EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 2 : 20 points March 28, 2019

---

1. Let G be a group whose identity element is e.
   (a) (2 points) Prove that if H and K are finite subgroups of G whose orders are relatively prime, then $H \cap K = \{e\}$.
   (b) (2 points) Let $g \in G$ be an element of order $k \geq 1$. If $g^n = e$ for some positive integer n, prove that k divides n.

2. (a) (2 points) Find the last two digits of the number 123^{403}.
   (b) (2 points) Suppose an RSA public key is $(N, e) = (55, 27)$. If the ciphertext is $c = 4$, find the corresponding plaintext m in $\mathbb{Z}_N^*$.

3. (4 points) Find all solutions of the following equation in $\mathbb{Z}_{77}$.

$$x^2 + 3x + 4 = 0 \bmod 77.$$

4. Let $N = pq$ where p, q are distinct n-bit odd primes.
   (a) (2 points) Prove that $\gcd(N, \phi(N)) = 1$.
   Hint: Since p, q are n-bit odd primes, their binary representations are of the form $p = 1\|p'\|1$ and $q = 1\|q'\|1$ where $p', q' \in \{0,1\}^{n-2}$. The $\|$ represents the concatenation operator.
   (b) (1 point) Prove that the order of $N + 1$ in $\mathbb{Z}_{N^2}^*$ is N.
   (c) (1 point) Consider the map f with domain $\mathbb{Z}_N \times \mathbb{Z}_N^*$ given by

$$f(a, b) = \left[(N+1)^a \cdot b^N\right] \bmod N^2.$$

   Prove that the range of f is $\mathbb{Z}_{N^2}^*$.
   (d) (4 points) Prove that the map f defined above is a bijection from $\mathbb{Z}_N \times \mathbb{Z}_N^*$ to $\mathbb{Z}_{N^2}^*$.