

FACTORING AND PRIMALITY USING MATHEMATICA

The following command gives a random integer.

```
In[50]:= Random[Integer, {100000, 999999}]
```

```
Out[50]= 497512
```

We can factor an integer using the following command.

```
In[51]:= FactorInteger[497512]
```

```
Out[51]= {{2, 3}, {62189, 1}}
```

This means the factorization is $2^3 * 62189$, and 62189 is prime.

Let ' s try a few larger integers

```
In[13]:= Random[Integer, 10^19, 9 * 10^20]
```

```
Out[13]= 1240271482892295188
```

```
In[14]:= FactorInteger[%]
```

```
Out[14]= {{2, 2}, {183462767, 1}, {1690086091, 1}}
```

You can use the following command to test if an integer is prime or not.

```
In[15]:= PrimeQ[121480776034706046820005461]
```

```
Out[15]= True
```

Fermat once conjectured numbers of the form $2^{(2^n)} + 1$ are all prime. Let ' s look at one.

```
In[16]:= 2^(2^7) + 1
```

```
Out[16]= 340282366920938463463374607431768211457
```

```
In[17]:= PrimeQ[2^(2^7) + 1]
```

```
Out[17]= False
```

Fermat was wrong. He didn't have a computer so probably wasn't able to test one this large.

We can use Mathematica to factor it for us.

```
In[39]:= FactorInteger[340282366920938463463374607431768211457]
```

```
Out[39]= {{59649589127497217, 1}, {5704689200685129054721, 1}}
```

Suppose we try a larger one,

```
In[18]:= 2^(2^10) + 1
```

```
Out[18]= 179769313486231590772930519078902473361797697894230657273430081157732675805500963132·  
70847732240753602112011387987139335765878976881441662249284743063947412437776789342·  
48654852763022196012460941194530829520850057688381506823424628814739131105408272371·  
63350510684586298239947245938479716304835356329624224137217
```

You can use the percent symbol % to denote the result of the previous calculation.

```
In[19]:= FactorInteger[%]
```

If you want to abort a calculation hit Command - period (at least on Mac's).

The PrimeQ command works faster than the FactorInteger command.

```
In[20]:= PrimeQ[2^(2^10) + 1]
```

```
Out[20]= False
```

But if an integer is really large *Mathematica* may have trouble factoring it. Consider the following product of two large prime numbers.

```
In[7]:= PrimeQ[5992830235524142758386850633773258681119]
```

```
Out[7]= True
```

```
In[8]:= PrimeQ[5991810554633396517767024967580894321153]
```

```
Out[8]= True
```

```
In[9]:= 5992830235524142758386850633773258681119 * 5991810554633396517767024967580894321153
```

```
Out[9]= 35907903457339702104254935751957912816937102439666041584158089414566285603410207
```

```
In[10]:= FactorInteger[
    35907903457339702104254935751957912816937102439666041584158089414566285603410207]
```

Note that Mathematica has trouble factoring this, even though it just multiplied the two primes together !

Let ' s try the PrimeQ command again :

```
In[21]:= PrimeQ[
    35907903457339702104254935751957912816937102439666041584158089414566285603410207]
```

```
Out[21]= False
```

How can Mathematica tell so quickly that the integer isn ' t prime without factoring it? We will learn how it does this. For more info we can load the PrimeQ package as below.

```
In[28]:= << NumberTheory`PrimeQ`
```

Aside : You must load the package before you type the command ProvablePrimeQ below. If you first type it by mistake you have to type the following.

```
In[30]:= Remove["ProvablePrimeQ"]
```

The following command asks if Mathematica can prove if the number is prime or composite. True means it can prove it is prime. False means it can prove it is composite.

```
In[31]:= ProvablePrimeQ[
    35907903457339702104254935751957912816937102439666041584158089414566285603410207]
```

```
Out[31]= False
```

Mathematica can tell us how it proved the number was composite by the following command.

```
In[32]:= PrimeQCertificate[
    35907903457339702104254935751957912816937102439666041584158089414566285603410207]
```

```
Out[32]= {2, 35907903457339702104254935751957912816937102439666041584158089414566285603410206,
    35907903457339702104254935751957912816937102439666041584158089414566285603410207}
```

The output {a, b, n} means the value of $a^b \pmod n$ determines the number is composite. The above says to compute $2^{(n-1)} \pmod n$. We can compute $a^b \pmod n$ by the command Powermod[a, b, n].

```
In[33]:= PowerMod[2,  
35907903457339702104254935751957912816937102439666041584158089414566285603410206,  
35907903457339702104254935751957912816937102439666041584158089414566285603410207]
```

```
Out[33]= 7016355335942126924211441982233147388320749784319983834115799312745415243951476
```

We will later learn why this implies the number is not a prime. Here is another example of a number which is composite for a different reason.

```
In[34]:= PrimeQCertificate[1195068768795265792518361315725116351898245581]  
{1195068768795265792518263537659322626328455738,  
2, 1195068768795265792518361315725116351898245581}
```

```
Out[34]= {1195068768795265792518263537659322626328455738,  
2, 1195068768795265792518361315725116351898245581}
```

This to compute $a^2 \pmod n$, with a the first number. We can do this with the regular Mod command

```
In[36]:= Mod[1195068768795265792518263537659322626328455738^2,  
1195068768795265792518361315725116351898245581]
```

```
Out[36]= 1
```

Note that $a^2 \pmod n$ is 1. We will learn why this implies n is not prime.

Suppose we look at a prime number, i.e. one of the ones above.

```
In[37]:= ProvablePrimeQ[48889032896862784894921]
```

```
Out[37]= True
```

```
In[38]:=
```

```
PrimeQCertificate[48889032896862784894921]
```

```
Out[38]= {{CertificatePrime → 48889032896862784894921,  
CertificatePoint → PointEC[6, 36945297602473259940164,  
3880081975941490861960, 14226967245118799770145, 48889032896862784894921],  
CertificateK → 5566464, CertificateM → 48889032896979841314816,  
CertificateNextPrime → 8782780755786769, CertificateDiscriminant → -7},  
{CertificatePrime → 8782780755786769, CertificatePoint →  
PointEC[2, 5066890707354902, 3624639676991363, 8271613621852088, 8782780755786769],  
CertificateK → 4473296, CertificateM → 8782780915918192,  
CertificateNextPrime → 1963380227, CertificateDiscriminant → -7},  
1963380227, 2, {2, {31, 3, {2, {3, 2, {2}}, {5, 2, {2}}}},  
{31667423, 5, {2, {521, 3, {2, {5, 2, {2}}, {13, 2, {2, {3, 2, {2}}}}}},  
{30391, 3, {2, {3, 2, {2}}, {5, 2, {2}}, {1013, 3,  
{2, {11, 2, {2, {5, 2, {2}}}}, {23, 5, {2, {11, 2, {2, {5, 2, {2}}}}}}}}}}}}}}}}
```

The proof that a number is prime is much more complicated and we won't be able to explain this in our course. References are given in the Mathematica Help Index.