ELEMENTARY NUMBER THEORY

HOMEWORK 5

(1) Download a windows executable version of pari from my webpage
`http://www.fen.bilkent.edu.tr/~franz/algeo05.html`
or, better yet, an updated full version from the pari website
`ftp://megrez.math.u-bordeaux.fr/pub/pari/windows`
Get familiar with it by doing a few calculations:

(a) Compute $2^{340} \bmod 341$. The residue class $2 \bmod 341$ is represented by `Mod(2,341)`. What is the difference between `Mod(2^340,341)` and `Mod(2,341)^340` (the results are the same, but the calculations differ). If you can't see what's going on, compute $2^{p-1} \bmod p$ for $p = 898476298723511$.

(b) Use pari to show that $\gcd(2^{125}-1, 2^{75}-1) = 2^{25}-1$ (check first what `gcd(15,21)` is doing). Can you guess a formula for $\gcd(2^a-1, 2^b-1)$?

(c) Type in `?bezout` and then compute the Bezout representation for the gcd-calculation above. In general you can copy results from the pari window to a file by rightclicking the blue frame on top and scrolling down the menu.

(d) Type in `factor(35)` and see what happens. The guy who first factored $2^{67}-1$ said it took him three years of sundays to find the factorization. Factor the number using pari.

(e) What does the command `nextprime` do? Find the smallest primes above 10^{10} and 10^{100}.

(2) Now exchange an RSA-encrypted message with your partner. Pick two primes p, q with at least 10 digits and form $N = pq$. Pick an exponent E coprime to $(p-1)(q-1)$. Pick a message consisting of at most 10 letters (if you want to send more, break them up into smaller pieces). Encode them and send N, E and the encrypted message to your partner.

Your second job is to decode the message you receive from him/her by factoring his N and finding the inverse D of $E \bmod (p-1)(q-1)$.

The homework will be collected in class next Wednesday.