Rozszerzony algorytm Euklidesa:

Niech dane będą dwie liczby $p<q$.

Zapisujemy sobie pierwsze dwa równania:

$$\begin{aligned} p&=(1)\cdot p+(0)\cdot q \\ q&=(0)\cdot p+(1)\cdot q \end{aligned}.$$

Teraz dzielimy sobie p modulo q . Dla ustalenia uwagi niech $p=k_1\cdot q+r_1$, wtedy dostajemy 3 równanie postaci:

$r_1=(1-0\cdot k_1)\cdot p+(0-1\cdot k_1)\cdot q$, a po uproszczeniu $r_1=(1)\cdot p+(-k_1)\cdot q$.

Możemy teraz zapisać nowy układ dwóch równań:

$$\begin{aligned} q&=(0)\cdot p+(1)\cdot q \\ r_1&=(1)\cdot p+(-k_1)\cdot q \end{aligned}.$$

Dla nich robimy to samo co dla pierwszych dwóch równań dostając jakieś r_2 .
Powtarzamy to, aż dojdziemy do momentu gdzie $r_i \, modulo \, r_{i+1}=0$.
Wtedy r_{i+1} jest największym wspólnym dzielnikiem liczb *p* i *q*.
Dodatkowo robiąc wszystkie kroki, otrzymujemy na końcu dwa współczynniki (w nawiasach), które są wykorzystywane w RSA i innych takich.

Przykład 1.

Dla 121 i 55 mamy:

$$\begin{aligned} 121&=(1)\cdot 121+(0)\cdot 55 \\ 55&=(0)\cdot 121+(1)\cdot 55 \end{aligned}.$$

Teraz zauważamy, że $121=2\cdot 55+11$ i otrzymujemy równanie:

$11=(1-2\cdot 0)\cdot 121+(0-2\cdot 1)\cdot 55=(1)\cdot 121+(-2)\cdot 55$.

Zapisujemy nowy układ równań:

$$\begin{aligned} 55&=(0)\cdot 121+(1)\cdot 55 \\ 11&=(1)\cdot 121+(-2)\cdot 55 \end{aligned}.$$

Teraz zauważamy, że $55=5\cdot 11+0$, zatem liczba 11 jest NWD (121, 55).
Rozwiązaniem problemu Pana Skiby jest ostatnie równanie, przy czym $x=1, y=-2$.

Przykład 2.

Dla 133, 64 mamy:

$$\begin{aligned} 133&=(1)\cdot 133+(0)\cdot 64 \\ 64&=(0)\cdot 133+(1)\cdot 64 \end{aligned}.$$

Widać, że $133=2\cdot 64+5$, zatem mamy nowy układ:

$$\begin{aligned} 64&=(0)\cdot 133+(1)\cdot 64\\ 5&=(1)\cdot 133+(-2)\cdot 64 \end{aligned}.$$

Dalej $64=12\cdot 5+4$. Dostajemy stąd nowe równanie:

$$\begin{aligned} 4&=(1\cdot 0-12\cdot 1)\cdot 133+(1\cdot 1-12\cdot(-2))\cdot 64\\ 4&=(-12)\cdot 133+(25)\cdot 64 \end{aligned}.$$

Nowy układ to:

$$\begin{aligned} 5&=(1)\cdot 133+(-2)\cdot 64\\ 4&=(-12)\cdot 133+(25)\cdot 64 \end{aligned}.$$

Teraz widać, że $5=1\cdot 4+1$, skąd otrzymujemy równanie:

$$\begin{aligned} 1&=(1\cdot 1-1\cdot(-12))\cdot 133+(1\cdot(-2)-1\cdot 25)\cdot 64\\ 1&=(13)\cdot 133+(-27)\cdot 64 \end{aligned}.$$

Ostatnie równanie jest rozwiązaniem problemu Pana Skiby, gdzie $x=13, y=-27$.

Enjoy ;)