Мультипликативность функции Эйлера

Функция Эйлера, теорема Эйлера. Функция Эйлера $\varphi(n)$ — количество чисел от 1 до n, взаимно простых с натуральным n. Одно из важнейших её применений — теорема Эйлера, заключающаяся в том, что для любого a, взаимно простого с n, выполнено

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

Доказательство факта сложности не представляет, так что для полноты картины приведём его. Пусть $r_1, r_2, \ldots, r_m$ — все остатки по модулю n, взаимно простые с n. Эти остатки можно друг на друга умножать по правилу: «произведение» r_i и r_j — это остаток от деления $r_i r_j$ на n. Нетрудно понять, что таким образом определённое «произведение» каждой паре r_i, r_j сопоставляет один из r_k (произведение чисел, взаимно простых с n, взаимно просто с n).

Более того, на множестве таких остатков (при $n > 1$) однозначно определено деление. Действительно, если r — один из r_k, то числа вида rr_i не сравнимы между собой при разных i (в противном случае $n|r(r_i - r_j)$, откуда следует $n|(r_i - r_j)$, откуда $r_i \equiv r_j$, что неверно при $i \neq j$). Значит, умножение на фиксированный остаток r в арифметике остатков по модулю n является биекцией, то есть обратимо. Обратное отображение называется делением на r.

Осталось заметить, что $r_1 r_2 \ldots r_m \equiv (rr_1)(rr_2)\ldots(rr_m)$ (справа те же остатки, только в другом порядке), откуда $r_1 r_2 \ldots r_m(1 - r^m) \equiv 0$. Осталось поделить это равенство на $r_1 r_2 \ldots r_m$. Вспоминая, что по определению $m = \varphi(n)$, получаем

$$1 - r^{\varphi(n)} \equiv 0,$$

что и требовалось доказать.

Мультипликативность функции Эйлера. Возникает вопрос: как же вычислить функцию Эйлера? Оказывается, это очень просто в силу её *мультипликативности*. А именно, если a и b взаимно просты, то $\varphi(ab) = \varphi(a)\varphi(b)$. Это свойство позволяет вычислить функцию Эйлера, умея вычислять функцию Эйлера от степени простого числа (убедитесь самостоятельно, что для простого p и натурального k выполнено $\varphi(p^k) = p^{k-1}(p-1)$). Далее будет приведено 4 различных доказательства мультипликативности.

Стандартное доказательство. Рассмотрим числа $U(x, y) = ax + y$ при $x = \overline{0, (b-1)}$, $y = \overline{0, (a-1)}$. Как нетрудно видеть, это — все числа от 0 до $ab - 1$. Фиксируем y. Если y имеет общий с a делитель, больший 1, то все числа $U(x, y)$ имеют этот же общий с a делитель, а значит, не взаимно просты и с ab. Если же y и a взаимно просты, то тогда $ax + y$ и a взаимно просты. Значит, $ax + y$ и ab имеют нетривиальный общий делитель ровно в тех случаях, когда $ax + y$ не взаимно просто с b.

Теперь надо осознать, что числа ax при x от 0 до $b - 1$ дают всевозможные остатки при делении на b (это следует из того, что все эти числа дают разные остатки при делении на b, что почти очевидно (если не очевидно, перечитайте ещё раз доказательство теоремы Эйлера)). Значит, и среди чисел $U(x, y)$ встречаются всевозможные остатки при делении на b, каждый по одному разу. Значит, среди этих чисел есть ровно $\varphi(b)$ взаимно простых с ab.

Получаем, что среди $U(x, y)$ есть взаимно простые с ab ровно при тех y, которые взаимно просты с a (количество таких y равно $\varphi(a)$). При каждом таком y есть ровно $\varphi(b)$ чисел $U(x, y)$, взаимно простых с ab. Значит, общее количество чисел $U(x, y)$ равно $\varphi(a)\varphi(b)$. С другой стороны, по определению оно равно $\varphi(ab)$.

То же самое, но с иного ракурса. Рассмотрим числа $V(x, y) = ax + by$ при $x = \overline{1, b}$, $y = \overline{1, a}$. Все они дают разные остатки по модулю ab. Действительно, из $ax_1 + by_1 \equiv ax_2 + by_2$ следует $a(x_1 - x_2) + b(y_1 - y_2) \equiv 0$. Первое слагаемое делится на a, значит, и второе слагаемое делится на a. В силу взаимной простоты a и b получаем, что $y_1 - y_2$ делится на a, что возможно только при $y_1 = y_2$. Значит, $a(x_1 - x_2) \equiv 0$ по модулю ab, откуда следует, что $x_1 - x_2$ делится на b, что бывает только при $x_1 = x_2$.

Осталось заметить, что $V(x, y)$ взаимно просто с ab тогда и только тогда, когда x взаимно прост с b, а y взаимно прост с a. Действительно, пусть $V(x, y)$ взаимно просто с ab, но (для определённости) x имеет общий с b делитель $d > 1$. Но тогда $d|V(x, y)$, что противоречит предположению.

Обратно, пусть пары x, b и y, a взаимно просты, но ab имеет общий с $V(x, y)$ делитель $d > 1$. Пусть p — произвольный простой делитель числа d. Тогда $p|ab$. Пусть (для определённости) $p|a$. Тогда p не делит y (в силу взаимной простоты a и y). Но $p|by$ (так как $p|(ax + by)$). Значит, $p|b$. Но тогда p — общий делитель a и b, что противоречит взаимной простоте a и b.

Остатков по модулю ab, взаимно простых с ab, ровно $\varphi(ab)$ штук, чисел x, взаимно простых с b, ровно $\varphi(b)$, чисел y, взаимно простых с a, ровно $\varphi(a)$. Значит, $\varphi(ab) = \varphi(a)\varphi(b)$.

Формула включений-исключений. Пусть A_1, A_2, $\dots A_n$ — некоторое конечное семейство конечных множеств. Записью $|X|$ будем обозначать количество элементов множества X. Также пусть B_1^m, B_2^m, $\dots B_{k_m}^m$ — всевозможные пересечения по m множеств из A_i (числа k_m, как нетрудно понять, равны C_n^m). Докажем очень полезную формулу (называемую формулой включений-исключений)

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{m=1}^{n} \left((-1)^{m-1} \sum_{i=1}^{k_m} |B_i^m| \right).$$

Пусть x — произвольный элемент множества из левой части равенства. Там он посчитан 1 раз. Посмотрим, сколько раз он учтён в правой части. Пусть он содержится в l множествах из A_i. Тогда в сумме $\sum_{i=1}^{k_m} |B_i^m|$ он посчитан C_{n-l}^{m-l} раз. Значит, во всей правой части он посчитан

$$\sum_{m=1}^{n} (-1)^{m-1} C_{n-l}^{m-l} \quad \text{раз.}$$

Этой сумме не хватает -1 до знакопеременной сумммы $(n-l)$-й строки треугольника Паскаля. Значит, она равна 1, что и требовалось доказать.

Теперь выведем формулу для подсчёта функции Эйлера. Пусть p_1, p_2, $\dots p_n$ — *различные* простые делители числа N. Пусть A_i — множество чисел от 1 до N, кратных p_i. Заметим, что $N - |B_1^n| = \varphi(N)$. Осталось всего лишь заметить, что множество $A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_l}$ содержит ровно $N/p_{i_1}p_{i_2}\dots p_{i_l}$ элементов. Следовательно, $N - |B_1^n|$ по формуле включений-исключений равно в точности

$$N \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right).$$

(Если не верите, просто раскройте все скобки в этом выражении.)

Мультипликативность теперь очевидна (да и, наверное, не нужна при наличии этой формулы).

Рекуррентное соотношение. Будем отталкиваться от соотношения

$$n = \sum_{d|n} \varphi(d). \tag{1}$$

Пусть m — минимальное натуральное число, такое что существует взаимно простая пара a, b, такая что $m = ab$, но $\varphi(m) \neq \varphi(a)\varphi(b)$. Пусть a_0, a_1, $\dots a_k$ — натуральные делители числа a, b_0, b_1, $\dots b_l$ — натуральные делители числа b. Пусть при этом $a_0 = a$, $b_0 = b$. Заметим, что в силу взаимной простоты a и b числа $a_i b_j$ — это всевозможные делители числа ab, причём каждый делитель встречается среди $a_i b_j$ ровно 1 раз. Значит,

$$ab = \varphi(ab) + \sum_{i,j \neq 0,0} \varphi(a_i b_j). \tag{2}$$

В силу минимальности m правую часть можно преобразовать следующим образом

$$\varphi(ab) + \sum_{i,j\neq 0,0} \varphi(a_i b_j) = \varphi(ab) + \sum_{i,j\neq 0,0} \varphi(a_i)\varphi(b_j) = \varphi(ab) - \varphi(a)\varphi(b) + \left(\sum_{i=0}^{k} \varphi(a_i)\right)\left(\sum_{j=0}^{l} \varphi(b_j)\right).$$

Если воспользоваться соотношением (1) для чисел a и b, получим

$$\varphi(ab) - \varphi(a)\varphi(b) + \left(\sum_{i=0}^{k} \varphi(a_i)\right)\left(\sum_{j=0}^{l} \varphi(b_j)\right) = \varphi(ab) - \varphi(a)\varphi(b) + ab.$$

Подставляя это выражение вместо правой части (2), получим

$$ab = \varphi(ab) - \varphi(a)\varphi(b) + ab,$$

откуда $\varphi(ab) = \varphi(a)\varphi(b)$, что противоречит нашему предположению.