COLLEGE of CHARLESTON

1770

MATH MEET 2019

Euclid's Algorithm All-Day Sprint

Euclid's algorithm is a way to find the greatest common divisor (GCD) of two integers. Here's the core idea. Given a and b, with $a > b$, use division with remainder to write

$$a = bq + r, \quad 0 \le r < b \tag{1}$$

or equivalently

$$a - bq = r \tag{2}$$

From (2), you can see that the GCD of a and b must also divide r. From (1), you can see that the GCD of b and r must also divide a. Putting all that together, the GCD of a and b must also be the GCD of b and r. Since r is less than b, we've narrowed down the possibilities for the GCD considerably. Now all you have to do is divide b by r, and keep repeating this process until you hit a remainder of zero. The last non-zero remainder is the GCD you're looking for.

Here's an example. Let's find the GCD of 288 and 120. First,

$$288 = 120 \times 2 + 48$$

So $\gcd(288, 120) = \gcd(120, 48)$. Repeat:

$$\begin{aligned} 120 &= 48 \times 2 + 24 \\ 48 &= 24 \times 2 \end{aligned}$$

So $\gcd(288, 120) = \gcd(120, 48) = \gcd(48, 24) = 24$. And sure enough, $288 = 24 \times 12$ and $120 = 24 \times 5$.

1. Use Euclid's algorithm to find $\gcd(720, 520)$.

40

   Interestingly, the steps of Euclid's algorithm allow you to find integers m and n that solve

$$am + bn = \gcd(a, b) \tag{3}$$

   Here's how it works for $a = 288$ and $b = 120$. Go back through the calculations and isolate the remainder in each step:

$$\begin{aligned} 288 - 120 \times 2 &= 48 \\ 120 - 48 \times 2 &= 24 \end{aligned} \tag{4}$$

Use the first step to replace the 48 in the second step

$$120-(288-120\times 2)\times 2=24$$

and simplify to get

$$120\times 5+288\times(-2)=24$$

Here's another example. Let's compute $\gcd(200,29)=1$.

$$\begin{aligned} 200 &= 29\times 6+26 & \qquad 200-29\times 6 &= 26\\ 29 &= 26\times 1+3 & 29-26\times 1 &= 3\\ 26 &= 3\times 8+2 & 26-3\times 8 &= 2\\ 3 &= 2\times 1+1 & 3-2\times 1 &= 1\\ 2 &= 1\times 2 & 2-1\times 2 &= 0 \end{aligned}$$

Now we go bottom up:

$$\begin{aligned} 3-2\times 1 &= 1\\ 3-(26-3\times 8)\times 1 = 26\times(-1)+3\times 9 &= 1\\ 26\times(-1)+(29-26\times 1)\times 9 = 29\times 9+26\times(-10) &= 1\\ 29\times 9+(200-29\times 6)\times(-10) = 200\times(-10)+29\times 69 &= 1 \end{aligned}$$

So a solution in integers of $200m+29n=1$ is $m=-10$, $n=69$.

2. Find integers m and n such that $720m+520n=\gcd(720,520)$.

$$\boxed{m=-5, n=7}$$

3. Find integers m and n such that $320m+119n=1$.

$$\boxed{m=45, n=-121}$$

4. Find an integer $0\le k<320$ such that $119k\equiv 1 \pmod{320}$.

$$\boxed{k=199}$$