

Криптография и теорема Эйлера

1. Для каких остатков a сравнение $3x \equiv a \pmod{10}$ имеет решение?
2. Для каких a и b существует единственное решение по модулю m у сравнения $ax \equiv b \pmod{m}$?
3. (a) Найдите все однозначные числа x такие, что $7x$ заканчивается на 1;
(b) Найдите все двузначные числа x такие, что $67x$ заканчивается на 01;
(c) Найдите все трёхзначные числа x такие, что $267x$ заканчивается на 001.
4. Даша и Саша любят посылать друг другу двузначные числа. Но они хотят, чтобы никто не догадался, какие числа они посылают.
Для этого, чтобы послать Саше двузначное число, Даша умножает его на 67 и отправляет ему две последние цифры результата.
(a) Всегда ли Саша может догадаться, какое число Даша имела ввиду? (Саша знает алгоритм Даши.)
(b) Саша хочет научиться быстро расшифровывать число Даши. Оказывается, ему достаточно умножить число, которое он получил, на определённое число a и сразу получить дашино число (какое бы она не загадывала). Чему равно a ?
(c) Даша и Саша иногда меняют систему и вместо числа 67 используют другое. Сколько всего двухзначных чисел подойдут для того, чтобы они могли так общаться?
5. Возьмём подмножество остатков, взаимно простых с числом m : $\Phi_m = \{x \in \mathbb{Z}_m \mid \text{НОД}(x, m) = 1\}$ и возьмём какой-то элемент a этого множества.
(a) Докажите, что умножение на a и последовательное взятие остатка по модулю m является биекцией на множестве Φ_m . Другими словами, это отображение задаёт перестановку элементов Φ_m .
(b) Докажите, что перестановка из предыдущего пункта разбивается на несколько циклов равной длины.
6. Докажите *теорему Эйлера*: если $\text{НОД}(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.
7. (a) Докажите, что для любого числа $1 < d < \varphi(n)$ взаимнопростого с $\varphi(n)$ найдётся такое число $e < \varphi(n)$, что $ed \equiv 1 \pmod{\varphi(n)}$.
(b) Докажите, что если $\text{НОД}(m, n) = 1$ и $c \equiv m^e \pmod{n}$, то $c^d \equiv m \pmod{n}$ (числа d и e берутся из предыдущего пункта).

Криптосистема RSA Пусть есть большое число $n = pq$, где p и q – простые числа. Выбирается произвольное число $1 < d < \varphi(n)$ взаимнопростое с $\varphi(n)$ и вычисляется число $e < \varphi(n)$ такое, что $ed \equiv 1 \pmod{\varphi(n)}$. Тогда пара чисел (e, n) называется открытым ключом, а пара (d, n) – закрытым. Открытый ключ знают все, закрытый ключ знает только его владелец.

Шифрование Пусть есть сообщение m . Тогда зашифрованное сообщение s вычисляется по формуле $s \equiv m^e \pmod{n}$.

Дешифрование Пусть есть зашифрованное сообщение s . Тогда исходное сообщение m может быть получено по формуле $m \equiv s^d \pmod{n}$.

8. Проверьте, что алгоритм работает для $n = 5 \cdot 13$, т.е. выберите подходящие d и e и объясните, как шифруется и дешифруется сообщение 10.

Для самостоятельного решения

9. Пусть $a > 1$, $\text{НОД}(a, b) = 1$. Докажите, что найдется такое n , что $1 + a + a^2 + a^3 + \dots + a^n$ делится на b .

10. Рациональное число $\frac{1}{m}$ (m взаимнопросто с 10) представили в виде периодической десятичной дроби. Докажите, что длина её периода является делителем числа $\varphi(m)$.

11. (a) Натуральные числа m_1, m_2, \dots, m_n попарно взаимнопросты. Докажите, что число $x = (m_2 m_3 \dots m_n)^{\varphi(m_1)}$ является решением системы: $x \equiv 1 \pmod{m_1}$, $x \equiv 0 \pmod{m_2}$, $x \equiv 0 \pmod{m_3}$, \dots , $x \equiv 0 \pmod{m_n}$.

(b) Выразите решение системы сравнений: $x \equiv r_1 \pmod{m_1}$, $x \equiv r_2 \pmod{m_2}$, $x \equiv r_3 \pmod{m_3}$, \dots , $x \equiv r_n \pmod{m_n}$ через $m_1, m_2, \dots, m_n, r_1, r_2, \dots, r_n$ и функции φ при помощи предыдущего пункта.