ОГЛАВЛЕНИЕ

Предисловие 3

Часть 1. Условия задач 4

1. Множества, функции, отношения 4
2. Модулярная арифметика 13
3. Комбинаторика 23
4. Математическая логика 26
5. Графы 48
6. Конечные автоматы 59

Часть 2. Примеры решения 71

7. Множества, функции, отношения (примеры решения) решения) 71
8. Модулярная арифметика (примеры решения) 83

8.1. Алгоритм вычисления h-ричной записи десятиричного числа a 83

8.2. Тест Соловэя–Штрассена для простоты числа 86

8.3. Тест Миллера–Рабина для простоты числа 86

8.4. Алгоритм Евклида нахождения нод(a,b), $a \geqslant b$ 88

8.5. Расширенный алгоритм Евклида нахождения $d=$нод(a,b) *тех целых чисел* u,v, *для которых* $d=au+bv$ 88

8.6. Алгоритм вычисления подходящих дробей 89

8.7. Алгоритм вычисления мультипликативного обратного элемента $a^{-1} \pmod n$ *в* $\mathbb{Z}_n$ 91

8.8. Алгоритм вычисления порядка элемента циклической группы $\mathbb{Z}_p^*$ *при простом* p *(перебор)* 91

8.9. Алгоритм вычисления генератора циклической группы $\mathbb{Z}_p^*$ *при простом* p *(перебор)* 91

8.10. Алгоритм модулярной степени натурального числа 93

8.11. Алгоритм Гаусса для системы сравнений

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots \\ x \equiv c_k \pmod{m_k} \end{cases}$$

с попарно взаимно простыми модулями 97

8.12. Алгоритм вычисления символа Якоби (и Лежандра) 102

8.13. Алгоритм Евклида для $\mathbb{Z}_p[x]$ 102
8.14. Расширенный алгоритм Евклида для $\mathbb{Z}_p[x]$ 102
8.15. Мультипликативный обратный элемент в $\mathbb{F}_{p^m}$ 108
8.16. Модулярня степень в $\mathbb{F}_{p^m}$ 108
8.17. Тестирование полинома из $\mathbb{Z}_p[x]$ *на неприводимость* 108
8.18. Порождение случайного неприводимого полинома над $\mathbb{Z}_p$ 109
8.19. Тестирование неприводимого полинома из $\mathbb{Z}_p[x]$ *на примитивность* 109
8.20. Порождение случайного нормированного примитивного полинома над $\mathbb{Z}_p$ 109
8.21. Вычисление порядка элемента конечной мультипликативной группы (алгоритм Гаусса) 109
8.22. Вычисление генератора конечной мультипликативной циклической группы (алгоритм Гаусса) 110
9. Комбинаторика (примеры решения) 129
10. Математическая логика (примеры решения) 133
10.1. Алгоритм минимизации функций в классе нормальных форм 135
10.2. Алгоритм Квайна–Мак–Класски построения минимальной ДНФ функции f 138
10.3. Алгоритм минимизации частично определенных функций в классе ДНФ 142
10.4. Алгоритм минимизации частично определенных функций в классе КНФ 143
10.5. Алгоритм совместной минимизации 145
10.6. Алгоритм совместной минимизации системы из k функций (жадный алгоритм приближенной минимизации) 149
10.7. Элементы функциональной декомпозиции 158
10.8. Алгоритм нахождения проверяющего и диагностического тестов для однократных неисправностей 165
11. Графы (примеры решения) 192
11.1. Помечивающий алгоритм (Дейкстры) поиска кратчайшего (с наименьшим весом) пути между двумя вершинами s и t в связном нагруженном ориентированном графе 193
11.1.1. Вычисление наименьшего веса

пути от s к t 193
11.1.2. Построение наименьшего пути от s к t 193
11.2. Алгоритм построения совершенного паросочетания для двудольного графа 204
11.3. Алгоритм построения наибольшего совершенного паросочетания в полном нагруженном двудольном графе 206
11.4. Алгоритм построения плоского изображения графа 209
11.5. Алгоритм вычисления всех наибольших внутренне устойчивых множеств вершин графа $G = (V,E)$ 213
11.6. Алгоритм вычисления всех наименьших внешне устойчивых множеств вершин графа $G = (V,E)$ 214
11.7. Алгоритм оптимальной раскраски (p,q)-графа $G = (V,E)$ 216
11.8. Помечивающий алгоритм вычисления максимального потока в транспортной сети 217
12. Пакет Mathcad–программ для работы в полях Галуа 227
12.1. Факторизация натурального числа n 227
12.2. Вычисление в факторизации $n=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$ векторов $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ 227
12.3. Выделение всех множителей k в n (представление числа n в виде $n=k^e\cdot s$, где k не делит s) 228
12.4. Конкатенация чисел 228
12.5. Обращение вектора 229
12.6. h–ричная запись десятиричного числа n 229
12.7. Модулярная степень $m^e \pmod n$ в $\mathbb{Z}_n$ 229
12.8. Алгоритм Евклида нахождения d=нод(a,b) 230
12.9. Расширенный алгоритм Евклида нахождения d=нод(a,b) и тех целых чисел u,v, для которых $d=au+bv$ 230
12.10. Остаток от деления a на p в $\mathbb{Z}$ $(a \bmod p)$ 231
12.11. Сумма чисел a,b из $\mathbb{Z}$ по $\bmod p$ 231
12.12. Разность чисел a,b из $\mathbb{Z}$ по $\bmod p$ 232
12.13. Умножение чисел a,b из $\mathbb{Z}$ по $\bmod p$ 232
12.14. Мультипликативный обратный элемент $a^{-1} \pmod p$ в $\mathbb{Z}_p^*$ с простым p 232

12.15. Деление a на b из $\mathbb{Z}_p^*$ по mod p 232
12.16. Тест Миллера–Рабина для простоты числа 232
12.17. Метод Гаусса решения системы сравнений $x \equiv c_i \pmod{m_i}$ с попарно простыми m_i, $i=1,2,\ldots,r$ 233
12.18. Удаление всех первых нулей в полиноме $P(x)$ из $\mathbb{Z}_p[x]$ 234
12.19. Вычисление символа Якоби 234
12.20. Сумма полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$ 235
12.21. Разность полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$ 235
12.22. Произведение полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$ 236
12.23. Частное и остаток от деления полинома $P(x)$ из $\mathbb{Z}_p[x]$ на полином $Q(x)$ из $\mathbb{Z}_p[x]$ 236
12.24. Частное и остаток от деления произведения полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$ по модулю неприводимого полинома $F(x)$ из $\mathbb{Z}_p[x]$ 237
12.25. Умножение в поле Галуа $GF(p^m)$ полиномов $P(x),Q(x)$ по модулю неприводимого над $\mathbb{Z}_p$ полинома $F(x)$ 238
12.26. Алгоритм Евклида нахождения $d(x)=\text{нод}(P(x),Q(x))$ для полиномов $P(x),Q(x)$ из $\mathbb{Z}_p[x]$ 238
12.26.1. Нахождение общего делителя $d(x)=\text{од}(P(x),Q(x))$ наибольшей степени 238
12.26.2. Нахождение $d(x)=\text{нод}(P(x),Q(x))$ 239
12.27. Расширенный алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$ нахождения $d(x)=\text{нод}(P(x),Q(x))$ и таких $u(x),v(x)$, что $d(x)=P(x)u(x)+Q(x)v(x)$ 239
12.27.1. Нахождение общего делителя $d(x)=\text{од}(P(x),Q(x))$ наибольшей степени и таких $u(x),v(x)$, что $d(x)=P(x)u(x)+Q(x)v(x)$ 239
12.27.2. Нахождение $d(x)=\text{нод}(P(x),Q(x))$ и таких $u(x),v(x)$ из $\mathbb{Z}_p[x]$, что $d(x)=P(x)u(x)+Q(x)v(x)$ 240
12.28. Мультипликативный обратный полином для полинома $P(x)$ в поле Галуа $GF(p^m)$ с неприводимым полиномом $F(x)$ 241
12.29. Модулярня степень e полинома $P(x)$

в поле Галуа $GF(p^m)$ с неприводимым полиномом $F(x)$ 241
12.30. Тестирование полинома $F(x)$ из $\mathbb{Z}_p[x]$ на неприводимость 242
12.31. Тестирование полинома $F(x)$ степени m из $\mathbb{Z}_p[x]$ на примитивность, факторизация $p^m-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$, векторы $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ 242
12.32. Порядок элемента a мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p (перебор) 243
12.33. Порядок элемента a мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p, факторизация $p-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$, векторы $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ (алгоритм Гаусса) 244
12.34. Порядок элемента $P(x)$ мультипликативной циклической группы поля Галуа $GF(p^m)$ по модулю неприводимого из $\mathbb{Z}_p[x]$ полинома $F(x)$ степени m (перебор) 244
12.35. Порядок элемента $P(x)$ мультипликативной циклической группы поля Галуа $GF(p^m)$ по модулю неприводимого над $\mathbb{Z}_p[x]$ полинома $F(x)$ степени m, факторизация $p^m-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$, векторы $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ (алгоритм Гаусса) 245
12.36. Тест для $a\in\mathbb{Z}_p^*$ быть генератором мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p (перебор) 246
12.37. Тест для $a\in\mathbb{Z}_p^*$ быть генератором мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом p, факторизация $p-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$, векторы $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ (алгоритм Гаусса) 246
12.38. Тест для $P(x)\in GF(p^m)$ быть генератором мультипликативной циклической группы поля Галуа $GF(p^m)$ по модулю неприводимого над $\mathbb{Z}_p[x]$ полинома $F(x)$ степени m

(*перебор*) 247
12.39. *Тест для* $P(x)\in\mathbb{Z}_p[x]$ *быть генератором мультипликативной циклической группы поля Галуа* $GF(p^m)$ *по модулю неприводимого над* $\mathbb{Z}_p$ *полинома* $F(x)$ *степени* m, *факторизация* $p^m-1=r_0^{e_0}r_1^{e_1}\ldots r_k^{e_k}$, *векторы* $r=(r_0,r_1,\ldots,r_k)$, $e=(e_0,e_1,\ldots,e_k)$ (*алгоритм Гаусса*) 247
12.40. *Квадратный корень из натурального числа* a *по простому модулю* $p\geqslant 2$, $1\leqslant a<p$ 248
12.41. *Квадратный корень из натурального числа* a *по простому модулю* p, $p\equiv 3 \pmod 4$ 249
12.42. *Квадратный корень из натурального числа* a *по простому модулю* p, $p\equiv 5 \pmod 8$ 249
12.43. *Квадратный корень из натурального числа* a *по простому модулю* $p>2$, $1\leqslant a<p$, *при больших* s *в представлении* $p-1=2^s\cdot t$, 2 *не делит* t (s *есть число двоек в факторизации* $p-1$) 250
12.44. *Квадратный корень из натурального числа* a *по модулю* n, *если факторизация* $n=p\cdot q$ *при простых* p *и* q *и если* a *есть квадратичный вычет по модулям* p *и* q 251
12.45. *Вычисление дискретного логарифма* $\log_a b$ *методом "малый шаг – большой шаг" в подгруппе* G *порядка* n *мультипликативной группы* $\mathbb{Z}_p^*$ *с простым* p 251
12.46. *Алгоритм Полларда rho вычисления дискретного логарифма* $\log_\alpha\beta$ *в подгруппе* G *простого порядка* n *мультипликативной группы* $\mathbb{Z}_p^*$ *с простым* p 253
12.47. *Алгоритм Полига–Неллмана вычисления дискретного логарифма* $\log_\alpha\beta$ *в мультипликативной подгруппе* G *порядка* n *группы* $\mathbb{Z}_p^*$ *с простым* p 254
12.48. *Алгоритм Полларда rho вычисления собственного делителя в* n (n *не есть степень простого числа*) 255
12.49. *Алгоритм Полларда* $p-1$ *вычисления собственного делителя в* n (n *не есть степень простого числа*) 256

12.50. Хэш-функция MASH–1 (*Modular Arithmetic Secure Hash*) 257
12.50.1. Хэш-значение для текстовой константы 262
12.50.2. Хэш-значение для элемента поля Галуа $GF(p^m)$ 262

13. Некоторые Mathcad–программы для работы с большими числами 263

13.1. Умножение h–ричных полином-чисел 263
13.2. Умножение полинома на число 265
13.3. Умножение 10-ричного полином-числа на 10-ричное положительное число 266
13.4. Вычитание 10-ричных полином-чисел P *и* Q, $P \geqslant Q$ 266
13.5. Сумма 10-ричных полином-чисел 267
13.6. Отношения "больше", "больше или равно", "меньше", "меньше или равно", для 10-ричных полином-чисел 267
13.7. Частное и остаток при делении двух 10-ричных полином-чисел 268
13.8. Модулярное умножение двух 10-ричных полином-чисел 270
13.9. Модулярная степень $P^e(\mathrm{mod}\, M)$ *10-ричных полином-чисел* P *и* M *при малых экспонентах* e 270
13.10. Бинарное полином-представление 10-ричных полином-чисел 270
13.11. h-ричное полином-представление 10-ричных полином-чисел 271
13.12. Модулярная степень $P^E(\mathrm{mod}\, M)$ *10-ричных полином-чисел* P, E, M 271

Литература 273