115A: Final Review Problems

1. Find integers x and y such that

$$130x + 151y = 1$$

2. (a) Let $i \geq 1$. Show that

$$\frac{10^i - 1}{9}$$

is an integer.

(b) Let $p \neq 2, 3, 5$ be a prime number. Show that p divides

$$\frac{10^{p-1} - 1}{9}$$

(c) Show that every prime $p \neq 2, 3, 5$ divides a number of the form

$$11 \cdots 1$$

3. (a) Find all solutions to

$$14x \equiv 38 \pmod{40}.$$

(b) Find all solutions to the system of linear congruences

$$\begin{aligned} 3x &\equiv 7 \pmod{10} \\ 4x &\equiv 1 \pmod{5} \end{aligned}$$

(c) Find all solutions to the system of linear congruences

$$\begin{aligned} x &\equiv 7 \pmod{8} \\ x &\equiv 3 \pmod{6} \\ x &\equiv 6 \pmod{9} \end{aligned}$$

4. (a) Calculate $\phi(7!)$.

(b) Suppose p and q are twin primes, i.e. $q = p + 2$. Show that

$$\phi(q) = \phi(p) + 2$$

(c) Suppose $n > 2$. Show that $\phi(n)$ is even.

5. Find the least non-negative residue of 3^{2011} modulo 22.

6. Let $n \geq 1$. Find
$$\gcd(n, 2n^2 + 1)$$

7. Let n be a positive integer. Suppose n is either not divisible by 5 or is divisible by 25. Show that $n^{41} \equiv n \pmod{75}$. Show that this is not true for all positive integers n.

8. Let p be a prime number greater than 2.

   (a) Show that $(p-2)! \equiv 1 \pmod{p}$.

   (b) Show that $(p-1)! \equiv p-1 \pmod{p(p-1)}$. *(Hint: use part (a) and the fact that $(p-1)! = (p-1)(p-2)!$)*

9. In an RSA cryptosystem, suppose $N = 71 \cdot 53 = 3763$ and $e = 9$. Describe how you would encode the credit card number 1234112024091746 using this cryptosystem (you need not complete all of the computations). Given that the encoded version of this credit card number is sent as the four messages P_1, P_2, P_3, P_4, describe how a receiver would decode to get the original credit card number.

10. (a) Solve the knapsack problem for the sequence $(2, 3, 7, 13, 28, 56, 117, 230, 500, 1000)$ and the number $S = 830$. Make sure to find all solutions.

    (b) Suppose you wanted to create a knapsack cryptosystem using the sequence from part (a). Describe one way in which you would do it (there are infinitely many correct answers here).

11. Mark each statement as True or False and give a quick explanation of why it is one or the other.

    (a) There are infinitely many primes that are at the same time 3 modulo 4 and 7 modulo 9.

    (b) If $\gcd(a, b) = \text{lcm}(a, b)$ then $a = b$.

    (c) There exists a multiplicative inverse of 3^{20} modulo $10^{50} - 1$.

    (d) If $n = ab$ then $\phi(n) = \phi(a)\phi(b)$.

    (e) The Diffie-Hellman key exchange was created to be able to use public key cryptosystems.

    (f) Ciphers like the Caesar cipher are difficult to decode and are still used in the modern world.