Name: ____________________

Directions: Show all work. No credit for answers without work.

1. **[15 points]** Solve the following system of congruences.

$$x \equiv 1 \pmod{41} \qquad x \equiv 2 \pmod{25} \qquad x \equiv 3 \pmod{11}$$

2. **[10 points]** Let $n = 61 \cdot 67 = 4087$. Both 1 and -1 are solutions to $x^2 \equiv 1 \pmod{n}$. Describe how to find a third, distinct solution modulo n (do not actually find it), or explain why no additional solutions exist.

3. [**15 points**] Note that 149 is prime. Solve for x in $x^{39} \equiv 33 \pmod{149}$.

4. [**5 points**] Alice claims she has access to the private key (N, d) associated with the RSA public key (N, e). How can Alice prove this to Eve, an untrusted third party, without compromising the security of her private key or previously encrypted messages?

5. [**5 points**] To make an RSA public/private key pair, Bob picks $p = 83$ and $q = 67$. For his public exponent, Bob wants to pick e such that $36 \leq e \leq 44$. Which of these values, if any, is possible, and why?

6. Alice generates an RSA key pair with $N = pq = 47 \cdot 41 = 1927$ and $e = 9$.

   (a) [**9 points**] What is Alice's private key?

   (b) [**8 points**] Bob wishes to encrypt and send Alice the message $m = 1718$. What should he send?

   (c) [**8 points**] Alice receives the ciphertext $c = 981$ from Bob. What is the corresponding plaintext? You may find the following table of powers of c modulo N useful. The first few values have been filled in.

t	1	2	4	8	16	32	64	128	256	512	1024
$c^t \pmod N$	981	788	450	165	247	1272	1231				

7. Let $n = 481$ and let $a = 11$.

    (a) **[10 points]** Execute a Miller–Rabin primality test on n with base a. It may be useful to know that $a^{15} \equiv 369 \pmod{n}$.

    (b) **[5 points]** Is a a Miller–Rabin witness for n? What does this tell us about the primality of n? Explain.

8. **[10 points]** Let E be the elliptic curve $y^2 = x^3 - 4x + 19$, let $P = (-3, 2)$, and let $Q = (1, 4)$. Find PQ.