frac{n}{n} \rfloor$.
2. Доказать, что $\sigma(1)+...+\sigma(n) = 1 \cdot \lfloor \frac{n}{1} \rfloor + ... + n \cdot \lfloor \frac{n}{n} \rfloor$.
3. Найти число точек с натуральными координатами под параболой $y = -ax^2$.
4. Найти число целых точек в эллипсе.

9 Проблема делителей Дирихле и проблема Гаусса о числе целых точек в круге

9.1 Целые точки

В предыдущем разделе мы рассмотрели фунуцию делителей

$$\tau(n) = \sum_{d|n} 1,$$

которая дает число натуральных делителей числа n. Это хорошо известная арифметическая функция, принимающая значения от 2, для любого $p \in P$, до n^ϵ для некоторых специальных натуральных чисел. Таким образом, асимптотическое поведение $\tau(n)$ очень специфично.

Но мы получим полезную информацию об асимптотическом поведении $\tau(n)$ "в среднем", то есть, исследуя функцию

$$D(x) = \sum_{1 \le n \le x} \tau(n),$$

которая является средним значением функции делителей на $[1, x]$. Эта функция ведет себя очень хорошо, именно, как $x \log x$ для больших x.

Точнее, мы можем получить следующую асимптотическую формулу для $D(x)$:

$$D(x) = \sum_{n \le x} \tau(n) = x \log x + (2\gamma - 1)x + \Delta(x),$$

где остаточный член

$$\Delta(x) = O(x^{1/2}),$$

и

$$\gamma = 0.5772157... = \lim_{N \to +\infty} (\sum_{k=1}^{N} k^{-1} - \log N)$$

- постоянная Эйлера. Этот классический результат был получен Дирихле (1849), и проблема нахождения точного значения остаточного члена $\Delta(x)$ при $x \to +\infty$ называется проблемой делителей Дирихле.

Обозначив через α наименьшее действительное число, для которого $\Delta(x) = O(x^\alpha)$, мы можем записать, что $1/4 \le \alpha \le 1/2$. Последние результаты в этой области имеют вид $\alpha = 1/3 - \epsilon$.

Напомним, что среднее значение $\tau(n)$ дает число точек с натуральными координатами под гиперболой $x_1x_2 = x$. Следовательно, проблема делителей Дирихле является примером проблемы вычисления числа целых точек в некоторой области.

Эще один известный пример такой проблемы - проблема Гаусса о числе целых точек в круге. Классический результат Гаусса дает следующую асимптотическую формулу для числа целых точек в круге радиуса $\sqrt{x}$:

$$\sum_{x_1^2+x_2^2\le x} 1 = \pi x + O(\sqrt{x}).$$

Функция Эйлера $\varphi(n)$ связана с еще одним примером такого рода.

Рассмотрим квадратную решетку Z^2 - множество всех целых точек плоскости.

Целая точка P называется *видимой из начала координат*, если отрезок, соединяющий точки P и O, не содержит других целых точек.

Легко показать, что точка P с координатами (a, b) видима из начала координат если и только если a и b взаимно-просты.

Тогда число $N^{'}(r)$ целых точек, видимых из начала координат, в квадрате со стороной $2r$ и центром O, равно

$$N^{'}(r) = 8\sum_{1\le n\le r}\ \sum_{1\le m\le n,(m,n)=1} 1,$$

или

$$N^{'}(r) = 8\sum_{1\le n\le r}\varphi(n).$$

Используя результат о среднем значении $\varphi(n)$, мы получим, что

$$N^{'}(r) = \frac{24r^2}{\pi^2} + O(r\log r).$$

Следовательно, целые точки, видимые из начала координат, составляют $\frac{24r^2/\pi^2}{4r^2} = \frac{24}{4\pi^2} = 0,61...$ часть всех целых точек плоскости.

9.2 Формула Эйлера-Маклорена

Theorem 17 *Пусть f непрерывно-дифференцируема на $[a,b]$; пусть $\rho(x) = \frac{1}{2} - \{x\}$. Тогда*

$$\sum_{a<x\le b} f(x) = \int_a^b f(x)dx + \rho(b)f(b) - \rho(a)f(a) - \int_a^b \rho(x)f^{'}(x)dx.$$

Доказательство. Мы имеем:

$$\int_a^b \rho(x)f^{'}(x)dx = \int_a^b \rho(x)df(x) = \int_a^{\lfloor a\rfloor+1}\rho(x)df(x) + \sum_{n=\lfloor a\rfloor+1}^{\lfloor b\rfloor-1}\int_n^{n+1}\rho(x)df(x)$$

$$+\int_{\lfloor b\rfloor}^b \rho(x)df(x) = \rho(x)f(x)|_a^{\lfloor a\rfloor+1} - \int_a^{\lfloor a\rfloor+1} f(x)d\rho(x) + \sum_{n=\lfloor a\rfloor+1}^{\lfloor b\rfloor-1}(\rho(x)f(x)|_n^{n+1}$$

$$-\int_n^{n+1} f(x)d\rho(x)) + (\rho(x)f(x)|_{\lfloor b\rfloor}^b - \int_{\lfloor b\rfloor}^b f(x)\rho(x)).$$

Для $n \le x < n+1$, $\rho(x) = \frac{1}{2} + n - x$, и $d\rho(x) = -dx$. Для $n \le x < n+1$, $\lim_{x\to n+1}\rho(x)f(x) = -\frac{1}{2}f(n+1)$, и $\rho(x)f(x)|_n^{n+1} = -\frac{1}{2}f(n+1) - \frac{1}{2}f(n)$. Аналогично, $\rho(x)f(x)|_a^{\lfloor a\rfloor+1} = -\frac{1}{2}f(\lfloor a\rfloor+1) - \rho(a)f(a)$. Наконец, $\rho(x)f(x)|_{\lfloor b\rfloor}^b = \rho(b)f(b) - \frac{1}{2}f(\lfloor b\rfloor)$, если b не является целым, и $\rho(x)f(x)|_{\lfloor b\rfloor}^b = 0 = \rho(b)f(b) - \frac{1}{2}f(\lfloor b\rfloor)$, если $b \in \mathbb{Z}$.

Тогда мы получим

$$\int_a^b \rho(x)f'(x)dx = \int_a^b f(x)dx - \rho(a)f(a) + \rho(b)f(b) - \frac{1}{2}f(\lfloor a\rfloor+1)$$

$$-\frac{1}{2}\sum_{n=\lfloor a\rfloor+1}^{\lfloor b\rfloor-1}(f(n+1)+f(n)) - \frac{1}{2}f(\lfloor b\rfloor).$$

Теперь,

$$\sum_{a<x\le b} f(x) = \int_a^b f(x)dx + \rho(b)f(b) - \rho(a)f(a) - \int_a^b \rho(x)f'(x)dx.$$

Можно получить и более точную формулу того же типа.

Theorem 18 *Пусть f дважды непрерывно-дифференцируема на $[a,b]$. Тогда*

$$\sum_{a<x\le b} f(x) = \int_a^b f(x)dx + \rho(b)f(b) - \rho(a)f(a) + \sigma(a)f'(a) - \sigma(b)f'(b) + \int_a^b \sigma(x)f''(x)dx,$$

где $\sigma(x) = \int_0^x \rho(u)du$.

Доказательство. Используя то, что $\sigma'(x) = \rho(x)$, и $\sigma(m) = 0$ для целого m, мы получим, что

$$\int_a^b \sigma(x)f''(x)dx = \int_a^b \sigma(x)sf'(x) = \sigma(b)f'(b) - \sigma(a)f'(a) - \int_a^b f'(x)\rho(x)dx.$$

Используя формулу для $\int_a^b f'(x)\rho(x)dx$, полученную в доказательстве предыдущей теоремы, мы получим доказательство нашего результата аналогичным образом.

9.3 Проблема делителей Дирихле

Theorem 19 *Число целых точек под гиперболой $xy = R$ $(R > 1)$ равно*

$$R(\ln R + 2\gamma - 1) + \Delta(R), \Delta(R) = O(\sqrt{R}).$$

Доказательство. Как было показано ранее, число T целых точек под гиперболой $xy = R$ равно $T = 2\sum_{o<x\le\sqrt{R}}\frac{R}{x} - R + O(\sqrt{R})$. Используя формулу Эйлера-Маклорена, мы получим

$$\sum_{1<x\le Y}\frac{1}{x} = \int_1^Y \frac{dx}{x} + \rho(Y)f(Y) - \rho(1)f(1) + \int_1^Y \rho(x)\frac{dx}{x^2}$$

$$= \ln Y + \frac{\rho(Y)}{Y} - \frac{1}{2} + \int_1^Y \frac{\rho(x)dx}{x^2},$$

и, следовательно,

$$\sum_{0<x\le Y} \frac{1}{x} = \ln Y + \frac{\rho(Y)}{Y} + \frac{1}{2} + \int_1^Y \frac{\rho(x)dx}{x^2}.$$

Тогда $\gamma = \lim_{Y\to\infty}(\sum_{x=1}^{Y} \frac{1}{x} - \ln Y) = \frac{1}{2} + \int_1^\infty \frac{\rho(x)dx}{x^2}$, и

$$\sum_{0<x\le\sqrt{R}} \frac{1}{x} = \frac{1}{2}\ln R + \frac{\rho(\sqrt{R})}{\sqrt{R}} + \frac{1}{2} + \int_1^{\sqrt{R}} \frac{\rho(x)dx}{x^2}.$$

Следовательно, $T = 2R(\frac{1}{2}\ln R + \gamma + O(\frac{1}{\sqrt{R}})) - R + O(\sqrt{R}) = R\ln R + R(2\gamma - 1) + O(\sqrt{R})$.

9.4 Проблема Гаусса о числе целых точек в круге

Theorem 20 *Число целых точке в круге $x^2 + y^2 \le R^2$ $(R > 1)$ равно*

$$\pi R^2 + \Delta(R), \Delta(R) = O(R).$$

Доказательство. Легко видеть, что число T целых точек в круге $x^2 + y^2 = R^2$ равно

$$T = 8\sum_{0<x\le\frac{R}{\sqrt{2}}} \lfloor\sqrt{R^2 - x^2}\rfloor - 4\lfloor\frac{R}{\sqrt{2}}\rfloor^2 + 4\lfloor R\rfloor + 1$$

$$= 8\sum_{0<x\le\frac{R}{\sqrt{2}}} \sqrt{R^2 - x^2} - 2R^2 + O(R).$$

Обозначим $\sum_{0<x\le\frac{R}{\sqrt{2}}} \sqrt{R^2 - x^2}$ как $\sum$. Тогда, по формуле Эйлера-Маклорена,

$$\sum = \int_0^{R/\sqrt{2}} \sqrt{R^2 - x^2}dx + \rho(\frac{R}{\sqrt{2}})\sqrt{R^2 - \frac{R^2}{2}} - \rho(0)\sqrt{R^2} - \int_0^{R/\sqrt{2}} \rho(x)f'(x)dx.$$

Здесь $f(x) = \sqrt{R^2 - x^2}$, и $| - \int_0^{R/\sqrt{2}} \rho(x)f'(x)dx| \le |f(x)||_0^{R/\sqrt{2}} = O(R)$, кроме того, рассматриваемый интеграл соответствует площади $1/8$ части круга, то есть, равен $\frac{1}{8}\pi R^2 + \frac{R^2}{4}$. Теорема доказана.

10 Целые точки и тригонометрические суммы

В этом разделе мы рассмотрим классические результаты в проблеме делителей Дирихле и проблеме Гаусса о числе целых точек в круге.

Число целых точек под гиперболой $xy = R$ $(R > 1)$ равно

$$R(\ln R + 2\gamma - 1) + \Delta(R), \Delta(R) = O(\sqrt[3]{R}).$$

Число целых точек в круге
$x^2 + y^2 \le R^2$ $(R > 1)$ равно

$$\pi R^2 + \Delta(R), \Delta(R) = O(R^{2/3}).$$

11 Многомерная проблема делителей

Рассмотрим арифметическую функцию

$$\tau_k(n) = \sum_{n_1 \dots n_k = n} 1,$$

которая дает число представлений n в виде произведения k натуральных множителей.

Легко видеть, что для $k = 2$ функция $\tau_2(n)$ совпадает с функцией $\tau(n)$, и, следовательно, функция $\tau_k(n)$ является обобщением функции делителей.

Рассмотрим функцию

$$D_k(x) = \sum_{n \le x} \tau_k(n) = \sum_{n_1 \dots n_k \le x} 1$$

- среднее значение функции $\tau_k(n)$. Она дает число целых точек под гиперболической поверхностью $x_1 \dots x_k = x$.

Элементарные рассуждения позволяют получить следующую асимптотическую формулу для $D_k(x)$:

$$D_k(x) = \sum_{n \le x} \tau_k(n) = xP_k(\log x) + \Delta_k(x),$$

где P_k - многочлен степени $k-1$, и $\Delta_k(x)$ - остаточный член.

Оценка данного остаточного члена известна как *многомерная проблема делителей.* Обобщение метода Дирихле дает следующую оценку для $\Delta_k(x)$:

$$\Delta_k(x) = O(x^{1-1/k} \log^{k-2} x),$$

но, используя теорию функции $\zeta(s)$, мы получим более точные результаты.

Пусть α_k - наименьшее действительное число, для которого

$$\Delta_k(x) = O(x^{\alpha_k + \epsilon})$$

для каждого положительного ϵ. Таким образом, многомерная проблема делителей состоит в получении возможно лучшей оценки величины α_k.

История оценок α_k такова:

- $\alpha_k \le 1 - \frac{1}{k}, k \ge 2$, Дирихле, 1849;
- $\alpha_k \le 1 - \frac{2}{k+1}, k \ge 2$, Вороной, 1903, $k = 2$, Ландау, 1912, $k \ge 3$;
- $\alpha_k \le 1 - \frac{3}{k+2}, k \ge 4$, Харди и Литтлвуд, 1922;
- $\alpha_k \le 1 - \frac{3}{k}, k \ge 8$, Хис-Браун, 1981;
- $\alpha_k \le 1 - \frac{165}{28k}, k \ge 120$, Ивич, 1989.

Заметим, что Вороной доказал, что $\alpha_2 \le 1/2$. С другой стороны, Харди и Литтлвуд независимо получили оценку $\alpha_2 \ge 1/4$ ($\alpha_k \ge \frac{1}{2} - \frac{1}{2k}$). Гипотеза $\alpha_2 = 1/4$ не доказана и не опровергнута.

Все эти результаты имеют вид

$$\alpha_k \le 1 - \frac{c}{k}, k \ge k_0, \tag{1}$$

где $c > 0$ - положительная постоянная.

В некоторых работах можно найти оценки другого рода:

- $\alpha_k \le 1 - \frac{\log k}{k}, k \ge k_0$, Рихерт, 1956;
- $\alpha_k \le 1 - \frac{c}{k^{2/3}}, k \ge k_0$, Рихерт, 1960;
- $\alpha_k \le 1 - \frac{c}{k^{2/3}}, k \ge 2$, Карацуба, 1972.

Эт оценки имеют вид

$$\alpha_k \le 1 - \frac{c}{k^{2/3}}. \tag{2}$$

Очевидно, вторая оценка принципиально лучше первой, но известные на сегодняшний день значения константы c из последней оценки малы, и мы получим улучшение только при очень больших k. Так, Ивич (1989) показал, что

$$\alpha_k \le 1 - \frac{1}{50k^{2/3}}, k \ge 100.$$

Это лучше, чем оценка

$$\alpha_k \le 1 - \frac{165}{28k}, k \ge 120$$

только для $k \ge 2,6 \cdot 10^7$.

Следовательно, проблема улучшения константы c очень интересна.

Мы получим следующую формулу:

$$D_k(x) = xP_k(\log x) + \theta x^{1-\frac{1}{13k^{2/3}}}(C\log x)^k,$$

где P_k - многочлен степени $k-1$, $2 \le k << \log^{5/6} x$, θ - комплексное число, $|\theta| \le 1$, $C > 0$-абсолютная константа.

Данный остаточный член равномерен для всех $k << \log^{5/6} x$, и значение константы c из оценки (2) для α_k равно $c = 1/13$, что лучше (1) уже при $k \ge 10^5$.

Проблема делителей является одной из классических теоретико-числовых проблем, связанных с изучением *рядов Дирихле*

$$f(s) = \sum_{n=1}^{+\infty} a_n n^{-s}, Res > \sigma_0,$$

где $a_n \in C$ - коэффициенты ряда, а $s = \sigma + it$ - комплекснозначный аргумент.

Наиболее известным рядом Дирихле является дзета-функция Римана, определяемая как

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s}$$

для $Res > 1$.

Примерами рядов Дирихле служат и функции

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\Lambda(n)}{n^s}, Res > 1$$

- логарифмическая производная дзета-функции, и

$$\zeta^k(s) = \sum_{n=1}^{+\infty} \frac{\tau_k(n)}{n^s}, Res > 1,$$

– k-я степень дзета-функции.

С рядом Дирихле $f(s)$ тесно связана функция

$$\Phi(x) = \sum_{n \le x} a_n,$$

которая называется *сумматорной функцией коэффициентов ряда Дирихле.*

Для многих рядов $f(s)$ можно использовать формулу обращения Перрона, связывающую функции $f(s)$ и $\Phi(x)$:

$$\Phi(x) = \frac{1}{2\pi i} \int_{c-\infty}^{c+\infty} f(s) \frac{x^s}{s} ds.$$

Это верно и для логарифмической производной дзета-функции, и для ее k-ой степени.

Сумматорная функция для первого случая - известная функция Чебышева

$$\psi(x) = \sum_{n \le x} \Lambda(n),$$

где $\Lambda(n)$ - функция Мангольдта ($\Lambda(n) = \log p, n = p^k, k \in N$, и $\Lambda(n) = 0$, иначе), и, пользуясь формулой обращения Перрона

$$\psi(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} (-\frac{\zeta'(s)}{\zeta(s)}) \frac{x^s}{s} ds,$$

мы получаем асимптотическую формулу

$$\psi(x) = x + O(xe^{-c\sqrt{\log x}}).$$

Это эквивалентно асимптотическому закону распределения простых чисел:

$$\pi(x) = \sum_{p \le x} 1 = \frac{x}{\log x} + O(xe^{-\frac{\alpha}{2}\sqrt{\log x}}).$$

Сумматорная функция для k-ой степени дзета-функции совпадает с функцией $D_k(x)$ - средним значением обобщенной функции делителей $\tau_k(n)$. По формуле обращения мы имеем

$$D_k(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \zeta^k(s) \frac{x^s}{s} ds.$$

Сдвигая линию интегрирования к некоторому c_1, меньшему 1, но достаточно близкому к 1, и замечая, что подинтегральная функция имеет только один полюс порядка k в точке $s = 1$, мы получим, по теореме Коши о вычетах,

$$D_k(x) = xP_k(\log x) + \Delta_k(x),$$

где

$$xP_k(\log x) = Res_{s=1}\frac{\zeta^k(s)x^s}{s},$$

и

$$\Delta_k(x) = \frac{1}{2\pi i}\int_{c_1-\infty}^{c_1+\infty}\zeta^k\frac{x^s}{s}ds, 0 < c_1 < 1.$$

L-функция Дирихле, определенная как

$$L(s,\chi) = \sum_{n=1}^{+\infty}\frac{\chi(n)}{n^s}$$

для $Res > 1$, является другим хорошо известным рядом Дирихле. Здесь $\chi(n)$ - характер Дирихле по модулю m. Заметим, что, для $m = 1$ и $\chi(n) = 1$ для всех целых n, L-функция $L(s,\chi)$ совпадает с $\zeta(s)$.

Рассмотрим произведение k L-функций Дирихле при $Res > 1$:

$$L_1(s,\chi_1)\dots L_k(s,\chi_k) = \sum_{n=1}^{+\infty}c_n n^{-s}.$$

Это произведение - новый ряд Дирихле с сумматорной функцией вида

$$C_k(x) = \sum_{n\le x}c_n = \sum_{n_1\dots n_k\le x}\chi_1(n_1)\dots\chi_k(n_k).$$

По формуле обращения мы получаем, что

$$C_k(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}L_1(s,\chi_1)\dots L_k(s,\chi_k)\frac{x^s}{s}ds.$$

Сдвигая линию интегрирования к некоторому положительному c_1, меньшему 1, мы получим для $C_k(x)$ асимптотическую формулу

$$C_k(x) = xP_m(\log x) + \Delta_k(x),$$

где

$$xP_m(\log x) = Res_{s=1}\frac{L_1(s,\chi_1)\dots L_k(s,\chi_k)x^s}{s}$$

является вычетом подинтегральной функции в точке $s = 1$, m - число главных характеров среди $\chi_1,\dots,\chi_k$, и

$$\Delta_k(x) = \frac{1}{2\pi i}\int_{c_1-\infty}^{c_1+\infty}L_1(s,\chi_1)\dots L_k(s,\chi_k)\frac{x^s}{s}ds.$$

Определим α_k как наименьшее действительное число, для которого

$$\Delta_k(x) = O(x^{\alpha_k+\epsilon}).$$

Ландау (1912) доказал, что

$$\alpha_k \le 1 - \frac{2}{k+1}, k \ge 2.$$

Карацуба (1972) получил для α_k оценку

$$\alpha_k \le 1 - \frac{c}{k^{2/3}}, k \ge 2.$$

Мы покажем, что

$$C_k(x) = xP_m(\log x) + \theta x^{1-\frac{1}{13k^{2/3}}}(C\log x)^k,$$

где P_m - многочлен степени $m-1$, m - число главных характеров среди характеров χ_1 по модулю m_1, …, χ_k по модулю m_k, $2 \le k << \log^{5/6} x$, $\max(m_1, \ldots, m_k) << \log^2 x$, θ - комплексное число, $|\theta| < 1$, $C > 0$ - абсолютная постоянная.

Оценка остаточного члена в последней формуле равномерна по k, а модули характеров Дирихле $\chi_1, \ldots, \chi_k$ могут расти как $\log^2 x$.

Таким образом, все наши результаты имеют вид

$$\alpha_k \le 1 - \frac{c}{k^{2/3}}, 2 \le k \le \log^{5/6} x$$

с

$$c = \frac{1}{13}.$$

Как мы получим данное значение c?

В 1972 Карацуба получил для c формулу

$$c = \frac{1}{2(2a)^{2/3}}, k \ge 2,$$

где a - константа из оценки дзета-функции Римана в критической полосе:

$$\zeta(\sigma + it) << t^{a(1-\sigma)^{3/2}} \log t,$$

$t \ge 2$ и $1/2 \le \sigma \le 1$.

Существует два пути улучшения константы c.

- Получить новую формулу, связывающую c и a. Так, Фиджи (1976) получил для c и a формулу

  $$c = \frac{1}{\sqrt{2}}(\sqrt{8}-1)^{-1/3}a^{-2/3}, k \ge k_0.$$

  Наш результат:

  $$c = \frac{1}{2a^{2/3}}, k \ge 2.$$

- Улучшить константу a. Много авторов рассматривало эту проблему. Так, Стас (1962) получил $a = 2^{15}$ для σ, близкого к 1. Рихерт (1967) доказал, что $a = 100$. Туран (1969) аннонсировал результат $a = 39$. Значение $a = 86$ упомянуто в книге "Рекорды простых чисел"Рибенбойма, 1985.

  Наш результат: $a = 15,25$.

Улучшение оценки дзета-функции Римана в критической полосе связано с исследованием тригонометрических сумм специального вида,

$$\sum_{n=1}^{N} n^{it}, \sum_{N<n\le 2n} n^{it},$$

которые называются *дзетовыми суммами.*

Такие суммы встречались уже у Гаусса, затем - у Харди и Литтлвуда, а позднее - у Коробова и Виноградова.

Оценка таких сумм методом Виноградова имеет вид

$$\sum_{N<n\le 2N} n^{it} << N^{1-\frac{\alpha_0}{r^2}},$$

где $r \ge r_0$, $t^{1/r} \le N \le t^{1/(r-1)}$, $\alpha_0 > 0$ - абсолютная постоянная.

Коробов получил для этой константы значение $1/2666000$, а Виноградов - значение $1/60000$.

Карацуба (1971) получил формулу, связывающую константы a и α_0:

$$a = \frac{2}{3\sqrt{3\alpha}}, \alpha \approx 0,49\alpha_0.$$

Наш результат:

$$\alpha_0 = 1/856, \alpha = 1/1570.$$

Таким образом, мы имеем несколько теорем.

Теорема 1

$$|\sum_{N<n\le N_1} n^{it}| \le ANe^{-\frac{1}{1570}\frac{\log^3 N}{\log^2 t}},$$

где $N_1 \le 2N \le t$, $A > 0$ - абсолютная постоянная.

Теорема 2

$$|\zeta(\sigma+it) \le B|t|^{15,25(1-\sigma)^{3/2}} \log^{2/3}|t|,$$

где $|t| \ge 2$, $1/2 \le \sigma \le 1$, $B > 0$ - абсолютная постоянная.

Теорема 3

$$\sum_{n\le x} \tau_k(n) = xP_k(\log x) + \theta x^{1-\frac{1}{13k^{2/3}}}(C\log x)^k,$$

где P_k - многочлен степени $k-1$, $2 \le k << \log^{5/6} x$, θ - комплексное число, $|\theta| \le 1$, $C > 0$ - абсолютная постоянная.

Теорема $1'$

$$|\sum_{N<n\le N_1}\chi(n)n^{it}|\le ANe^{-\frac{1}{1570}\frac{\log^3 ND^{-1}}{\log^2 t}},$$

где χ - характер Дирихле по модулю D, $D\le N$, $N_1\le 2N\le t$, $A>0$ - абсолютная постоянная.

Теорема $2'$

$$|L(\sigma+it,\chi)|\le BD^{1-\sigma}|t|^{15,25(1-\sigma)^{3/2}}\max(\log D,\log^{2/3}|t|),$$

где χ - характер Дирихле по модулю D, $|t|\ge 2$, $1/2\le\sigma\le 1$, $B>0$ - абсолютная постоянная.

Теорема $3'$

$$\sum_{n_1\dots n_k\le x}\chi_1(n_1)\dots\chi_k(n_k)=xP_m(\log x)+\theta x^{1-\frac{1}{13k^{2/3}}}(C\log x)^k,$$

где $\chi_1,\dots\chi_k$ - характеры Дирихле по модулям $D_1,\dots D_k$, P_m - многочлен степени $m-1$, m - число главных характеров среди $\chi_1,\dots,\chi_k$, $2\le k<<\log^{5/6}x$, $\max(D_1,\dots,D_k)<<\log^2 x$, θ - комплексное число, $|\theta|\le 1$, $C>0$ - абсолютная постоянная.

Рассмотрим идеи доказательств теорем 1, 2 и 3 (для L-функций Дирихле доказательства аналогичны, но содержат больше технических деталей).

Доказательство теоремы 1.

Пусть γ определено из равенства $N=t^\gamma$, то есть, $\gamma=\frac{\log N}{\log t}$. Пусть $b=N^\omega$, где $\omega=0,239$. Пусть $x,y\in[1,b]$. Рассмотрим дзетовую сумму $S(N,t)$. Сдвигая интервал суммирования, получим:

$$S(N,t)=\sum_{N<n\le N_1}n^{it}=\sum_{N+xy<n\le N_1+xy}e^{it\log n}+\sum_1-\sum_2=\sum_{N<n\le N_1}e^{it\log(n+xy)}+\theta b^2.$$

Разложив $\log(n+xy)$ по формуле Тейлора, получим:

$$\log(n+xy)=\log n+F_r(x,y)+R(x,y),$$

где $F_r(x,y)$ - многочлен степени $r=\frac{1}{\gamma(1-2\omega)}$, и суммируя по всем x,y из $[1,b]$, получим для $S(n,t)$ оценку

$$\sum_{x=1}^{b}\sum_{y=1}^{b}S(n,t)<<NW,S(N,t)<<Nb^{-2}W,$$

где

$$W=\sum_{x=1}^{b}|\sum_{y=1}^{b}e^{itF_r(x,y)}|=\sum_{x=1}^{b}|\sum_{y=1}^{b}e^{2\pi if(x,y)}|$$

с

$$f(x,y)=\alpha_1xy+\dots\alpha_rx^ry^r,\alpha_m=\frac{(-1)^{m-1}t}{2\pi mn^m}$$

- специальная тригонометрическая сумма, которую мы оценим с помощью *теоремы о среднем Виноградова*:

$$\int_0^1 \cdots \int_0^1 |W|^{2k} << b^{2k-\Delta_k}.$$

Выбирая $k \sim 0,9r$, мы получим оценку

$$W << b^2 t^{\Delta}, \Delta = \Delta(\gamma, \omega) = -\frac{1}{1570}\gamma^3,$$

и, следовательно, оценку

$$S(N,t) << Nt^{\Delta} << Ne^{-\frac{1}{1570}\frac{\log^3 N}{\log^2 t}}.$$

Доказательство теоремы 2.

Пусть $\alpha = 1/1570$. Используя для дзета-функции частное суммирование, мы получим:

$$\zeta(s) = \zeta(\sigma + it) = \sum_{n \le t} n^{-\sigma} n^{-it} + R << \sigma \int_1^t (\sum_{n \le u} n^{-it}) u^{-1-\sigma} du = \sigma \int_0^{\log t} e^{f(v)} dv,$$

где

$$f(v) = -\alpha \frac{v^3}{\log^2 t} + (1-\sigma)v.$$

Максимум $f(v)$ достигается в точке $v_0 = \sqrt{\frac{1-\sigma}{3\alpha}} \log t$, и

$$f(v_0) = \frac{2}{3\sqrt{3\alpha}}(1-\sigma)^{3/2} \log t.$$

Таким образом,

$$\zeta(s) << t^{a(1-\sigma)^{3/2}} \log^{2/3} t, a = \frac{2}{3\sqrt{3\alpha}}.$$

Для $\alpha = 1/1570$ мы получим $a = 15,25$.

Доказательство теоремы 3.

В 1972 Карацуба получил для ряда Дирихле

$$f(s) = \sum_{n=1}^{+\infty} a_n n^{-s}$$

и его сумматорной функции

$$\Phi(\xi) = \sum_{n \le \xi} a_n$$

интегральную формулу

$$\int_1^x \Phi(\xi) d\xi = \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \frac{f(s) x^{s+1}}{s(s+1)} ds + R(x).$$

Для $f(s) = \zeta^k(s)$ и $\Phi(\xi) = \sum_{n \le \xi} \tau_k(n)$ мы имеем:

$$\int_1^x \Phi(\xi) d\xi = \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \frac{\zeta^k(s) x^{s+1}}{s(s+1)} ds + R_1(x).$$

Для $b = 1 + \frac{1}{\log x}$, $T = x^{1-\eta}$, $\eta = 1 - (ak)^{-2/3}$, $a = 15,25$

$$R_1(x) = \theta x^{1+\eta}(C\log x)^k.$$

Рассмотрим контур Γ с вершинами $\eta \pm iT$, $b \pm iT$, и интеграл

$$J = \frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{f(s)x^{s+1}}{s(s+1)}ds$$

по контуру Γ.

По теореме о вычетах,

$$J = Res_{s=1}\frac{\zeta^k(s)x^{s+1}}{s(s+1)} = x^2P_k(\log x).$$

Следовательно,

$$\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{f(s)x^{s+1}}{s(s+1)}ds = J - J_1 - J_2 - J_3 = x^2P_k(\log x) + R_2(x),$$

$$R_2(x) = \theta x^{1+\eta}(C\log x)^k.$$

Здесь J_1, J_2 и J_3 - интегралы по верхней, нижней и левой сторонам контура Γ. Таким образом,

$$\int_1^x \Phi(\xi)dx = x^2P_k(\log x) + \theta x^{1+\eta}(C\log x)^k.$$

Используя так называемое *дискретное дифференцирование*, мы получим

$$\Phi(x) = xP_k(\log x) + \theta x^{\frac{1+\eta}{2}}(C\log x)^k.$$

Так как $\frac{1+\eta}{2} = 1 - \frac{1}{2a^{2/3}}k^{-2/3}$, мы получаем, для $a = 15,25$, $\frac{1}{2a^{2/3}} = \frac{1}{13}$.

Упражнения

1. Получить асимптотическую формулу

$$\sum_{n\le x}\tau_{k_1}(n)\cdot\dots\cdot\tau_{k_l}(n) = xP_m(\log x) + \theta x^{1-\frac{1}{13m^{2/3}}}(C\log x)^m,$$

где $l \ge 1$, $k_1, \dots, k_l \ge 2$, $m = k_1\cdot\dots\cdot k_l$, P_m - многочлен степени $m-1$, θ - комплексное число, $|\theta| \le 1$, $m \le \log^{\frac{5}{6}} x$, $C > 0$ - абсолютная постоянная.

2. Получить асимптотическую формулу

$$\sum_{n\le x}\tau_k(n^2) = xP_m(\log x) + \theta x^{1-\frac{1}{13m^{2/3}}}(C\log x)^m,$$

где $m = \frac{k(k+1)}{2}$, P_m - многочлен степени $m-1$, θ - комплексное число, $|\theta| \le 1$, $m \le \log^{\frac{5}{6}} x$, $C > 0$ - абсолютная постоянная.

3. Пусть $\mathrm{Z}[i] = \{\alpha = a + bi | a, b \in \mathrm{Z}\}$ - кольцо целых чисел Гаусса. Норма Гауссова числа $\alpha = a + bi$ определяется как $\mathrm{N}(\alpha) = a^2 + b^2$. Известно, что $\mathrm{N}(\alpha\cdot\beta) = \mathrm{N}(\alpha)\cdot\mathrm{N}(\beta)$. Пусть $\tau_k^G(n) = \sum_{\mathrm{N}(\alpha_1\cdot\dots\cdot\alpha_k)=n} 1$.

   Получить асимптотическую формулу
$$D_k^G(x) = \sum_{n\le x} \tau_k^G(n) = xP_k(\log x) + \theta x^{1-\frac{1}{15}k^{-2/3}}(C\log x)^{2k},$$
   где P_k - многочлен степени $k-1$, θ - комплексное число, $|\theta| \le 1$, $k \le \log^{\frac{5}{6}} x$, $C > 0$ - абсолютная постоянная.

4. Получить асимптотическую формулу
$$\sum_{n\le x} \tau_{k_1}^G(n)\cdot\dots\cdot\tau_{k_l}^G(n) = xP_m(\log x) + \theta x^{1-\frac{1}{13m^{2/3}}}(C\log x)^m,$$
   где $l \ge 1$, $k_1, \dots, k_l \ge 2$, $m = k_1\cdot\dots\cdot k_l$, P_m - многочлен степени $m-1$, θ - комплексное число, $|\theta| \le 1$, $m \le \log^{\frac{5}{6}} x$, $C > 0$ - абсолютная постоянная.

5. Получить асимптотическую формулу
$$\sum_{n\le x} \tau_k^G(n^2) = xP_m(\log x) + \theta x^{1-\frac{1}{13m^{2/3}}}(C\log x)^m,$$
   где $m = \frac{k(k+1)}{2}$, P_m - многочлен степени $m-1$, θ - комплексное число, $|\theta| \le 1$, $m \le \log^{\frac{5}{6}} x$, $C > 0$ - абсолютная постоянная.

Список литературы

[Бухш66] Бухштаб А. А. *Теория чисел*, Москва: Просвещение, 1966.

[Кара83] Карацуба А.А. *Основы аналитической теории чисел*, М.: Наука, 1983.

[Кара72] Карацуба А.А. *Равномерная оценка остаточного члена в проблеме делителей Дирихле*, Изв. АН СССР, Мат., 36, 3, 1972.

[Мард39] Марджанишвили К.К. *Оценка одной арифметической суммы*, Докл. АН СССР, 22, 7, 1939.

[Пант88] Пантелеева Е. И. *Проблема делителей Дирихле в чмсловых полях*, Мат. заметки, 4, Т. 44, 1988.

[Пант94] Пантелеева Е.И. *О средних значениях некоторых арифметических функций*, Мат. заметки, 55, Т. 2, 1994.

[CoGa96] Conway J. H., Guy R. K. *The Book of Numbers*, New York: Springer-Verlag, 1996.

[CoRo96] Courant R. and Robbins H. *What Is Mathematics?: An Elementary Approach to Ideas and Methods*, 2-nd ed., Oxford University Press, 1996.

[Dickson05] Dickson L. E. *History of the Theory of Numbers*, New York: Dover, 2005.

[Diri49] Dirichlet P. *Über die Bestimmung der mittleren Werte in der Zahlentheorie*, Berlin: Abh. Acad. Wiss., Werke 2, 1849.

[Gaus01] Gauss C. F. *Disquisitiones Arithmeticae*, Leipzig, 1801.

[Guy94] Guy R. K. *Unsolved Problems in Number Theory*, 2-nd ed., New York: Springer-Verlag, 1994.

[HaWr79] Hardy G. H., Wright E. M. *An Introduction to the Theory of Numbers*, 5-th ed., Oxford, Clarendon Press, 1979.

[KLS01] Krízek M., Luca F., Somer L. *17 Lectures on Fermat Numbers: from Number Theory to Geometry*, CMS Books in Mathematics, v. 9, New York: Springer-Verlag, 2001.

[Ore48] Ore O. *Number Theory u Its History*, Dover Publications, 1948.

[PM] PlanetMath.org, http://planetmath.org/encyclopedia/

[PoSz76] Polya G.? Szege G. *Problems and Theorems in Analysis*, Berlin: Springer-Verlag, 1976.

[Ribe96] Ribenboim P. *New Book of Prime Number Records*, New York: Springer-Verlag, 1996.

[Ries94] Riesel H. *Prime Numbers and Computer Methods for Factorization*, 2-nd ed., Basel: Birkhouser, 1994.

[Robi54] Robinson R. M. *Mersenne and Fermat Numbers*, Proc. Amer. Math. Soc. 5, 1954.

[Shan93] Shanks D. *Solved and Unsolved Problems in Number Theory*, 4-th ed., New York: Chelsea, 1993.

[Sloa03] Sloane N.J. *The On-line Encyclopedia of Integer Sequences*, http://www.research.att.com/ njas/sequences/