Margaret Bilu
Office 604

bilu@cims.nyu.edu

Algebra homework 3
Congruences

Exercise 1. Describe the set $(\mathbf{Z}/12\mathbf{Z})^\times$. Give an inverse for each of its elements.

Exercise 2. Check 32 is invertible modulo 1265 and compute an inverse.

Exercise 3.

1. Find all integers $x \in \mathbf{Z}$ satisfying $9x \equiv 3 \pmod 5$.
2. Find all integers $x \in \mathbf{Z}$ satisfying $5x + 1 \equiv 4 \pmod{26}$.

Exercise 4.

1. Show that for any $a \in \mathbf{Z}$, the integer a^2 is congruent either to 0 or to 1 modulo 4.
2. Show that for any $a, b \in \mathbf{Z}$, the integer $a^2 + b^2$ cannot be congruent to 3 modulo 4.
3. Can 1735 be written as a sum of two squares?

Exercise 5. Show that the square of an integer never has 2,3,7 or 8 as its last digit. (Hint: work modulo 10)

Exercise 6 (Divisibility criteria)**.** Let $a \geq 1$ be an integer. We may write

$$a = 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10a_1 + a_0$$

for some $d \geq 0$ so that $a_0, \ldots, a_d$ are integers in the set $\{0, \ldots, 9\}$, with $a_d \neq 0$. The integers $a_d, \ldots a_0$ are the digits of the integer a. Show that:

1. The integer a is even if and only if its last digit a_0 is even.
2. The integer a is divisible by 5 if and only if its last digit a_0 is either 0 or 5.
3. The integer a is divisible by 4 if and only if the number $10a_1 + a_0$ given by its last two digits is divisible by 4.
4. The integer a is divisible by 3 if and only if the sum $a_d + \ldots + a_0$ of its digits is divisible by 3.
5. The integer a is divisible by 9 if and only if the sum $a_d + \ldots + a_0$ of its digits is divisible by 9.
6. The integer a is divisible by 11 if and only if the alternating sum

   $$\sum_{k=0}^{d} (-1)^k a_k = (-1)^d a_d + (-1)^{d-1} a_{d-1} + \ldots + (-1)a_1 + a_0$$

   of its digits is divisible by 11.
7. Apply these criteria to determine the decomposition into prime factors of the integer 152460.