

Дискретная математика, Коллоквиум 2

Балюк Игорь
@lodthe, [GitHub](#)

2019 — 2020

Материалы взяты из учебника Александра Рубцова.

Содержание

1	Определения	3
1.1	Деление целых чисел с остатком.	3
1.2	Сравнения по модулю. Основные свойства.	3
1.3	Арифметика остатков (вычетов). Обратимые остатки (вычеты).	3
1.4	Малая теорема Ферма.	3
1.5	Функция Эйлера. Теорема Эйлера.	3
1.6	Наибольший общий делитель. Алгоритм Евклида.	4
1.7	Расширенный алгоритм Евклида нахождения решения линейного диофантова уравнения.	4
1.8	Простые числа, формулировка основной теоремы арифметики.	4
1.9	Равномощные множества.	4
1.10	Счётные множества.	4
1.11	Множества мощности континуум.	4
1.12	Основные определения элементарной теории вероятностей: исходы, события, вероятность события.	4
1.13	Формулировка формулы включений и исключений для вероятностей.	4
1.14	Условная вероятность.	4
1.15	Независимые события. Основные свойства независимых событий.	4
1.16	Формула полной вероятности.	4
1.17	Случайная величина и математическое ожидание. Линейность математического ожидания.	4
1.18	Формулировка неравенства Маркова.	4
1.19	Определение схемы в некотором функциональном базисе. Представление схем графами.	4
1.20	Полный базис. Примеры полных и неполных базисов.	4
1.21	Полином Жегалкина (в стандартном виде).	4
1.22	Схемная сложность функции (размер схемы).	4
2	Вопросы на знание доказательств	5
2.1	Сравнение $ax \equiv 1 \pmod{N}$ имеет решение тогда и только тогда, когда $\text{НОД}(a, N) = 1$.	5
2.2	Малая теорема Ферма.	5
2.3	Теорема Эйлера.	5
2.4	Корректность алгоритма Евклида и расширенного алгоритма Евклида.	5
2.5	Основная теорема арифметики.	5
2.6	Китайская теорема об остатках.	5
2.7	Мультипликативность функции Эйлера. Формула для функции Эйлера.	5
2.8	Формула Байеса. Формула полной вероятности.	5
2.9	Парадокс дней рождений (математическое ожидание числа людей с совпавшими днями рождений)	5
2.10	Неравенство Маркова.	5
2.11	Нижняя оценка на максимальное количество ребер в разрезе.	5
2.12	Любое бесконечное множество содержит счётное подмножество. Любое подмножество счётного множества конечно или счётно.	5
2.13	Конечное или счётное объединение конечных или счётных множеств конечно или счётно	5

2.14	Счётность декартова произведения счетных множеств. Счётность множества рациональных чисел.	5
2.15	Равномощность отрезков, интервалов, лучей и прямых (явные биекции).	5
2.16	Несчетность множества бесконечных двоичных последовательностей.	5
2.17	Теорема Кантора-Бернштейна.	5
2.18	Нижняя оценка на число монотонных булевых функций: монотонных булевых функций от $2n$ переменных не меньше $2^{\frac{2^n}{2n+1}}$	5
2.19	Существование и единственность полинома Жегалкина (в стандартном виде) для любой булевой функции.	5
2.20	Разложение в ДНФ и КНФ булевой функции.	5
2.21	Верхняя оценка $O(n2^n)$ схемной сложности булевой функции от n переменных.	5
2.22	Булевы схемы для сложения и умножения n -битовых чисел. Оценка размера.	5
2.23	Булева схема для задачи о связности графа. Оценка размера.	5
2.24	Задача об угадывании числа. Верхняя и нижняя оценки.	5
2.25	Задача о сортировке нижняя оценка.	5
2.26	Задача о нахождении самой тяжелой монеты. Верхние и нижние оценки.	5

1 Определения

Контрольный вопрос на понимание определений включает в себя формулировку одного определения из списка ниже и контрольный вопрос по этому определению. Пример: «Определение полного прообраза. Пусть $f(x) = x^2$ — функция из \mathbb{Z} в \mathbb{Z} . Найдите полный прообраз множества $\{1, 2, 3, 4\}$ ».

1. Деление целых чисел с остатком.

Говорят, что целое число a делится на целое число b , если $a = bk$ для некоторого целого числа k . В этом случае говорят также « a кратно b », и « b является делителем числа a ».

Теперь определим деление с остатком. Пусть b — целое положительное число. Деля на b с остатком, мы связываем предметы в пачки по b в каждой, пока это возможно: количество полных пачек называется частным (говорят ещё «неполное частное», чтобы отличать от частного как дроби), и сколько-то предметов останется, их количество и называют остатком.

Формально: разделить целое a на целое положительное b означает найти такое целое q (*частное*) и такое r (*остаток*), что

$$a = b \cdot q + r; \quad 0 \leq r < b.$$

2. Сравнения по модулю. Основные свойства.

Если два числа a и b дают одинаковые остатки при делении на положительное число N , то говорят, что они *сравнимы* по модулю N , и пишут $a \equiv b \pmod{N}$.

Эквивалентное определение: a и b сравнимы по модулю N , если разность $a - b$ делится на N . В самом деле, если они дают одинаковый остаток r , то $a = k \cdot N + r$, $b = l \cdot N + r$, и $a - b = k \cdot N - l \cdot N = (k - l) \cdot N$. Наоборот, если $a - b = m \cdot N$, и b даёт остаток r , то $b = l \cdot N + r$ и $a = (a - b) + b = m \cdot N + l \cdot N + r = (m + l) \cdot N + r$, то есть a даёт тот же остаток r .

Можно сказать, что при данном N все целые числа разбиваются на N классов в зависимости от остатков по модулю N : два числа в одном классе сравнимы, а числа в разных классах — нет.

Важное свойство сравнений: чтобы узнать, в какой класс попадет сумма или произведение двух чисел, достаточно знать, в каком классе лежат слагаемые или сомножители: если одно из слагаемых (один из сомножителей) изменить на кратное N , то сумма (произведение) тоже изменится на кратное N .

В самом деле, если к одному из слагаемых прибавить $k \cdot N$, то к сумме тоже прибавится $k \cdot N$, аналогично для разности. С произведением: $(a + k \cdot N) \cdot b = a \cdot b + k \cdot b \cdot N \equiv a \cdot b \pmod{N}$.

Благодаря этому свойству в выражении, содержащем операции сложения и умножения (или возведение в целую степень, которое сводится к многократному умножению), можно заменять слагаемые или сомножители на сравнимые по модулю N — если результат нам важен лишь по модулю N .

Например, можно найти $2^{100} \pmod{7}$ (остаток от деления 2^{100} на 7): поскольку $2^3 = 8 \equiv 1 \pmod{7}$, то $2^{99} = (2^3)^{33} \equiv 1^{33} = 1 \pmod{7}$, так что $2^{100} = 2^{99} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{7}$.

3. Арифметика остатков (вычетов). Обратимые остатки (вычеты).

Остаток (вычет) по модулю N называется **обратимым**, если в произведении с каким-то другим остатком он даёт 1. Другими словами, a обратим, если уравнение $a \cdot x \equiv 1 \pmod{N}$ имеет решение.

4. Малая теорема Ферма.

Теорема. Если p — простое число, то

$$a^{p-1} \equiv 1 \pmod{p}$$

при любом a , не делящемся на p .

5. Функция Эйлера. Теорема Эйлера.

Теорема. Пусть $N > 1$ — произвольное целое число, а $\varphi(N)$ равно количеству остатков среди $0, 1, \dots, N-1$, взаимно простых с N . Пусть a — один из этих остатков. Тогда

$$a^{\varphi(N)} \equiv 1 \pmod{N}.$$

Функцию φ называют **функцией Эйлера** и традиционно обозначают буквой φ . Если N простое, то $\varphi(N) = N - 1$, и теорема Эйлера превращается в малую теорему Ферма.

6. Наибольший общий делитель. Алгоритм Евклида.

Наибольшим общим делителем (НОД) для двух целых чисел m и n называется наибольший из их общих делителей. Пример: для чисел 54 и 24 наибольший общий делитель равен 6.

Алгоритм нахождения НОДа алгоритмом Евклида:

1. Большее число делим на меньшее.
2. Если делится без остатка, то меньшее число и есть НОД (следует выйти из цикла).
3. Если есть остаток, то большее число заменяем на остаток от деления.
4. Переходим к пункту 1.

7. Расширенный алгоритм Евклида нахождения решения линейного диофантова уравнения.

8. Простые числа, формулировка основной теоремы арифметики.

Целое число $p > 1$ называется простым, если оно не разлагается в произведение меньших чисел (то есть не имеет положительных делителей, кроме 1 и p).

Теорема. *Всякое целое положительное число, большее 1, разлагается на простые множители, причём единственным образом: любые два разложения отличаются только перестановкой сомножителей.*

9. Равномощные множества.

Множество A называется равномощным множеству B , если существует биекция множества A в множество B .

10. Счётные множества.

Множество называется счётным, если оно равномощно множеству натуральных чисел \mathbb{N} .

11. Множества мощности континуум.

Множество имеет мощность **континуум**, если оно равномощно \mathbb{R} .

12. Основные определения элементарной теории вероятностей: исходы, события, вероятность события.

Вероятностным пространством называется конечное множество U , его элементы называются **возможными исходами**. **Событием** называется произвольное подмножество $A \subseteq U$.

На вероятностном пространстве задана функция $Pr : U \rightarrow [0; 1]$, такая что $\sum_{x \in U} Pr[x] = 1$. Функция Pr называется **вероятностным распределением**, а число $Pr[x]$ называется **вероятностью исхода** $x \in U$. Вероятностью события A называется число $Pr[A] = \sum_{x \in A} Pr[x]$.

13. Формулировка формулы включений и исключений для вероятностей.

14. Условная вероятность.

15. Независимые события. Основные свойства независимых событий.

16. Формула полной вероятности.

17. Случайная величина и математическое ожидание. Линейность математического ожидания.

18. Формулировка неравенства Маркова.

19. Определение схемы в некотором функциональном базисе. Представление схем графами.

20. Полный базис. Примеры полных и неполных базисов.

21. Полином Жегалкина (в стандартном виде).

22. Схемная сложность функции (размер схемы).

2 Вопросы на знание доказательств

1. Сравнение $ax \equiv 1 \pmod{N}$ имеет решение тогда и только тогда, когда $\text{НОД}(a, N) = 1$.
2. Малая теорема Ферма.
3. Теорема Эйлера.
4. Корректность алгоритма Евклида и расширенного алгоритма Евклида.
5. Основная теорема арифметики.
6. Китайская теорема об остатках.
7. Мультипликативность функции Эйлера. Формула для функции Эйлера.
8. Формула Байеса. Формула полной вероятности.
9. Парадокс дней рождений (математическое ожидание числа людей с совпавшими днями рождений)
10. Неравенство Маркова.
11. Нижняя оценка на максимальное количество ребер в разрезе.
12. Любое бесконечное множество содержит счётное подмножество. Любое подмножество счётного множества конечно или счётно.
13. Конечное или счётное объединение конечных или счётных множеств конечно или счётно
14. Счётность декартова произведения счетных множеств. Счётность множества рациональных чисел.
15. Равномощность отрезков, интервалов, лучей и прямых (явные биекции).
16. Несчетность множества бесконечных двоичных последовательностей.
17. Теорема Кантора-Бернштейна.
18. Нижняя оценка на число монотонных булевых функций: монотонных булевых функций от $2n$ переменных не меньше $2^{\frac{2^n}{2n+1}}$
19. Существование и единственность полинома Жегалкина (в стандартном виде) для любой булевой функции.
20. Разложение в ДНФ и КНФ булевой функции.
21. Верхняя оценка $O(n2^n)$ схемной сложности булевой функции от n переменных.
22. Булевы схемы для сложения и умножения n -битовых чисел. Оценка размера.
23. Булева схема для задачи о связности графа. Оценка размера.
24. Задача об угадывании числа. Верхняя и нижняя оценки.
25. Задача о сортировке нижняя оценка.
26. Задача о нахождении самой тяжелой монеты. Верхние и нижние оценки.