Recitation 4: Power Set, Coprimes, Euler totient, RSA

Instructions: Submit to gradescope by the deadline.

Problem 1 : Power Set(a), Coprimes

i. Prove that 22^{12001} has a multiplicative inverse modulo 175

ii. What is the multiplicative $order(22) \mod 175$?

iii. What is the division remainder of 22^{12001} by 175?

iv. ★ What is the last digit of $7^{7^{7^7}}$?
Hint: Compute the powers of 7 mod 10. If $order(7) = v$, it comes down to finding $7^{7^7} \mod v$ and so forth.

Problem 2 Prove that $n^{13} \equiv n \mod 10$ for any integer n. Do this in two separate cases: for n coprimes and non-coprimes with 10.

Problem 3 Fermat's primality test For each one of these n test primality by randomly picking several $a \in \mathbb{Z}_n$ and check if $a^{n-1} \equiv 1 \mod n$. As discussed in class, if any of the tests fail n is certainly not prime; but if all tests succeed there is a high chance (not guaranteed) for n to be prime. You can use a calculator for power and modulo.

i. $n = 1429$; try $a = 2, 3, 5, 7$

ii. $n = 6601$; try $a = 2, 3, 5$

iii. $n = 1105$; try $a = 2, 3, 7, 11$

Problem 4 RSA Simulate RSA. Form teams of 2-3 students.

i. choose your primes p, q in range 10-40. Compute $n = pq$ and $\varphi(n) = (p-1)(q-1)$.

ii. choose the public key e (try $e = 3, 5, 7..$) such that $\gcd(e, \varphi(n)) = 1$. Write on the board your team name, together with your n, e. Keep everything else secret.

iii. compute your private key d that is the inverse of e mod $\varphi(n)$. You can use Extended Euclid or a calculator online (but make sure $ed \equiv 1 \mod \varphi(n)$)

iv. Pick one of these messages m and send the encrypted version to another team. The encryption is the integer $\widehat{m} = m^e \mod n$ using the published (n, e) of the team receiving the encrypted messasge. Other teams can send encryted messages to you (using your n, e)

m=2: Greetings and salutations!
m=3: Yo, wassup?
m=4: You guys are slow!
m=5: All your base are belong to us.
m=6: Someone on our team thinks someone on your team is cheating.
m=7: You are the weakest link. Goodbye.

v. decrypt the message received and send it back. The decryption is computed as the integer $m = \widehat{m}^d \mod n$. Other tems can decypt encrypted message you sent to them and send it back to you.

Problem 5(optional, no credit) ★★★
Lets denote $\pi(n)$ = the number of primes up to n. For example $\pi(10) = 4$ because there are 4 primes less or equal to 10 (2,3,5,7). Prove that
$\pi(n) > \frac{n}{3 \ln n}$
which means there are quite a few prime numbers.