Math 261, Number Theory — Fall 2009–2010
Course website: `http://people.aub.edu.lb/~kmakdisi/`
Problem set 2, due Friday, October 23 at the beginning of class

Exercise 2.1: We have seen that the equation $ax + by = c$ (where a, b, c are given and x, y are unknowns) is solvable if and only if c is divisible by (a, b). Suppose that this is the case, and that $x = x_P, y = y_P$ is a particular solution.

Show that the general solution is then $x = x_P + b'k$, $y = y_P - a'k$ for arbitrary $k \in \mathbf{Z}$, where $d = (a, b)$, $a = da'$, and $b = db'$.

Exercise 2.2: a) Find all (integer) solutions of each of the following equations:

$$357x + 400y = 1, \qquad 57x + 105y = 0, \qquad 57x + 105y = 87.$$

b) Find all solutions of $6x+10y+15z = 103$. (Hint: $6x+10y$ can equal any even number $2w$.)

c) Given a, b, c, show that the equation $ax + by + cz = m$ is solvable if and only if m is a multiple of the GCD (a, b, c). (Bonus: find all the solutions.)

Exercise 2.3: Solve each of the following congruences:

$$357x \equiv 1 \pmod{400}, \qquad 57x \equiv 87 \pmod{105},$$

$$19x \equiv 4 \pmod{30}, \qquad 20x \equiv 4 \pmod{30}.$$

Exercise 2.4: Find all solutions to the following systems of linear equations $\pmod 9$. Hint: try to eliminate variables, but make sure that you always maintain an **equivalent** system of equations.

$$\begin{cases} 2x + y \equiv 5 & \pmod 9 \\ x + 4y \equiv 7 & \pmod 9 \end{cases}, \qquad \begin{cases} 2x + y \equiv 5 & \pmod 9 \\ x + 2y \equiv 7 & \pmod 9 \end{cases}, \qquad \begin{cases} 2x + y \equiv 5 & \pmod 9 \\ x + 2y \equiv 5 & \pmod 9 \end{cases}.$$

Exercise 2.5: a) Show that an integer is divisible by 11 iff the alternating sum of its digits is divisible by 11. For example, $3141 \equiv -3+1-4+1 \not\equiv 0 \pmod{11}$ but $31416 \equiv 3-1+4-1+6 \equiv 0 \pmod{11}$.

b) Show that a number $10a + b$ is divisible by 7 if and only if $a - 2b$ is divisible by 7. Deduce a test for divisibility by 7. (Hint: a is the number you get by "crossing out" the last digit of $10a + b$, and b is the last digit of $10a + b$.)

Exercise 2.6: a) Find the remainder of 2^{110236} divided by 5.

b) Find the remainder of 3^{110236} divided by 7.

Hints: show first that $2^4 \equiv 1 \pmod 5$, and $3^6 \equiv 1 \pmod 7$.

Exercise 2.7: a) Show that if p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ has no zero divisors. (In other words, $\overline{a}\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.)

b) Show that if p is a prime other than 2, then the equation $x^2 \equiv 4 \pmod p$ has exactly two solutions. However, give an example where $x^2 \equiv 3 \pmod p$ has no solutions.

c) Find all solutions to $x^2 \equiv 4 \pmod{15}$. (You may need to use trial and error.)

d) Find all solutions to $x^2 + 10x + 6 \equiv 0 \pmod{15}$. Hint: complete the square and use c).