ELEMENTARY NUMBER THEORY

HOMEWORK 3

(1) Select two random primes p, q of about 10 to 20 digits, form $N = pq$, select e coprime to $(p-1)(q-1)$, and send the pair (N, e) to another student in class; similarly, he will send you his pair.

Now exchange messages using RSA. Write down the encrypted messages c you receive, compute an inverse d of e mod $(p-1)(q-1)$ from a Bezout representation, and decode the messages.

You will need pari for this task. For choosing a 11-digit prime, pick a 11-digit random number like 123456789010 (of coourse this is not random - I'm merely illustrating the idea) and then type `p=nextprime(123456789010)` into `pari`. The answer will be $p = 12345678923$. Pick q, and try a few random values e (they need to be odd – why?) coprime to $(p-1)(q-1)$; you can check this by typing in `gcd(e,(p-1)*(q-1))`.

After you've sent off (N, e), compute a Bezout representation with
`bezout(e,(p-1)*(q-1))`;
to understand the output, type in `?bezout`. Make sure that d is positive; if not, replace it by $d + (p-1)(q-1)$.

Finally, computing powers modulo N is done via

```
c = Mod(m,N)^e
```

If you type in

```
c = Mod(m^e,N)
```

instead, you will get the same result or an error message, depending on the size of e. Can you explain this?

(2) Show that the numbers $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17, \ldots, F_n = 2^{2^n} + 1$ are pairwise coprime.

Deduce that there are infinitely many primes.

(3) Apply the Euclidean algorithm to the pair $(77, 101)$, use the calculation to produce a Bezout representation of the gcd, and finally give the inverse of 77 mod 101.