ЛАБОРАТОРНАЯ РАБОТА №4

Вычисление наибольшего общего делителя

Пусть числа a и b целые и $b \neq 0$. Разделить a на b с остатком – значит представить a в виде $a = qb + r$, где $q, r \in Z$ и $0 \leq r \leq |b|$. Число q называется неполным частным, число r – неполным остатком от деления a на b.

Целое число $d \neq 0$ называется *наибольшим общим делителем* целых чисел $a_1, a_2, \dots, a_k$ (обозначается $d =$ НОД$(a_1, a_2, \dots, a_k)$), если выполняются следующие условия:

1. каждое из чисел $a_1, a_2, \dots, a_k$ делится на d;
2. если $d_1 \neq 0$ – другой общий делитель чисел $a_1, a_2, \dots, a_k$, то d делится на d_1.

Например, НОД(12345, 24690) = 12345, НОД(12345, 54321) = 3, НОД(12345, 12541) = 1.

Ненулевые целые числа a и b называются *ассоциированными* (обозначается $a \sim b$), если a делится на b и b делится на a.

Для любых целых чисел $a_1, a_2, \dots, a_k$ существует наибольший общий делитель d и его можно представить в виде *линейной комбинации* этих чисел:

$$d = c_1 a_1 + c_2 a_2 + \dots + c_k a_k,\ c_i \in Z\ (Z \text{ – множество целых чисел}).$$

Например, НОД чисел 91, 105, 154 равен 7. В качестве линейного представления можно взять

$$7 = 7 \cdot 91 + (-6) \cdot 105 + 0 \cdot 154,$$

либо

$$7 = 4 \cdot 91 + 1 \cdot 105 - 3 \cdot 154.$$

Целые числа $a_1, a_2, \dots, a_k$ называются *взаимно простыми в совокупности*, если НОД$(a_1, a_2, \dots, a_k)$=1. Целые числа a и b называются *взаимно простыми*, если НОД(a,b)=1.

Целые числа $a_1, a_2, \dots, a_k$ называются *попарно взаимно простыми*, если НОД(a_i, a_j)=1 для всех $1 \leq i \neq j \leq k$.

Алгоритмы вычисления наибольшего общего делителя.

Для вычисления наибольшего общего делителя двух целых чисел применяется способ повторного деления с остатком, называемый *алгоритмом Евклида*.

1. Алгоритм Евклида.

Вход. Целые числа a, b; $0 < b \le a$.

Выход. $d = \text{НОД}(a, b)$.

1. Положить $r_0 \leftarrow a, r_1 \leftarrow b, i \leftarrow 1$.
2. Найти остаток r_{i+1} от деления r_{i-1} на r_i.
3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$. В противном случае положить $i \leftarrow i + 1$ и вернуться на шаг 2.
4. Результат: d.

Бинарный алгоритм Евклида является более быстрым при реализации на компьютере, поскольку использует двоичное представление чисел a и b. Бинарный алгоритм Евклида основан на следующих свойствах наибольшего общего делителя (считаем, что $0 < b \le a$):

1) если оба числа a и b четные, то $\text{НОД}(a, b) = 2 \cdot \text{НОД}(\frac{a}{2}, \frac{b}{2})$;
2) если число a – нечетное, число b – четное, то $\text{НОД}(a, b) = \text{НОД}(a, \frac{b}{2})$;
3) если оба числа a и b нечетные, $a > b$, то $\text{НОД}(a, b) = \text{НОД}(a - b, b)$;
4) если $a = b$, то $\text{НОД}(a, b) = a$.

2. Бинарный алгоритм Евклида.

Вход. Целые числа a, b; $0 < b \le a$.

Выход. $d = \text{НОД}(a, b)$.

1. Положить $g \leftarrow 1$.
2. Пока оба числа a и b четные, выполнять $a \leftarrow \frac{a}{2}$, $b \leftarrow \frac{b}{2}$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения a или b.
3. Положить $u \leftarrow a, v \leftarrow b$.
4. Пока $u \ne 0$ выполнять следующие действия:

4.1. Пока u четное, полагать $u \leftarrow \frac{u}{2}$.

4.2. Пока v четное, полагать $v \leftarrow \frac{v}{2}$.

4.3. При $u \geq v$ положить $u \leftarrow u - v$. В противном случае положить $v \leftarrow v - u$.

5. Положить $d \leftarrow gv$.
6. Результат: d

3. Расширенный алгоритм Евклида.

Вход. Целые числа a, b; $0 < b \leq a$.

Выход. $d = \text{НОД}(a, b)$; такие целые числа x, y, что $ax + by = d$.

1. Положить $r_0 \leftarrow a, r_1 \leftarrow b, x_0 \leftarrow 1, x_1 \leftarrow 0, y_0 \leftarrow 0, y_1 \leftarrow 1, i \leftarrow 1$.
2. Разделить с остатком r_{i-1} на r_i: $r_{i-1} = q_i r_i + r_{i+1}$.
3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$, $x \leftarrow x_i$, $y \leftarrow y_i$. В противном случае положить $x_{i+1} \leftarrow x_{i-1} - q_i x_i, y_{i+1} \leftarrow y_{i-1} - q_i y_i, i \leftarrow i + 1$ и вернуться на шаг 2.
4. Результат: d, x, y.

4. Расширенный бинарный алгоритм Евклида.

Вход. Целые числа a, b; $0 < b \leq a$.

Выход. $d = \text{НОД}(a, b)$.

1. Положить $g \leftarrow 1$.
2. Пока числа a и b четные, выполнять $a \leftarrow \frac{a}{2}$, $b \leftarrow \frac{b}{2}$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения a или b.
3. Положить $u \leftarrow a, v \leftarrow b, A \leftarrow 1, B \leftarrow 0, C \leftarrow 0, D \leftarrow 1$.
4. Пока $u \neq 0$ выполнять следующие действия:

4.1. Пока u четное:

4.1.1. Положить $u \leftarrow \frac{u}{2}$.

4.1.2. Если оба числа A и B четные, то положить $A \leftarrow \frac{A}{2}, B \leftarrow \frac{B}{2}$. В противном случае положить $A \leftarrow \frac{A+b}{2}, B \leftarrow \frac{B-a}{2}$.

4.2. Пока v четное:

4.2.1. Положить $v \leftarrow \frac{v}{2}$.

4.2.2. Если оба числа C и D четные, то положить $C \leftarrow \frac{C}{2}, D \leftarrow \frac{D}{2}$. В противном случае положить $C \leftarrow \frac{C+b}{2}, D \leftarrow \frac{D-a}{2}$.

4.3. При $u \geq v$ положить $u \leftarrow u - v, A \leftarrow A - C, B \leftarrow B - D$. В противном случае положить $v \leftarrow v - u, C \leftarrow C - A, D \leftarrow D - B$.

5. Положить $d \leftarrow gv, x \leftarrow C, y \leftarrow D$.
6. Результат: d, x, y.

Задания к лабораторной работе

Реализовать все рассмотренные алгоритмы программно.