

Here we give some examples of using Jacobi symbols and Euler ' s Criterion to show an integer is composite. The idea is that if a large odd integer  $n$  fails to satisfy Euler ' s Criterion, i.e. if  $a^{(n-1)/2}$  is NOT congruent to the Jacobi Symbol  $(a/n)$ , then  $n$  MUST be composite. This is called the Solovay - Strassen Probabilistic Primality test, which I will abbreviate to SS test.

If the congruence does hold, then the probability that  $n$  is composite is less than  $1/2$ , and if the congruence holds for  $k$  different values of  $a$  then the probability that  $n$  is composite is less than  $1/2^k$ . Thus if an integer passes the test for a large number different  $a$  ' s it is probably prime (with the probability of error being  $1/2^k$ ).

```
In[145]:= 1 + 1
```

```
Out[145]= 2
```

```
In[153]:=
```

```
    n = 1857241
```

```
Out[153]= 1857241
```

```
In[154]:=
```

```
    PowerMod[2, (n - 1) / 2, n]
```

```
Out[154]= 1
```

```
In[155]:= JacobiSymbol[2, n]
```

```
Out[155]= 1
```

It passes the test. So one might think the probability that  $n$  is composite is less than  $1/2$ . But perhaps we shouldn ' t view 2 as a random integer  $< n$ . Instead let ' s try a random integer  $< n$ .

```
In[156]:=
```

```
    Random[Integer, {1, n}]
```

```
Out[156]= 1301700
```

```
In[157]:=
```

```
    PowerMod[1301700, (n - 1) / 2, n]
```

```
Out[157]= 1
```

```
In[158]:=
```

```
    JacobiSymbol[1301700, n]
```

```
Out[158]= -1
```

Here we see that the power and the Jacobi Symbol do NOT agree . This tells us that  $n$  is composite.

Here is another one to try :

```
In[163]:=
      n = 14469841
```

```
Out[163]= 14469841
```

```
In[167]:= Random[Integer, {1, n}]
```

```
Out[167]= 5855355
```

```
In[168]:=
      PowerMod[5855355, (n - 1) / 2, n]
```

```
Out[168]= 1
```

```
In[169]:=
      JacobiSymbol[5855355, n]
```

```
Out[169]= 1
```

**The power and the Jacobi symbol agree,  
so the probability that n is composite is  $< 1/2$ . Let 's try another value.**

```
In[170]:=
      Random[Integer, {1, n}]
```

```
Out[170]= 5743676
```

```
In[171]:=
      PowerMod[5743676, (n - 1) / 2, n]
```

```
Out[171]= 1
```

```
In[172]:=
      JacobiSymbol[5743676, n]
```

```
Out[172]= 1
```

**Now the probability that n is composite is  $< 1/2^2$ , i.e.  $< 1/4$ . Let 's try another value.**

```
In[173]:=
      Random[Integer, {1, n}]
```

```
Out[173]= 14258763
```

```
In[174]:=
      PowerMod[14258763, (n - 1) / 2, n]
```

```
Out[174]= 1
```

```
In[175]:=
      JacobiSymbol[14258763, n]
```

```
Out[175]= -1
```

**The power and the Jacobi Symbol disagree for this value, hence n must be composite.**