12-я летняя школа «Комбинаторика и алгоритмы»

В этом листке есть задачи (возможно переформулированные), рассказанные на лекции. Они помечены кружком и стоят 1 балл. Остальные задачи стоят 2 балла (пункт не является отдельной задачей). Для получения зачёта по этому листку достаточно набрать 20 баллов.

Остатки по модулю m

Множество $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ называется *системой вычетов* по модулю m. На ней определены операции сложения и умножения.

Будем называть элемент $a \in \mathbb{Z}_m$ *обратимым*, если существует обратный к a элемент, то есть такое b, что $a \cdot b \equiv 1 \pmod m$. Обратный к a элемент обозначается как a^{-1}. Множество обратимых элементов $\mathbb{Z}_m$ называется *приведенной системой вычетов* и обозначается $\mathbb{Z}_m^*$.

1°. Приведите пример, когда произведение двух ненулевых классов вычетов по модулю m является нулевым классом. Такие классы называют *делителями нуля* в $\mathbb{Z}_m$.

2°. Докажите, что ненулевой класс не является делителем нуля если и только если он обратим.

3. **а)** Докажите, что целое $m > 1$ простое если и только если для любого ненулевого класса в $\mathbb{Z}_m$ найдётся обратный к нему класс из $\mathbb{Z}_m$. **б)** Докажите, что обратный класс единствен.

4. Решите уравнения **а)** $8x = 3$ в $\mathbb{Z}_{13}$; **б)** $7x = 2$ в $\mathbb{Z}_{11}$; **в)** $x^2 = 1$ в $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$.

5°. Изобразим элементы $\mathbb{Z}_m$ точками, зафиксируем *обратимый (по умножению)* элемент $\alpha \in \mathbb{Z}_m$ и из каждой точки $\omega \in \mathbb{Z}_m$ проведём стрелку в точку $\alpha \cdot \omega$. Докажите, что на этой картинке

а) движение по стрелкам распадается на непересекающиеся циклы;

б) каждый цикл, содержащий хоть один обратимый класс, весь состоит из обратимых классов;

в) циклы, состоящие из обратимых классов, имеют одинаковую длину.

6°. *(Теорема Эйлера)* Пусть $m \in \mathbb{N}$, $\varphi(m)$ — количество натуральных чисел, не превосходящих m и взаимно простых с m. Докажите, что $a^{\varphi(m)} \equiv 1 \pmod m$, если $a \in \mathbb{Z}$ и $(a, m) = 1$.

7. Найдётся ли **а)** 3^k, оканчивающееся на 0001; **б)** $2^k - 1$, делящееся на данное нечётное x?

Первообразные корни

В этой части листка p — нечётное простое число.

Назовём *показателем* $\mathrm{ord}(x)$ элемента $x \in \mathbb{Z}_m^*$ такое минимальное $k \geqslant 1$, что $x^k = 1$.

8°. Докажите, что для каждого $x \in \mathbb{Z}_m^*$ показатель существует.

9. Найдите показатель **а)** $1 \in \mathbb{Z}_m$; **б)** $-1 \in \mathbb{Z}_m$ **в)** всех элементов $\mathbb{Z}_m^*$ при $m = 4, 5, 6, 7$.

10. Пусть $\mathrm{ord}(g) = k$, $g \in \mathbb{Z}_m$. Докажите, что

а) $1, g, g^2, \ldots, g^{k-1} \in \mathbb{Z}_m$ — попарно различные числа;

б) если $k \mid l - l'$, то $g^l = g^{l'}$;

в) $g^s = 1 \Leftrightarrow k \mid s$;

г) $\varphi(m) \,\vdots\, k$.

11. Докажите, что $\mathrm{ord}\,(g^l) = \dfrac{\mathrm{ord}(g)}{(l, \mathrm{ord}(g))}$.

Число g называется *первообразным корнем* по модулю m, если $\mathrm{ord}(g) = \varphi(m)$.

12°. Найдите все первообразные корни для $\mathbb{Z}_m$, $m \leqslant 7$.

Теорема 1. *Первообразный корень по модулю n существует тогда и только тогда, когда $n \in \{2, 4, p^\alpha, 2p^\alpha\}$, где p — нечётное простое, α — положительное целое.*

13. Найдите какой-нибудь первообразный корень по модулю **а)** 13; **б)** 17; **в)** 19.

14. Найдите все первообразные корни по модулю **а)** 13; **б)** 17.

15. Решите сравнения: **а)** $x^8 \equiv 5 \pmod{17}$; **б)** $x^4 \equiv 4 \pmod{17}$; **в)** $x^6 \equiv 11 \pmod{19}$.

Тест Ферма

Пусть $B_n = \{a \in \mathbb{Z}_n \mid (a, n) = 1, a^{n-1} \equiv 1 \pmod n\}$.

16°. Либо $B_n = \mathbb{Z}_n^*$, либо $|B_n| \leqslant \frac{1}{2}|\mathbb{Z}_n^*|$.

Числом Кармайкла называется такое число $n > 1$, что $B_n = \mathbb{Z}_n^*$.

17. Пусть n — число, свободное от квадратов и для любого простого делителя $p \mid n$ верно, что $n-1$ делится на $p - 1$. Тогда n — число Кармайкла.

12-я летняя школа «Комбинаторика и алгоритмы»

Для зачёта по этому листку достаточно набрать 15 баллов. Задачи с кружком были на лекции и стоят 1 балла, без кружка — 2 баллов. Зачёт по курсу ставится, если имеется зачёт по обоим листкам.

Китайская теорема об остатках

1. Укажите все целые числа, которые удовлетворяют системе

а) $\begin{cases} x \equiv 3 \pmod 5; \\ x \equiv 7 \pmod{17}. \end{cases}$ **б)** $\begin{cases} x \equiv 2 \pmod{13}; \\ x \equiv 4 \pmod{19}. \end{cases}$

Числа Кармайкла

2°. Пусть n — число, свободное от квадратов и для любого простого делителя $p \mid n$ верно, что $n-1$ делится на $p-1$. Тогда n — число Кармайкла.

3°. Пусть $n = p^k \cdot d$, где $(d,p) = 1$, p — простое и $k \geqslant 2$. **а)** Найдётся число a с условием: $a \equiv 1+p \pmod{p^k}$, $a \equiv 1 \pmod d$. **б)** n не может быть числом Кармайкла.

4°. Пусть n — число Кармайкла. Тогда

а) n свободно от квадратов (т.е. не делится на p^2 для простого p).

б) если n делится на простое число p, то $n-1$ делится на $p-1$.

5. n является числом Кармайкла тогда и только тогда, когда для любого $a \in \mathbb{Z}$ верно, что $a^n \equiv a \pmod n$.

6. Число Кармайкла является нечётным.

7. Пусть для натурального числа k числа $6k+1$, $12k+1$, $18k+1$ являются простыми. Тогда число $(6k+1)\cdot(12k+1)\cdot(18k+1)$ является числом Кармайкла.

Квадратичные вычеты

Определение 1. Пусть p — простое число. Будем говорить, что a является *квадратичным вычетом по модулю p* , если $(a,p) = 1$ и найдётся такой $x \in \mathbb{Z}_p$, что $a = x^2$, и *квадратичным невычетом*, если $(a,p) = 1$ и такого $x \in \mathbb{Z}_p$, что $x^2 = a$ не существует.

Определение 2. Для простого нечётного p назовём *символом Лежандра* следующее выражение:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p; \\ 0, & \text{если } (a,p) \neq 1. \end{cases}$$

Читается: символ a по p.

8°. **а)** Докажите, что если a — квадратичный вычет по модулю p, то у уравнения $x^2 = a$ в $\mathbb{Z}_p$ есть ровно два корня.

б) Докажите, что есть ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов по модулю p.

в) Докажите, что $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

9. При каких простых p число -1 является квадратичным вычетом?

10. Укажите квадратичные вычеты по модулю 17; 23.

Тест Миллера-Рабина

Пусть $n-1 = 2^s \cdot k$ для некоторой степени s и нечётного числа k. Рассмотрим множество

$$B_{MR}(n) = \{a \in \mathbb{Z}_n^* \mid a^k = 1 \text{ или } a^{k2^i} = -1 \text{ для некоторого } 0 \leqslant i < s\}.$$

11°. (*Тест Миллера-Рабина*) Для нечётного n

а) $B_{MR}(n) \subset B_n$ (определение B_n смотрите в Листке 1);

б) Если $B_{MR}(n) = \mathbb{Z}_n^*$, то n — простое.

Теорема 1. (Рабин) *Если $n > 9$ — нечётное составное число, то* $|B_{MR}(n)| \leqslant \frac{1}{4}|\mathbb{Z}_n^*|$.

12. Какие числа проходят проверку на простоту в тесте Миллера-Рабина для $n = 8, 9, 10$?

13. Покажите, что если уравнение $b^k \equiv c \pmod n$ имеет хотя бы одно решение b по модулю n для данного c, то оно имеет столько же решений, сколько уравнение $b^k \equiv 1 \pmod n$.

Тест Люка-Лемера.

Числом Мерсенна M_k называется простое число вида $2^k - 1$.

14. **а)** Какие из чисел Мерсенна являются простыми при $1 \leqslant k \leqslant 10$? **б)** В числе Мерсенна $p = 2^k - 1$ число k является простым.

Теорема 2. (Лемер, 1930) *Пусть p — простое нечётное. Число Мерсенна $M_p = 2^p - 1$ простое тогда и только тогда, когда оно делит нацело $(p-2)$-й член последовательности S_k, задаваемой рекуррентно:*

$$S_k = \begin{cases} 4, & \text{если } k = 0, \\ S_{k-1}^2 - 2 & \text{если } k > 0. \end{cases}$$

15. Проверьте теорему Лемера для $p = 3, 5$.