Олександр Рудик

Подання найбільшого спільного дільника лінійною комбінацією з цілими коефіцієнтами (розширений алгоритм Евкліда)

Алгоритм Евкліда пошуку найбільшого спільного дільника можна сформулювати таким чином. Нехай $\{a_n\}$ — така послідовність елементів *евклідового кільця* (наприклад, множини цілих чисел або множини многочленів), у якій a_{n+1} — остача від ділення a_{n-1} на a_n при n=2, 3, … При цьому *евклідова норма* (відповідно абсолютна величина цілого числа або степінь многочлена) членів послідовності спадає і набуває натуральних значень. Через це існує таке натуральне k, при якому a_k відмінне від 0, $a_{k+1} = 0$. Тоді найбільші спільні дільники (НСД) пар сусідніх членів такої послідовності збігаються з a_k, що є дільником усіх членів послідовності.

Відомо, що НСД(a, b), можна подати сумою $ax + by$, що має найменшу евклідову норму. З означеннями й доведеннями відповідних тверджень можна ознайомитися, наприклад, за таким посібником: *Олександр Рудик. Початки алгебри, аналізу, аналітичної геометрії і теорії ймовірностей. — Тернопіль, Навчальна книга – Богдан, 2005, 416 с.* Цей посібник є викладом теоретичних основ відповідних розділів шкільного курсу математики, адаптованим для учнів класів з поглибленим вивченням математики.

Зробимо зауваження щодо способу знаходження коефіцієнтів x та y у поданні найбільшого спільного дільника лінійною сумою. Нехай у послідовності, побудованій згідно з алгоритмом Евкліда, справджуються такі рівності:

$$a_1 = a,\ a_2 = b,\ a_n = x_n a + y_n b \text{ при } x_1 = 1,\ y_1 = 0,\ x_2 = 0,\ y_2 = 1.$$

Позначимо через q_n частку від ділення a_{n-1} на a_n . Для справдження такої рівності:

$$x_{n-1}a + y_{n-1}b = q_n(x_n a + y_n b) + x_{n+1}a + y_{n+1}b$$

зі зліченої множини розв'язків можна вибрати:

$$x_{n+1} = x_{n-1} - q_n x_n ,$$
$$y_{n+1} = y_{n-1} - q_n y_n .$$

Зауважимо, що і первісний, і розширений алгоритми Евкліда можна застосовувати і до цілих чисел, і до многочленів. Подамо приклад програми мовою Pascal, що використовує описаний алгоритм для невід'ємних цілих чисел.

```
const a=12345;  b=67890;
var   d,x,y: longint;

function sign(x:longint):longint;BEGIN
if x<0 then sign:=-1 else
if x>0 then sign:= 1 else sign:=0  END;

procedure  gcd     (a,b: longint;
           var a1,x1,y1: longint);
var q,a2,x2,y2,a3,x3,y3: longint;BEGIN
if (a=0) and (b=0) then begin
   a2:=0;  x2:=0;  y2:=0  end else
if (a=0)           then begin
   a2:=b;  x2:=0;  y2:=1  end else
if (a=b)           then begin
   a2:=a;  x2:=1;  y2:=0  end else
                        begin
   a1:=a;  x1:=1;  y1:=0;
   a2:=b;  x2:=0;  y2:=1;
   REPEAT
      q:=a1 div a2;  x3:=x1-q*x2;
     a3:=a1 mod a2;  y3:=y1-q*y2;
     a1:=a2;  x1:=x2;  y1:=y2;
     a2:=a3;  x2:=x3;  y2:=y3
   UNTIL a3=0             end      END;
                                 BEGIN
gcd(a,b,d,x,y);
write('НСД(',a,',',b,')=',d,
                      '=',x,'*',a);
if y>=0 then write('+');
writeln(y,'*',b)                   END.
```