```
public int Mystery(int m, int n){
     if(m<n){
          int temp = m;
          m=n;
          n=temp;
     }
     while(n != 0) {
          int rem = m % n;
          m=n;
          n=temp;
     }
     return m;
}
```

Key Steps in RSA

Given two numbers, we can find their gcd quickly.

If we have an equation

$ax \equiv b (\text{mod } n)$

And $\gcd(a, n) = 1$ then we can quickly find a number to multiply the equation by to solve for x.

How do we accomplish those steps?

That fact? You can prove it in the extra credit problem on HW5. It's a nice combination of lots of things we've done with modular arithmetic.

Let's talk about finding $C = a^e \% n$.

e is a BIG number (about 2^{16} is a common choice)

```
int total = 1;
for(int i = 0; i < e; i++){
    total = (a * total) % n;
}
```

An application of all of this modular arithmetic

Amazon chooses random 512-bit (or 1024-bit) prime numbers p, q and an exponent e (often about 60,000).

Amazon calculates $\mathrm{n} = pq$. They tell your computer (n, e) (not p, q)

You want to send Amazon your credit card number a.

You compute $C = a^e \% n$ and send Amazon C.

Amazon computes d, the multiplicative inverse of e $(mod\ [p-1][q-1])$

Amazon finds $C^d \% n$

Fact: $a = C^d \% n$ as long as $0 < a < n$ and $p \nmid a$ and $q \nmid a$