Number Theory: The Euclidean Algorithm

Written by Rachel Singh, last updated Oct 30, 2018

About

In this part we will look at an algorithm to find the greatest common divisor of two integers.

1. The Euclidean Algorithm

If the following is true:

$$r = a \bmod b$$

then this is also true:

$$gcd(a, b) = gcd(b, r)$$

Notes

If r = a mod b,
then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example: 2 = 18 mod 4

gcd(18, 4) = ?

gcd(4, 2) = ?

Notes

If r = a mod b, then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example: 2 = 18 mod 4

gcd(18, 4) = ?

gcd(4, 2) = ?

Divisors of 2: 1, 2
Divisors of 4: 1, 2, 4
Divisors of 18: 1, 2, 3, 6, 9

Notes

If r = a mod b, then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example: 2 = 18 mod 4

gcd(18, 4) = ?
= 2

gcd(4, 2) = ?
= 2

Divisors of 2: 1, 2
Divisors of 4: 1, 2, 4
Divisors of 18: 1, 2, 3, 6, 9

Notes

If r = a mod b, then
gcd(a,b) = gcd(b,r)

Example 2

$$6 = 30 \bmod 12$$

What is gcd(30, 12) and gcd(12, 6)?

Notes

If r = a mod b,
then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example 2

$$6 = 30 \bmod 12$$

What is gcd(30, 12) and gcd(12, 6)?

6: 1, 2, 3, 6
12: 1, 2, 3, 6, 12
30: 1, 2, 3, 5, 6, 10, 15, 30

gcd(30,12) = 6 gcd(12,6) = 6

Notes

If r = a mod b, then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Instead of taking the time to list out all divisors, we can use the Euclidean Algorithm instead.

Notes

If r = a mod b, then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Input: *a* and *b* (nonnegative integers, not both zero)
Output: Greatest common divisor of *a* and *b*.

```
gcd(a, b) {
   /* make a largest */
   if ( a < b )       swap( a, b );

   while ( b != 0 ) {
      r = a % b;      // % is mod
      a = b;
      b = r;
   }
   return a;
}
```

Notes

If r = a mod b,
then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Python functions:

```
def swap( a, b ):
    c = a
    a = b
    b = c


def gcd( a, b ):
    if ( a < b ):
        swap( a, b )

    while ( b is not 0 ):
        r = a % b
        a = b
        b = r

    return a
```

C++ functions:

```
void swap( int& a, int& b )
{
    int c = a;
    a = b;
    b = c;
}

int gcd( int a, int b )
{
    int r;
    if ( a < b ) { swap( a, b ); }

    while ( b != 0 )
    {
        r = a % b;
        a = b;
        b = r;
    }

    return a;
}
```

Notes

If r = a mod b, then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example: What is gcd(120, 144) ? (Use the algorithm)

```
gcd(a, b) {
    if ( a < b )
        swap( a, b );

    while ( b != 0 ) {
        r = a % b;
        a = b;
        b = r;
    }
    return a;
}
```

Notes

If r = a mod b,
then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example: What is gcd(120, 144) ? (Use the algorithm)

gcd(120, 144)
if (120 < 144) *TRUE*
a = 144, b = 120

while (b != 0) *TRUE, b = 120…*
r = a % b; *r = 24*

a = b; *a = 120*
b = r; *b = 24*

```
gcd(a, b) {
    if ( a < b )
        swap( a, b );

    while ( b != 0 ) {
        r = a % b;
        a = b;
        b = r;
    }
    return a;
}
```

Notes

If r = a mod b,
then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example: What is gcd(120, 144) ? (Use the algorithm)

gcd(120, 144)
if (120 < 144) *TRUE*
a = 144, b = 120

while (b != 0) *TRUE, b = 120…*
r = a % b; *r = 24*

a = b; *a = 120*
b = r; *b = 24*

```
gcd(a, b) {
    if ( a < b )
        swap( a, b );

    while ( b != 0 ) {
        r = a % b;
        a = b;
        b = r;
    }
    return a;
}
```

Notes

If r = a mod b,
then
gcd(a,b) = gcd(b,r)

1. The Euclidean Algorithm

Example: What is gcd(120, 144) ? (Use the algorithm)

a = 120, b = 24

while (b != 0)	*TRUE, b = 24…*
r = a % b;	*r = 0*
a = b;	*a = 24*
b = r;	*b = 0*
while (b != 0)	FALSE
return a;	*a = 24*

gcd(120, 144) = 24.

```
gcd(a, b) {
    if ( a < b )
        swap( a, b );

    while ( b != 0 ) {
        r = a % b;
        a = b;
        b = r;
    }
    return a;
}
```

Notes

If r = a mod b,
then
gcd(a,b) = gcd(b,r)

Conclusion

Practice stepping through the algorithm to make sure that you understand each step!