ELEMENTARY NUMBER THEORY

HOMEWORK 5

(1) (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).

We find that $2^{340} \equiv 1 \bmod 341$. Note that $341 = 11 \cdot 31$ is not prime. Here is a general method for constructing such "pseudoprimes": let $p > 3$ be a prime and put $q = (2^{2p} - 1)/3$. Then q is not prime because $q = (2^p - 1)(2^p + 1)/3$. On the other hand we have $2^{2p} \equiv 1 \bmod q$ and $q \equiv 1 \bmod 2p$ (clearly $q \equiv 1 \bmod 2$, $2^{2p} \equiv 4 \bmod p$ by Fermat's Little Theorem, hence $q = \frac{1}{3}(2^{2p} - 1) \equiv 1 \bmod 2p$). Thus $2p \mid q - 1$, and therefore $2^{q-1} \equiv 1 \bmod q$.

(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 $\gcd(2^a - 1, 2^b - 1)$?

In general we have $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. There is a simple proof using the Euclidean algorithm. A similar formula (and a similar proof) hold for Fibonacci numbers, by the way.

(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.

$2^{25-1} = 2^{75} + 1(2^{75} - 1) - 2^{25}(2^{125} - 1)$.

(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.

$2^{67} - 1 = 193707721 \cdot 761838257287$

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

It computes the smallest prime greater than or equal to the input.

(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 $E \bmod (p-1)(q-1)$.

Almost all of you did not do this correctly. If you use 20-digit keys, you should concatenate 10 letters into one word and encrypt it, not encrypt the individual letters because such a system can be broken easily (I mean, every A gets transmitted as 1, and equal letters produce equal codes). Thus if you pick $N = 10821521144116749678691$ and $E = 2345$,and if your message is METAL STORM, then $T = 13052001122719201518 13$, the encrypted message is $C = 4561092614508840795 58$.

For decoding, compute $D = -5676107038878579428 71$ (if you want a positive value, replace D by $D + (p-1)(q-1)$) from the Bezout representation of E and $(p1-)(q-1)$, and then $C^D \equiv T \bmod N$.