Классические теоремы теории чисел

Малая теорема Ферма. Если p — простое число, а a не делится на p, то $(a^{p-1}-1)$ делится на p.

Альтернативная формулировка. Если p — простое число, то $(a^p - a)$ делится на p.

1. **(a)** Вспомните, что $(a+b)^n = a^n + na^{n-1}b + \ldots + C_n^k a^{n-k}b^k + \ldots + b^n$.
(b) Осознайте, что C_p^l делится на p, если p — простое число, а $0 < l < p$.
(c) Докажите, что $\big((a+1)^p - a^p - 1\big)$ делится на p и выведите отсюда доказательство малой теоремы Ферма по индукции.

2. **(a)** Пусть a не делится на p. Докажите, что среди чисел

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

все ненулевые остатки при делении на p содержатся по одному разу.
(b) Из того, что произведение остатков в одинаковых наборах дают одинаковые остатки, выведите малую теорему Ферма.

3. **(a)** Отметим на бумаге произвольным образом $(p-1)$ точку. Каждой точке сопоставим какой-то ненулевой остаток при делении на p. Проведем из остатка k стрелочку в остаток ka.
(b) Убедитесь, что из каждой точки выходит одна стрелочка, и в кажду точку входит одна стрелочка.
(c)

Поймите, что тогда все точки разбиваются на циклические маршруты.
(d)

Докажите, что у всех циклических маршртутов одна и та же длина и она делит $(p-1)$.
(e) Выведите отсюда малую теорему Ферма.

Пусть n — натуральное число. Обозначим $\varphi(n)$ количество чисел, не превосходящих n, взаимно простых с n. Функция $\varphi(n)$ называется *функцией Эйлера*.

Теорема Эйлера. Пусть n — натуральное число, a — взаимно простое с n. Тогда $(a^{\varphi(n)} - 1)$ делится на n.

4. Найдите $\varphi(p)$, где p простое, $\varphi(100)$, $\varphi(2^l)$, $\varphi(p^k)$.

5. **(a)** Докажите, что если умножить все взаимно простые с n остатки на a (которое с n тоже взаимно просто), то получатся все взаимно простые с n остатки по одному разу.
(b) Проведите рассуждения, аналогичные второму доказательству малой теоремы Ферма и докажите теорему Эйлера.

6. Докажите, что $(n^{561} - n)$ делится на 561.

7. **(a)** Докажите, что $(n^{84} - n^4)$ делится на 6800 для любого натурального n.
(b) Можно ли вместо 6800 доказать для какого-то большего числа?

8. Докажите, что $2^{3^k} + 1$ делится на 3^{k+1}.

9. **(a)** Пусть p и q — два различных простых числа. Докажите, что $\varphi(pq) = (p-1)\cdot(q-1)$.
(b) Докажите, что если a и b взаимно просты, то $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
(c) Пусть $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ (предполагаем, что все p_i различны). Чему равно $\varphi(n)/n$?