Margaret Bilu
Office 604

Fall 2019
bilu@cims.nyu.edu

# Algebra homework 3
# Congruences and $\mathbf{Z}/n\mathbf{Z}$

Due October 2nd, 2019

Please hand in your homework stapled, with your name written on it. All answers have to be justified.

**Exercise 1.** Describe the set $(\mathbf{Z}/14\mathbf{Z})^\times$. Give an inverse for each of its elements.

*Solution.*

1. The units of $\mathbf{Z}/14\mathbf{Z}$ are exactly the elements of $\mathbf{Z}/14\mathbf{Z}$ relatively prime with 14. Therefore, $(\mathbf{Z}/14\mathbf{Z})^\times = \{1, 3, 5, 9, 11, 13\}$.

2. If you used the Euclidean algorithm to compute the gcd of these numbers with 12, you can apply the extended algorithm to find the inverses, but since the set of units is very small, its quicker to guess them directly. Answers are:

   $1^{-1} = 1$, $3^{-1} = 5$, $5^{-1} = 3$, $9^{-1} = 11$, $11^{-1} = 9$, $13^{-1} = 13$.

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

*Solution.*

1. We have: $32 = 2^5$ and $2 \nmid 1265$. Therefore, 32 and 1265 are relatively prime, i.e. 32 is invertible modulo 1265.

2. An inverse of 32 can be obtained by applying the Euclidean algorithm and then the extended Euclidean algorithm:

$$1265 = 32 \times 39 + 17$$
$$39 = 17 \times 2 + 5$$
$$17 = 5 \times 3 + 2$$
$$3 = 2 \times 1 + 1$$
$$1 = 1 \times 1 + 0$$

By using the extended Euclidean algorithm, you will obtain:

$$32 \times 593 + 1265 \times (-15) = 1$$

Therefore 593 is an inverse of 32 modulo 1265.

**Exercise 3.** 1. Find all integers $x \in \mathbf{Z}$ satisfying $7x \equiv 3 \pmod{9}$.

*Solution.* Note that 4 is an inverse of 7 modulo 9, since $4 \times 7 = 28 \equiv 1 \pmod{9}$. Multiplying both sides by 4, we see that this congruence is equivalent to $x \equiv 12 \pmod{9}$, which is the same as $x \equiv 3 \pmod{9}$. Thus, the solutions are all of the integers of the form $3 + 9k$, for $k \in \mathbf{Z}$.

2. Find all integers $x \in \mathbf{Z}$ satisfying $6x + 1 \equiv 4 \pmod{41}$.

*Solution.* This equation is equivalent to $6x \equiv 3 \pmod{41}$. Note that 7 is an inverse of 6 modulo 41. Multiplying by 7 on both sides, we get that this congruence is equivalent to $x \equiv 21 \pmod{41}$. Thus, the solutions are the integers of the form $21 + 41k$, $k \in \mathbf{Z}$.

**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.

*Solution.* Let $a$ be an integer. Then there exists $k$ such that $a = 2k$ ( when $a$ is even) or $a = 2k + 1$ (when $a$ is odd). In the first case, we have $a^2 = (2k)^2 = 4k^2 \equiv 0 \pmod{4}$, and in the second case, we have

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4}.$$

2. Show that for any $a, b \in \mathbf{Z}$, the integer $a^2 + b^2$ cannot be congruent to 3 modulo 4.

*Solution.* Using the result of question 1, the possible values for $a^2 + b^2$ modulo 4 are 0 (when both $a^2$ and $b^2$ are congruent to 0 modulo 4), 1 (when one of them is congruent to 1 modulo 4 and the other to 0) or 2 (when both are congruent to 1 modulo 4).

3. Can 1847 be written as a sum of two squares?

*Solution.* You can check that 1847 is congruent to 3 modulo 4. Therefore, according to the previous result, it can't be written as the sum of two squares.

**Exercise 5** (Divisibility criteria)**.** Let $a \geq 1$ be an integer. We may write

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

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.

*Solution.* We have

$$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10 a_1 + a_0 \pmod{2}.$$

But all powers of 10 greater than 1 are even. Therefore:

$$a \equiv a_0 \pmod 2$$

and it follows that $a$ is even if and only if $a_0$ is even.

2. The integer $a$ is divisible by 5 if and only if its last digit $a_0$ is either 0 or 5.

   *Solution.*
   $$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10 a_1 + a_0 \pmod 5$$
   But all powers of 10 greater than 1 are multiples of 5. Therefore:
   $$a \equiv a_0 \pmod 5$$
   Tt follows that $a$ is a multiple of 5 if and only if $a_0$ is 0 or 5, since these are the only non-negative multiples of 5 between 0 and 9.

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.

   *Solution.* We have
   $$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10 a_1 + a_0 \pmod 4$$
   But all powers of 10 greater than $10^1$ are multiples of 4. Therefore:
   $$a \equiv 10a_1 + a_0 \pmod 4$$
   It follows that $a$ is a multiple of 4 if and only if $10a_1 + a_0$ is a multiple of 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.

   *Solution.* We have
   $$a \equiv 10^d a_d + 10^{d-1} a_{d-1} + \ldots + 10 a_1 + a_0 \pmod 3$$
   But $10 \equiv 1 \pmod 3$, so that $10^i \equiv 1 \pmod 3$ for all $i \geq 0$. Therefore:
   $$a \equiv a_d + \cdots + a_1 + a_0 \pmod 3$$
   It follows that $a$ is a multiple of 3 if and only if the sum of its digits is a multiple of 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.

   *Solution.* In the same way as in the previous question, $10 \equiv 1 \pmod 9$, so that $10^i \equiv 1 \pmod 9$ for all $i \geq 0$. Therefore:
   $$a \equiv a_d + \cdots + a_1 + a_0 \pmod 9$$
   and it follows that $a$ is a multiple of 9 if and only if the sum of its digits is a multiple of 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.

*Solution.* We have $10 \equiv -1 \pmod{11}$. Therefore:

$$a \equiv (-1)^d a_d + (-1)^{d-1} a_{d-1} + \cdots - a_1 + a_0 \pmod{11}$$

and it follows that $a$ is a multiple of 11 if and only if the alternating sum of its digits is a multiple of 11.

7. Apply these criteria to determine the decomposition into prime factors of the integer 304920.

*Solution.* Computing the alternating sum of the digits of this number, we see it must be divisible by 11. We find $304920 = 11 \times 27720$. This new number is again seen to be divisible by 11, so we get $27720 = 11 \times 2520$. 2520 is not divisible by 11, but we see e.g. that it is divisible by 9 because its sum of digits is 9. We get $2520 = 9 \times 280$. Finally, 280 is easily seen to be equal to $7 \times 40 = 7 \times 2^3 \times 5$. Thus, we find $304920 = 2^3 \times 5 \times 3^2 \times 7 \times 11^2$.