Группа жести, теория чисел, составитель А.Ефимов, 15.04.06

Теорема (Эйлера). Если n — натуральное число, a — взаимно простой с n вычет по модулю n, то $a^{\varphi(n)} \equiv 1(\mathrm{mod}\ n)$, где $\varphi(n)$ – количество натуральных чисел, не превосходящих n, взаимно простых с n (функция Эйлера).
Следствие (малая теорема Ферма). Если p — простое, n — натуральное, $p \nmid n$, то $n^{p-1} \equiv 1(modp)$.
Китайская теорема об остатках. Если $n_1, \ldots, n_k$ — попарно взаимно простые натуральные числа, $a_1, \ldots, a_k$ — целые, то система сравнений $x_1 \equiv a_1(\mathrm{mod}\ n_1), \ldots, x_k \equiv a_k(\mathrm{mod}\ n_k)$ имеет ровно одно решение по модулю $n_1 \ldots n_k$.

Задачи.

0. а) Доказать китайскую теорему об остатках;
б) Доказать малую теорему Ферма;
в) Доказать теорему Эйлера.

1. а) Доказать, что существует бесконечно много натуральных n, таких, что $n \mid (2^n + 1)$;
б) Найти все такие простые n.

2*. Найти все нечетные числа n, такие, что $n \mid 3^n + 1$.

3. Доказать, что для нечетных n имеем $n \mid 2^{n!} - 1$.

4. Доказать, что НОД $(n, 2^{2^n} + 1) = 1$.

5. Доказать, что а) если a, b, c — попарно различные целые числа, то существует бесконечно много натуральных n, таких, что числа $a + n$, $b + n$, $c + n$ попарно взаимно простые.
б)* если A, B, C — целые точки плоскости, то существует бесконечно много целых точек D, таких, что на отрезках AD, BD, CD нет целых точек, отличных от концов.

6. Решить в простых числах уравнение $p(p + 1) + q(q + 1) = r(r + 1)$.

7. Доказать, что для каждого натурального s существует такое натуральное n, такое, что число $2^n - 1$ имеет хотя бы s различных простых делителей.

8. а) Доказать, что при целом n число $n^2 + 1$ не имеет простых делителей вида $4k + 3$.
б)* Решить в целых числах уравнение $x^2 - y^3 = 7$.

9. Пусть P(x) – непостоянный многочлен с целыми коэффициентами. Доказать, что
а) найдутся бесконечно много таких простых р, для каждого из которых найдется такое целое m, что $p|P(m)$.
б)* найдутся бесконечно много таких простых р, для каждого из которых для любого натурального n найдется такое целое m, что $p^n|P(m)$.