EE 720: Introduction to Number Theory and Cryptography (Autumn 2024)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 5: 20 points Date: October 24, 2024

1. [5 points] Let $p = rq + 1$ where p, q are primes. Then prove that

$$G = \left\{ h^r \bmod p \mid h \in \mathbb{Z}_p^* \right\}$$

is a subgroup of $\mathbb{Z}_p^*$ of order q.

2. [5 points] Consider the group G given in the previous question. Suppose there exists a non-identity element $h \in \mathbb{Z}_p^*$ such that $h^q = 1 \bmod p$. Prove that h is a generator of G. **Hint**: *You can use the fact that $\mathbb{Z}_p^*$ is cyclic without proof.*

3. [5 points] Suppose an RSA encryption scheme has public key $\langle N, e \rangle = \langle 2537, 13 \rangle$. Find the decryption exponent d.

4. [5 points] Prove that the El Gamal encryption scheme is not CCA-secure.