Арифметика V: Теорема Лежандра

Соглашение. Все числа в этом листке, про которые не сказано иное, целые. Числа p и q — простые натуральные.

Задача 0. а) Любой ненулевой вычет a по модулю p может быть представлен в виде $a = \dfrac{x}{y} \pmod p$, так что $0 < |x|, |y| < \sqrt{p}$ *("лемма Туэ").*
б) Выведите из леммы Туэ Рождественскую теорему Ферма.

Задача 1. Пусть a, b, c — попарно взаимно простые свободные от квадратов числа, такие что bc — полный квадрат по модулю a, ca — по модулю b, $-ab$ — по модулю c.
а) Если p — простой делитель числа c, то существуют такие линейные функции L_p и M_p, что

$$ax^2 + by^2 - cz^2 = L_p(x, y, z)M_p(x, y, z) \pmod p.$$

б) Существуют такие линейные функции L и M, что

$$ax^2 + by^2 - cz^2 = L(x, y, z)M(x, y, z) \pmod{abc}.$$

в) Существуют такие числа x, y и z (не все равные нулю), что $ax^2 + by^2 - cz^2$ есть либо 0, либо abc.
Указание. Вспомните доказательство Рождественской теоремы Ферма через лемму Туэ.

Задача 2 (теорема Лежандра). Пусть числа a, b и c попарно взаимно просты и свободны от квадратов. Уравнение

$$ax^2 + by^2 + cz^2 = 0$$

имеет нетривиальные решения в целых числа если и только если оно имеет нетривиальные решения в действительных числах и по всем простым модулям.
Указание. Пусть $ax^2 + by^2 - cz^2 = abc$. Воспользуйтесь тем, что $abc \cdot z^2 = ab \cdot cz^2$.

Задача 3. Если ни одно из чисел a, b, c не делится на p, то число решений сравнения $ax^2+by^2+cz^2 = 0 \pmod p$ делится на p; в частности, это сравнение имеет нетривиальные решения.
Указание. Для подсчета числа решений сравнения воспользуйтесь малой теоремой Ферма.

Задача 4. а) Пусть $p = 4k + 3$. Выведите из теоремы Лежандра, что

$$\left(\frac{p}{q}\right) = 1 \Rightarrow \left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}}.$$

б**) Выведите из теоремы Лежандра квадратичный закон взаимности[1].

[1] Лежандр (1752–1833) пытался сделать это с 1785 года, но преуспел лишь частично. В 1858 году Парижская Академия объявила конкурс на устранение пробела в одной из лемм Лежандра. В 1930 году эта лемма была опровергнута.