7-27-2018

Emmy Noether and Modular Arithmetic Activity

Cynthia J. Huffman Ph.D.
Pittsburg State University, cjhuffman@pittstate.edu

Emmy Noether Activity

Dr. Cynthia Huffman, Pittsburg State University

Overview: This activity was originally created for a Women in Mathematics course to provide students, who may not have had an abstract algebra class, with a small taste of some basic mathematics connected to the work of Emmy Noether. The activity has the students perform some basic modular (clock) arithmetic and then investigate real world applications of modular arithmetic to ISBN and UPC codes. It could also be used in other courses, such as a general education mathematics course.

http://www-history.mcs.st-andrews.ac.uk/PictDisplay/Noether_Emmy.html

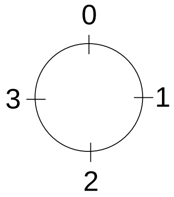
Emmy Noether did important work in abstract algebra, including ring theory and theory of ideals. In this activity, we will take a look at a family of rings called the integers modulo *n*, and then some applications of the integers modulo *n* in the real world.

Part 1. Emmy Noether did pioneer work in ring theory in the area of abstract algebra. A ring is defined to be a non-empty set *R* together with 2 operations that satisfy certain properties. The operations are typically called addition (+) and multiplication (*), although they may not be typical addition and multiplication. The properties that must be satisfied are:

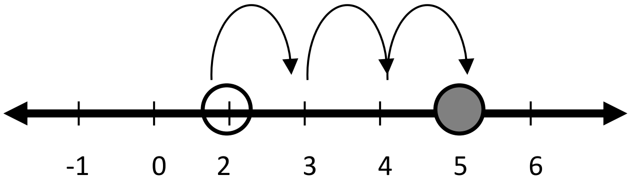
1. + is closed; i.e., if a and b are elements of R, then $a + b$ is in R.
2. * is closed; i.e., if a and b are elements of R, then $a * b$ is in R.
3. + is commutative; i.e., $a + b = b + a$ for every a, b in R.
4. + is associative; i.e., $(a + b) + c = a + (b + c)$ for every a, b, c in R.
5. There is an additive identity, 0_R in R, such that $a + 0_R = a$ for every a in R.
6. Every element a in R has an additive inverse, $-a$, such that $a + (-a) = 0_R$.
7. * is associative; i.e., $(a * b) * c = a * (b * c)$ for every a, b, c in R.
8. * distributes over +; i.e., $a*(b+c) = (a*b) + (a*c)$ and $(b+c)*a = (b*a) + (c*a)$ for all a, b, c in R.

The set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ with usual addition and multiplication satisfy all 8 of these properties, and thus, form a ring. Also, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ form rings with respect to usual addition and multiplication. Much of high school algebra works because the set of polynomials with rational coefficients forms a ring with usual polynomial addition and multiplication. So, you already have practice working with some infinite rings. Next, let's investigate a family of finite rings, $\mathbb{Z}_n$, where n is a positive integer.

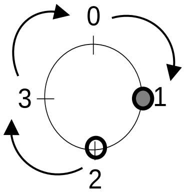
Modular addition and modular multiplication are just addition and multiplication done on a "clock" instead of on a number line. They are also called clock addition and clock multiplication. Let's suppose we have a "clock" with four numbers on it: 0, 1, 2, 3. This set $\{0,1,2,3\}$ together with modular addition and modular multiplication will end up forming the ring $\mathbb{Z}_4$.



On a number line, to add 2 and 3, we think of starting at 2 and moving 3 units to the right.



Since we end up at 5, we write $2+3=5$. To add 2 and 3 modulo 4, we think of starting at the 2 on the "modulo 4" clock and moving clockwise 3 spaces. Since we end up at 1, we write $2+3=1\,(\text{mod}\,4)$.



Since multiplication can be viewed as repeated addition, modular multiplication is similar – just do the operation on the "clock". You can also do the operation in the "usual" way and then take the remainder when you divide by the modulus 4. For example, $3\bullet 3=1\,(\text{mod}\,4)$, since 3 times 3 is 9, which divided by 4 gives a remainder of 1, or if you move clockwise 9 spaces on the "modulo 4" clock above, you will end up at 1.

Try these problems "mod 4", that is in the ring $\mathbb{Z}_4$, using modular addition and modular multiplication.

a. $3+3=$ _____ b. $1+3=$ _____ c. $2\bullet 2=$ _____

Now fill in an addition "mod 4" table.

+ (mod 4)	**0**	**1**	**2**	**3**
0		1		3
1		2		
2		3		
3		0		

Next fill in a multiplication “mod 4” table.

* (mod 4)	0	1	2	3
0		0		0
1		1		
2		2		
3		3		

Complete an addition “mod 6” table.

+ (mod 6)	0	1	2	3	4	5
0						
1						
2						
3	3	4	5	0	1	2
4						
5						

Complete a multiplication “mod 6” table.

* (mod 6)	0	1	2	3	4	5
0						
1						
2						
3	0	3	0	3	0	3
4						
5						

Part 2. The rings $\mathbb{Z}_n$ are used in many situations. We will take a look at 3 real world examples: ISBN-10, ISBN-13, and UPC bar codes.

ISBN-10: ISBN is an acronym for International Standard Book Number. This book identifier originated in 1970. It is now known as an ISBN-10 since it is 10 digits long. An ISBN-10 is arranged in 4 groups. The first digit corresponds to the language of the book, the next 2 to 7 digits give the publisher, the next 1 to 6 digits are for the title, and the final digit is a check digit for detecting errors (this scheme catches all single digit errors and most double digit transposition errors). The check digit is assigned so that the dot product of the ISBN with the vector <10, 9, 8, 7, 6, 5, 4, 3, 2, 1> is 0 in $\mathbb{Z}_{11}$. Since $\mathbb{Z}_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$, but 10 takes 2 digits to write instead of 1, the letter X is used for 10 (X is the Roman numeral for 10). For example, 0-201-05709-3 is a valid ISBN-10 since

$$\begin{aligned}
&< 0,2,0,1,0,5,7,0,9,3 > \bullet < 10,9,8,7,6,5,4,3,2,1 > \pmod{11} \\
&= (0\cdot 10)+(2\cdot 9)+(0\cdot 8)+(1\cdot 7)+(0\cdot 6)+(5\cdot 5)+(7\cdot 4)+(0\cdot 3)+(9\cdot 2)+(3\cdot 1) \pmod{11} \\
&= 0+18+0+7+0+25+28+0+18+3 \pmod{11}, \\
&= 99 \pmod{11} = 0 \pmod{11}
\end{aligned}$$

while 0-1001-1204-X is not a valid ISBN-10 since

$$\begin{aligned}
&< 0,1,0,0,1,1,2,0,4,X > \bullet < 10,9,8,7,6,5,4,3,2,1 > \pmod{11} \\
&= (0\cdot 10)+(1\cdot 9)+(0\cdot 8)+(0\cdot 7)+(1\cdot 6)+(1\cdot 5)+(2\cdot 4)+(0\cdot 3)+(4\cdot 2)+(X\cdot 1) \pmod{11} \\
&= 0+9+0+0+6+5+8+0+8+10 \pmod{11}, \\
&= 46 \pmod{11} = 2 \pmod{11} \neq 0 \pmod{11}
\end{aligned}$$

Find 3 ISBN-10 examples and show the work (like in the examples above) verifying that they are valid.

ISBN-13: Since an ISBN-10 only allocates 1 digit for the language of the book, this allows only 10 languages, not nearly enough. To correct this (and also to allow more publishers and titles), ISBN-13 went into effect on January 1, 2007, using 13 digits. The check digit scheme was also changed to use a different vector for the dot product, <1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1>, and to use $\mathbb{Z}_{10}$ instead of $\mathbb{Z}_{11}$. (It is much easier to compute what a number is modulo 10 than 11 – just take the units digit! No division required!)

For example, 978-0486474175 is a valid ISBN-13 since

$$\begin{aligned}
&< 9,7,8,0,4,8,6,4,7,4,1,7,5 > \bullet < 1,3,1,3,1,3,1,3,1,3,1,3,1 > \pmod{10} \\
&= (9\cdot1)+(7\cdot3)+(8\cdot1)+(0\cdot3)+(4\cdot1)+(8\cdot3)+(6\cdot1)+(4\cdot3)+(7\cdot1)+(4\cdot3)+(1\cdot1)+(7\cdot3)+(5\cdot1) \pmod{10} \\
&= 9+21+8+0+4+24+6+12+7+12+1+21+5 \pmod{10}, \\
&= 130 \pmod{10} = 0 \pmod{10}
\end{aligned}$$

while 978-1001123456 is not a valid ISBN-13 since

$$\begin{aligned}
&< 9,7,8,1,0,0,1,1,2,3,4,5,6 > \bullet < 1,3,1,3,1,3,1,3,1,3,1,3,1 > \pmod{10} \\
&= (9\cdot1)+(7\cdot3)+(8\cdot1)+(1\cdot3)+(0\cdot1)+(0\cdot3)+(1\cdot1)+(1\cdot3)+(2\cdot1)+(3\cdot3)+(4\cdot1)+(5\cdot3)+(6\cdot1) \pmod{10} \\
&= 9+21+8+3+0+0+1+3+2+9+4+15+6 \pmod{10}, \\
&= 81 \pmod{10} = 1 \pmod{10} \neq 0 \pmod{10}
\end{aligned}$$

Find 3 ISBN-13 examples and show the work (like in the example) to verify they are valid.

Will there ever be an X in an ISBN-13? Why or why not?

UPC: A UPC or Universal Product Code is a 12 digit bar code that is scanned when you purchase an object at a store. The first digit depends on the type of object, digits 2 through 6 are assigned to the manufacturer, and digits 7 through 12 are assigned by the manufacturer to distinguish the product. The check digit scheme is similar to the one for ISBN-13 using $\mathbb{Z}_{10}$ and alternating 1's and 3's in the vector used for the dot product, except it starts with 3, <3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1>.

For example, 071662168124 is a valid UPC since

$$
\begin{aligned}
&< 0,7,1,6,6,2,1,6,8,1,2,4 > \bullet < 3,1,3,1,3,1,3,1,3,1,3,1 > \pmod{10} \\
&= (0\cdot 3)+(7\cdot 1)+(1\cdot 3)+(6\cdot 1)+(6\cdot 3)+(2\cdot 1)+(1\cdot 3)+(6\cdot 1)+(8\cdot 3)+(1\cdot 1)+(2\cdot 3)+(4\cdot 1) \pmod{10} \\
&= 0+7+3+6+18+2+3+6+24+1+6+4 \pmod{10}, \\
&= 80 \pmod{10} = 0 \pmod{10}
\end{aligned}
$$

while 123123123123 is not a valid UPC since

$$
\begin{aligned}
&< 1,2,3,1,2,3,1,2,3,1,2,3 > \bullet < 3,1,3,1,3,1,3,1,3,1,3,1 > \pmod{10} \\
&= (1\cdot 3)+(2\cdot 1)+(3\cdot 3)+(1\cdot 1)+(2\cdot 3)+(3\cdot 1)+(1\cdot 3)+(2\cdot 1)+(3\cdot 3)+(1\cdot 1)+(2\cdot 3)+(3\cdot 1) \pmod{10} \\
&= 3+2+9+1+6+3+3+2+9+1+6+3 \pmod{10}, \\
&= 48 \pmod{10} = 8 \pmod{10} \neq 0 \pmod{10}
\end{aligned}
$$

Find 3 UPC examples and show the work (like above) verifying that they are valid.