Алгоритм Евкліда

Баринова Катерина, 5 курс, ФВЕ

Вступ

- Ефективний алгоритм для пошуку найбільшого спільного дільника (або спільної міри двох відрізків)
- Пара додатніх цілих чисел
- Формується нова пара, яка складається з меншого числа і різниці між більшим і меншим числом
- Процес повторюється, поки числа не стануть однаковими
- Знайдене число і є НСД

Застосування

- В 21 ст. алгоритм застосовується також на інші типи математичних об’єктів
- Цілі числа Гауса, поліноми однієї змінної
- Евклідове кільце
- Вузли, поліноми багатьох змінних
- Основа для криптографічного алгоритму с відкритим ключем RSA
- Розв’язок діофантових рівнянь, побудова неперервних дробів, метод Штурма
- Теорема Лагранжа про суму чотирьох квадратів, основна теорема арифметики

a і b - цілі числа, які одночасно не дорівнюють нулю

$$a > b > r_1 > r_2 > r_3 > r_4 > \ \dots \ > r_n$$

$$\begin{aligned}
a &= bq_0 + r_1, \\
b &= r_1 q_1 + r_2, \\
r_1 &= r_2 q_2 + r_3, \\
&\dots \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k, \\
&\dots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \\
r_{n-1} &= r_n q_n .
\end{aligned}$$

Приклад

Шаг k	Равенство	Частное и остаток
0	$1071 = q_0\ 462 + r_0$	$q_0 = 2$ и $r_0 = 147$
1	$462 = q_1\ 147 + r_1$	$q_1 = 3$ и $r_1 = 21$
2	$147 = q_2\ 21 + r_2$	$q_2 = 7$ и $r_2 = 0$; алгоритм заканчивается

$1071 > 462 > 147 > 21$

НСД(1071, 462) = 21

Прискорені версії алгоритму

- Симетричний залишок $r_i \equiv r_{i-2} \pmod{r_{i-1}}$,

$$-\frac{r_{i-1}}{2} \leq r_i \leq \frac{r_{i-1}}{2}.$$

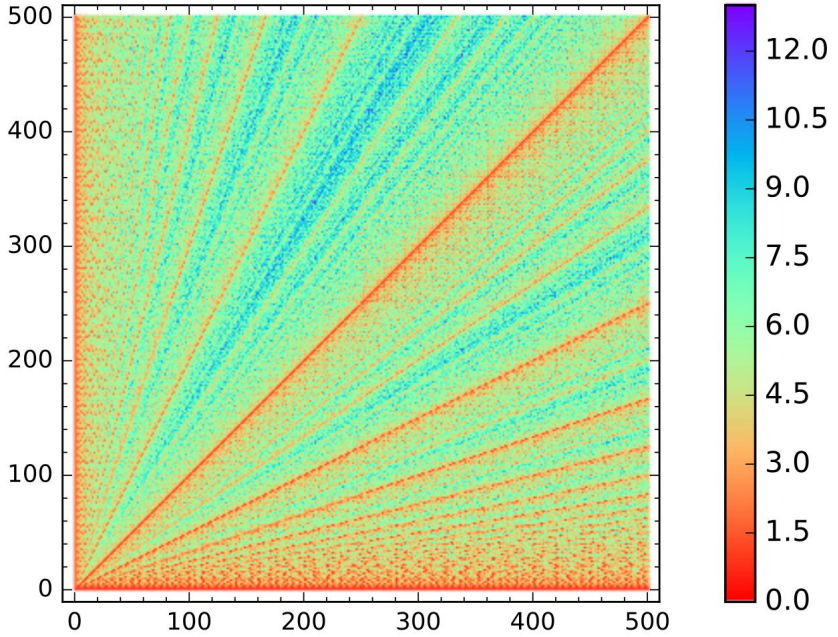
- Divide and conquer

Кількість кроків

- $v/2 + 2$
- $2 \log_2 v + 1$

$O(h)$

$O(h^2)$



Дякую за увагу