Обратные остатки

1. Дано натуральное число n. Рассмотрим *полную систему вычетов* — множество всех остатков по модулю n:

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

(а) Пусть дано натуральное m такое, что m и n взаимно просты. Докажите, что множество

$$\{0 \cdot m, 1 \cdot m \pmod n, 2 \cdot m \pmod n, \ldots, (n-1) \cdot m \pmod n\}$$

совпадает с полной системой вычетов.
(б) Докажите с помощью пункта (а), что для каждого остатка k существует единственный остаток x, такой, что $mx \underset{n}{\equiv} k$. В частности, нас будет интересовать $k = 1$.
(в) Пусть m и n не взаимно просты. Докажите, что множество из пункта (а) в этом случае не совпадает с полной системой вычетов. В частности, остаток 1 не будет лежать в этом множестве.

Определение. Остаток b называется *обратным к остатку a по модулю n*, если $ab \underset{n}{\equiv} 1$. Обозначение: $b \underset{n}{\equiv} a^{-1}$.

Важное свойство остатков: Пусть $b \underset{n}{\equiv} a^{-1}, d \underset{n}{\equiv} c^{-1}$. Тогда: $bd \underset{n}{\equiv} (ac)^{-1}$.

2. **(а)** У каких остатков по натуральному модулю n существуют обратные?
(б) Докажите, что обратный остаток (если он существует) единственен.
(в) Пусть остаток b — обратный к остатку a по модулю n. Докажите, что остаток a — обратный к остатку b по модулю n. Таким образом, обратимые остатки по модулю n разбиваются на пары.
(г) Пусть $b \underset{p}{\equiv} a^{-1}$. Выразите через a и n остаток, обратный к b^n.
(д) Найдите остаток a, если $5a \underset{59}{\equiv} 13$.

3. Пусть a, b, x, y, n — натуральные числа. Известно, что

$$ax \underset{n}{\equiv} 1, by \underset{n}{\equiv} 1, x + y \underset{n}{\equiv} 1.$$

Докажите, что $ab - a - b \underset{n}{\equiv} 0$.

4. **(а) Теорема Вильсона**. Докажите, что для любого простого числа p верно $(p-1)! \underset{p}{\equiv} -1$.

(б) Обратная теорема Вильсона. Докажите, что если для натурального числа n выполнено $(n-1)! \underset{n}{\equiv} -1$, то n — простое.

5. **Малая теорема Ферма**. Даны простое p и натуральное a, не кратное p. Докажите, что $a^{p-1} \underset{p}{\equiv} 1$.

6. Пусть $p > 3$ — простое число. Рациональное число

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

представили в виде несократимой дроби. Докажите, что числитель этой дроби делится на p.

7. Дано простое число p. Для каждого натурального $1 \leqslant x \leqslant p-1$ рассмотрим выражение x^2+3x+1. Оказалось, что ровно 1 из них делится на p. Найдите все возможные значения p.

8. Докажите, что для любого простого $p > 3$ существует бесконечно много натуральных n таких, что $2^n + 3^n + 6^n - 1$ делится на p.