MATH 135: Extra Practice Set 8

These problems are for extra practice and are not to be handed in. Solutions will not be posted but, unlike assignment problems, they may discussed in depth on Piazza.

- The warm-up exercises are intended to be fairly quick and easy to solve. If you are unsure about any of them, then you should review your notes and possibly speak to an instructor before beginning the corresponding assignment.
- The recommended problems supplement the practice gained by doing the corresponding assignment. Some should be done as the material is learned and the rest can be left for exam preparation.
- A few more challenging extra problems are also included for students wishing to push themselves even harder. Do not worry if you cannot solve these more difficult problems.

Warm-up Exercises

1. Solve
$$\begin{aligned} x &\equiv 7 \pmod{11} \\ x &\equiv 5 \pmod{12} \end{aligned}$$
2. Given the public RSA encryption key $(e, n) = (5, 35)$, find the corresponding decryption key (d, n).
3. Express $\dfrac{2-i}{3+4i}$ in standard form.

Recommended Problems

1. Solve
$$\begin{aligned} 3x - 2 &\equiv 7 \pmod{11} \\ 5 &\equiv 4x - 1 \pmod{9} \end{aligned}$$
2. The Chinese Remainder Theorem deals with the case where the moduli are coprime. We now investigate what happens if the moduli are not coprime.
   (a) Consider the following two systems of linear congruences:
$$A: \begin{cases} n \equiv 2 \pmod{12} \\ n \equiv 10 \pmod{18} \end{cases} \qquad B: \begin{cases} n \equiv 5 \pmod{12} \\ n \equiv 11 \pmod{18} \end{cases}$$
   Determine which one has solutions and which one has no solutions. For the one with solutions, give the complete solutions to the system. For the one with no solutions, explain why no solutions exist.
   (b) Let a_1, a_2 be integers, and let m_1, m_2 be positive integers. Consider the following system of linear congruences
$$S: \begin{cases} n \equiv a_1 \pmod{m_1} \\ n \equiv a_2 \pmod{m_2} \end{cases}$$
   Using your observations in (a), complete the following two statements. The system S has a solution if and only if _____. If n_0 is a solution to S, then the complete solution is
$$n \equiv \_\_\_\_\_.$$

(c) Prove the first statement.

3. Solve $x^3 \equiv 17 \pmod{99}$.

4. Solve $x^3 - 29x^2 + 35x + 38 \equiv 0 \pmod{195}$.

5. Find the smallest positive integer a such that $5n^{13} + 13n^5 + a(9n) \equiv 0 \pmod{65}$ for all integers n.

6. Prove that for distinct primes p and q, $\left(p^{q-1} + q^{p-1}\right) \equiv 1 \pmod{pq}$.

7. A basket contains a number of eggs and, when the eggs are removed 2, 3, 4, 5 and 6 at a time, there are 1, 2, 3, 4 and 5 respectively, left over. When the eggs are removed 7 at a time there are none left over. Assuming none of the eggs broke during the preceding operations, determine the minimum number of eggs that were in the basket.

8. If a and b are integers, $3 \nmid a$, $3 \nmid b$, $5 \nmid a$, and $5 \nmid b$, prove that $a^4 \equiv b^4 \pmod{15}$.

9. Set up an RSA scheme using two-digit prime numbers. Select values for the other variables and test encrypting and decrypting messages.

10. Express the following complex numbers in standard form.

    (a) $\dfrac{(\sqrt{2} - i)^2}{(\sqrt{2} + i)(1 - \sqrt{2}i)}$

    (b) $(\sqrt{5} - i\sqrt{3})^4$

11. Prove the properties of complex arithmetic given in Proposition 1 in Chapter 30 of the course notes. Only one of the nine results is proved in the notes. A few others may have been proved in class.

12. Let $n \in \mathbb{N}$. Prove by induction that if $n \equiv 1 \pmod{4}$, then $i^n = i$.

Challenge(s)

1. Write a computer program to implement RSA encryption and decryption.