Обратимые вычеты

1. Найдите все $x \in \mathbb{Z}$ такие, что $5x \equiv_7 1$.
2. Найдите все $y, z \in \mathbb{Z}$ такие, что $4y + 9z = 1$.
3. Найдите все $t \in \mathbb{Z}$ такие, что $6t \equiv_{11} 5$.

! Вычет a называется *обратимым* по модулю m, если существует вычет b такой, что $a \cdot b \equiv_m 1$. В таком случае вычет b называется *обратным* к a.

!! Вычет a обратим по модулю m тогда и только тогда, когда $a \perp m$.

4. Докажите, что если вычет обратим, то обратный к нему единственный.
5. Дано $p \in \mathbb{P}$. Найдите числа в множестве $1, 2, ..., p-1$, представляющие вычеты, обратные к 2, $p-1$, $p-2$, $\dfrac{p-1}{2}$ по модулю p.
6. Дана арифметическая прогрессия $c_1, c_2, ..., c_m$ с разностью d.
   a) Предположим, что $d \perp m$.
   Докажите, что все члены прогрессии дают различные остатки при делении на m.
   b) Пусть $(d, m) = k$.
   Сколько различных остатков получается при делении $c_1, c_2, ..., c_m$ на m?

!! **Китайская теорема об остатках.**
Пусть $m_1, m_2, ..., m_n$ — попарно взаимно простые натуральные числа, $b_1, b_2, ..., b_n$ — произвольные целые числа. Система сравнений

$$x \underset{m_1}{\equiv} b_1, \quad x \underset{m_2}{\equiv} b_2, \quad ..., \quad x \underset{m_n}{\equiv} b_n$$

имеет решение, единственное по модулю $m_1 m_2 ... m_n$.

7. Докажите, что, какие бы ни были различные простые p_1, p_2, ..., p_n и натуральные t_1, t_2, ..., t_n, найдутся n подряд идущих натуральных чисел $a_1, a_2, ..., a_n$, таких что

$$a_1 \vdots p_1^{t_1}, \quad a_2 \vdots p_2^{t_2}, \quad ..., \quad a_n \vdots p_n^{t_n}$$

8. Докажите, что найдутся 1000 подряд идущих натуральных чисел, среди которых ровно 10 простых.
9. Найдите остаток от деления числа $(n-1)!$ на n в зависимости от n.

!! **Теорема Вильсона.** Если $p \in \mathbb{P}$, то $(p-1)! \equiv_p -1$.

10. Докажите, что простое число $p = 4k + 1$ делит число $((2k)!)^2 + 1$.

Обратимые вычеты

1. Найдите все $x \in \mathbb{Z}$ такие, что $5x \equiv_7 1$.
2. Найдите все $y, z \in \mathbb{Z}$ такие, что $4y + 9z = 1$.
3. Найдите все $t \in \mathbb{Z}$ такие, что $6t \equiv_{11} 5$.

! Вычет a называется *обратимым* по модулю m, если существует вычет b такой, что $a \cdot b \equiv_m 1$. В таком случае вычет b называется *обратным* к a.

!! Вычет a обратим по модулю m тогда и только тогда, когда $a \perp m$.

4. Докажите, что если вычет обратим, то обратный к нему единственный.
5. Дано $p \in \mathbb{P}$. Найдите числа в множестве $1, 2, ..., p-1$, представляющие вычеты, обратные к 2, $p-1$, $p-2$, $\dfrac{p-1}{2}$ по модулю p.
6. Дана арифметическая прогрессия $c_1, c_2, ..., c_m$ с разностью d.
   a) Предположим, что $d \perp m$.
   Докажите, что все члены прогрессии дают различные остатки при делении на m.
   b) Пусть $(d, m) = k$.
   Сколько различных остатков получается при делении $c_1, c_2, ..., c_m$ на m?

!! **Китайская теорема об остатках.**
Пусть $m_1, m_2, ..., m_n$ — попарно взаимно простые натуральные числа, $b_1, b_2, ..., b_n$ — произвольные целые числа. Система сравнений

$$x \underset{m_1}{\equiv} b_1, \quad x \underset{m_2}{\equiv} b_2, \quad ..., \quad x \underset{m_n}{\equiv} b_n$$

имеет решение, единственное по модулю $m_1 m_2 ... m_n$.

7. Докажите, что, какие бы ни были различные простые p_1, p_2, ..., p_n и натуральные t_1, t_2, ..., t_n, найдутся n подряд идущих натуральных чисел $a_1, a_2, ..., a_n$, таких что

$$a_1 \vdots p_1^{t_1}, \quad a_2 \vdots p_2^{t_2}, \quad ..., \quad a_n \vdots p_n^{t_n}$$

8. Докажите, что найдутся 1000 подряд идущих натуральных чисел, среди которых ровно 10 простых.
9. Найдите остаток от деления числа $(n-1)!$ на n в зависимости от n.

!! **Теорема Вильсона.** Если $p \in \mathbb{P}$, то $(p-1)! \equiv_p -1$.

10. Докажите, что простое число $p = 4k + 1$ делит число $((2k)!)^2 + 1$.