Лепреконы

16 ноября 2013 г.

Системы вычетов по модулю целого числа

Определение. $\varphi(n)$ — количество натуральных чисел от 1 до n, взаимно простых с n. Выражение $\varphi(n)$ называется *функцией Эйлера.*

1. Докажите, что при $n > 2 \quad \varphi(n) \vdots 2$.

2. (Теорема Эйлера.) Пусть n — натуральное число, a — целое число, взаимно простое с n. Докажите, что $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Указание. Воспользуйтесь свойствами приведённой системы вычетов.

3. Простое число p больше пяти. Докажите, что число из $p-1$ единицы делится на p.

4. Число n нечётно. Докажите, что $2^{n!} - 1$ делится на n.

Определение. Вычет b называется *обратным* к вычету a, если $ab \equiv 1 \pmod{m}$.

5. Пусть p — простое число. а) Докажите, что для любого a от 1 до $p-1$, существует ровно один обратный вычет. б) Докажите, что если $x^2 \equiv 1 \pmod{p}$, то $x \equiv \pm 1 \pmod{p}$. в) **(Теорема Вильсона.)** Докажите, что $(p-1)! \equiv -1 \pmod{p}$. г) Докажите, что если для $m > 1$ имеет место сравнение $(m-1)! \equiv -1 \pmod{m}$, то m — простое.

6. Пусть $p \in \mathbb{P}$. Докажите, что $(2p-1)! - p$ делится на p^2.

7. Докажите, что для любых натуральных чисел m и n существует такое рациональное число x, что $\frac{1}{3} \leq \{mx\} \leq \frac{2}{3}$ и $\frac{1}{3} \leq \{nx\} \leq \frac{2}{3}$. (Через $\{y\}$ обозначается дробная часть числа y).

Лепреконы

16 ноября 2013 г.

Системы вычетов по модулю целого числа

Определение. $\varphi(n)$ — количество натуральных чисел от 1 до n, взаимно простых с n. Выражение $\varphi(n)$ называется *функцией Эйлера.*

1. Докажите, что при $n > 2 \quad \varphi(n) \vdots 2$.

2. (Теорема Эйлера.) Пусть n — натуральное число, a — целое число, взаимно простое с n. Докажите, что $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Указание. Воспользуйтесь свойствами приведённой системы вычетов.

3. Простое число p больше пяти. Докажите, что число из $p-1$ единицы делится на p.

4. Число n нечётно. Докажите, что $2^{n!} - 1$ делится на n.

Определение. Вычет b называется *обратным* к вычету a, если $ab \equiv 1 \pmod{m}$.

5. Пусть p — простое число. а) Докажите, что для любого a от 1 до $p-1$, существует ровно один обратный вычет. б) Докажите, что если $x^2 \equiv 1 \pmod{p}$, то $x \equiv \pm 1 \pmod{p}$. в) **(Теорема Вильсона.)** Докажите, что $(p-1)! \equiv -1 \pmod{p}$. г) Докажите, что если для $m > 1$ имеет место сравнение $(m-1)! \equiv -1 \pmod{m}$, то m — простое.

6. Пусть $p \in \mathbb{P}$. Докажите, что $(2p-1)! - p$ делится на p^2.

7. Докажите, что для любых натуральных чисел m и n существует такое рациональное число x, что $\frac{1}{3} \leq \{mx\} \leq \frac{2}{3}$ и $\frac{1}{3} \leq \{nx\} \leq \frac{2}{3}$. (Через $\{y\}$ обозначается дробная часть числа y).