

Computer Tutorial 11

Start MAGMA and type `load "tut11data.txt";`.

1. According to the Prime Number Theorem, the probability that a random number less than 10^{100} is prime is about $1/100 \ln(10)$, which is about 0.004343. (Get Magma to confirm this value: type `1/(100*Log(10));`). How many random numbers less than 10^{100} will you have to choose to have a better than even chance of getting a prime?
2. The file `tut11data.txt` that you loaded defines two functions: `choosesafeprime` and `prdl`. Type `p,b:=choosesafeprime(15);`. Then `p` will be a safe prime of 15 bits and `b` a primitive root mod `p`. (The function chooses primes randomly until it finds one that is a safe prime, and then tries 2, 3, ... , until it finds a primitive root.) Now choose a random number less than `p` via the command `a:=Random(p-1);`. The function `prdl` will compute the discrete log of `a` to the base `b` using the Pollard Rho method, printing out the results of the calculations at each step. Type `prdl(a,b,p);`, and see how many steps the algorithm takes. (I claimed in lectures that the expected number of steps is of the order of \sqrt{p} .)

Repeat the experiment a few times, possibly increasing the size of the prime a little. (Note: this implementation will only work for safe primes.) Use `Modexp` to check the answers.

3. Try the following MAGMA commands:

```
Modexp(3,2^(2^1),2^(2^1)+1);
Modexp(3,2^(2^2),2^(2^2)+1);
Modexp(3,2^(2^3),2^(2^3)+1);
Modexp(3,2^(2^4),2^(2^4)+1);
```

Do you think you can guess what `Modexp(3,2^(2^5),2^(2^5)+1);` will return? Caution: think before you guess

4. Fermat's Little Theorem tells us that if `n` is a prime number and `a` any positive integer less than `n` then `Modexp(a,n-1,n)` will return 1. In Exercise 4 of Computer Tutorial 6 we found by experimentation that if `Modexp(a,n-1,n)` returns 1 then it is rather likely that `n` is prime. (We assume that `a` is greater than 1 and less than `n-1`.) We may encounter a composite number `n` such that `Modexp(a,n-1,n)` equals 1 for some `a`, but then it is very unlikely that `Modexp(a,n-1,n)` will also be equal to 1 for another value of `a`. And very very unlikely that it will be equal to 1 for three values of `a`.

Find all the odd composite integers `n` less than 1000 such that `Modexp(2,n-1,n)` returns 1. Here is a suitable loop:

```
for n:=3 to 999 by 2 do
  if Modexp(2,n-1,n) eq 1 then
    if not IsPrime(n) then
      print n;
    end if;
  end if;
end for;
```

5. You should have discovered that $2^{340} \equiv 1 \pmod{341}$. If 341 were prime it would follow that $2^{170} \equiv \pm 1 \pmod{341}$. (Why?) Check that in fact $2^{170} \equiv 1 \pmod{341}$. But check that $2^{85} \not\equiv \pm 1 \pmod{341}$, and deduce that 341 is not prime. Do similar calculations for 561 and 645 to show that they also are composite.

Let n be an odd positive integer and 2^k the highest power of 2 dividing $n - 1$. Thus $n - 1 = 2^k m$, with m odd. Suppose first that n is prime, and let a be any integer such that $n \nmid a$. Then $a^{2^k m} \equiv 1 \pmod{n}$ (by Fermat), and so $a^{2^{k-1} m} \equiv \pm 1 \pmod{n}$. If $a^{2^{k-1} m} \equiv 1$ and $k - 1 > 0$ then the same reasoning gives $a^{2^{k-2} m} \equiv \pm 1$. Continuing in this way, one can find the smallest i such that $a^{2^i m} \equiv 1 \pmod{n}$. If $i > 0$ then the choice of i tells us that $a^{2^{i-1} m} \not\equiv 1$, and since $(a^{2^{i-1} m})^2 = a^{2^i m} \equiv 1$ it follows that $a^{2^{i-1} m} \equiv -1$. So either $a^m \equiv 1 \pmod{n}$ (corresponding to the case $i = 0$) or else there is a j such that $a^{2^j m} \equiv -1 \pmod{n}$.

This conclusion was based on the assumption that n is prime. So if we want to show that n is not prime, it is sufficient to find an a between 1 and $p - 1$ such that the above condition is not satisfied. That is, n is not prime if $a^m \not\equiv 1$ and there is no j such that $a^{2^j m} \equiv -1$. Such an a is called a *witness to the compositeness of n* . If a is not a witness to the compositeness of n then n is called a *strong pseudoprime to the base a* .

6. Show that 25326001 is a strong pseudoprime to the bases 2, 3 and 5. (It is the smallest such number that is not actually prime.) Show, however, that it is not a pseudoprime to the base 7.

There is a theorem of Rabin that says that if n is a strong pseudoprime to the base a for more than $n/4$ bases a between 1 and $n - 1$ then n is prime. So if n is composite and a is randomly chosen in $\{1, 2, \dots, n - 1\}$ then the probability that n is a strong pseudoprime to the base a is no more than $1/4$ (usually a lot less than this). So the probability of a composite number being a strong pseudoprime to 20 different bases is at most $(1/4)^{20} \approx 10^{-12}$. (MAGMA's `IsProbablyPrime` function returns true only if the number in question is a strong pseudoprime to 20 different randomly chosen bases. I don't believe that it has ever given a "false positive".)

7. Find all odd composite n less than 10000 such that $2^{n-1} \equiv 1 \pmod{n}$ and $3^{n-1} \equiv 1 \pmod{n}$. Show that none of them are strong pseudoprimes to the base 2. (Your loop should start with

```
for n:=3 to 9999 by 2 do
  if not IsPrime(n) then
    if Modexp(2,n-1,n) eq 1 then
      if Modexp(3,n-1,n) eq 1 then
        n;
```

etc.. You will find that there are seven numbers to examine more closely.)

8. Returning to Exercise 3, show that 3 is a witness to the compositeness of the Fermat numbers $2^{2^i} + 1$ for all $i \in \{5, 6, 7, 8, 9, 10\}$.