Algoritmo di Euclide

Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Troviamo $d \in \mathbb{Z}$ tale che $d = \gcd(a, b)$ e x_0, y_0 (non unici) tali che $d = ax_0 + by_0$ (**identità di Bézout**).

Algoritmo

Se $a = 0$ si scambiano a e b, poi:

$$\begin{aligned}
a &= q_0 \underbrace{b}_{=r_0} + r_1 && 0 \leq r_1 < |b| \\
r_0 &= q_1 r_1 + r_2 && 0 \leq r_2 < r_1 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_n \underbrace{r_n}_{=d} + 0
\end{aligned}$$

Risalendo nelle equazioni si trovano i coefficienti dell'identità di Bézout.

Pseudocodice

EuclideEsteso(a, b)

```
1  if b == 0
2        return ⟨a, 1, 0⟩
3  else
4        ⟨d, x, y⟩ = EuclideEsteso(b, a mod b)
5        return ⟨d, y, x − ⌊a/b⌋y⟩
```

Termina in tempo polinomiale.