Остатки для Монстров.

1. Дана последовательность: a_0, $a_1 = a^{a_0}$, ..., $a_{n+1} = a^{a_n}$, и число q. Докажите, что последовательность остатков a_n по модулю q стабилизируется.

2. Найти период $7^{7^n} \mod 100$.

3. *Неприводимым* корнем из единицы степени n называется корень из единицы степени n, не являющийся корнем из единицы меньшей степени. m и n взаимно просты. Докажите, что произведение неприводимых корней из единицы степеней m и n является неприводимым корнем из единицы степени mn.

4. p — простое число, $p = 3k + 1$, $\varphi(x) = x^{\frac{(p-1)}{3}} \mod p$. Сколько остатков по модулю p принимает $\varphi(x)$?

а) Доказать, что их количество не меньше 4.

б) Доказать, что их количество не больше 4.

5. Сформулируйте и докажите аналогичное утверждение для простых чисел вида $4k + 1$.

6. Докажите, что по модулю p каждый остаток есть корень $(p-1)$-й степени из 1.

7. Докажите, что по модулю p есть неприводимый корень $(p-1)$-й степени из 1.

8. $P(x) \neq const$ — многочлен с целыми коэффициентами. Докажите, что простых делителей значений $P(x)$ бесконечно много.

9. а) $P(x) = x^2 + 1$, p делит $x^2 + 1$ при некотором x. Доказать, что $p = 4k + 1$.

б) p делит $x^2 + x + 1$ при некотором x. Доказать, что $p = 3k + 1$.

в) Докажите, что простых чисел вида $64k + 1$ бесконечно много.

г) Докажите, что простых чисел вида $2009! \cdot k + 1$ бесконечно много.

10. а) Докажите, что для любого a последовательность остатков $a^n \mod q$ периодична (возможно с предпериодом), причем период делит $\varphi(q)$.

б) Докажие, что если q делится на 8 или на произведение двух различных нечетных простых, то период не может совпадать с $\varphi(q)$.

в) Тот же самое, если период делится на число вида $4k$, k — нечетное простое.

11. $a \equiv 1 \mod p^k$, $a \not\equiv 1 \mod p^{k+1}$.

а) $a^p \equiv 1 \mod p^{k+1}$.

б) $a^p \not\equiv 1 \mod p^{k+2}$ кроме случая $p = 2$, $k = 1$.

в) $a^n \equiv 1 \mod p^{k+l}$, $a^n \not\equiv 1 \mod p^{k+l+1}$, если n делится на p^l, но не делится на p^{l+1}, кроме случая $p = 2$, $k = 1$ (лемма Гензеля).

12. а) $q = p^k$, p — нечетное простое. Тогда при некотором a период $a^n \mod q$ в точности равен $\varphi(q) = p^{k-1}(p-1)$.

б) Тот же вопрос для чисел вида $q = 2p^k$.

13. $q = 2^k$. Тогда для некоторого a остатки $a^4 \mod q$ повторяются с периодом $\frac{q}{4}$.

14. $q = p_1^{k_1} \cdots p_l^{k_l}$, p_i — различные простые. $\Pi(q)$ — максимальный период $a^n \mod q$. Докажите, что $\Pi(q) = HOK(\Pi(p_1^{k_1}, \ldots, \Pi(p_l^{k_l})))$ (воспользуйтесь Китайской теоремой об остатках).