Lecture 14 - The Miller - Rabin primality test

Recall last time that we spoke about Fermat's primality test, which *rules out primes* rather than showing numbers are primes. If n is a prime, then Fermat's little theorem asserts that a^n is congruent to a mod (n) for any integer a. Of course, if a and n have a common factor, then n is not prime (unless n divides a), and typically we are in a situation where it is not immediately obvious whether or not n is prime.

We saw you could tell certain numbers are composite using this test. For example

In[4]:=
```
PowerMod[2, 91, 91]
```

Out[4]=
```
37
```

shows that 2^{91} is congruent to 37, rather than 2 (mod 91), so 91 is not prime ($91 = 13 \times 7$). We can conclusively conclude that 91 is not prime. However, sometimes things go wrong:

In[3]:=
```
PowerMod[3, 91, 91]
```

Out[3]=
```
3
```

This means that 91 passes this naive primality test, even though 91 is not prime. The terminology is that "2 is a wtiness" for the compositeness of 91, but that 3 is not.

A naive hope is that ever composite number has lots of witnesses to its compositeness, but this turns out to be very false for certain numbers, called Carmichael numbers, the smallest of which is 561.

In[7]:=
```
Table[{a, PowerMod[a, 561, 561]}, {a, 10}] // TableForm
```

Out[7]//TableForm=

1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10

Not only is a^{561} congruent to a for these a from 1 to 10, it actually holds for all integers! This is a bad situation: 561 appears to be a "pseudoprime" as far as the Fermat test goes.

There are in fact better tests that work in about the same amount of time,

but they are more complicated. Here I shall explain examples of how the Miller – Rabin primality test works. We consider a number n, and a witness a. Before doing this, we should first check that n isn't divisible by some small primes, and that a and n are relatively prime to each other (if this is the case, the test below doesn't work right -- not to mention completely unnecessary).

We factor n – 1 as a power of 2 times an odd number, $n - 1 = 2^k q$, q odd. Let b be congruent to a^q mod n. If b is congruent to 1 mod n, then we give up. We successively look at b, b^2, b^4, b^8, b^{16}, ... and make sure that we do not have – 1 until we get to b^{k-1}. If this is the case, then we showed mathematically that n cannot be prime. We say "b is a Miller–Rabin witness for the compositeness of n". There may be "false positives" for this test, but they are rare : at most 25 % of random a's will be false positives (this can be rigorously proven). So executing this test, say, 100 times that a numbe is composite with very high probability 2^{-100}.

Here is some mathematica code :

In[2]:=
```
MillerRabin[n_, a_] := (k = 0; q = n - 1; While[EvenQ[q], q = q / 2; k = k + 1];
  b = PowerMod[a, q, n]; If[b == 1, Print["b is 1"]; Return["fail"]];
  TableForm[Table[b = PowerMod[b, 2, n]; {i, b}, {i, 2, k - 1}]])
```

These are the book' s examples :

In[34]:=
```
MillerRabin[561, 2]
```

Out[34]//TableForm=

2	166
3	67

In[36]:=
```
MillerRabin[172 947 529, 17]
```

```
b is 1
```

Out[36]= fail

In[37]:=
```
MillerRabin[172 947 529, 3]
```

Out[37]//TableForm=

2	1

In[38]:=
```
MillerRabin[172 947 529, 23]
```

Out[38]//TableForm=

2	2 257 065

More examples :

In[50]:=
```
MillerRabin[1001, 911]
```

```
b is 1
```

Out[50]= fail

In[3]:=
```
MillerRabin[1001, 729]
```

```
b is 1
```

Out[3]=
```
fail
```

In[52]:=
```
Position[Table[MillerRabin[1001, a], {a, 1, 1001}], "fail"]
```

```
b is 1
b is 1
b is 1
b is 1
b is 1
```

Out[52]=
```
{{1}, {92}, {456}, {729}, {911}}
```

```
(* Only 5 bad ones *)
```

Let' s try a bigger example

In[1]:=
```
Prime[100] Prime[120]
```

Out[1]=
```
356 519
```

In[4]:=
```
Count[Table[MillerRabin[356 519, a], {a, 1, 356 519}], "fail"]
```

```
b is 1
```

Out[4]=
```
1
```

This shows that only one of the a’s fails to witness the compositeness of this large number.