Элементарные теоретико-числовые функции

Беребердина Наталья 23.12.2020

Оглавление

Элементарные теоретико-числовые функции

- Арифметической функцией называется любая функция $f: \mathrm{N} \to \mathrm{C}$
- Известные арифметические функции:

1. Количество делителей числа
2. Сумма делителей числа
3. Функция Эйлера
4. Функция Мебиуса

Мультипликативность

- Определение: f мультипликативна, если $f(ab) = f(a)f(b)$ для любых взаимно простых чисел a и b. Вообще говоря, для произвольных арифметических функций это свойство не всегда выполняется. Сегодня мы рассмотрим только некоторые из функций и изучим их свойства.

Суммы степеней делителей

- Рассмотрим арифметическую функцию $\sigma_k(n) = \sum_{d|k} d^k$

Тогда в частности σ_0 – количество делителей, σ_1 – сумма делителей.

- Заметим, что функция $\sigma_k(n)$ мультипликативна.
- Доказательство: $d|ab \Rightarrow d = d_1 d_2$, где $d_1|a$ и $d_2|b$. Причём, для взаимно простых a и b такое представление единственно. Получаем:

$$\left(\sum_{d_1|a} {d_1}^k\right) \times \left(\sum_{d_2|b} {d_2}^k\right) = \sum_{\substack{d_1|a \\ d_2|b}} {d_1}^k {d_2}^k = \sum_{d|ab} d^k$$

Формула $\sigma_k(n)$

- Зная мультипликативность функции, можем получить формулу для $\sigma_k(n)$:
- Пусть $a = p_1^{t1} * p_2^{t2} * \ldots p_n^{tn}$ — каноническое разложение числа a.

Тогда в силу мультипликативности: $\sigma_k(a) = \sigma_k(p_1^{t1}) * \sigma_k(p_2^{t2}) * \ldots \sigma_k(p_n^{tn})$.

Осталось найти $\sigma_k(p^t) = 1^k + p^k + p^{2k} \ldots p^{kt} = (1 - p^{k(t+1)}) / (1 - p^k)$ (при $k \neq 0$).

Тогда в общем виде получаем формулу:

$\sigma_k(a) = (1 - p_1^{k(t1+1)}) / (1 - p_1^k) * \ldots * (1 - p_n^{k(tn+1)}) / (1 - p_n^k)$

В частности для $k = 1$: $(1 - p_1^{t1+1}) / (1 - p_1) * \ldots * (1 - p_n^{tn+1}) / (1 - p_n)$.

Функция Эйлера

- Рассмотрим арифметическую функцию: $\varphi(n) = \#\{1 \le k \le n: (n, k) = 1\}$
- Эта функция называется функцией Эйлера. Докажем ее мультипликативность:

Функция Эйлера так же мультипликативна. Вспомним Китайскую Теорему об Остатках: любая пара чисел $r_a = n \bmod a$ и $r_b = n \bmod b$ кодирует ровно одно число r_{ab}.

Чтобы n было взаимнопросто с ab достаточно, чтобы r_a было взаимнопросто с a и r_b было взаимнопросто с b. Отсюда сразу следует $\varphi(ab) = \varphi(a)\varphi(b)$.

Формула для чисел Эйлера

- Зная мультипликативность, достаточно найти φ от степени простого:

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}\left(1 - \frac{1}{p}\right)$$

- Тогда в общем виде:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

Свойства функции Эйлера в теории чисел

Пусть $x_1, \ldots, x_{\varphi(m)}$ — все различные натуральные числа, меньшие m и взаимно простые с ним.

Рассмотрим все возможные произведения $x_i a$ для всех i от 1 до $\varphi(m)$.

Поскольку a взаимно просто с m и x_i взаимно просто с m, то и $x_i a$ также взаимно просто с m, то есть $x_i a \equiv x_j \pmod{m}$ для некоторого j.

Отметим, что все остатки $x_i a$ при делении на m различны. Действительно, пусть это не так, тогда существуют такие $i_1 \neq i_2$, что

$$x_{i_1} a \equiv x_{i_2} a \pmod{m}$$

или

$$(x_{i_1} - x_{i_2}) a \equiv 0 \pmod{m}.$$

Так как a взаимно просто с m, то последнее равенство равносильно тому, что

$$x_{i_1} - x_{i_2} \equiv 0 \pmod{m} \text{ или } x_{i_1} \equiv x_{i_2} \pmod{m}.$$

Это противоречит тому, что числа $x_1, \ldots, x_{\varphi(m)}$ попарно различны по модулю m.

Свойства функции Эйлера в теории чисел

Перемножим все сравнения вида $x_i a \equiv x_j \pmod{m}$. Получим:

$$x_1 \cdots x_{\varphi(m)} a^{\varphi(m)} \equiv x_1 \cdots x_{\varphi(m)} \pmod{m}$$

или

$$x_1 \cdots x_{\varphi(m)} (a^{\varphi(m)} - 1) \equiv 0 \pmod{m}.$$

Так как число $x_1 \cdots x_{\varphi(m)}$ взаимно просто с m, то последнее сравнение равносильно тому, что

$$a^{\varphi(m)} - 1 \equiv 0 \pmod{m}$$

или

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \blacksquare$$

Умножение Дирихле

- Введем операцию умножения Дирихле:

$$(f \circ g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a) g(b)$$

- Очевидны свойства:

1. $f \circ g = g \circ f$
2. $[f \circ (g \circ \mathrm{h})](n) = [(f \circ g) \circ \mathrm{h}](n) = \sum_{abc=n} f(a) g(b) \mathrm{h}(c)$
3. $f \circ (g + \mathrm{h}) = f \circ g + f \circ \mathrm{h}$

Коммутативное ассоциативное кольцо

Определение 1. **Кольцом** $(R,+,\cdot)$ называется множество R с двумя бинарными алгебраическими операциями сложением $+$ и умножением $\cdot$, связанными законами дистрибутивности. При этом $(R,+)$ — абелева группа, $(R,\cdot)$ — группоид. Иными словами, операции кольца удовлетворяют следующим аксиомам:

1) операция сложения ассоциативна: $(a+b)+c=a+(b+c)$ для любых $a,b,c \in R$;

2) существует нулевой элемент $0 \in R$ такой, что $a+0=0+a=a$ для любого $a \in R$;

3) существует противоположный элемент: для любого $a \in R$ существует $-a \in R$ такой, что $-a+a=a+(-a)=0$;

4) операция сложения коммутативна: $a+b=b+a$ для любых $a,b \in R$;

5) выполнены законы дистрибутивности: $a \cdot (b+c) = a \cdot b + a \cdot c$ для любых $a,b,c \in R$, $(a+b) \cdot c = a \cdot c + b \cdot c$ для любых $a,b,c \in R$.

Определение 2. Если кольцо $(R, + ,\cdot)$ удовлетворяет дополнительному условию: $a \cdot b = b \cdot a$ для любых $a,b \in R$ (коммутативность операции умножения), то кольцо называется **коммутативным**

Определение 3. Если кольцо $(R, + ,\cdot)$ удовлетворяет дополнительному условию: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых $a,b,c \in R$ (ассоциативность операции умножения), то кольцо называется **ассоциативным**

Коммутативное ассоциативное кольцо

Определим следующие функции и приведём некоторые формулы с ними:

1. $Id(n) = n$

2. $I(n) = 1$

3. $e(n) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$

1. $f \circ e = e \circ f = f$

2. $(f \circ I)(n) = \sum d|n \ f(d)$

3. $\sigma_0 = I \circ I$

4. $\sigma_1 = Id \circ I$

5. $\varphi \circ I = Id$

6. $\sigma_1 = Id \circ I = (\varphi \circ I) \circ I = \varphi \circ (I \circ I) = \varphi \circ \sigma_0$

Итак, мы показали, что арифметические функции образуют коммутативное ассоциативное кольцо относительно операций сложения и умножения Дирихле, где функция e является единицей. Когда же функция f имеет обратную g (такую что $f \circ g = e$)?

Поиск обратной функции

В качестве примера, найдём $f = Id^{-1}$. Выполнение соотношений $(f \circ Id)(n) = e(n)$ для всех n – необходимое и достаточное условием того, чтобы f была обратной функцией к Id. Подставляя разные значения n, вычислим начальные значения функции f:

$$1f(1) = 1$$
$$2f(1) + 1f(2) = 0$$
$$3f(1) + 1f(3) = 0$$
$$4f(1) + 2f(2) + 1f(4) = 0$$
$$6f(1) + 3f(2) + 2f(3) + 1f(6) = 0$$
$$8f(1) + 4f(2) + 2f(4) + 1f(8) = 0$$

$$f(1) = 1$$
$$f(2) = -2$$
$$f(3) = -3$$
$$f(4) = 0$$
$$f(6) = 6$$
$$f(8) = 0$$

Поиск обратной функции

- Давайте посмотрим на частные случаи *f(n):*

Мы знаем что $f(1) = 1$.

Рассмотрим $1 f(p) + p * f(1) = 0 \quad \Rightarrow \quad f(p) = -p;$

Рассмотрим теперь $f(p^n)$: $\quad p^n f(1) + p^{n-1} f(p) + \ldots + 1 f(p^n)$:

Индукция показывает, что $f(p^n)$ (при $n > 1$).

Давайте теперь получим *f(n)* для произвольного n.

Для этого давайте докажем что мультипликативные функции образуют группу относительно умножения Дирихле. Тогда, зная что Id мультипликативна и f единственна, получим, что f мультипликативна.

Мультипликативность обратной функции

- Для этого заметим, что если f и g мультипликативные функции, то $f \circ g$ тоже мультипликативна.
- $(f \circ g)(ab) = \sum_{kt=ab} f(k)g(t)$
- $(f \circ g)(a) * (f \circ g)(b) = \sum_{k_1t_1=a} f(k_1)g(t_1) * \sum_{k_2t_2=b} f(k_2)g(t_2) = \sum_{kt=ab} f(k)g(t)$
- Теперь давайте заметим, что
- Для мультипликативной функции f построим функцию g так, чтобы $(f \circ g)(p^a) = e(p^a)$ и $g(p_1^{\alpha_1} \dots p_r^{\alpha_r}) = g(p_1^{\alpha_1}) \dots g(p_r^{\alpha_r})$. Тогда согласно определению g мультипликативна и согласно пункту 2 функция $f \circ g$ определяется своими значениями на p^α, на которых она совпадает с функцией e.

Поиск обратной функции

В общем случае можно поступить точно так же. Из следующей системы видно, что f обратима, в том и только в том случае, если $f(1) \neq 0$.

$$\begin{cases} f(1)g(1) = e(1) = 1 \\ \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = e(n) = 0, n > 1 \end{cases} \Rightarrow \begin{cases} g(1) = f(1)^{-1} \\ g(n) = -f(1)^{-1} \times \sum_{\substack{d|n \\ d \neq n}} f(d)g\left(\frac{n}{d}\right), n > 1 \end{cases}$$

Если раскрыть скобки в формуле для функции Эйлера:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_r}\right) = n \sum_{M \subseteq \{1,\dots,r\}} \frac{(-1)^{|M|}}{\prod_{i \in M} p_i} = n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \mu(d) \times \frac{n}{d}$$

Где μ – ***функция Мёбиуса***, которая определяется так, чтобы выполнялось предыдущее равенство:

$$\mu(n) = \begin{cases} (-1)^k, \text{если } n = p_1 \dots p_k \\ 0, \text{если } \exists M > 1 : M^2 | n \end{cases}$$

Функция Мебиуса

С функцией Мёбиуса мы уже встречались: $Id^{-1}(n) = \mu(n) \times n$. Кроме того, мы только что установили два соотношения, которые показывают, что она тесно связана с функцией Эйлера:

$$\varphi = \mu \circ Id$$

$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

Для удобства дальнейшего повествования введём унарную операцию * на арифметических функциях: $f^*(n) = \frac{f(n)}{n}$. Тогда второе соотношение является простым следствием первого с учётом того факта, что $(f \circ g)^* = f^* \circ g^*$, причём в новых обозначениях оно примет вид $\varphi^* = \mu^* \circ I$.

Вспомним теперь, что сумма $\varphi(d)$ по делителям числа равна ему самому:

$$\begin{cases} \varphi \circ I = Id \\ \varphi = \mu \circ Id \end{cases} \Rightarrow (\mu \circ Id) \circ I = Id \Rightarrow \mu \circ I = e$$

Формула обращения Мебиуса

Таким образом, мы нашли обратную к ещё одной функции $I^{-1} = \mu$ и тем самым только что доказали ***формулу обращения Мёбиуса***, которая гласит:

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu(n/d)$$

$$f = g \circ I \Leftrightarrow g = f \circ \mu$$

В самом деле, формулы получаются друг из друга умножением на μ или I.

Задача об ожерельях

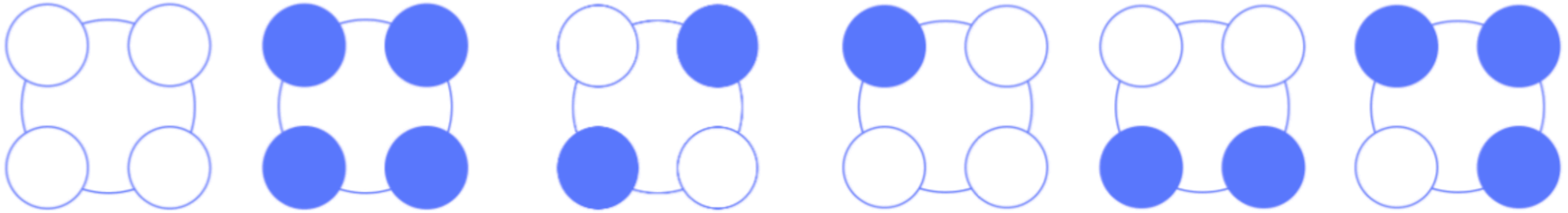
Приведём одно из приложений формулы обращения Мёбиуса. Всем известно следующее фольклорное доказательство малой теоремы Ферма. Будем рассматривать ожерелья из p бусинок, где каждая бусинка покрашена в один из a цветов. Ожерелья, которые совмещаются поворотом, будем считать одинаковыми и зададимся вопросом, сколько существует различных ожерелий? Всего ожерелий без учёта поворота ap. Каждое одноцветное ожерелье встречается среди них ровно один раз, а любое другое ровно p раз. Одноцветных ожерелий a штук, а не

одноцветных $ap - a$. Значит ответ на задачу $a + \frac{ap-a}{p}$. В частности, $(ap - a) \vdots p$.

А что будет, если рассматривать ожерелья из n бусинок, где n – произвольное число? Периодом ожерелья назовём такое минимальное число d, что при повороте на d, рисунок на ожерелье совмещается сам с собой. Очевидно, что d является делителем числа n.

Обобщение задачи

Таким образом, если $n = p$, то существуют только ожерелья периода 1 (одноцветные) и ожерелья периода p (все остальные). На рисунке показаны все 6 раскрасок в 2 цвета ожерелий из 4 бусинок:



Период 1 Период 2 Период 4

Обозначим за $\Phi_a(d)$ количество ожерелий периода d с точностью до поворота, где каждая бусинка покрашена в один из a цветов. В таком случае ответ на задачу $A(n) = \sum_{d|n} \Phi_a(d)$. Но каждое ожерелье периода d будет учтено в сумме a^n в точности d раз. Значит $a^n = \sum_{d|n} d \times \Phi_a(d)$. Обозначим $P(n) = a^n$ и применим операцию * к обеим частям последнего равенства. Получим: $P^* = \Phi_a \circ I^* \Rightarrow \Phi_a = P^* \circ \mu^* = (P \circ \mu)^*$. Теперь можно перейти к вычислению ответа на задачу: $A = \Phi_a \circ I = (P^* \circ \mu^*) \circ I = P^* \circ (\mu^* \circ I) = P^* \circ \varphi^* = (P \circ \varphi)^*$. В итоге:

$$\Phi_a(d) = \frac{1}{d} \sum_{k|d} a^k \mu(d/k)$$

$$A(n) = \frac{1}{n} \sum_{d|n} a^d \varphi(n/d)$$

Несократимые дроби

Укажем на связи теории чисел с теорией вероятности. Вероятность того, что наугад выбранное число из отрезка $1 \dots n$ будет взаимно просто с n равна:

$$\varphi^*(n) = \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

Обозначим, за A_{p_ν} события «число не делится на p_k». Несложно посчитать их вероятность:

$$\mathcal{P}\left(A_{p_k}\right) = \frac{n - n/p_k}{n} = 1 - \frac{1}{p_k}$$

Если бы мы знали, что события A_{p_k} независимы, мы могли бы вывести формулу для функции Эйлера следующим изящным способом:

$$\varphi^*(n) = \mathcal{P}\left(A_{p_1} \dots A_{p_r}\right) = \mathcal{P}\left(A_{p_1}\right) \dots \mathcal{P}\left(A_{p_r}\right) = \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

К сожалению, этот факт требует проверки, которая эквивалента доказательству формулы. Однако под таким углом зрения, эта формула становится намного понятнее.

Несократимые дроби

Решим теперь настоящую задачу. С какой вероятностью наугад выписанная дробь будет несократимой? Дробь несократима, если её нельзя сократить ни на 2, ни на 3, ни на 5, ни на 7, ни на 11… Дробь можно сократить на p если и числитель, и знаменатель делятся на p. В случае натурального ряда делимость на простые – независимые события, значит ответ на задачу:

$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{7^2}\right)\left(1-\frac{1}{11^2}\right)\ldots=\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^2}\right)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}$$

Здесь и в дальнейшем $\mathbb{P}$ обозначает множество простых чисел.

Чтобы получить явный ответ на задачу, нам пригодится следующая лемма: $\left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right)\left(\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}\right)=1$

Ряд Дирихле

Если правильно посмотреть на эту формулу, она становится очевидна. Определим ***ряд Дирихле***:

$$DG(f,s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$$

Нас не интересует вопрос сходимости, все операции над ними можно проделывать формально. Верно общее утверждение относительно рядов Дирихле: $DG(f,s)\times DG(g,s)=DG(f\circ g,s)$

$$\left(\sum_{a=1}^{\infty}\frac{f(a)}{a^s}\right)\left(\sum_{b=1}^{\infty}\frac{g(b)}{b^s}\right)=\sum_{n=1}^{\infty}\left(\sum_{ab=n}\frac{f(a)g(b)}{n^s}\right)=\sum_{n=1}^{\infty}\frac{(f\circ g)(n)}{n^s}$$

Применяя этот результат к нашей лемме: $DG(I,2)\times DG(\mu,2)=DG(e,2)\equiv\frac{e(1)}{1^2}=1.$

Как гласит известная Базельская задача, $\sum\frac{1}{n^2}=\frac{\pi^2}{6}$, а значит вероятность того, что случайная дробь будет несократима, равна $\frac{6}{\pi^2}$.