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. **Euler's totient function**

   Euler's totient function is defined as follows:

   $$\phi(n) = \mid \{i : 1 \leq i \leq n, \texttt{gcd}(n,i) = 1\} \mid$$

   In other words, $\phi(n)$ is the total number of positive integers less than n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

   For m,n such that $\texttt{gcd}(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

   (a) Let p be a prime number. What is $\phi(p)$?

   (b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

   (c) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod p$?
   (Hint: use Fermat's Little Theorem.)

   (d) Let b be a number whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
   Show that for any a relatively prime to b, the following holds:

   $$\forall i \in \{1, 2, \ldots, k\}, \ a^{\phi(b)} \equiv 1 \pmod{p_i}$$