Семинар 6. Тесты на простоту

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Задача 1. (а) Назовём число n *псевдопростым* по основанию a, если

$$a^{n-1} \equiv 1 \pmod{n}.$$

Найдите самое маленькое псевдопростое составное число по основанию 2.

(б) Назовём число n *строго составным*, если оно не является псевдопростым хотя бы по одному основанию $a > 1$. Покажите, что если n строго составное, то найдётся не менее $[\frac{n}{2}]$ вычетов a по модулю n таких, что

$$a^n - a \neq 0 \pmod{n}.$$

Задача 2 (Тест Ферма)**.** Используя предыдущую задачу, придумайте вероятностный тест для проверки того, является ли n строго составным так, чтобы вероятность ошибки была не более чем $\frac{1}{10^3}$.

Задача 3 (Числа Кармайкла)**.** Приведите пример составного, но не строго составного числа.

Задача 4. (а) Докажите, что если число n простое, то сравнение

$$x^2 \equiv 1 \pmod{n}$$

имеет ровно два различных решения по модулю n.

(б) Докажите, что если у нечётного составного числа n есть два различных простых делителя, то сравнение

$$x^2 \equiv 1 \pmod{n}$$

имеет по крайней мере четыре различных решения по модулю n.

Задача 5. (а) Пусть n — нечётное простое число, и 2^s — максимальная степень двойки, на которую делится $n-1$. Докажите, что для любого ненулевого вычета a последовательность вычетов

$$(a^{n-1},\ a^{(n-1)/2}, \dots\ a^{(n-1)/2^s})$$

имеет вид $(1, \dots, 1)$ или $(1, \dots, 1, -1, \star, \dots, \star)$.

(б) Покажите, что число 949 составное, используя пункт (а) для $a = 64$.

Задача 6 (Тест Миллера–Рабина)**.** Используя результаты двух предыдущих задач, придумайте вероятностный тест для проверки числа на простоту.