Extended Euclid's Algorithm

The extended Euclid's algorithm can be used to express $\gcd(a,b)$ as an integer linear combination of a and b, i.e., we can use it to find integers x and y such that

$$ax + by = \gcd(a,b).$$

Let's illustrate it by finding integers x and y such that

$$1124x + 84y = \gcd(1124, 84).$$

First we use Euclid's algorithm to find $\gcd(1124, 84)$.

$$\begin{aligned}
1124 &= 84(13) + 32 \\
84 &= 32(2) + 20 \\
32 &= 20(1) + 12 \\
20 &= 12(1) + 8 \\
12 &= 8(1) + \boxed{4} \longleftarrow \text{(the last nonzero remainder is the answer)} \\
8 &= 4(2) + 0
\end{aligned}$$

We conclude that $\gcd(1124, 84) = 4$.

We now use back substitution to express 4 as a linear combination of 1124 and 84 as follows.

$$\begin{aligned}
4 &= 12 - \mathbf{8} \\
&= 12 - \boxed{(20 - 12)} = \mathbf{12}(2) - 20 \\
&= \boxed{(32 - 20)}(2) - 20 = 32(2) - \mathbf{20}(3) \\
&= 32(2) - \boxed{(84 - 32(2))}(3) = \mathbf{32}(8) - 84(3) \\
&= \boxed{(1124 - 84(13))}(8) - 84(3) = 1124(8) - 84(107)
\end{aligned}$$

We conclude that an integer solution of $1124x + 84y = \gcd(1124, 84)$ is

$$x = 8 \quad \text{and} \quad y = -107.$$

If x_0, y_0 is an integer solution of $ax + by = \gcd(a,b)$, then for any integer k

$$x = x_0 + \frac{bk}{\gcd(a,b)} \quad \text{and} \quad y = y_0 - \frac{ak}{\gcd(a,b)}$$

is also a solution.

In the above example we conclude that

$$x = 8 + 21k \quad \text{and} \quad y = -107 - 281k$$

are solutions for any integer k.

The following is a Python version of the extended Euclid's algorithm. If we input (a, b), it returns $(x, y, \gcd(a, b))$.

```
def xgcd(a,b):
  if b == 0:
    return [1,0,a]
  else:
    x,y,d = xgcd(b, a%b)
    return [y, x - (a//b)*y, d]  # Note that a//b is floor(a/b) in Python.
```

Let's test it by typing this code and saving it in a file called `xgcd.py`.

```
>>> from xgcd import *
>>> xgcd(1124,84)
[8, -107, 4]
```

Let's see why this code works. We want to find integers x, y so that

$$\gcd(a, b) = ax + by. \tag{1}$$

First observe that if $b = 0$, then $x = 1$, $y = 0$, and $\gcd(a, 0) = a$. Now, assume that we have integers x' and y' so that

$$\gcd(b, a \bmod b) = bx' + (a \bmod b)y'.$$

Since

$$a \bmod b = a - \lfloor a/b \rfloor \cdot b$$

and

$$\gcd(a, b) = \gcd(b, a \bmod b),$$

then

$$\begin{aligned} \gcd(a, b) &= bx' + (a - \lfloor a/b \rfloor \cdot b)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor \cdot y'). \end{aligned}$$

We see that

$$x = y' \quad \text{and} \quad y = x' - \lfloor a/b \rfloor \cdot y'$$

are solutions of (1).