Призовые задачи по курсу «Теоретико-числовые методы в криптографии»

2021/2022

1. (Мультипликативные функции) Для данных натуральных чисел m и n определите, сколько существует пар (a, b) взаимно простых натуральных чисел, для которых дробь

$$\frac{ma^2 + nb^2}{a + b}$$

является целым числом.

2. (Сравнения с неизвестным) Решите сравнение

$$x^{101} + 111 \equiv 0 \pmod{2022}.$$

Зная, что сравнение

$$x^{1001} + 111 \equiv 0 \pmod{2022}.$$

разрешимо, найдите число его решений.

3. (Разрешимое сравнение I) Докажите, что сравнение

$$x^2 + 17xy + 17y^2 + 1 \equiv 0 \pmod{m}$$

разрешимо для любого модуля m. Предложите алгоритм, с помощью которого можно по заданному m найти хотя бы одно решение $(x, y) \in \mathbb{Z}^2$ этого сравнения.

4. (Стабильный остаток) Пусть a — натуральное число. Степенной башней с основанием a называется числовая последовательность $\{A_j\}$, заданная рекуррентно:

$$A_1 = a, \quad A_{j+1} = a^{A_j} \quad (j = 1, 2, \dots).$$

Докажите, что для любого натурального числа m степенная башня с основанием a стабилизируется по модулю m, т. е. найдется такой остаток S от деления на m, что

$$A_j \equiv S \pmod{m}$$

для всех достаточно больших j. Предложите алгоритм, вычисляющий $S = S(a, m)$.

5. (Дискретное логарифмирование) Пусть $g \in \mathbb{Z}_p^*$ — фиксированный первообразный корень по простому модулю $p > 2$. Докажите, что если $y \in \mathbb{Z}_p^*$ и $y = g^x$ для некоторого $x \in \{1, 2, \dots, p-1\}$, то справедливо равенство

$$x \cdot 1 = \sum_{j=1}^{p-2} \frac{y^j}{1 - g^j}.$$

6. (Сумма в поле вычетов) Вычислите сумму

$$\sum_{a \in \mathbb{Z}_p} \frac{a}{a^2 + a - 1},$$

где $p \equiv \pm 2 \pmod{5}$ — нечетное простое число.

7. (Произведение в поле вычетов) Вычислите произведение

$$\prod_{a\in\mathbb{Z}_p}(a^2+a+1),$$

где $p\equiv -1 \pmod 3$ — нечетное простое число.

8. (Двойное произведение) Целые числа A, B, C и нечетное простое число p таковы, что $D=B^2-4AC$ — квадратичный невычет по модулю p. Пусть

$$P=\prod_{0<x<y<p}(Ax^2+Bxy+Cy^2).$$

Докажите, что $P^2\equiv 1 \pmod p$.

9. (Разрешимое сравнение II) Пусть p — нечетное простое число. Докажите, что сравнение

$$x^{(p+1)/2}+(x+a)^{(p+1)/2}\equiv a \pmod p$$

разрешимо для любого целого числа a.

10. (Число решений) Пусть $a\in\mathbb{Z}_p$, где $p>2$ — простое число. Докажите, что число решений $(x,y,z)\in\mathbb{Z}_p^3$ уравнения $x^2+y^2+z^2=a$ над полем $\mathbb{Z}_p$ равно

$$p^2+\left(\frac{-a}{p}\right)p.$$

11. (Корень уравнения) Дано простое число $p\equiv -1 \pmod{12}$. Предположим, что дискриминант $D=-4a^3-27b^2$ кубического многочлена $f(x)=x^3+ax+b\in\mathbb{Z}[x]$ удовлетворяет условию

$$\left(\frac{D}{p}\right)=-1.$$

Докажите, что в поле $\mathbb{Z}_p$ уравнение $f(x)=0$ имеет единственный корень $x=x_1$, где

$$x_1=\gamma_+^{(2p-1)/3}+\gamma_-^{(2p-1)/3},\quad \gamma_\pm=-\frac{b}{2}\pm\frac{(-3D)^{(p+1)/4}}{18}.$$

Предложите альтернативный способ найти этот корень.

12. (Образ отображения) Пусть $p>3$ — простое число. Рассмотрим отображение $f:\mathbb{Z}_p\to\mathbb{Z}_p$, заданное правилом $f(x)=x^3-x$. Докажите, что

$$|\operatorname{Im}(f)|=\frac{1}{3}\left(2p+\left(\frac{-3}{p}\right)\right).$$

13. (Неприводимый многочлен) Докажите, что многочлен

$$f(x)=x^p-x-1$$

неприводим над полем $\mathbb{Z}_p$ (здесь p — любое простое число).

Примечание. Нужно выбрать и решить две задачи. Пары выбранных задач не должны пересекаться. Компьютер использовать можно, но решения без собственных рассуждений (полученные исключительно за счет компьютерных вычислений) не засчитываются.