Math 640:348 Prof. Kontorovich Spring 2015, 3/27 lecture

We will try to find a prime of size about a million by the Miller-Rabin test

First try numbers of the form

```
In[1]:= n = 2 × 3 × 5 × 7 × 11 × 13 j + 23
Out[1]= 23 + 30 030 j
```

because these are guaranteed to be coprime to 2, 3, 5, 7, 11, and 13, so we have slightly better odds of finding a prime. (This is sometimes called “pre-sieving”.) Let’s start, say, with

```
In[2]:= j = 200;
```

so that n is

```
In[3]:= n
Out[3]= 6 006 023
```

First we write n as 2^k r with r odd.

```
In[4]:= r = (n - 1) / 2
Out[4]= 3 003 011
```

We only took out one power of 2, so can only square once.

Now let’s take a random number and test whether it is a witness, say,

```
In[5]:= a = 2;
        PowerMod[a, n - 1, n]
Out[6]= 2 311 920
```

Aha, so 2 is already a “Fermat witness” for the compositeness of n, and we are now certain that it is not prime.

Try another value of j

```
In[7]:= j = 201;
```

Then n is

```
In[8]:= n
Out[8]= 6 036 053
```

Again we compute r, the odd part of n-1

```
In[9]:= r = (n - 1) / 2
Out[9]= 3 018 026
```

Nope, take out more 2's

```
In[10]:= r = (n - 1) / 2^2
Out[10]= 1 509 013
```

Ok good, so when we get to the squaring step, we will be able to square twice.

Again let's try as our first witness

```
In[11]:= a = 2;
         PowerMod[a, n - 1, n]
Out[12]= 1 853 105
```

And again we immediately find that n is composite, since a^(n-1) is not 1 mod n.

Increment j again

```
In[13]:= j = 202;
         n
Out[14]= 6 066 083
```

Now compute r

```
In[15]:= r = (n - 1) / 2
Out[15]= 3 033 041
```

So we will only be able to square once (which by Matt's observation means we don't need to square at all -- if a^r is not +/-1, then n must be composite). Trying our first witness:

```
In[16]:= a = 2;
         PowerMod[a, n - 1, n]
Out[17]= 1
```

Ok, this n might finally be prime. So begin the Miller-Rabin challenge. Raise a to the r mod n:

```
In[18]:= b = PowerMod[a, r, n]
Out[18]= 6 066 082
```

Looks random at first, but no! That's just n-1, i.e., -1. Just for fun, let's square b

```
In[19]:= b1 = PowerMod[b, 2, n]
Out[19]= 1
```

Of course, that's what it had to come out to. So the value a=2 does not give us a witness for the compositeness of n. With "75% certainty", n is prime. Let's try another (more random) value

```
In[20]:= a = 31 231;
         PowerMod[a, n - 1, n]
Out[21]= 1
```

And compute b

```
In[22]:= b = PowerMod[a, r, n]
Out[22]= 1
```

So this value of a is also not a witness. Now we are

```
In[23]:= N[1 - (1 / 4) ^2]
Out[23]= 0.9375
```

"93% certain" that n is prime. Another random value

```
In[24]:= a = 3121;
         PowerMod[a, n - 1, n]
Out[25]= 1

In[26]:= b = PowerMod[a, r, n]
Out[26]= 6 066 082
```

With 3 witnesses, we are

```
In[27]:= N[1 - (1 / 4) ^3]
Out[27]= 0.984375
```

“98% certain” that n is prime. If we tried another 97 witnesses, all of whom failed to force the compositeness of n, we would know that n is prime with “probability”

```
In[28]:= N[1 - (1 / 4) ^100, 100]
Out[28]= 0.9999999999999999999999999999999999999999999999999999999999993776984722138858292\
 85593594621987575940 97
```

Indeed,

```
In[29]:= PrimeQ[n]
Out[29]= True
```

and we’ve found our desired large prime.

Now

Change this file and follow along with Example 3.19 on p. 128 in the book, as well as Example 3.22 on p. 130.