Научно-исследовательская практика Лето 2020

Бинарный алгоритм нахождения НОД

Завертанов Владислав

1 Описание

Бинарный алгоритм нахождения НОД —метод нахождения наибольшего общего делителя двух целых чисел. Данный алгоритм быстрее обычного алгоритма Евклида, т.к. вместо медленных операций деления и умножения используются сдвиги. Возможно, алгоритм был известен еще в Китае 1-го века, но опубликован был лишь в 1967 году израильским физиком и программистом Джозефом Стайном.Он основан на использовании свойств НОД,а именно НОД$(2m, 2n) = 2$ НОД(m, n), НОД$(2m, 2n + 1) =$ НОД$(m, 2n + 1)$, НОД$(-m, n) =$ НОД(m, n).

2 Алгоритм

Algorithm 1 Бинарный алгоритм Евклида

Ввод: a>0, b>0

Вывод: (a, b)

1: представить **a** и **b** в виде $a = 2^i a_1$,$b = 2^j b_1$, где a_1, b_1 - нечетные
2: положить $a = a_1, b = b_1$, и найти $k = min(i, j)$
3: пока **a** и **b** не равны, выполняй:
4: **if** $a < b$ **then** поменять a и b местами
5: вычислить $c = a - b$ и представить в виде $c = 2^s c_1$, где c_1-нечетное
6: положить $a = c_1$
7: **return** $2^k a$

3 Анализ

3.1 Описание

Алгоритм был реализован на *Sage* — системе компьютерной алгебры, покрывающей много областей математики, включая алгебру, комбинаторику, вычислительную математику и матанализ. Вся вычислительная нагрузка приходилась на облачный ресурс Collaborative Calculation and Data Science (Cocalc).

3.2 Сравнение результатов

Для проверки корректности реализации алгоритма была использована встроенная в *Sage* функция *gcd(a, b)*. Были зафиксированы результаты работы и среднее время их исполнения.

Параметры		Собственная реализация		Sage	
a	b	Результат	Время, с	Результат	Время, с
321^{245}	768^{82}	1330...7449678409	0.00	1330...7449678409	0.00
12304^{24322}	8246^{15633}	10044358...951726592	0.01	10044358...951726592	0.01
1230424^{243222}	824823^{15633}	1	0.07	1	0.06
123456789^{24322}	77777777777^{15633}	1	0.11	1	0.09