Теорема Эйлера и малая теорема Ферма. Методы решения сравнений

Определение. Функция $\theta : \mathbf{R} \to \mathbf{R}$ (или, более общо, $\theta : \mathbf{C} \to \mathbf{C}$) называется мультипликативной если:

1). Функция θ определена всюду на $\mathbf{N}$ и существует $a \in \mathbf{N}$ такой, что $\theta(a) \neq 0$.

2). Для любых взаимно простых натуральных чисел a_1 и a_2 выполняется $\theta(a_1 \cdot a_2) = \theta(a_1) \cdot \theta(a_2)$.

Пример 1. $\theta(a) = a^s$, где s - любое (хоть действительное, хоть комплексное) число. Проверка аксиом 1) и 2) из определения мультипликативной функции не составляет труда, а сам пример показывает, что мультипликативных функций по меньшей мере континуум, т.е. много.

Определение **.** Функция $\varphi(m)$, определенная на множестве натуральных чисел называется функцией Эйлера, если значение $\varphi(m)$ равно числу натуральных чисел не превышающих m и взаимно простых с m, а $\varphi(1)=1$.

Если $m>1$ имеет разложение на простые множители вида $m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot .....\cdot p_k^{\alpha_k}$, то $\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)$

Пример. Вычислить $\varphi(180)$

Решение. $180=2^2\cdot 3^2\cdot 5$. Следовательно

$$\varphi(180)=180\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=180\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}=48.$$

Теорема (Эйлер). Пусть $m>1$, $(a,m)=1$, $\varphi(m)$ – функция Эйлера. Тогда:

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m) .$$

Доказательство. Пусть x пробегает приведенную систему вычетов по $mod\ m$:

$$x=r_1,r_2,...,r_c$$

где $c=\varphi(m)$ их число, $r_1,r_2,...,r_c$ - наименьшие неотрицательные вычеты по $mod\ m$. Следовательно, наименьшие неотрицательные вычеты, соответствующие числам ax суть соответственно:

$$\rho_1,\ \rho_2,...,\ \rho_c$$

– тоже пробегают приведенную систему вычетов, но в другом порядке
Значит:

$$a\cdot r_1\equiv\rho_{\varphi 1}(mod\ m)$$
$$a\cdot r_2\equiv\rho_{\varphi 2}(mod\ m)$$
$$...$$
$$a\cdot r_c\equiv\rho_{\varphi\chi}(mod\ m)$$

Перемножим эти c штук сравнений. Получится:

$$a^c r_1 r_2 ... r_c\equiv\rho_{j1}\rho_{j2}...\ \rho_{jc}(mod\ m)$$

Так как $r_1 r_2 ... r_c=\rho_1\rho_2...\ \rho_c\neq 0$ и взаимно просто с модулем m , то, поделив последнее сравнение на $r_1 r_2 ... r_c$, получим $a^{\varphi(m)}\equiv 1(mod\ m)$.

♦

Теорема (Ферма). Пусть p – простое число, p не делит a . Тогда:

$$a^{p-1} \equiv 1 (mod\ p) .$$

Доказательство 1. Положим в условии теоремы Эйлера $m=p$, тогда $\varphi(m)=p-1$
Получаем $a^{p-1} \equiv 1 (mod\ p)$.

♦

Необходимо отметить важность условия взаимной простоты модуля и числа a в формулировках теорем Эйлера и Ферма. Простой пример: сравнение $6^2 \equiv 1 (\mathrm{mod}\ 3)$ очевидно не выполняется. Однако можно легко подправить формулировку теоремы Ферма, чтобы снять ограничение взаимной простоты.

Следствие 1. Без всяких ограничений на $a \in \mathbf{Z}$,

$$a^{p} \equiv a(mod\ p)\ .$$

Доказательство. Умножим обе части сравнения $a^{p-1} \equiv 1(mod\ p)$ на a. Ясно, что получится сравнение, справедливое и при a, кратном p.

♦

Другое (элементарное) доказательство теоремы Ферма.

Доказательство 2. Так как p - простое число, то все биномиальные коэффициенты: (кроме C_0^p и C_p^p) делятся на p, ибо числитель выписанного выражения содержит p, а знаменатель не содержит этого множителя. Если вспомнить бином Ньютона, то становится понятно, что разность $(A+B)^p - A^p - B^p = C_p^1 A^{p-1} B^1 + C_p^2 A^{p-2} B^2 + \ldots + C_p^{p-2} A^2 B^{p-2} + C_p^{p-1} A^1 B^{p-1}$, где A и B – какие угодно целые числа, всегда делится на p. Последовательным применением этого незатейливого наблюдения получаем, что $(A+B+C)^p - A^p - B^p - C^p = \{[(A+B)+C]^p - (A+B)^p - C^p\} + (A+B)^p - A^p - B^p$ всегда делится на p; $(A+B+C+D)^p - A^p - B^p - C^p - D^p$ всегда делится на p; и вообще, $(A+B+C+\ldots+K)^p - A^p - B^p - C^p - \ldots - K^p$ всегда делится на p. Положим теперь в последнем выражении $A=B=C=\ldots=K=1$ и возьмем количество этих чисел равным a. Получится, что $a^p - a$ делится на p, а это и есть теорема Ферма в более общей формулировке.

♦

Следствие 2. $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Применение теорем Эйлера и Ферма

Пример 1. Девятая степень однозначного числа оканчивается на 7. Найти это число.

Решение. $a^{9} \equiv 7 (\mathrm{mod}\ 10)$ – это дано. Кроме того, очевидно, что (7, 10)=1 и (a , 10)=1. По теореме Эйлера, $a^{\varphi(10)} \equiv 1 (\mathrm{mod}\ 10)$. Следовательно, $a^{4} \equiv 1 (\mathrm{mod}\ 10)$ и, после возведения в квадрат, $a^{8} \equiv 1 (\mathrm{mod}\ 10)$. Поделим почленно $a^{9} \equiv 7 (\mathrm{mod}\ 10)$ на $a^{8} \equiv 1 (\mathrm{mod}\ 10)$ и получим $a \equiv 7 (\mathrm{mod}\ 10)$. Это означает, что a=7.

Пример 2. Доказать, что $1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18} \equiv -1 (\mathrm{mod}\ 7)$

Доказательство. Числа 1, 2, 3, 4, 5, 6 взаимно просты с 7. По теореме Ферма имеем:

$$\begin{cases} 1^{6} \equiv 1 (\mathrm{mod}\ 7) \\ 2^{6} \equiv 1 (\mathrm{mod}\ 7) \\ \vdots \\ 6^{6} \equiv 1 (\mathrm{mod}\ 7) \end{cases}$$

Возведем эти сравнения в куб и сложим:

$1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18} \equiv 6 (\mathrm{mod}\ 7) \equiv -1 (\mathrm{mod}\ 7)$

Пример 3. Найти остаток от деления 7^{402} на 101 .

Решение. Число 101 – простое, (7, 101)=1, следовательно, по теореме Ферма: $7^{100} \equiv 1(\text{mod } 101)$. Возведем это сравнение в четвертую степень: $7^{400} \equiv 1(\text{mod } 101)$, домножим его на очевидное сравнение $7^{2} \equiv 49(\text{mod } 101)$, получим: $7^{402} \equiv 49(\text{mod } 101)$. Значит, остаток от деления 7^{402} на 101 равен 49.

Пример 4. Найти две последние цифры числа 243^{402}.

Решение. Две последние цифры этого числа суть остаток от деления его на 100. Имеем: 243=200+43; $200+43 \equiv 43 \pmod{100}$ и, возведя последнее очевидное сравнение в 402-ую степень, раскроем его левую часть по биному Ньютона (мысленно, конечно). В этом гигантском выражении все слагаемые, кроме последнего, содержат степень числа 200, т.е. делятся на 100, поэтому их можно выкинуть из сравнения, после чего понятно, почему $243^{402} \equiv 43^{402} \pmod{100}$. Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера, $43^{\varphi(100)} \equiv 1 \pmod{100}$. Считаем:

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = (10-5)(10-2) = 40.$$

Имеем сравнение: $43^{40} \equiv 1 \pmod{100}$, которое немедленно возведем в десятую степень и умножим почленно на очевидное сравнение, проверенное на калькуляторе: $43^2 \equiv 49 \pmod{100}$. Получим:

$$\times \begin{cases} 43^{400} \equiv 1 \pmod{100} \\ 43^2 \equiv 49 \pmod{100} \end{cases}$$

$$43^{402} \equiv 49 \pmod{100},$$

следовательно, две последние цифры числа 243^{402} суть 4 и 9 .

Пример 5. Доказать, что $(73^{12}-1)$ делится на 105.

Решение. Имеем: $105=3 \cdot 5 \cdot 7$, $(73,3)=(73,5)=(73,7)=1$. По теореме Ферма:

$$73^{2} \equiv 1(\mathrm{mod}\ 3)$$
$$73^{4} \equiv 1(\mathrm{mod}\ 5)$$
$$73^{6} \equiv 1(\mathrm{mod}\ 7)$$

Перемножая, получаем:

$$73^{12} \equiv 1(\mathrm{mod}\ 3),(\mathrm{mod}\ 5),(\mathrm{mod}\ 7),$$

откуда, по свойствам сравнений, изложенным в пункте 16, немедленно следует:

$$73^{12}-1 \equiv 0(\mathrm{mod}\ 105),$$

ибо 105 - наименьшее общее кратное чисел 3, 5 и 7 . Именно это и требовалось.

Цепные дроби. Разложение числа в конечную цепную дробь

Пусть $a>0,\ m>0$ и $(a,m)=1$. Применяя к дроби $\frac{a}{m}$ алгоритм Евклида имеем

$$a = mq_0 + a_1 \qquad (1)$$
$$m = a_1 q_1 + a_2 \qquad (2)$$
$$a_1 = a_2 q_2 + a_3 \qquad (3)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{k-2} = a_{k-1} q_{k-1} + a_k \qquad (k)$$
$$a_{k-1} = a_k \cdot q_k + 0 \qquad (k+1)$$

Из равенства (1) имеем $\frac{a}{m} = q_0 + \frac{a_1}{m} = q_0 + \frac{1}{m}$.

Из равенства (2) имеем $\frac{m}{a_1} = q_1 + \frac{a_2}{a_1} = q_1 + \frac{1}{\frac{a_1}{a_2}}$

Откуда

$$\frac{a}{m} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{a_1}{a_2}}} \qquad (*)$$

Из равенства (3) имеем $\frac{a_1}{a_2} = q_2 + \frac{a_3}{a_2} = q_2 + \frac{1}{\frac{a_2}{a_3}}$. Подставляя $\frac{a_1}{a_2}$ в равенство (*) имеем

$$\frac{a}{m} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{a_2}{a_3}}}$$

Продолжая этот процесс для оставшихся равенств, получим

$$\frac{a}{m} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}$$

Правую часть этого равенства называют конечной цепной дробью и обозначают ее $[q_0, q_1, q_2, ..., q_k]$. Итак, получили разложение числа $\frac{a}{m}$ в конечную цепную дробь $\frac{a}{m} = [q_0, q_1, q_2, ..., q_k]$.

Пример. Разложить число $\frac{985}{533}$ в цепную дробь при помощи алгоритма Евклида.

Решение. Применяя к числу $\frac{985}{533}$ алгоритм Евклида получим:

$985 = 533 \cdot 1 + 452$
$533 = 452 \cdot 1 + 81$
$452 = 81 \cdot 5 + 47$
$81 = 47 \cdot 1 + 34$
$47 = 34 \cdot 1 + 13$
$34 = 13 \cdot 2 + 8$
$13 = 8 \cdot 1 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2$

Тогда $\frac{985}{533} = [1,1,5,1,1,2,1,1,1,1,2]$.

Подходящие дроби и их вычисление

Дроби вида $\delta_0 = q_0,\ \delta_1 = q_0 + \frac{1}{q_1},\ \delta_2 = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}, \ldots$ называются подходящими дробями к цепной дроби $[q_0, q_1, q_2, \ldots, q_k] = \frac{a}{m}$. Подходящими дробями к цепной дроби [1,1,5,1,1,2,1,1,1,1,2] являются

$$\delta_0 = 1 = \frac{1}{1},\ \delta_1 = 1 + \frac{1}{1} = \frac{2}{1},\ \delta_2 = 1 + \cfrac{1}{1 + \cfrac{1}{5}},\ \delta_3 = 1 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1}}}, \ldots\ldots,$$

$$\delta_{10} = 1 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}}}}}}}}$$

Вывод рекуррентной формулы вычисления подходящей дробей основан на простой идее представления подходящей дроби δ_k в виде $\frac{P_k}{Q_k}$.

$$\delta_0 = q_0 = \frac{q_0}{1} = \frac{P_0}{Q_0} \qquad (q_0 = p_0; Q_0 = 1)$$

$$\delta_1 = q_0 + \frac{1}{q_1} = \frac{q_0 + \frac{1}{q_1}}{1} = \frac{q_1 q_0 + 1}{q_1 \cdot 1 + 0} = \frac{q_1 P_0 + P_{-1}}{q_1 Q_0 + Q_{-1}} = \frac{P_1}{Q_1} \quad (P_{-1} = 1, Q_{-1} = 0)$$

$$\delta_2 = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = \frac{\left(q_1 + \frac{1}{q_2}\right)q_0 + 1}{\left(q_1 + \frac{1}{q_2}\right)\cdot 1 + 0} = \frac{\left(q_1 + \frac{1}{q_2}\right)\cdot P_0 + P_{-1}}{\left(q_1 + \frac{1}{q_2}\right)\cdot Q_0 + Q_{-1}} =$$

$$= \frac{q_1 \cdot P_0 q_2 + P_0 + q_2 P_{-1}}{q_1 \cdot Q_0 q_2 + Q_0 + q_2 Q_{-1}} = \frac{q_2\left(q_1 P_0 + P_{-1}\right) + P_0}{q_2\left(q_1 Q_0 + Q_{-1}\right) + Q_0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2}$$

и так далее и вообще при $n \geq 0$ имеем

$$\delta_n = \frac{q_n P_{n-1} + P_{n-2}}{q_n Q_{n-1} + Q_{n-2}} = \frac{P_n}{Q_n}, \text{ где } P_{-1} = 1, \quad Q_{-1} = 0$$

При $n = 0$ имеем $\delta_0 = \frac{q_0 P_{-1} + P_{-2}}{q_0 Q_{-1} + Q_{-2}} = \frac{q_0 + P_{-2}}{0 + Q_{-2}}$, но $\delta_0 = q_0$, поэтому потребуем еще: $P_{-2} = 0, \quad Q_{-2} = 1.$

Таким образом, при $n \geq 0$ числители и знаменатели подходящих дробей к цепной дроби $\frac{a}{m} = [q_0, q_1, q_2, ..., q_k]$ вычисляются по формулам

$$P_n = q_n P_{n-1} + P_{n-2} \text{ при условии, что } P_{-2} = 0, \quad P_{-1} = 1$$
$$Q_n = q_n Q_{n-1} + Q_{n-2} \text{ при условии, что } Q_{-2} = 1, \quad Q_{-1} = 0$$

Ради удобства, вычисления оформим в виде таблицы 1:
Таблица 1

n	-2	-1	0	1	2	·	·	k-1	k
q_n			q_0	q_1	q_2	·	·	q_{k-1}	q_k
P_n	0	1	P_0	P_1	P_2	·	·	P_{k-1}	P_k
Q_n	1	0	Q_0	Q_2	Q_2	·	·	Q_{k-1}	Q_k

Из определения подходящей дроби, следует, что $q_k = \frac{P_k}{Q_k} = \frac{a}{m}$. Так как $(a, m) = 1$, то $P_k = a,\ Q_k = m$.

Можно показать, что $P_k \cdot Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$. Умножая это равенство на $(-1)^{k-1}$ получим:

$$(-1)^{k-1} \cdot P_k \cdot Q_{k-1} - P_{k-1} \cdot (-1)^{k-1} \cdot Q_k = (-1)^{2k-2} = 1$$

Учитывая, что $P_k = a,\ \ Q_k = m$ имеем

$$(-1)^{k-1} \cdot Q_{k-1} \cdot a - m \cdot (-1)^{k-1} P_{k-1} = 1 \qquad (*)$$

Пример. Найти подходящие дроби к цепной дроби

$$\frac{985}{533} = [1,1,5,1,1,2,1,1,1,1,2].$$

Решение. Вычисления $\{P_n\}$ и $\{Q_n\}$ сведем в таблицу 2.

Таблица 2

n	-2	-1	0	1	2	3	4	5	6	7	8	9	10
q_n			1	1	5	1	1	2	1	1	1	1	2
P_n	0	1	1	2	11	13	24	61	85	146	231	377	985
Q_n	1	0	1	1	6	7	13	33	46	79	125	204	533

Цепные дроби могут быть применены для решения сравнений первой степени.

Пример 1. Решите уравнение $985 \cdot x \equiv 1 (\mathrm{mod}\, 533)$.

Решение. Из рассмотренного ране примера (смотри таблицу № 2) следует, что $k = 10$, $Q_{k-1} = Q_9 = 204$ и поэтому решением уравнения является $x \equiv (-1)^9 \cdot 204 (\mathrm{mod}\, 533)$ или $x \equiv -204 (\mathrm{mod}\, 533)$ или $x + 204 = 533 \cdot t$, $t \in z$. При $t = 0$, $x = -204$. Проверим это решение $985 \cdot (-204) = -200940 = 533(-377) + 1 \equiv$ $\equiv 1 (\mathrm{mod}\, 533)$.

Таблица 2

n	-2	-1	0	1	2	3	4	5	6	7	8	9	10
q_n			1	1	5	1	1	2	1	1	1	1	2
P_n	0	1	1	2	11	13	24	61	85	146	231	377	985
Q_n	1	0	1	1	6	7	13	33	46	79	125	204	533