Первообразные корни

1. **(a)** Докажите, что показателю k по модулю p может принадлежать не более k остатков.
(b) Докажите, что если a принадлежит по модулю p показателю d, а b — показателю k, при этом $(d, k) = 1$, то число ab принадлежит по модулю p показателю dk.
(c) Пусть d_i — показатель числа i по модулю p. Докажите, что

$$[d_1, d_2, \ldots, d_{p-1}] = p - 1.$$

(d) Из предыдущих пунктов выведите, что по простому модулю p существует *первообразный корень*, то есть число, показатель которого по этому модулю равен $p - 1$.

2. Докажите, что по простому модулю p существует не один первообразный корень, а ровно $\varphi(p - 1)$ штук.

3. Найдите наименьшее n, такое, что $17^n - 1 \vdots 2^{2020}$.

4. **(a)** Докажите, что 2 — первообразный корень по модулю 29.
(b) Как выяснить, является ли a первообразным корнем по модулю m, возводя a не во все $\varphi(m)$ степеней?

5. **(a)** Решите сравнение $1 + x + \ldots + x^6 \equiv 0 \pmod{29}$.
(b) Как найти все решения сравнения $x^d \equiv 1 \pmod{p}$, если известен первообразный корень?

6. Докажите, что для каждого n найдется такое m, что $2^m + 2020 \vdots 3^n$.

7. Найдите сумму для целых d (для отрицательных тоже)

$$\sum_{n=0}^{p-1} n^d \pmod{p}.$$