Extended Euclid's Algorithm

Dragan Marković

This algorithm find's coefficients (x, y) such that $a \cdot x + b \cdot y = gcd(a, b)$ for given a and b. Extended Euclid's Algorithms main use is in solving linear Diophantine equations, which are of the form $a \cdot x + b \cdot y = c$. It is easy to deduce from the algorithm that this equation has solution only if $gcd(a, b)|c$.

Standard Euclid's algorithm finds sequence $r_0, r_1, ..., r_k$ such that:
$r_0 = a$
$r_1 = b$
$r_i = r_{i-2} \% r_{i-1}$
Algorithm terminates when $r_{k+1} = 0$ and $gcd(a, b)$ is stored in r_k. Here $x \ \% \ y$ denotes the remainder of dividing x by y.

We'd like to extend this algorithm by adding two numbers (t_i, s_i) such that $r_i = t_i \cdot a + s_i \cdot b$ at each iteration of the algorithm. Since $r_0 = a$ and $r_1 = b$ it's obvious that $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$.

So it follows that $s_0 = 1, t_0 = 0, s_1 = 0$ and $t_1 = 1$. Let's try to generalize and find out s_k and t_k:

$$
\begin{aligned}
r_{k-1} &= a \cdot s_{k-1} + b \cdot t_{k-1} \\
r_k &= a \cdot s_k + b \cdot t_k \\
r_{k+1} &= ? \\
r_{k-1} &= r_k \cdot q + r_{k+1} \, (From\, definition\, of\, "r"\, sequence,\, r_i = r_{i-2} \% r_{i-1}) \\
r_{k+1} &= r_{k-1} - r_k \cdot q \\
r_{k+1} &= a \cdot s_{k-1} + b \cdot t_{k-1} - (a \cdot s_k + b \cdot t_k) \cdot q \\
r_{k+1} &= a \cdot (s_{k-1} - s_k \cdot q) + b \cdot (t_{k-1} - t_k \cdot q) \\
r_{k+1} &= a \cdot s_{k+1} + b \cdot t_{k+1}
\end{aligned}
$$

We finally have $s_{k+1} = s_{k-1} - q \cdot s_k$ and $t_{k+1} = t_{k-1} - q \cdot t_k$. If $r_{k+1} = 0$ Then $a \cdot s_k + b \cdot t_k = gcd(a, b)$ so the solution to our equation for $a \cdot x + b \cdot y = c$ is $(x_0, y_0) = (s_k \cdot \frac{c}{r_k}, t_k \cdot \frac{c}{r_k})$. If Diophantine equation has one solution it has infinitely many!!! We can simply write $a \cdot x + b \cdot y = a \cdot (x - kb) + b \cdot (y + ka)$. Therefore the general solution for an equation is $(x_n, y_n) = (x_0 - n \cdot b, y_0 + n \cdot a)$.

Example : $2 \cdot x - 5 \cdot y = 1$

i	q	r_i	s_i	t_i
0	0	2	1	0
1	0	-5	0	1
2	0	2	1	0
3	-2	-1	2	1

$\frac{1}{-1} = -1$

$(x_0, y_0) = (-2, -1)$

$(x_n, y_n) = (-2 + 2 \cdot n, -1 + 5 \cdot n)$.

Example : $87 \cdot x - 64 \cdot y = 3$

i	q	r_i	s_i	t_i
0	0	87	1	0
1	0	-64	0	1
2	-1	23	1	1
3	-2	-18	2	3
4	-1	5	3	4
5	-3	-3	11	15
6	-1	2	14	19
7	-1	-1	25	34

$\frac{3}{-1} = -3$

$(x_0, y_0) = (-75, -102)$

$(x_n, y_n) = (-75 + 64 \cdot n, -102 + 87 \cdot n)$.