CS 70 Discrete Mathematics and Probability Theory
Fall 2016 Seshia and Walrand

Discussion 5B

1. **Repeated Squaring** Compute $3^{383} \pmod 7$. (Via repeated squaring!)

2. **Modular Potpourri**

   (a) Evaluate $4^{96} \pmod 5$

   (b) Prove or Disprove: There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod 6$.

   (c) Prove or Disprove: $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$

3. **Just a Little Proof**

   Suppose that p and q are distinct odd primes and a is an integer such that $\gcd(a, pq) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

4. **RSA Warm-Up**

   Consider an RSA scheme modulus $N = pq$, where p and q are prime numbers larger than 3.

   (a) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

   (b) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

   (c) What is the private key?

   (d) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message she sends using the public key?

   (e) Alice receives the message $y = 24$ back from Bob. What equation would she use to decrypt the message?