


Д. В. Чупраков

Компьютерная алгебра

Алгоритмы теории чисел

A magnifying glass with a black handle and silver rim is positioned over the text. The lens is centered on the mathematical formulas, making them appear larger and more prominent. The background of the cover is a green circuit board pattern.
$$a^{2k} = (a^k)^2$$
$$a^{2k+1} = (a^k)^2 a$$

Киров
2012

Федеральное государственное бюджетное
образовательное учреждение
высшего профессионального образования
«Вятский государственный гуманитарный университет»

Д. В. Чупраков

Компьютерная алгебра Алгоритмы теории чисел

Учебное пособие

Рекомендовано советом УМО по математике
педвузов и университетов Волго-Вятского региона
в качестве учебного пособия для студентов
математических направлений подготовки

Киров

2012

УДК 512.6+511.1(075.8)

ББК 22.183.4я73

Ч-92

*Печатается по решению редакционно-издательского совета
Вятского государственного гуманитарного университета и сове-
та УМО по математике педвузов и университетов Волго-Вят-
ского региона*

Научный редактор — **Е. М. Вечтомов**, доктор физико-матема-
тических наук, профессор кафедры алгебры и дискретной матема-
тики ВятГГУ

Рецензенты:

А. С. Махнев, доктор физико-математических наук, профессор
кафедры высшей математики ВятГУ;

В. В. Чермных, доктор физико-математических наук, профессор
кафедры алгебры и дискретной математики ВятГГУ

Чупраков Д. В.

Ч-92 Компьютерная алгебра. Алгоритмы теории чисел: учебное
пособие / Д. В. Чупраков. — Киров: Изд-во ВятГГУ, 2012. —
152 с.

ISBN 978-5-456-00134-4

В учебном пособии изложен материал, читаемый при изучении дис-
циплины «Компьютерная алгебра» студентам бакалавриата математиче-
ских направлений подготовки. Пособие может быть использовано студен-
тами и магистрантами для изучения дисциплины «Компьютерная алгеб-
ра», «Математические методы в информатике», «Криптография и защита
информации», «Программирование», «Теория чисел» в качестве учебного
пособия или справочника теоретико-числовых алгоритмов.

УДК 512.6+511.1(075.8)

ББК 22.183.4я73

ISBN 978-5-456-00134-4

© Вятский государственный гума-
нитарный университет (ВятГГУ),
2012

© Чупраков Д. В., 2012

Оглавление

Предисловие	7
Глава 1. Системы компьютерной алгебры	10
1.1. История систем компьютерной алгебры	10
1.2. Система компьютерной алгебры Maxima	12
1.3. Первые шаги в Maxima	13
1.3.1. Калькулятор	13
1.3.2. Переменные и их значения	14
1.3.3. Функции	15
1.3.4. Графики функций	16
1.3.5. Основные преобразования выражений	16
1.4. Элементы программирования в Maxima	18
1.4.1. Конструкция следования	19
1.4.2. Конструкция ветвления	19
1.4.3. Циклическая конструкция	20
1.4.4. Списки	24
Глава 2. Фундаментальные понятия компьютерной алгебры	30
2.1. Сложность алгоритмов	30
2.1.1. Асимптотическая сложность алгоритма	32
2.1.2. Классы сложности алгоритмов	33
2.1.3. Построение эффективных алгоритмов	35
2.2. Задача представления	36
2.3. Абстрактные типы данных	37

2.3.1.	Алгебры и алгебраические системы	37
2.3.2.	Сигнатуры	39
2.3.3.	Термы	40
2.3.4.	Абстрактные типы данных	41
2.4.	Представление классических математических объектов	42
2.4.1.	О структуре памяти	42
2.4.2.	Представление целых чисел	43
2.4.3.	Алгоритмы перевода числа из одной системы счисления в другую	44
2.4.4.	Представление рациональных чисел	46
2.4.5.	Представление многочленов	47
2.4.6.	Представление математических выражений	47
Глава 3.	Арифметика в числовых кольцах	51
3.1.	Операция сложения	51
3.2.	Операция умножения	53
3.2.1.	Египетский алгоритм умножения	53
3.2.2.	Алгоритм умножения столбиком	54
3.2.3.	Алгоритм умножения Карацубы	56
3.3.	Возведение в степень	60
3.3.1.	Бинарное возведение в степень	60
3.3.2.	Вычислительная сложность бинарного алго- ритма возведения в степень	62
3.3.3.	Метод множителей показателя	65
Глава 4.	Делимость	67
4.1.	Деление с остатком	67
4.1.1.	Евклидово кольцо	67
4.1.2.	Алгоритм деления с остатком вычитанием	68
4.1.3.	Бинарный алгоритм деления с остатком	68
4.1.4.	Сложность бинарного алгоритма деления с остатком	72
4.2.	Наибольший общий делитель. Алгоритм Евклида	73
4.2.1.	Наибольший общий делитель	73
4.2.2.	Свойства НОД целых чисел	74

4.2.3. Алгоритм Евклида	75
4.2.4. Сложность алгоритма Евклида в полукольце \mathbb{N}_0	77
4.2.5. Расширенный алгоритм Евклида	80
4.2.6. Бинарный алгоритм Стайна	82
Глава 5. Алгоритмы теории чисел в компьютерной алгебре	87
5.1. Сравнения	87
5.1.1. Представления классов \mathbb{Z}_m	88
5.1.2. Решение сравнений первой степени	89
5.1.3. Алгоритм решения сравнения первой степени	90
5.2. Китайская теорема об остатках	92
Глава 6. Простые числа	97
6.1. Свойства простых чисел	99
6.1.1. Основная теорема арифметики	99
6.1.2. Малая теорема Ферма	100
6.1.3. Критерий Вильсона	101
6.1.4. Тест Поплинга	102
6.1.5. Полиномиальный тест Агравала — Каяла — Саксены	103
6.2. Распределение простых чисел	105
6.3. Алгоритмы получения всех простых чисел на промежутке	112
6.3.1. Перебор делителей	112
6.3.2. Решето Эратосфена	112
6.3.3. Решето Аткина	114
6.4. Простые числа специального вида	119
6.5. Вероятностный алгоритм проверки числа на простоту	122
6.5.1. Сильно псевдопростые числа	122
6.5.2. Тест Миллера — Рабина	123
Глава 7. Применения методов компьютерной алгебры	130
7.1. Разложение числа на множители	130
7.1.1. Метод Ферма	130
7.1.2. Метод Диксона	131

7.2. Асимметричное шифрование 136

7.2.1. Криптографические системы с открытым ключом 136

7.2.2. Криптосистема RSA 137

7.2.3. Атаки на RSA 139

Библиографический список 144

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500