Приведенная система вычетов

Определение

- Числа одного и того же класса по модулю M имеют с модулем один и тот же общий наибольший делитель. Особенно важны классы, для которых этот делитель равен единице, т.е. классы, содержащие числа, взаимно простые с модулем.
- Взяв от каждого такого класса по одному вычету, получим приведенную систему вычетов по модулю M. Приведенную систему вычетов, следовательно, можно составить из чисел полной системы, взаимно простых с модулем. Обыкновенно приведенную систему вычетов выделяют из системы наименьших неотрицательных вычетов: 0,1, . . ., M-1. Так как среди этих чисел число взаимно простых с M есть f(M), то число чисел приведенной системы, равно как и число классов, содержащих числа, взаимно простые с модулем, есть f(M).

Пример

- **Пример.** Приведенная система вычетов по модулю 42 будет

  1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

Функция Эйлера

- Функция Эйлера $\phi(a)$ есть количество чисел из ряда 0, 1, 2,..., a–1, взаимно простых с a.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

Лемма

- Пусть
- Тогда

1) $$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)$$ (формула Эйлера);

2) $$\varphi(a) = \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2-1}\right)\cdots\left(p_n^{\alpha_n} - p_n^{\alpha_n-1}\right),$$

- в частности, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\phi(p) = p-1$.

Лемма2

модулю m и взаимно простые с модулем, образуют приведенную систему вычетов по модулю m.

- 2) Если $d(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m, то ax так же пробегает приведенную систему вычетов по модулю m.
- **Доказательство**. Утверждение 1) – очевидно. Докажем утверждение 2). Числа ax попарно несравнимы (это доказывается так же, как в лемме 1 этого пункта), их ровно $\phi(m)$ штук. Ясно также, что все они взаимно просты с модулем, ибо $d(a, m)=1$, $d(x,m)=1 \Rightarrow d(ax, m)=1$. Значит, числа ax образуют приведенную систему

Лемма3

- Пусть $m_1, m_2, \ldots, m_k$ – попарно взаимно просты и $m_1 m_2 \ldots m_k = M_1 m_1 = M_2 m_2 = \ldots = M_k m_k$, где $M_j = m_1 \ldots m_{j-1} m_{j+1} \ldots m_k$
- 1) Если $x_1, x_2, \ldots, x_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 x_1 + M_2 x_2 + \ldots + M_k x_k$ пробегают полную систему вычетов по модулю $m = m_1 m_2 \ldots m_k$.
- 2) Если $\xi_1, \xi_2, \ldots, \xi_k$ пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 \xi_1 + M_2 \xi_2 + \ldots + M_k \xi_k$ пробегают приведенную систему вычетов по модулю $m = m_1 m_2 \ldots m_k$.

Лемма4

- Пусть $x_1, x_2, \ldots, x_k$, x пробегают полные, а $\xi_1, \xi_2, \ldots, \xi_k, \xi$ – пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ и $m = m_1 m_2 \ldots m_k$ соответственно, где $(m_i m_j) = 1$ при $i \neq j$. Тогда дроби $\{x_1/m_1 + x_2/m_2 + \ldots + x_k/m_k\}$ совпадают с дробями $\{x/m\}$, а дроби $\{\xi_1/m_1 + \xi_2/m_2 + \ldots + \xi_k/m_k\}$ совпадают с дробями $\{\xi/m\}$.
- Обозначим через ε_k k-ый корень m- ой степени из единицы:

$$\varepsilon_k = \cos\frac{2\pi k}{m} + i\sin\frac{2\pi k}{m} = e^{i\frac{2\pi k}{m}}$$

Здесь k=0,1,…,m-1 – пробегает полную систему вычетов по модулю m.

Напомню, что сумма $\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{m-1}$ всех корней m -ой степени из единицы равна нулю для любого m. Действительно, пусть $\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{m-1} = a$. Умножим эту сумму на ненулевое число ε_1. Такое умножение геометрически в комплексной плоскости означает поворот правильного m-угольника, в вершинах которого расположены корни $\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{m-1}$, на ненулевой угол $2\pi/m$. Ясно, что при этом корень ε_0 перейдет в корень ε_1, корень ε_1 перейдет в корень ε_2, и т.д., а корень ε_{m-1}перейдет в корень ε_0, т.е. сумма $\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{m-1}$ не изменится. Имеем $\varepsilon_1 a = a$, откуда $a=0$.

Теорема1

- Пусть $m>0$ – целое число, $a \in \mathbf{Z}$, x пробегает полную систему вычетов по модулю m. Тогда, если a кратно m, то

$$\sum_x e^{2\pi i \frac{ax}{m}} = m$$

- в противном случае, при a не кратном m,

$$\sum_x e^{2\pi i \frac{ax}{m}} = 0$$

Теорема2

- Пусть $m>0$ – целое число, ξ пробегает приведенную систему вычетов по модулюm. Тогда (сумма первообразных кс

$$\sum_{\xi} e^{2\pi i \frac{\xi}{m}} = \mu(m),$$

где μ(m) – функция Мебиуса.