Арифметика вычетов по модулю

1. Пусть p – простое число. Докажите, что:
   а) $C_{p+1}^k \equiv_p 0,\ 1 < k < p$;
   б) $C_{p-1}^k \equiv_p (-1)^k,\ 0 \le k \le p-1$.
2. Найдите остаток от деления числа $(n-1)!$ на n в зависимости от n.
3. а) Пусть $x_1, y_1, x_2, y_2 \in \mathbb{Z}$. Докажите, что $\exists x, y \in \mathbb{Z}$: $(x_1^2 + y_1^2)(x_2^2 + y_2^2) = x^2 + y^2$.
   б) Пусть $q \in \mathbb{P}$, $q \equiv_4 3$. Докажите, что если $x^2 + y^2 \vdots q$, то $x \vdots q$, $y \vdots q$.
   в) * Дано $n \in \mathbb{N}$. Докажите, что $\exists\, x, y \in \mathbb{Z}$ такие, что $n = x^2 + y^2$ тогда и только тогда, когда для любого простого $q \equiv_4 3$ справедливо $\nu_q(n) \vdots 2$.
4. Дана арифметическая прогрессия с разностью d, состоящая из m целых чисел. Сколько различных остатков дают члены этой прогрессии при делении на m?
5. Целые числа a, b, c, d, e, f таковы, что $a^{12} + b^{12} + c^{12} + d^{12} + e^{12} + f^{12} \vdots 13$. Докажите, что $abcdef \vdots 13^6$.
6. * Дано простое $p > 3$. Положим $n = \dfrac{2^{2p} - 1}{3}$. Докажите, что $2^n - 2 \vdots n$.
7. Найдите остаток от деления 7^{120} на 143.
8. * Дано простое $r > 2$. Будем называть натуральное число m *смешным*, если mr представимо в виде суммы четырёх квадратов целых чисел, не все из которых кратны r.
   а) Докажите, что найдётся хотя бы одно смешное $m < r$.
   б) Докажите, что если $2m$ смешное, то и m смешное, и наоборот.
   в) Пусть нечётное $m > 1$ смешное и $mr = t_1^2 + t_2^2 + t_3^2 + t_4^2$.
   Рассмотрим $\widehat{t_\ell} \equiv_m t_\ell$, $|\widehat{t_\ell}| < m/2$ для $\ell = 1, 2, 3, 4$.
      i. Докажите, что $\widehat{t_1}^2 + \widehat{t_2}^2 + \widehat{t_3}^2 + \widehat{t_4}^2 = mk$, причём $k \in \mathbb{N}$ и $k < m$.
      ii. Докажите, что $m^2 k$ смешное.
      iii. Докажите, что k смешное.

   Выведите из всего этого, что любое натуральное число можно представить в виде суммы четырёх квадратов (теорема Лагранжа).
9. Найдите три последние цифры числа $17^{1000001}$.
10. Докажите, что если $a \perp n$, то $\varphi(n) \vdots \mathrm{ord}_n(a)$. (За ord_n мы обозначили $\mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}$.)
11. Пусть $m \perp k$, $a \perp m$, $a \perp k$. Докажите, что $\mathrm{ord}_{mk} a = [\mathrm{ord}_m a, \mathrm{ord}_k a]$.

Арифметика вычетов по модулю

1. Пусть p – простое число. Докажите, что:
   а) $C_{p+1}^k \equiv_p 0,\ 1 < k < p$;
   б) $C_{p-1}^k \equiv_p (-1)^k,\ 0 \le k \le p-1$.
2. Найдите остаток от деления числа $(n-1)!$ на n в зависимости от n.
3. а) Пусть $x_1, y_1, x_2, y_2 \in \mathbb{Z}$. Докажите, что $\exists x, y \in \mathbb{Z}$: $(x_1^2 + y_1^2)(x_2^2 + y_2^2) = x^2 + y^2$.
   б) Пусть $q \in \mathbb{P}$, $q \equiv_4 3$. Докажите, что если $x^2 + y^2 \vdots q$, то $x \vdots q$, $y \vdots q$.
   в) * Дано $n \in \mathbb{N}$. Докажите, что $\exists\, x, y \in \mathbb{Z}$ такие, что $n = x^2 + y^2$ тогда и только тогда, когда для любого простого $q \equiv_4 3$ справедливо $\nu_q(n) \vdots 2$.
4. Дана арифметическая прогрессия с разностью d, состоящая из m целых чисел. Сколько различных остатков дают члены этой прогрессии при делении на m?
5. Целые числа a, b, c, d, e, f таковы, что $a^{12} + b^{12} + c^{12} + d^{12} + e^{12} + f^{12} \vdots 13$. Докажите, что $abcdef \vdots 13^6$.
6. * Дано простое $p > 3$. Положим $n = \dfrac{2^{2p} - 1}{3}$. Докажите, что $2^n - 2 \vdots n$.
7. Найдите остаток от деления 7^{120} на 143.
8. * Дано простое $r > 2$. Будем называть натуральное число m *смешным*, если mr представимо в виде суммы четырёх квадратов целых чисел, не все из которых кратны r.
   а) Докажите, что найдётся хотя бы одно смешное $m < r$.
   б) Докажите, что если $2m$ смешное, то и m смешное, и наоборот.
   в) Пусть нечётное $m > 1$ смешное и $mr = t_1^2 + t_2^2 + t_3^2 + t_4^2$.
   Рассмотрим $\widehat{t_\ell} \equiv_m t_\ell$, $|\widehat{t_\ell}| < m/2$ для $\ell = 1, 2, 3, 4$.
      i. Докажите, что $\widehat{t_1}^2 + \widehat{t_2}^2 + \widehat{t_3}^2 + \widehat{t_4}^2 = mk$, причём $k \in \mathbb{N}$ и $k < m$.
      ii. Докажите, что $m^2 k$ смешное.
      iii. Докажите, что k смешное.

   Выведите из всего этого, что любое натуральное число можно представить в виде суммы четырёх квадратов (теорема Лагранжа).
9. Найдите три последние цифры числа $17^{1000001}$.
10. Докажите, что если $a \perp n$, то $\varphi(n) \vdots \mathrm{ord}_n(a)$. (За ord_n мы обозначили $\mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}$.)
11. Пусть $m \perp k$, $a \perp m$, $a \perp k$. Докажите, что $\mathrm{ord}_{mk} a = [\mathrm{ord}_m a, \mathrm{ord}_k a]$.