**Math 210, Spring 2019** **Jerry L. Kazdan**

# Problem Set 9

DUE: Thurs. April 18 in class. [Late papers accepted (without penalty) until 1:00 PM Fri.]

## Problems

1. Two cubic polynomials $y = ax^3 + bx^2 + cx + d$ and $y = \alpha x^3 + \beta x^2 + \gamma x + \delta$ are called *similar* if by using a horizontal shift: $x \to x - x'$, vertical shift: $y \to y'$ and a magnification $x \to \lambda x$, $y \to \lambda y$ ($\lambda > 0$). the polynomias agree.

   In class we showed that every quadratic polynomial $y = ax^2 + bx + c$ is similar to either $y = x^2$ or $y = -x^2$.

   Show that every cubic polynomial is similar to either a polynomial of the form $x^3 + rx$ or $-x^3 + rx$ for some choice of the constant $r$. [SUGGESTION: To get rid of the $bx^2$ term in a cubic polynomial $p(x)$ do a horizontal translation so that the inflection point (where $p''(x) = 0$) is on the vertical axis.

2. Using the Caesar cipher (shift by +3), encrypt the message ATTACK AT DAWN.

3. The ciphertext message LFDPH LVDZL FRQTX HUHG has been encrypted using the Caesar cipher. Decrypt it.

4. Compute the remainder when $3^{1000}$ is divided by 7.

5. Use the Euclidean algorithm to find the greatest common divisor $c$ of 252 and 198. Then use your computation to find integers $x$ and $y$ so that $252x + 198y = c$.

6. a) Find all the integers $x$, $y$ so that $4x + 13y = 1$.

   b) Find all the integers $x$, $y$ so that $4x + 13y = 3$.

7. In the group $Z_{14}^*$ of the invertible elements in $Z_{14}$, find the inverse of 11.

8. Find the greatest common divisor of 70, 98, and 105.

9. If $n = pq = 14,647$ and $\varphi(n) = 14,400$ find the primes $p$ and $q$. [HINT: You have two equations for the twp unknowns $p$ and $q$. They give you $pq$ amd $p + q$, and thus $(p - q)^2 = (p + q)^2 - 4pq$.]

10. Suppose a cryptanalyst discovers a message block P that is not relatively prime to the enciphering modulus $n = pq$ used in an RSA cipher. (She can confirm this by running the Euclidean algorithm.) Show that she can factor $n$. [HINT: The size of any message block must be less than $n$.]

[Last revised: April 12, 2019]