8В, спецкурс, занятие 19

9 февраля 2024

Функция Эйлера и теорема Эйлера

Определение. *Функция Эйлера* $\varphi(n)$ вычисляет количество остатков по модулю n, взаимно простых с n.

Предложение. Если p простое, то $\varphi(p) = p - 1$ и $\varphi(p^k) = p^k - p^{k-1}$.

Доказательство. Среди p^k остатков $0, 1, \ldots, p^k - 1$ каждый p-й делится на p, поэтому есть ровно p^{k-1} остатков, не взаимно простых с p^k. □

Предложение. Функция Эйлера *мультипликативна*: для любых взаимно простых a и b выполняется $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство. Пусть $x_1, \ldots, x_{\varphi(a)}$ – остатки по модулю a, взаимно простые с a, и $y_1, \ldots, y_{\varphi(b)}$ – остатки по модулю b, взаимно простые с b.

Нас интересуют все такие остатки z по модулю ab, которые взаимно просты и с a, и с b. Иными словами, $\begin{cases} z \equiv x_i \pmod a \\ z \equiv y_j \pmod b \end{cases}$ для каких-то i, j. По КТО, у каждой такой системы будет ровно одно решение по модулю ab (у разных систем эти решения, естественно, разные). А всего таких систем можно написать $\varphi(a)\varphi(b)$, так как мы может выбрать любой x_i и любой y_j.

Следовательно, остатков по модулю ab, взаимно простых с ab, ровно $\varphi(a)\varphi(b)$, что и требовалось. □

Следствие. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Тогда

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_1^{\alpha_1} - p_k^{\alpha_k - 1}) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$

Теорема (Эйлер)**.** Пусть НОД$(a, n) = 1$. Тогда $a^{\varphi(n)} \equiv 1 \pmod n$.

Доказательство. Пусть $x_1, x_2, \ldots, x_{\varphi(n)}$ – все остатки по модулю n, взаимно простые с ним. Остатки $ax_1, ax_2, \ldots, ax_{\varphi(n)}$ все разные и каждый из них также взаимно прост с n. Поэтому это те же самые остатки $x_1, x_2, \ldots, x_{\varphi(n)}$, только возможно в другом порядке. Поэтому

$$ax_1 \cdot ax_2 \cdot \ldots \cdot ax_{\varphi(n)} \equiv x_1 x_2 \ldots x_{\varphi(n)} \pmod n \Longrightarrow a^{\varphi(n)} \equiv 1 \pmod n.$$

□

Примеры. Найдем остаток от деления 5^{11234} на 666. Поскольку $666 = 2 \cdot 3^2 \cdot 37$, то $\varphi(666) = 1 \cdot 6 \cdot 36 = 216$. Далее, $11234 \equiv 2 \pmod{216}$, поэтому по теореме Эйлера $5^{11234} \equiv 5^2 = 25 \pmod{666}$.

Найдем остаток от деления 9^{66} на 48. Тут нельзя использовать теорему Эйлера напрямую, потому что 9 и 48 не взаимно просты. Ищем остатки по модулям 3 и 16. Так как $\varphi(16) = 8$, то $9^{66} \equiv 9^2 \equiv 1 \pmod{16}$. Также, $21^{66} \equiv 0 \pmod 3$. По КТО находим, что $9^{66} \equiv 33 \pmod{48}$.

На последнем шаге проще всего не решать систему сравнений, а перебрать остатки по модулю 48, сравнимые с 1 по модулю 16. Это 1, 17, 33, из них на 3 делится только 33.

1$^{\vee}$ Вычислите остатки от деления:
a $17^{16} \mod 32$; b $502^{567} \mod 100$; c $35^{17} \mod 120$; d $77^{21} \mod 675$;
Указание: в некоторых пунктах полезно разложить модуль на два взаимно простых множителя и смотреть остатки отдельно по каждому из них.

2 a Докажите, что $5^{\left(6^7\right)} - 1$ делится на $2016 = 2^5 \cdot 3^2 \cdot 7$.
b Какой остаток дает $21^{\left(211^{2112}\right)}$ при делении на 100?

3 Решите уравнения в натуральных числах
a $\varphi(7^x) = 294$; b $\varphi(3^x 5^y) = 360$; c $\varphi(n) = \frac{n}{2}$; d $\varphi(n) = \frac{n}{3}$.

4 Докажите, что $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ для взаимно простых a и b.

5 a Докажите, что $2^{n!} - 1$ делится на n, если n нечетно.
b Докажите, что $2^{n!} - 1$ делится на $n^2 - 1$, если n четно.

6 Докажите, что $n^{561} \equiv n \pmod{561}$ для любого n.

7 a В ряд выписали все правильные дроби со знаменателем n

$$\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$$

и сократили их. Сколько дробей с каким знаменателем получилось?
b (*Тождество Гаусса*) Докажите, что $\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_k) = n$, где $d_1, d_2, \ldots, d_k$ – всевозможные делители числа n, включая 1 и само n.

8 Имеется бесконечное количество карточек, на каждой из которых написано какое-то натуральное число. Известно, что для любого натурального числа n существуют ровно n карточек, на которых написаны делители этого числа. Докажите, что каждое натуральное число встречается хотя бы на одной карточке.

9 Докажите, что для любого натурального n существует число с суммой цифр n, делящееся на n.

10$^{\bigstar}$ Докажите, что $\underbrace{2^{2^{\cdot^{\cdot^{\cdot^2}}}}}_{n \text{ раз}} - \underbrace{2^{2^{\cdot^{\cdot^{\cdot^2}}}}}_{n-1 \text{ раз}}$ делится на n для любого натурального $n \geq 2$.