

# Дробные вычеты

5 июля

**Опр.** Через  $\mathbb{Z}_n$  будем обозначать систему вычетов по модулю  $n$ .

**I.** Для простого  $p$  сравнение  $b x \equiv a \pmod{p}$  имеет решение, и при том единственное.

**II.** Для какого-нибудь составного  $n$  приведите пример сравнение, которое **(а)** не имеет решения; **(б)** имеет единственное решение; **(в)** имеет несколько решений.

**Опр.** Обратным вычетом  $x^{-1}$  к вычету  $x$  по модулю  $n$  называется такой вычет  $y$ , что  $xy \equiv 1 \pmod{n}$ .

**Фокус.** Давайте решение  $x$  (если оно есть) сравнения  $b x \equiv a \pmod{n}$  записывать как  $b^{-1}a$  или  $\frac{a}{b}$ , что удобнее. Теперь хорошо было бы доказать, что вычеты, записанные в виде дробей действительно ведут себя как дроби.

**III.** Докажите, что если  $x \equiv \frac{a}{b}$ , а  $y \equiv \frac{c}{d} \pmod{p}$ , то **(а)**  $x * y \equiv \frac{ac}{bd}$ ; **(б)**  $x : y \equiv \frac{ad}{bc}$ ;

**(в)**  $x + y \equiv \frac{ad + bc}{bd}$ ; **(г)**  $x - y \equiv \frac{ad - bc}{bd}$ .

**1.** **(а)** Определите, какому классу вычетов принадлежит  $\frac{3}{4}$  по модулю 7. **(б)** Целое число  $a$  таково, что  $a^{52} \equiv 36 \pmod{73}$  и  $a^{53} \equiv 59 \pmod{73}$ . Какой остаток дает число  $a$  при делении на 73? **(в)** Какой остаток дает  $92!$  при делении на 97?

**2.** Докажите, что если  $3 \neq p \in \mathbb{P}$  и  $\exists a \in \mathbb{Z} : a^2 + 9 \vdots p$ , то  $\exists c \in \mathbb{Z} : c^2 + 1 \vdots p$ .

**3.** Натуральные числа  $a$  и  $b$  таковы, что число  $a^{2022} + 1$  делится на  $ab + 1$ . Докажите, что число  $b^{2022} + 1$  тоже делится на  $ab + 1$ .

**4. (Теорема Вильсона)**  $(p - 1)! \equiv -1 \pmod{p}$ .

**5. (Теорема Эйлера)** Пусть  $k \in \{1, 2, \dots, n\}$  такое число, что  $\text{НОД}(n, k) = 1$ . Обозначим за  $\varphi(n)$  количество этих чисел. Докажите, что  $k^{\varphi(n)} \equiv 1 \pmod{n}$ .

**6.** Пусть  $p$  — простое число. Найдите остаток от деления числа  $C_{2p}^p$  на  $p$ .

**7.** Докажите, что при простом  $p > 2$  числитель дроби

$$\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1}$$

после приведения делится на  $p$ .

**8.** Даны натуральные числа  $a$ ,  $b$  и  $c$  такие, что  $ab + 9b + 81$  и  $bc + 9c + 81$  делятся на 101. Докажите, что тогда и  $ca + 9a + 81$  тоже делится на 101.

**9.** Для простого числа  $p$  и натурального  $k > p$  докажите, что  $C_k^p \equiv \left[ \frac{k}{p} \right] \pmod{p}$ .

**10.** Докажите, что для любого простого числа  $p$  существует натуральное число  $n$  такое, что  $2^n + 3^n + 6^n \equiv 1 \pmod{p}$ .

**11.** Дано простое  $p$ . Докажите, что существует такая перестановка  $(a_1, a_2, \dots, a_p)$  чисел  $1, 2, 3, \dots, p$ , что числа  $a_1, a_1 a_2, a_1 a_2 a_3, \dots, a_1 a_2 \dots a_p$  дают разные остатки при делении на  $p$ .

# Дробные вычеты

5 июля

**Опр.** Через  $\mathbb{Z}_n$  будем обозначать систему вычетов по модулю  $n$ .

**I.** Для простого  $p$  сравнение  $b x \equiv a \pmod{p}$  имеет решение, и при том единственное.

**II.** Для какого-нибудь составного  $n$  приведите пример сравнение, которое **(а)** не имеет решения; **(б)** имеет единственное решение; **(в)** имеет несколько решений.

**Опр.** Обратным вычетом  $x^{-1}$  к вычету  $x$  по модулю  $n$  называется такой вычет  $y$ , что  $xy \equiv 1 \pmod{n}$ .

**Фокус.** Давайте решение  $x$  (если оно есть) сравнения  $b x \equiv a \pmod{n}$  записывать как  $b^{-1}a$  или  $\frac{a}{b}$ , что удобнее. Теперь хорошо было бы доказать, что вычеты, записанные в виде дробей действительно ведут себя как дроби.

**III.** Докажите, что если  $x \equiv \frac{a}{b}$ , а  $y \equiv \frac{c}{d} \pmod{p}$ , то **(а)**  $x * y \equiv \frac{ac}{bd}$ ; **(б)**  $x : y \equiv \frac{ad}{bc}$ ;

**(в)**  $x + y \equiv \frac{ad + bc}{bd}$ ; **(г)**  $x - y \equiv \frac{ad - bc}{bd}$ .

**1.** **(а)** Определите, какому классу вычетов принадлежит  $\frac{3}{4}$  по модулю 7. **(б)** Целое число  $a$  таково, что  $a^{52} \equiv 36 \pmod{73}$  и  $a^{53} \equiv 59 \pmod{73}$ . Какой остаток дает число  $a$  при делении на 73? **(в)** Какой остаток дает  $92!$  при делении на 97?

**2.** Докажите, что если  $3 \neq p \in \mathbb{P}$  и  $\exists a \in \mathbb{Z} : a^2 + 9 \vdots p$ , то  $\exists c \in \mathbb{Z} : c^2 + 1 \vdots p$ .

**3.** Натуральные числа  $a$  и  $b$  таковы, что число  $a^{2022} + 1$  делится на  $ab + 1$ . Докажите, что число  $b^{2022} + 1$  тоже делится на  $ab + 1$ .

**4. (Теорема Вильсона)**  $(p - 1)! \equiv -1 \pmod{p}$ .

**5. (Теорема Эйлера)** Пусть  $k \in \{1, 2, \dots, n\}$  такое число, что  $\text{НОД}(n, k) = 1$ . Обозначим за  $\varphi(n)$  количество этих чисел. Докажите, что  $k^{\varphi(n)} \equiv 1 \pmod{n}$ .

**6.** Пусть  $p$  — простое число. Найдите остаток от деления числа  $C_{2p}^p$  на  $p$ .

**7.** Докажите, что при простом  $p > 2$  числитель дроби

$$\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1}$$

после приведения делится на  $p$ .

**8.** Даны натуральные числа  $a$ ,  $b$  и  $c$  такие, что  $ab + 9b + 81$  и  $bc + 9c + 81$  делятся на 101. Докажите, что тогда и  $ca + 9a + 81$  тоже делится на 101.

**9.** Для простого числа  $p$  и натурального  $k > p$  докажите, что  $C_k^p \equiv \left[ \frac{k}{p} \right] \pmod{p}$ .

**10.** Докажите, что для любого простого числа  $p$  существует натуральное число  $n$  такое, что  $2^n + 3^n + 6^n \equiv 1 \pmod{p}$ .

**11.** Дано простое  $p$ . Докажите, что существует такая перестановка  $(a_1, a_2, \dots, a_p)$  чисел  $1, 2, 3, \dots, p$ , что числа  $a_1, a_1 a_2, a_1 a_2 a_3, \dots, a_1 a_2 \dots a_p$  дают разные остатки при делении на  $p$ .