1 Задачи работы

Каждое из указанных чисел разложить на множители:

1. ро-методом Полларда.
2. (p-1)-методом Полларда.

В отчёте привести:

1. В случае результативного завершения работы программы: результат разложения.

2. Для ро-метода Полларда:

2.0. Параметры алгоритма (использованное отображение, начальное значение (несколько, если их пришлось менять)).

2.1. При результативном завершении работы – первые 5 и последние 5 значений a, b, НОД(a – b, n), число итераций, время работы программы, выводы (объяснение результативного завершения).

2.2. При работе программы более нескольких часов – первые 5 и последние (на момент прерывания программы) 5 значений a, b, НОД(a – b, n), число выполненных итераций, время, затраченное на их выполнение, расчетное время, оставшееся до завершения работы (через оценку сложности алгоритма), выводы (объяснение нерезультативного завершения).

3. Для (p-1)-метода Полларда:

3.1 Базу разложения (первоначальную, измененную (если потребовалось изменение, обосновать необходимость изменения)).

3.2 Значения показателей l_i.

3.3 При результативном завершении работы – основание a, при котором выполнено разложение (несколько, если потребовалось изменять основание).

3.4 При невозможности найти разложение более нескольких часов – основание a, при котором выполнено разложение (несколько, если потребовалось изменять основание), число выполненных итераций (одна итерация – прогон алгоритма с одним основанием a), время, затраченное на их выполнение, расчетное время, оставшееся до завершения работы (через оценку сложности алгоритма), выводы (объяснение нерезультативного завершения).

2 Теоретические сведения

Задача разложения составного числа на множители формулируется так: для данного положительного целого числа n найти его каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где p_i – попарно различные простые числа, $\alpha_i \geq 1$.

Нетривиальные сомножители – числа p и q, удовлетворяющие следующим выражениям: $n = pq$, $1 < p \leq q < n$, где n – положительное целое число.

Пусть $B = \{p_1, p_2, \dots, p_s\}$ – множество различных простых чисел. Назовем множество B базой разложения. Целое число назовем B-гладким, если все его простые делители являются элементами множества B.

2.1 Ро-метод Полларда

Вход. Число n, начальное значение c, функция f, обладающая сжимающими свойствами.

Выход. Нетривиальный делитель p числа n.

1. Положить a ← c, b ← c.
2. Вычислить a ← f(a) (mod n), b ← f(b) (mod n), b ← f(b) (mod n).
3. Найти d ← НОД (a – b, n).
4. Если 1 < d < n, то положить p ← d и результат: p. При d = n результат: «Делитель не найден»; при d = 1 вернуться на шаг 2.

2.2 (p-1)-метод Полларда

Вход. Составное число n.

Выход. Нетривиальный делитель p числа n.

1. Выбрать базу разложения $B = \{p_1, p_2, \dots, p_s\}$.
2. Выбрать случайное целое a, $2 \leq a \leq n - 2$, и вычислить $d \leftarrow$ НОД(a, n). При $d \geq 2$ положить $p \leftarrow d$ и результат: p.
3. Для $i = 1, 2, \dots, s$ выполнить следующие действия.
4. Вычислить $l \leftarrow \left[\frac{\ln n}{\ln p_i}\right]$.

5. Положить $a \leftarrow a^{p_i^l} \pmod{n}$.
6. Вычислить $d \leftarrow$ НОД (a – 1, n).
7. При d = 1 или $d = n$ результат: «Делитель не найден». В противном случае положить $p \leftarrow d$ и результат: p.

3 Ход работы

3.1 Результаты работы программы

Разработанная программа была запущена для всех наборов чисел. Результаты работы программы представлены в Таблица 1-6.

Для числа $n_1 = 13611195493017228143$ при помощи Ро-метода Полларда был успешно найден делитель $p = 2978456527$. Использовалось отображение $f(x) = x^2 + 5$ и начальное значение $c = 1$.

Время работы программы: 0.23500657081604004 с, число итераций: 32508.

Таблица 1 – Результаты работы программы для числа n1

i	a	b	d
1	1	1	1
2	6	41	1
3	41	2842601	1
4	1686	10861542182831571302	1
5	2842601	111405573951963106	1
32504	8040085432563274102	6601940779760971423	1
32505	216314951270981850	7737930714978469926	1
32506	6877377558007139165	2185002310513441404	1
32507	2365514650370259930	8014394833696004580	1
32508	2365514650370259930	11661310219253604802	2978456527

Для числа $n_2 = 577481594046145019923902459952027954091$ при помощи Ро-метода Полларда не был найден делитель. Использовалось отображение $f(x) = x^2 + 5$ и начальное значение $c = 1$.

Время работы программы: 3600.0193858146667 с, число итераций: 236571971. Длительность одной итерации составляла $t_0 = 1.5217438357541802e-05$ с, поэтому расчётное время выполнения программы: $t_o * \sqrt[4]{n} = 4902126754.715017 * t_0 = 74597.81171073222\ c =$ 20.0 ч 43.0 м 17.811710732217 76 с .

Таблица 2 – Результаты работы программы для числа n2

i	a	b	d
1	1	1	1
2	6	41	1
3	41	2842601	1
4	1686	652925481392675147683824 41	1
5	2842601	214050005624614091191316969469017447925	1
236571967	5441237855947053691723492832288803960025	5759697656730599033010808358208600870470	1
236571968	1183763432266417844216134313538354715 16	1270956695047727578099280736906895552 36	1
236571969	1183763432266417844216134313538354715 16	2326162175058582250509251163915866206 03	1
236571970	3198913554141052384096104409435094891 12	3948257643322630984590980563656352230 22	1
236571971	3024156920468178424735522851987049772 29	5010791704914322042676739149878752084 31	1

Для числа $n_3 =$ 527084215895878375136898400730821410269463448373678940194583076204765726696000 09 при помощи Ро-метода Полларда не был найден делитель. Использовалось отображение $f(x) = x^2 + 5$ и начальное значение $c = 1$.

Время работы программы: 3600.019764661789 с, число итераций: 113996191. Длительность одной итерации составляла $t_0 = 3.1580175908349335e-05$с, поэтому расчётное время выполнения программы: $t_o * \sqrt[4]{n} = 8.520596565431583e+19 * t_0 = 2690819383804065.5\ c =$ 85325322.0 лет 338.0 дней 2.0 ч 27.0 м 45.5 с.

Таблица 3 – Результаты работы программы для числа n3

i	a	b	d
1	1	1	1
2	6	41	1
3	41	2842601	1
4	1686	652925481392675147683824 41	1
5	2842601	400869747545409760216050395336455902594122860762796860499448246639191390706458 3	1
113996187	219649857877513901936593400257938690115438653229329284474510782700480980922129 23	217151213763053209011990153887394027614393420151492437299283134832822401730839 91	1
113996188	426063820459353258205972383658928995708037177023948887170563467342341472881826 77	191066617232035797049989681746371057929507291518489076311486877477362034131600 50	1
113996189	175828679267328040086170850683343607437013333100537032992642175406185699549069 23	408648041730648833463339348557808480360096501238245434919523233163918300169476 05	1
113996190	322534737820754049097786638640149122757930720006451541713932085209206980920480 40	301499181299919475278187351240714408688206042875362302019991282071175857184762 25	1
113996191	219673521134105671444544769860337388207567203521596244595006161918356686668252 04	323037167878678550123938575763262329376510763163997082526817189307691831062092 99	1

Для числа $n_1 = 136111954930172281 43$ при помощи (p-1)-метода Полларда был успешно найден делитель $p = 4569882209$. Была использована база, состоящая из 63277 простых чисел от 3 и далее по порядку.

Время работы программы: 4.033313751220703 с, число итераций: 63277.

Таблица 4 – Результаты работы программы для числа n1

i	B[i]	l	a	d
1	3	40.0	3687749254297312991	1
2	5	27.0	8692880039870333589	1
3	7	22.0	5691559321014900988	1
4	11	18.0	1615089452164815405	1
5	13	18.0	9319623394481832626	1
63273	788947	3.0	1043905493486501487	1
63274	788959	3.0	3410672726039318558	1
63275	788971	3.0	12381063393251996094	1
63276	788993	3.0	9504370413971455350	1
63277	788999	3.0	8802506059902891931	4569882209

Для числа $n_1 = 577481594046145019923902459952027954091$ при помощи (p-1)-метода Полларда был успешно найден делитель $p = 13063260683520389893$. Была использована база, состоящая из 3081 простых чисел от 3 и далее по порядку.

Время работы программы: 4.033313751220703 с, число итераций: 63277.

Таблица 5 – Результаты работы программы для числа n2

i	B[i]	l	a	d
1	3	81.0	191050789305901844563329713287875840628	1
2	5	55.0	935181263889590899785118565202489254 32	1
3	7	45.0	298587173235620183211554128957687409771	1
4	11	37.0	298587173235620183211554128957687409771	1
5	13	34.0	391376160859571964510084716196235300065	1

3077	27941	8.0	1855556276037157605902095400732991477 11	1
3078	27943	8.0	468524795562505022733624210661168465195	1
3079	27947	8.0	391705780648624445024545993955485664740	1
3080	27953	8.0	158964764778163763233368679450088225377	1
3081	27961	8.0	426946945315885514696486201517688752861	1306326068352038989 3

Для числа $n_3 =$ $52708421589587837513689840073082141026946344837367894019458307620476572669600009$ при помощи (p-1)-метода Полларда не был найден делитель. Была использована база, состоящая из 13347952 простых чисел от 3 и далее по порядку.

Время работы программы: 3600.0539615154266 с, число итераций: 13347952. Длительность одной итерации составляла $t_0 =$ 0.000269708338890897 с, поэтому расчётное время выполнения программы: $t_o * (B * \ln B * (\ln n)^2) =$ $7379499494401.028 * t_0 = 1990312550.4811158\ c =$ 63.0 лет 41.0 дней 0.0 ч 35.0 м 50.48111581802368 с.

Таблица 6 – Результаты работы программы для числа n3

i	B[i]	l	a	d
1	3	167.0	28736456788329733128524573051367718394041538 80089803230215460592200712425030687 2	1
2	5	114.0	48916792648447425777043166681892373564001863 37225886461011761915983235480713396 0	1
3	7	94.0	48916792648447425777043166681892373564001863 37225886461011761915983235480713396 0	1
4	11	76.0	28666136978879204330377772189319096691397256 74089036662258421215605817285641249 9	1
5	13	71.0	47752977649077434201800276953171120422210988	1

			28352824778376628516785663218335790 8	
13347948	24358 1449	9.0	47752977649077434201800276953171120422210988 28352824778376628516785663218335790 8	1
13347949	24358 1449	9.0	38334809395607709558466748608776899675244366 83153966313934662348110907500498687 6	1
13347950	24358 1473	9.0	15759866025848500481624223568852278914075916 93381273095447492210750884006528 82	1
13347951	24358 1483	9.0	12868596477417269448619706286319967592631685 58323205094015097308280696010959625 3	1
13347952	24358 1543	9.0	15653295895228838303554466166102380654264424 84891883593108294683836030290220461 2	1

4 Выводы

В ходе выполнения лабораторной работы были реализованы два алгоритма разложения числа на нетривиальные множители. Ро-метод Полларда дал результаты только для первого числа. Этот алгоритм менее эффективен, чем (p-1)-метод Полларда. Второй метод дал результаты для двух чисел, а также этот алгоритм конечен и в большей степени зависит от мощности базы разложения (которая определяет число итераций цикла).