Обратные остатки

1. **(a)** Рассмотрим целое число a и простое p такие, что $(a, p) = 1$. Докажите, что в последовательности

$$0 \cdot a,\ 1 \cdot a,\ 2 \cdot a,\ \ldots,\ (p-1) \cdot a$$

все числа дают разные остатки при делении на p.

(b) Рассмотрим целое число a и натуральное n такие, что $(a, n) = 1$. Пусть a_1, a_2, ..., a_k — остатки по модулю n взаимно простые с n. Докажите, что в последовательности

$$a_1 \cdot a,\ a_2 \cdot a,\ \ldots,\ a_k \cdot a$$

все числа дают разные остатки при делении на n.

(c) Найдите необходимое и достаточное условие на числа a и n, чтобы существовал единственный остаток x такой, что $ax \equiv 1 \pmod{n}$.

2. Выведите из предыдущей задачи

(a) *теорему Вильсона*: если p — простое, то $(p-1)! \equiv -1 \pmod{p}$;

(b) *теорему Эйлера*: если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$; в частности, для простого $p > 2$ выполнено сравнение $a^{p-1} \equiv 1 \pmod{p}$ (*малая теорема Ферма*).

---

3. Пусть a_1, a_2, ..., a_p — конечная арифметическая прогрессия с разностью, не кратной p. Докажите, что существует k такое, что $a_k + a_1 a_2 \ldots a_p$ делится на p^2.

4. Пусть $p > 3$ — простое число.

(a) Преобразуем сумму

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

в дробь m/n. Докажите, что m делится на p.

(b) Преобразуем сумму

$$\frac{1}{1} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(p-1)^2}$$

в дробь m/n. Докажите, что m делится на p.

(c) Преобразуем сумму

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1}$$

в дробь m/n. Докажите, что m делится на p^2.

(d) *Теорема Вольстенхольма.* Докажите, что выполняется сравнение

$$C_{2p}^{p} \equiv 2 \pmod{p^3}.$$

5. Пусть $a_1, a_2, ..., a_k$ — остатки по модулю n взаимно простые с n.

(a) Докажите, что $a_1 a_2 \dots a_k \equiv \pm 1 \pmod{n}$.

(b) Докажите, что

$$a_1 a_2 \dots a_k \equiv \begin{cases} -1 \pmod{n}, & \text{если } n = 4,\ p^\alpha,\ 2p^\alpha; \\ 1 \pmod{n} & \text{иначе.} \end{cases}$$