Малая теорема Ферма

1. Пусть a — некоторое число, которое не делится на простое число p.
(a) Докажите, что в последовательности $0\cdot a, 1\cdot a, 2\cdot a, \ldots, (p-1)\cdot a$ все числа дают разные остатки по модулю p.
(b) Докажите, что $(1\cdot a)\cdot(2\cdot a)\cdot\ldots\cdot((p-1)\cdot a) \underset{p}{\equiv} (p-1)!$.
(c) **Малая теорема Ферма** Докажите, что $a^{p-1} \underset{p}{\equiv} 1$.

2. Найдите остаток от деления 23^{1600} на 41.

3. Докажите, что $300^{3000}-1$ делится на 1001.

4. Докажите, что n^7-n делится на 42.

5. Докажите, что либо $n^{18}-1$, либо $n^{18}+1$ делится на 37.

6. Докажите, что число $40^{81}+17^{160}$ является составным.

7. Пусть p — простое число.
(a) Докажите, что для любых чисел a и b верно, что $(a+b)^p \underset{p}{\equiv} a^p+b^p$.
(b) Выведите из этой задачи малую теорему Ферма.

8. Отметим на бумаге произвольным образом $p-1$ точку. Каждой точке сопоставим какой-то ненулевой остаток при делении на p. Проведём из остатка k стрелочку в остаток ka.
(a) Убедитесь, что из каждой точки выходит одна стрелочка, и в кажду точку входит одна стрелочка.
(b) Поймите, что тогда все точки разбиваются на циклические маршруты.
(c) Докажите, что у всех циклических маршртутов одна и та же длина, и она делит $p-1$.
(d) Выведите отсюда малую теорему Ферма.

9. Пусть p и q различные простые числа. Докажите, что $p^q+q^p \underset{pq}{\equiv} p+q$.

10. Докажите, что для любого простого $p>5$ справедливо, что
(a) число $\underbrace{111\ldots11}_{p-1}$ делится на p;
(b) число $\underbrace{111\ldots11}_{p}$ не делится на p.

11. Найти все такие простые числа p, что число $5^{p^2}-1$ делится на p.

12. Докажите, что для любого простого p число $2^{2^p}-4$ делится на 2^p-1.

Теорема Вильсона

1. Известно, что x^2-1 делится на простое число p. Какие остатки может давать x при делении на p?

2. Дано простое число p и его некоторый ненулевой остаток a.
(a) Докажите, что существует и при том единственный остаток b, что $ab \underset{p}{\equiv} 1$ (такой остаток b называется *обратным* остатка a).
(b) Какие остатки совпадают со своими обратными остатками?

3. Найдите обратные остатки:
(a) 2 и 3 по модулю 11;
(b) 5 по модулю 23;
(c) 17 по модулю 37.
(d) Сопоставьте каждому остатку его обратный по модулю 7.

4. **(Теорема Вильсона)** Пусть p – некоторое простое число. Докажите, что $(p-1)! \underset{p}{\equiv} -1$.

5. Докажите, что если $(n-1)! \underset{n}{\equiv} -1$, то число n — простое.

6. Пусть p — простое число. Докажите, что $(p-k)!\cdot(k-1)! \underset{p}{\equiv} (-1)^k$.

7. Пусть p — простое число. Докажите, что $(2p-1)!-p$ делится на p^2.

8. Пусть числа p и $p+2$ являются простыми числами-близнецами. Докажите, что справедливо $4((p-1)!+1)+p \underset{p^2+2p}{\equiv} 0$.

9. **(a)** На доске написаны числа $\frac{100}{1}, \frac{99}{2}, \ldots, \frac{2}{99}, \frac{1}{100}$. Можно ли выбрать какие-то пять из них, произведение которых равняется единице?
(b) Пусть произведение каких-то $2k+1$ чисел, написанных на доске, равно $\frac{m}{n}$. Докажите, что $m \underset{101}{\equiv} -n$.

10. Пусть $a_1, \ldots, a_p$ – конечная арифметическая прогрессия с разницей не кратной p. Докажите, что:
(a) существует некоторый член последовательности a_m, делящийся на p;
(b) существует некоторый член a_k, такой что $a_k + a_1\cdot a_2\cdot\ldots a_p$ делится на p;
(c) существует некоторый член a_k, такой что $a_k + a_1\cdot a_2\cdot\ldots a_p$ делится на p^2.

11. **(a)** Найдите все простые числа p, такие что $(p-2)!$ не делится на $(p-1)$.
(b) Дано простое число p. При каких n число p^n-1 делится на $(p-1)^2$.
(c) Для каких натуральных n число $(n-1)!+1$ является точной степенью n.