Задачи по алгебре. I курс, весна 1999 года.
Листок № 4.

1) Доказать, что длина хотя бы одной стороны пифагорова треугольника (прямоугольного треугольника с целыми длинами сторон) делится на 5.

2) а) Доказать, что класс вычетов $[k]_m$ обратим в $\mathbb{Z}_m$ $\Leftrightarrow$ $[k]_m$ не является делителем нуля в $\mathbb{Z}_m$ $\Leftrightarrow$ $(k, m) = 1$.

   б) Доказать, что кольцо $\mathbb{Z}_m$ является полем $\Leftrightarrow$ m — простое.

3) а) Найти все такие $x \in \mathbb{Z}_p$ (p — простое), что $x^2 = 1$.

   б) Чему равно произведение всех ненулевых элементов $\mathbb{Z}_p$ (p — простое)?

   в) Доказать терему Вильсона: Число p является простым тогда и только тогда, когда $(p-1)! + 1 \equiv 0 \pmod{p}$.

4) Доказать, что ровно половина элементов $\mathbb{Z}_p^*$ является квадратами (p — простое, $p > 2$, $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid x \neq 0\}$).

5) Доказать, что уравнение $x^2 + y^2 = -1$ всегда разрешимо в кольце $\mathbb{Z}_p$ (p — простое).

6) Найти остаток 3^{1000} по модулю 13.

7)* Решить сравнение: $2^n \equiv n \pmod p$ (p — простое).

8) Обозначим через $\varphi(m)$ число обратимых элементов в кольце $\mathbb{Z}_m$ (то есть количество натуральных чисел, меньших m и взаимно простых с m). Эта функция называется функцией Эйлера. Доказать теорему Эйлера:

Если класс вычетов $[a]_m$ обратим, то $a^{\varphi(m)} \equiv 1 \pmod m$.

9) Доказать, что если $m = m_1 \cdots m_k$, где m_i попарно взаимно просты, то $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$.

10) Доказать, что функция Эйлера мультипликативна, т. е. если $(k,l)=1$, то $\varphi(kl) = \varphi(k)\varphi(l)$.

11) Доказать, что если $m = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ (p_i — различные простые числа), то

$$\varphi(m) = m\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_n}\Big).$$

12) Доказать, что кольцо $\Bbbk[x,y]$ многочленов от двух переменных не является кольцом главных идеалов.

13) Сколько корней имеет уравнение $x^7 = 35$ в $\mathbb{Z}_{601}$?

14) Пусть $f(x) = x^3 + b \in \mathbb{F}_7[x]$. Для каких $b \in \mathbb{F}_7$ существует ненулевой гомоморфизм колец $\mathbb{F}_7[x]/(f(x)) \to \mathbb{F}_7$?