Modular Arithmetic II: Congruency Classes and Powers

March 1, 2015

Warm Up Problems

1. A reactor that creates ammonia is to be maintained at an optimal temperature of 500°F. Since no process is perfect, a chemical engineer is asked to maintain the reactor temperature within 50°F of the optimal temperature. Otherwise, the reaction will not occur.

   - What is the largest and smallest temperatures in which the reaction will occur?

   450, 550

   To show that a number can either be added or subtracted by another number, we use the symbol $\pm$. Depending on the context, the $\pm$ symbol can mean either an addition or subtraction where the result can be one of two numbers, or it can mean that the addition and subtraction represents a range of numbers.

   - In this problem, we can write that the temperature is to be 500 ± 50°F. Is this a range of numbers or does this represent two distinct numbers?

   Range

2. If the temperature of a pool is to be maintained at 83°F with an error of 1°F, write down the expression that shows the possible range of temperatures the pool can be at.

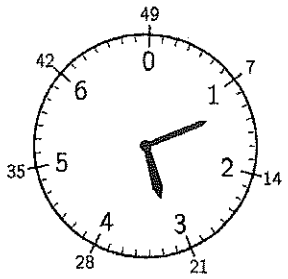
   83 ± 1

3. A biologist observed that a certain bacterium doubles in number every day. If one bacterial cell is placed on a petri dish, it takes 100 days for the bacteria to cover the area of the petri dish. How long would it take for the bacteria to cover half of the area of the petri dish if two bacterial cells are initially placed?

   98 days

Clock Arithmetic Continued

The planet of Heptadium in a galaxy far, far away makes one full rotation around its axis in 7 heptahours. The people inhabiting Heptadium have heptahour clocks similar to the one pictured below:



They further divide a heptahour into 49 heptaminutes and a heptaminute into 49 heptaseconds. The heptahours are marked on the inside of the clock, and the heptaminutes are marked on the outside.

1. What times does the clock show?

   3:09

2. One heptadian tells another, "The next day will begin in one minute." What time is his watch showing?

   6:48

3. What modulus do the heptadiums use when discussing the hours?

   7

4. Reduce the following numbers in modular arithmetic.

   (a) $500 \equiv$ (mod 49)

   (b) $-14 \equiv$ (mod 49)

(c) $7 \times 7 \equiv$ (mod 49)

(d) $1 \div 2 \equiv$ (mod 49)

(e) $1 \div 5 \equiv$ (mod 49)

(f) $5 - 9 \equiv$ (mod 7)

(g) $1 \div 4 \equiv$ (mod 7)

(h) $4 \div 5 \equiv$ (mod 7)

5. Are there any zero divisors in mod 49 arithmetic? If so, what are they?

7

6. Are there any zero divisors in mod 7 arithmetic? If so, what are they?

0

Congruence Classes

The notation $n \pmod 7$ represents not a single number, but all of the numbers of the form:

$$\ldots,\ n-14,\quad n-7,\quad n,\quad n+7,\quad n+14,\ \ldots$$

The infinite set

$$n \pmod 7 = \{n,\ n \pm 7,\ n \pm 14,\ n \pm 21,\ \ldots\}$$

is called a *congruence class*. For example,

$$2 \pmod 7 = \{\ldots,\ -19,\ -12,\ -5,\ 2,\ 9,\ 16,\ 23,\ \ldots\}$$

1. Write down 6 representations of the congruence class 5 (mod 7).

2. Are the classes 0 (mod 7) and 7 (mod 7) the same? Why or why not?

3. Write down two positive and two negative equivalent numbers for each of the following two congruence classes.

   (a) 4 (mod 7)

   -
   -
   -
   -

   Divide each of these numbers by seven. Compare the remainders.

(b) 6 (mod 7)

-
-
-
-

Divide each of these numbers by seven. Compare the remainders.

4. How many different remainders for division by 7 are there?

7

5. How many different mod 7 congruence classes are there? Why?

7

6. Reduce the following numbers in mod 7 arithmetic.

(a) 1000 (mod 7) $\equiv$ 6

(b) 7000 (mod 7) $\equiv$ 0

(c) 8000 (mod 7) $\equiv$ 6

(d) Reduce the last two numbers without using division. (Hint: Use the answer you got for the first number).

7. Write 3000 in the form $3000 = n \times 7 + r$, where r can be one of the numbers $\{0, 1, ..., 6\}$.

$3000 = 48 \times 7 + 4$

8. An experiment in a Heptadium nuclear lab starts at 0 : 00 and runs for 2000 heptahours. Remember that there are 49 heptaminutes in a heptahour and 49 heptaseconds in a heptaminute.

   (a) What time will the experiment end?

   5:00

   (b) How many full days have passed?

   28

9. They also run three experiments in a Heptadium biological lab, where all three experiments take the same amount of time. The experiments are run one after another without time gaps. The first begins at 2 : 00 and the last ends at 5 : 00. The first experiment takes more than a day, but less than two days and lasts a whole number of hours. How long does each experiment take?

8 hours

$3n \equiv 3 \pmod 7$

$n \equiv 1 \pmod 7$

10. The Heptadians now run four experiments, where the first three take an equal amount of time and the last one takes as long as the first three together. The first experiment begins at 1 : 00, and the last ends at 2 : 00. If the first experiment takes more than a day, but less than two days, and last a whole number of hours, how long does the last experiment take?

$6n \equiv 1 \pmod 7$

$6n \equiv -6 \pmod 7$

$n \equiv -1 \pmod 7$

$n > 7$, $n < 14$

$n = \frac{1}{6}, \frac{7}{6}, \frac{14}{6}$

48

$6n = 78$

50, 57, 64, 71, 78, 85

$n = 13$

$13 \times 3 = 39$ hours

Properties of Modular Arithmetic

The following properties are very useful when working with modular arithmetic.

- $a \pm b \pmod{c} \equiv a \pmod{c} \pm b \pmod{c}$
- $a \times b \pmod{c} \equiv a \pmod{c} \times b \pmod{c}$

An easy example that applies this is as follows:

- $4 \times 5 \pmod{3} \equiv 4 \pmod{3} \times 5 \pmod{3} \equiv 1 \times 2 \pmod{3} \equiv 2 \pmod{3}$

1. Use this to reduce the following expressions in modular arithmetic

   (a) $8 + 10 + 100 + 99 \equiv$ 1 $\pmod{9}$

   (b) $17381291 + 27398490 - 183281 + 18293 \equiv$ 1 $\pmod{2}$

   (c) $64 \times 19 \times 4 \times 3 \times 20 \times 3 \equiv$ 0 $\pmod{10}$

   (d) $5 + 4 \times 81 - 15 \times 82 \equiv$ 4 $\pmod{5}$

   (e) $4 \times 4 \times 4 \times 4 \times 4 \times 4 \equiv$ 1 $\pmod{3}$

   (f) $(-1) \times (-1) \times (-1) \equiv$ 6 $\pmod{7}$

   (g) $6 \times 6 \times 6 \times 6 \times 6 \times 6 \equiv$ $\pmod{7}$

2. Use your answers from part (e) and (f) of Problem 1 to reduce the following expressions:

(a) $11^{100} \equiv$ (mod 10)

1

(b) $9^4 \equiv$ (mod 10)

$(-1)^4 = 1$

(c) Challenge: $4^n \equiv$ (mod 5) (Hint: your answer will be a power of -1)

$(-1)^n$ n odd → 4

n even → 1

Powers

Recall that to raise a number a to the power n means to multiply a by itself n times. In other words,

$a^n = a \times a \times ...(n \text{ times})... \times a$

1. Please simplify the following expressions involving powers.

(a) $2^3 =$

(b) $4^3 =$

(c) $(-1)^2 =$

(d) $(-1)^3 =$

(e) $(-1)^{10} =$

2. Following are numbers that are being multiplied with exponents. Please determine the correct values of y.

(a) $2^3 \times 2^2 = 2^y$

(b) $3^2 \times 3^6 = 3^y$

(c) $4^4 \times 4^y = 4^9$

(d) $4^2 \times 4^y = 2^{20}$

(e) $a^2 \times a^6 = a^y$

(f) $a^m \times a^n = a^y$

(g) When two exponents with the same base are multiplied together, we can add the powers together to obtain the result of the multiplication. In other words:

$$a^m \times a^n = a^{m+n}$$

It is important to note that the bases **must** be the same. Why is the expression above true?

$a \times a \times \cdots \times a \times a \times \cdots \times a$

m times $\quad$ n times

total : $m+n$

a^{m+n}

3. Let's now see how we can simplify numbers with powers in modular arithmetic. The goal of this problem is to reduce 3^{100} in mod 7 arithmetic. There are two ways to solve this. The first requires more work but is more obvious. Let us take a look at the consecutive powers of three. Please fill in the blank spaces.

$3 \xrightarrow{-1} 2 \xrightarrow{-3} 6 \xrightarrow{-2} 4 \xrightarrow{-6} 5 \xrightarrow{-4} 1 \xrightarrow{-5} 3$
$+6 \quad +4 \quad +5 \quad +1 \quad +3 \quad +2$

- $3^1 = 3 \equiv 3 \pmod 7$
- $3^2 = 3^1 \times 3 = 9 \equiv 2 \pmod 7$
- $3^3 = 3^2 \times 3 \equiv 2 \times 3 \equiv 6 \pmod 7$
- $3^4 = 3^3 \times 3 \equiv 6 \times 3 \equiv \underline{18} \equiv \underline{4} \pmod 7$
- $3^5 = 3^4 \times 3 \equiv \underline{4} \times 3 \equiv \underline{12} \equiv \underline{5} \pmod 7$
- $3^6 = \underline{3^5} \times 3 \equiv \underline{5} \times 3 \equiv \underline{15} \equiv \underline{1} \pmod 7$
- $3^7 = \underline{3^6} \times 3 \equiv \underline{1} \times 3 \equiv \underline{3} \equiv \underline{3} \pmod 7$
- $3^8 = \underline{3^7} \times 3 \equiv \underline{3} \times 3 \equiv \underline{6} \equiv \underline{2} \pmod 7$

(a) Based on the pattern you see, what is 3^9 in mod 7?

6

(b) What is 3^{15} in mod 7?

$3^3 \rightarrow 6$

(c) What is 3^{100} in mod 7?

$3^{100} \rightarrow 3$

(d) How would you obtain the reduced value of 3^n in mod 7 where n is positive?

$n \div 6 \rightarrow$ remainder

4. Let us look at a different way to reduce 3^{100} in mod 7. This method involves taking 3 to the power which is a power of 2. (Remember that $2^0 = 1$). Please fill in the blanks.

(a) $3^1 = 3 \equiv 3 \pmod 7$
$3^2 = 3^1 \times 3^1 \equiv 3 \times 3 \equiv 9 \equiv 2 \pmod 7$
$3^4 = 3^2 \times 3^2 \equiv 2 \times 2 \equiv 4 \equiv 4 \pmod 7$

$3^8 \equiv 3^4 \times 3^4 \equiv \quad \equiv \quad \equiv \quad \pmod 7$

$3^{16} \equiv \quad \equiv \quad \equiv \quad \equiv \quad \pmod 7$

$3^{32} \equiv \quad \equiv \quad \equiv \quad \equiv \quad \pmod 7$

$3^{64} \equiv \quad \equiv \quad \equiv \quad \equiv \quad \pmod 7$

(b) Please write down 100 as a sum of powers of 2.

$100 = 64 + 32 + 4$

(c) Using your answer to part (b), write down 3^{100} as a product of 3's with powers, which is shown below.

$$3^{100} = 3^{\square} \times 3^{\square} \times 3^{\square}$$

$3^{64} \times 3^{32} \times 3^4$

(d) Use your answer to part (c) to determine what 3^{100} is in mod 7.

$4 \pmod 7$

5. Use the first method to reduce the following numbers in modular arithmetic.

(a) $4^{70} \pmod 5$

$(-1)^{70} \rightarrow 1$

(b) $5^{1234} \pmod 7$

2 mod 7

6. Use the second method to reduce the following numbers in modular arithmetic.

(a) $4^{70} \pmod 5$

(b) $5^{1234} \pmod 7$

1024

1024 = 512 + 512 = 256 + 256 + 256 + 256

$5^{256} \times 4$

210 = 128 +

7. Which method do you prefer and why?