

**Using Mathematica to solve  $x^k = b \pmod{m}$**

**Let ' s try to solve  $x^{113} = 491 \pmod{1219}$ .**

**Let ' s first see if there is a solution.**

```
In[15]:= GCD[491, 1219]
```

```
Out[15]= 1
```

```
In[16]:= EulerPhi[1219]
```

```
Out[16]= 1144
```

```
In[17]:= GCD[113, 1144]
```

```
Out[17]= 1
```

**Since  $\gcd(b, m) = 1$  and  $\gcd(k, \phi(m)) = 1$  there is a solution.**

**We can use the ExtendedGCD command to find  $u$  such that  $k * u + \phi(m) * v = 1$ .**

```
In[18]:= ExtendedGCD[113, 1144]
```

```
Out[18]= {1, {81, -8}}
```

**This says  $113 * 81 + 1144 * (-8) = 1$ . So  $113 * 81 = 1 \pmod{1144}$ . Let ' s check this.**

```
In[20]:= Mod[113 * 81, 1144]
```

```
Out[20]= 1
```

**So  $u = 81$  and we calculate  $b^u \pmod{m}$ .**

```
In[21]:= PowerMod[491, 81, 1219]
```

```
Out[21]= 807
```

**So 807 should be our solution. Let ' s check.**

```
In[22]:= PowerMod[807, 113, 1219]
```

```
Out[22]= 491
```

**It is. DONE !**