Гимназия 1543, математический спецкурс, 8 В

Занятие 14: системы сравнений

Пара упражнений

У1) Когда Скупой рыцарь раскладывает свои монеты стопками по девять штук, у него остается восемь монет. Сколько монет может оставаться, когда он будет раскладывать монеты стопками по 18 штук?

У2) Известно, что число a при делении на 5 дает остаток 4, а при делении на 7 дает остаток 3. Найдите остаток от деления числа a на 35.

Немного о сравнениях

Напомним, что любое сравнение вида $ax \equiv b \pmod{n}$ либо не имеет решений (в случае, когда НОД(a, n) не делит b), либо эквивалентно сравнению вида $x \equiv c \pmod{m}$. То есть, мы научились отвечать на вопрос, когда одиночное линейное сравнение разрешимо (и даже искать все его решения).

Этот листок посвящён следующему этапу — системам линейных сравнений *с одной переменной*. Случаи, когда какое-то из сравнений системы не имеет решений, отсеиваются сразу. В остальных случаях система приводится к виду

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ \dots \\ x \equiv c_n \pmod{m_n} \end{cases} \tag{1}$$

Для таких систем есть очень полезное *достаточное условие* разрешимости.

Теорема (китайская теорема об остатках)**.** *Если модули m_i попарно взаимно просты, то система* (1) *имеет решение, единственное по модулю $m_1 m_2 \dots m_n$.*

Задачи

1) Пусть m и n взаимно просты. Докажите, что $x \equiv a \pmod{m}$ и $x \equiv b \pmod{n}$ тогда и только тогда, когда $x \equiv aNn + bMm \pmod{mn}$, где M и N — решение диофантова уравнения $mM + nN = 1$.

2) Известно, что число a при делении на 3 дает остаток 1, при делении на 5 дает остаток 3, а при делении на 7 — остаток 4. Найдите все возможные значения числа a.

3) Докажите китайскую теорему об остатках. (Подсказка: воспользуйтесь первой задачей и индукцией.)

4) Верно ли утверждение, обратное китайской теореме об остатках? (Другими словами, следует ли из однозначной разрешимости системы по произведению модулей их попарная взаимная простота?)

5) Докажите, что решение системы (1) имеет вид

$$x \equiv c_1(M_1 m_2 \dots m_n) + c_2(m_1 M_2 m_3 \dots m_n) + \dots + c_n(m_1 \dots m_{n-1} M_n) \pmod{m_1 m_2 \dots m_n},$$

где M_i — величина, обратная $(m_1 \dots m_{i-1} m_{i+1} \dots m_n)$ по модулю m_i.

6) Решите сравнение $n^2 + 3n + 1 \equiv 0 \pmod{55}$.

7) У генерала есть n солдат, но от 1 до 37 солдат болеет. Генерал хочет построить солдат в одинаковые квадратные каре (каре должно содержать больше 1 человека; каре $k \times k$ содержит k^2 человек). Докажите, что существует такое n, что генерал сможет осуществить своё намерение независимо от количества больных солдат.

8) Число x таково, что число x^2 заканчивается на 001. Каковы могут быть три последние цифры числа x?