

Лабораторная работа №6

Разложение чисел на множители. Метод Полларда

Исламова С.М.

Информация

Докладчик

- Исламова Сания Маратовна
- студент уч. группы НПИмд-01-24
- Российский университет дружбы народов
- 1132249576@pfur.ru
- <https://github.com/SaniyaIslamova26>



Вводная часть

Актуальность

- Реализация ρ -алгоритма Полларда для разложения чисел на множители
- Работа с большими числами в языке Julia
- Понимание вероятностных методов факторизации

Объект и предмет исследования

- ρ -алгоритм Полларда
- Факторизация больших чисел
- Псевдослучайные последовательности
- Вычисление наибольшего общего делителя (НОД)
- Язык программирования Julia

Цели и задачи

- Реализовать ρ -алгоритм Полларда для факторизации чисел
- Исследовать эффективность метода на различных входных данных
- Проанализировать поведение алгоритма на составных числах

Теоретическая часть

Метод Полларда

- Вероятностный алгоритм для нахождения нетривиальных делителей
- Основан на поиске циклов в псевдослучайной последовательности
- Использует “черепаху” и “зайца” для обнаружения циклов
- Временная сложность: $O(\sqrt{p})$, где p - наименьший простой делитель

Алгоритм

1. Выбираем псевдослучайную функцию $f(x) = (x^2 + c) \bmod n$
2. Инициализируем $a = b = 1$
3. На каждой итерации:

- $a = f(a)$ (один шаг)
 - $b = f(f(b))$ (два шага)
 - $d = \text{НОД}(|a - b|, n)$
4. Если $1 < d < n$ - найден нетривиальный делитель

Практическая реализация

Реализация на языке программирования Julia разложение чисел на множители: p -алгоритма Полларда для разложения чисел на множители

```

print("n = "); n = parse(BigInt, readline())          # 1
# Выводим приглашение "n = " и сразу считываем введённое число как BigInt.
# BigInt нужен, потому что в задании числа могут быть очень большими (сотни цифр),
# а обычный Int переполнится. readline() читает строку из терминала.

let                                         # 2
# Создаём локальный блок let – это важно!
# Благодаря Let все переменные внутри (a, b, i, f) будут локальными,
# и Julia не будет ругаться на «global variable» и не выдаст UndefVarError.
# Это самый чистый и правильный способ в скрипте.

a = b = 1                                     # 3
# Согласно лабораторной (стр. 25): «Положить  $a \leftarrow c$ ,  $b \leftarrow c$ », а  $c = 1$ .
# Поэтому оба указателя («черепаха» a и «заяц» b) стартуют с значения 1.

i = 1                                         # 4
# Счётчик итераций. Начинаем с 1, потому что в таблице из методички
# первая строка после заголовка – это  $i = 2$  (уже после первого шага).

f(x) = (x*x + 5) % n                         # 5
# Определяем полиномиальную функцию  $f(x) = x^2 + 5 \pmod{n}$ .
# Именно +5 требует методичка (пример на стр. 25).
# % n – это взятие остатка по модулю n, чтобы числа не росли бесконечно.

```

```

println(" i\t a\t\t b\t\t d") # 6
# Печатаем шапку таблицы точно как в лабораторной.
# \t – табуляция для выравнивания столбцов.

while true # 7
# Запускаем бесконечный цикл – будем выходить из него вручную через break,
# когда найдём нетривиальный делитель.

a = f(a); b = f(f(b)); i += 1 # 8
# Один шаг алгоритма Полларда:
# • «черепаха» a делает один шаг: a ← f(a)
# • «заяц» b делает два шага: b ← f(f(b))
# • увеличиваем счётчик итераций

d = gcd(abs(a - b), n) # 9
# Вычисляем НОД от |a-b| и n – это ключевая идея метода Полларда.
# Если последовательности зациклятся в каком-то подмодуле,
# то |a-b| будет кратно одному из простых делителей n.

println("$i\t $a\t $b\t $d") # 10
# Печатаем текущую строку таблицы: номер итерации, значения a, b и d.
# Интерполяция $ позволяет подставить значения переменных прямо в строку.

if 1 < d < n # 11
    println("\nНетривиальный делитель: $d и $(n ÷ d)")
    # Если найден нетривиальный делитель (не 1 и не всё n),
    # выводим результат и завершаем работу.
    # n ÷ d – это целочисленное деление (в Julia ÷ = \div + TAB)

    break # 12
    # Выходим из цикла – задача решена.

end
end
# Конец блока let – все локальные переменные автоматически уничтожаются.

```

```
Файл Правка Выделение Вид Переход ... ⌘ cmd
C:\Users\Asya\Downloads\A (запуск) ...
1 Текущий файл не содержит
2 Текущий файл не содержит
3 Время: Пятница, 18 марта 2022
4 Пользователь: Альбина Светлана
5
6
7 print("n = 2 и n нечетное, решаем!")
8 # Несколько проверяю, что в машине может быть много блоков (стечи цикла).
9 # Right скрипты, потому что в машине может быть много блоков (стечи цикла).
10 # Right скрипты, потому что в машине может быть много блоков (стечи цикла).
11 # Это самый чистый и правильный способ в сценарии.
12
13 # Создаем логический блок Let - это можно!
14 # Блоки Let не могут иметь друга (a, b, c, f) будут именами,
15 # которые можно использовать в других блоках, но не имеют областей.
16 # Это самый чистый и правильный способ в сценарии.
17
18 a = b + 1
19 # Согласно наблюдению (стр. 25), добавляем a = b + 1, a <= b.
20
21 # Создаем блок Let, чтобы не пересекаться с именами f и a.
22 # Считаем отладчик. Несколько с 1, потому что в таблице на мониторе
23 # первая строка после заголовка - это с 1 + 2 (умно же первое число).
24
25 f(a) = (a * a + 5) * a
26 # Установка логического блока f(a) < a + 5 (под f).
27 # f(a) = a * a + 5 (под f).
28 # f(a) = a * a + 5 (под f).
29
30 print("f(1) = ", f(1))
31
32 while true
33     # Кнопка бесконечного цикла - будет нажимать на него группой через break,
34     # когда видите непрерывный цикл.
35
36     a = f(a); b = f(f(b)); i = 1
37
38     if a == b
39         print("a = b")
40         break
41
42     else
43         print("a > b")
44
45     print("a = ", a)
46
47     print("b = ", b)
48
49     print("i = ", i)
50
51     i += 1
52
53     print("f(i) = ", f(i))
54
55     if i > 1000000000
56         print("i > 1000000000")
57         break
58
59     end
60
61 end
62
63 # Конец блока Let - все дополнение переменные автоматически уничтожаются.
```

```
Файл Правка Выделение Вид Переход ... ⌘ cmd
Лаб05.jl * Julia REPL (v1.11.6) * cmd
julia> 1359331
1359331
1   a           b           d
2   6           41          1
3   41          123939  1
4   1686        391594  1
5   123939      438157  1
6   1           a           b           d
7   41          123939  1
8   1686        391594  1
9   123939      438157  1
10  1686        391594  1
11  123939      438157  1
12  1686        391594  1
13  123939      438157  1
14  1686        391594  1
15  123939      438157  1
16  1686        391594  1
17  123939      438157  1
18  1686        391594  1
19  123939      438157  1
20  1686        391594  1
21  123939      438157  1
22  1686        391594  1
23  123939      438157  1
24  1686        391594  1
25  123939      438157  1
26  1686        391594  1
27  123939      438157  1
28  1686        391594  1
29  123939      438157  1
30  1686        391594  1
31  123939      438157  1
32  1686        391594  1
33  123939      438157  1
34  1686        391594  1
35  123939      438157  1
36  1686        391594  1
37  123939      438157  1
38  1686        391594  1
39  123939      438157  1
40  1686        391594  1
41  123939      438157  1
42  1686        391594  1
43  123939      438157  1
44  1686        391594  1
45  123939      438157  1
46  1686        391594  1
47  123939      438157  1
48  1686        391594  1
49  123939      438157  1
50  1686        391594  1
51  123939      438157  1
52  1686        391594  1
53  123939      438157  1
54  1686        391594  1
55  123939      438157  1
56  1686        391594  1
57  123939      438157  1
58  1686        391594  1
59  123939      438157  1
60  1686        391594  1
61  123939      438157  1
62  1686        391594  1
63  123939      438157  1
64  1686        391594  1
65  123939      438157  1
66  1686        391594  1
67  123939      438157  1
68  1686        391594  1
69  123939      438157  1
70  1686        391594  1
71  123939      438157  1
72  1686        391594  1
73  123939      438157  1
74  1686        391594  1
75  123939      438157  1
76  1686        391594  1
77  123939      438157  1
78  1686        391594  1
79  123939      438157  1
80  1686        391594  1
81  123939      438157  1
82  1686        391594  1
83  123939      438157  1
84  1686        391594  1
85  123939      438157  1
86  1686        391594  1
87  123939      438157  1
88  1686        391594  1
89  123939      438157  1
90  1686        391594  1
91  123939      438157  1
92  1686        391594  1
93  123939      438157  1
94  1686        391594  1
95  123939      438157  1
96  1686        391594  1
97  123939      438157  1
98  1686        391594  1
99  123939      438157  1
100 1686        391594  1
101 123939      438157  1
102 1686        391594  1
103 123939      438157  1
104 1686        391594  1
105 123939      438157  1
106 1686        391594  1
107 123939      438157  1
108 1686        391594  1
109 123939      438157  1
110 1686        391594  1
111 123939      438157  1
112 1686        391594  1
113 123939      438157  1
114 1686        391594  1
115 123939      438157  1
116 1686        391594  1
117 123939      438157  1
118 1686        391594  1
119 123939      438157  1
120 1686        391594  1
121 123939      438157  1
122 1686        391594  1
123 123939      438157  1
124 1686        391594  1
125 123939      438157  1
126 1686        391594  1
127 123939      438157  1
128 1686        391594  1
129 123939      438157  1
130 1686        391594  1
131 123939      438157  1
132 1686        391594  1
133 123939      438157  1
134 1686        391594  1
135 123939      438157  1
136 1686        391594  1
137 123939      438157  1
138 1686        391594  1
139 123939      438157  1
140 1686        391594  1
141 123939      438157  1
142 1686        391594  1
143 123939      438157  1
144 1686        391594  1
145 123939      438157  1
146 1686        391594  1
147 123939      438157  1
148 1686        391594  1
149 123939      438157  1
150 1686        391594  1
151 123939      438157  1
152 1686        391594  1
153 123939      438157  1
154 1686        391594  1
155 123939      438157  1
156 1686        391594  1
157 123939      438157  1
158 1686        391594  1
159 123939      438157  1
160 1686        391594  1
161 123939      438157  1
162 1686        391594  1
163 123939      438157  1
164 1686        391594  1
165 123939      438157  1
166 1686        391594  1
167 123939      438157  1
168 1686        391594  1
169 123939      438157  1
170 1686        391594  1
171 123939      438157  1
172 1686        391594  1
173 123939      438157  1
174 1686        391594  1
175 123939      438157  1
176 1686        391594  1
177 123939      438157  1
178 1686        391594  1
179 123939      438157  1
180 1686        391594  1
181 123939      438157  1
182 1686        391594  1
183 123939      438157  1
184 1686        391594  1
185 123939      438157  1
186 1686        391594  1
187 123939      438157  1
188 1686        391594  1
189 123939      438157  1
190 1686        391594  1
191 123939      438157  1
192 1686        391594  1
193 123939      438157  1
194 1686        391594  1
195 123939      438157  1
196 1686        391594  1
197 123939      438157  1
198 1686        391594  1
199 123939      438157  1
200 1686        391594  1
201 123939      438157  1
202 1686        391594  1
203 123939      438157  1
204 1686        391594  1
205 123939      438157  1
206 1686        391594  1
207 123939      438157  1
208 1686        391594  1
209 123939      438157  1
210 1686        391594  1
211 123939      438157  1
212 1686        391594  1
213 123939      438157  1
214 1686        391594  1
215 123939      438157  1
216 1686        391594  1
217 123939      438157  1
218 1686        391594  1
219 123939      438157  1
220 1686        391594  1
221 123939      438157  1
222 1686        391594  1
223 123939      438157  1
224 1686        391594  1
225 123939      438157  1
226 1686        391594  1
227 123939      438157  1
228 1686        391594  1
229 123939      438157  1
230 1686        391594  1
231 123939      438157  1
232 1686        391594  1
233 123939      438157  1
234 1686        391594  1
235 123939      438157  1
236 1686        391594  1
237 123939      438157  1
238 1686        391594  1
239 123939      438157  1
240 1686        391594  1
241 123939      438157  1
242 1686        391594  1
243 123939      438157  1
244 1686        391594  1
245 123939      438157  1
246 1686        391594  1
247 123939      438157  1
248 1686        391594  1
249 123939      438157  1
250 1686        391594  1
251 123939      438157  1
252 1686        391594  1
253 123939      438157  1
254 1686        391594  1
255 123939      438157  1
256 1686        391594  1
257 123939      438157  1
258 1686        391594  1
259 123939      438157  1
260 1686        391594  1
261 123939      438157  1
262 1686        391594  1
263 123939      438157  1
264 1686        391594  1
265 123939      438157  1
266 1686        391594  1
267 123939      438157  1
268 1686        391594  1
269 123939      438157  1
270 1686        391594  1
271 123939      438157  1
272 1686        391594  1
273 123939      438157  1
274 1686        391594  1
275 123939      438157  1
276 1686        391594  1
277 123939      438157  1
278 1686        391594  1
279 123939      438157  1
280 1686        391594  1
281 123939      438157  1
282 1686        391594  1
283 123939      438157  1
284 1686        391594  1
285 123939      438157  1
286 1686        391594  1
287 123939      438157  1
288 1686        391594  1
289 123939      438157  1
290 1686        391594  1
291 123939      438157  1
292 1686        391594  1
293 123939      438157  1
294 1686        391594  1
295 123939      438157  1
296 1686        391594  1
297 123939      438157  1
298 1686        391594  1
299 123939      438157  1
300 1686        391594  1
301 123939      438157  1
302 1686        391594  1
303 123939      438157  1
304 1686        391594  1
305 123939      438157  1
306 1686        391594  1
307 123939      438157  1
308 1686        391594  1
309 123939      438157  1
310 1686        391594  1
311 123939      438157  1
312 1686        391594  1
313 123939      438157  1
314 1686        391594  1
315 123939      438157  1
316 1686        391594  1
317 123939      438157  1
318 1686        391594  1
319 123939      438157  1
320 1686        391594  1
321 123939      438157  1
322 1686        391594  1
323 123939      438157  1
324 1686        391594  1
325 123939      438157  1
326 1686        391594  1
327 123939      438157  1
328 1686        391594  1
329 123939      438157  1
330 1686        391594  1
331 123939      438157  1
332 1686        391594  1
333 123939      438157  1
334 1686        391594  1
335 123939      438157  1
336 1686        391594  1
337 123939      438157  1
338 1686        391594  1
339 123939      438157  1
340 1686        391594  1
341 123939      438157  1
342 1686        391594  1
343 123939      438157  1
344 1686        391594  1
345 123939      438157  1
346 1686        391594  1
347 123939      438157  1
348 1686        391594  1
349 123939      438157  1
350 1686        391594  1
351 123939      438157  1
352 1686        391594  1
353 123939      438157  1
354 1686        391594  1
355 123939      438157  1
356 1686        391594  1
357 123939      438157  1
358 1686        391594  1
359 123939      438157  1
360 1686        391594  1
361 123939      438157  1
362 1686        391594  1
363 123939      438157  1
364 1686        391594  1
365 123939      438157  1
366 1686        391594  1
367 123939      438157  1
368 1686        391594  1
369 123939      438157  1
370 1686        391594  1
371 123939      438157  1
372 1686        391594  1
373 123939      438157  1
374 1686        391594  1
375 123939      438157  1
376 1686        391594  1
377 123939      438157  1
378 1686        391594  1
379 123939      438157  1
380 1686        391594  1
381 123939      438157  1
382 1686        391594  1
383 123939      438157  1
384 1686        391594  1
385 123939      438157  1
386 1686        391594  1
387 123939      438157  1
388 1686        391594  1
389 123939      438157  1
390 1686        391594  1
391 123939      438157  1
392 1686        391594  1
393 123939      438157  1
394 1686        391594  1
395 123939      438157  1
396 1686        391594  1
397 123939      438157  1
398 1686        391594  1
399 123939      438157  1
400 1686        391594  1
401 123939      438157  1
402 1686        391594  1
403 123939      438157  1
404 1686        391594  1
405 123939      438157  1
406 1686        391594  1
407 123939      438157  1
408 1686        391594  1
409 123939      438157  1
410 1686        391594  1
411 123939      438157  1
412 1686        391594  1
413 123939      438157  1
414 1686        391594  1
415 123939      438157  1
416 1686        391594  1
417 123939      438157  1
418 1686        391594  1
419 123939      438157  1
420 1686        391594  1
421 123939      438157  1
422 1686        391594  1
423 123939      438157  1
424 1686        391594  1
425 123939      438157  1
426 1686        391594  1
427 123939      438157  1
428 1686        391594  1
429 123939      438157  1
430 1686        391594  1
431 123939      438157  1
432 1686        391594  1
433 123939      438157  1
434 1686        391594  1
435 123939      438157  1
436 1686        391594  1
437 123939      438157  1
438 1686        391594  1
439 123939      438157  1
440 1686        391594  1
441 123939      438157  1
442 1686        391594  1
443 123939      438157  1
444 1686        391594  1
445 123939      438157  1
446 1686        391594  1
447 123939      438157  1
448 1686        391594  1
449 123939      438157  1
450 1686        391594  1
451 123939      438157  1
452 1686        391594  1
453 123939      438157  1
454 1686        391594  1
455 123939      438157  1
456 1686        391594  1
457 123939      438157  1
458 1686        391594  1
459 123939      438157  1
460 1686        391594  1
461 123939      438157  1
462 1686        391594  1
463 123939      438157  1
464 1686        391594  1
465 123939      438157  1
466 1686        391594  1
467 123939      438157  1
468 1686        391594  1
469 123939      438157  1
470 1686        391594  1
471 123939      438157  1
472 1686        391594  1
473 123939      438157  1
474 1686        391594  1
475 123939      438157  1
476 1686        391594  1
477 123939      438157  1
478 1686        391594  1
479 123939      438157  1
480 1686        391594  1
481 123939      438157  1
482 1686        391594  1
483 123939      438157  1
484 1686        391594  1
485 123939      438157  1
486 1686        391594  1
487 123939      438157  1
488 1686        391594  1
489 123939      438157  1
490 1686        391594  1
491 123939      438157  1
492 1686        391594  1
493 123939      438157  1
494 1686        391594  1
495 123939      438157  1
496 1686        391594  1
497 123939      438157  1
498 1686        391594  1
499 123939      438157  1
500 1686        391594  1
501 123939      438157  1
502
```

Результаты

- Выполнены все необходимые действия для реализации задач лабораторной работы №6: успешно реализовано на языке программирования Julia разложение чисел на множители: ρ -алгоритма Полларда для разложения чисел на множители.

Вывод

Реализовано на языке программирования Julia разложение чисел на множители: ρ -алгоритма Полларда для разложения чисел на множители