

Задание для подготовки к семинару 6

Теория чисел

1 Что стоит вспомнить

Не смотря на то, что вы изучали теорию чисел в рамках курса алгебры, скорее всего вам стоит освежить эти знания. Для этого вполне подойдёт Кормен. В этом разделе я напишу на что стоит обратить особое внимание, но это не означает, что остальной материал по теории чисел из Кормена читать не надо. В следующий раз я дам контрольную на понимание определений и знание формулировок из теории чисел, на которой нельзя будет пользоваться литературой.

- Аддитивная группа \mathbb{Z}_n и мультипликативная группа \mathbb{Z}_n^*
- Функция Эйлера $\phi(n)$ (число взаимнопростых чисел с n).
- Формула Эйлера

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- Первообразный корень (генератор).
- Дискретный логарифм.
- Алгоритм Евклида, **обобщённый алгоритм Евклида**.
- Разрешимость уравнений вида

$$\begin{aligned}ax &\equiv b \pmod{n}; \\x^2 &\equiv a \pmod{p}, p \in \text{PRIMES}; \\x^2 &\equiv 1 \pmod{n}.\end{aligned}$$

- Теорема Лагранжа
- Теоремы Эйлера и Ферма
- Китайская теорема об остатках.

Аддитивной группой \mathbb{Z}_n называется группа с элементами $\{0, 1, \dots, n-1\}$ с операцией сложения по модулю n . Вообще говоря, можно считать, что элементы \mathbb{Z}_n есть классы эквивалентности вида $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$.

Мультипликативной группой \mathbb{Z}_n^* называется группа элементами которой являются числа, взаимнопростые с n . Операция определена как умножение по модулю n . Мощность группы выражается через формулу Эйлера: $|\mathbb{Z}_n^*| = \phi(n)$.

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

где p – простые числа, а отношение $|$ обозначает отношение «быть делителем».

Первообразным корнем или генератором группы \mathbb{Z}_n^* называется такой её элемент g , что любой другой элемент $a \in \mathbb{Z}_n^*$ является степенью g . Число x называется индексом числа a по основанию g . Решение уравнения $g^x = a$ называется дискретным логарифмом элемента a по основанию g .

Алгоритм Евклида позволяет вычислить наибольший общий делитель $\gcd(a, b)$ чисел a и b . Пусть $\gcd(a, b) = d$. Тогда найдутся такие целые числа x и y , что $d = ax + by$. Их позволяет вычислить обобщённый алгоритм Евклида. Также с его помощью можно решать уравнения вида $ax = b \pmod n$ (а значит и искать обратные элементы в аддитивной группе!).

2 Задачи для подготовки

Задача 1. Найдите все решения сравнения $x^2 \equiv 1 \pmod{200}$.

Задача 2. Докажите, что сравнение $x^2 \equiv 1 \pmod p$, $p \in \text{PRIMES}$, $p > 2$ всегда имеет только два решения. Какие?

Указание: воспользуйтесь Китайской теоремой об остатках.

Задача 3. Сколько решений имеет сравнение $x^2 \equiv 1 \pmod n$? (Ответ зависит от n .)

Задача 4. Докажите, что все решения сравнения $x^2 \equiv 1 \pmod n$ образуют подгруппу \mathbb{Z}_n^* .