Семинар 3. Теорема Ферма (малая)

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Задача 1. (а) Найдите последние две цифры числа 2^{65537}.

(б) Найдите коэффициент при x и свободный член многочлена $(x+1)^{65537}$ над $\mathbb{F}_2$.

(в) Найдите остатки при делении гауссова целого числа $(1+i)^{65537}$ на 3 и на 5.

Задача 2. Пусть p — простое натуральное число.

(а) Докажите "тождество ленивого школьника":

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

(Подсказка: используйте бином Ньютона.)

(б) Выведите из "тождества ленивого школьника" малую теорему Ферма:

$n^p - n$ делится на p для любого натурального n.

Задача 3. (а) Докажите, что если число $2^n + 1$ простое, то n обязательно является степенью двойки, то есть $n = 2^m$ для некоторого натурального m. (Простые числа вида $2^{2^m} + 1$ называются *простыми числами Ферма*[1].)

(б) Верно ли обратное?

Задача 4. (а) Докажите, что если число $2^n - 1$ простое, то n обязательно является простым числом. (Простые числа вида $2^n - 1$ называются *простыми числами Мерсенна*.)

(б) Верно ли обратное?

Задача 5. Будет ли простым число $257^{1092} + 1092$? (Подсказка: сначала проверьте, является ли простым число 1093.)

Задача 6. Пусть $p > 2$ — простое число. Рассмотрим множество X всех раскрасок вершин правильного p-угольника в n цветов. На множестве X действует группа G вращений правильного p-угольника.

(а) Сколько раскрасок не меняются при поворотах многоугольника? (Выражаясь научно, сколько неподвижных точек у действия группы G на X?)

(б) Есть ли орбиты, порядок которых отличен от 1 и p?

(в) Сколько орбит порядка p при действии группы G на X?

(г) Используя результаты пунктов (а)–(в) докажите малую теорему Ферма.

[1] Самое большое известное простое число Ферма — это 65537. Это же число часто используется в качестве открытой экспоненты в алгоритме RSA. Почему?