3 Structure of Modular Multiplication

Unlike addition, multiplication in $\mathbb{Z}_M$ is fairly strange. There may not always be an inverse, you can multiply two non-zero numbers together and get zero, and in general things look scrambled. A good way to get a feel for the structure modular system is to construct a table.

First, for addition modulo 6:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Nice clean pattens. Probably don't even need to make the table in the first place. If you want to find a number's additive inverse, you just find the zero in its row. For example, in row 4 we find that $4 + 2 = 0$, so $-4 = 2$.

For multiplication modulo 6:

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	2	4
5	0	5	4	3	2	1

In the future we'll ignore the zero row and column. It will never be surprising.

In order to find a number's multiplicative inverse (hereafter just "inverse"), you just find the 1 in its row.

Notice that in rows 2, 3, and 4 you can never multiply things together to get 1, and even worse, there are things you can multiply together to get zero.

Q 3.0.1: Why is that?

Q 3.0.2: Construct the multiplication tables for $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, and $\mathbb{Z}_8$.

We've seen these problems before. The multiplicative properties of numbers coprime to the mod are much nicer than the properties of the other numbers. For example, $[5^{-1}]_{10}$ doesn't exist because $gcd(5, 10) \neq 1$, but $[3^{-1}]_{10}$ does exist ($[3^{-1}]_{10} = [7]_{10}$), because $gcd(3, 10) = 1$.

The set of numbers in $\mathbb{Z}_M$ that are coprime to M are denoted $\mathbb{Z}_M^\times$. For example:

$\mathbb{Z}_{18} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$
$\mathbb{Z}_{18}^{\times} = \{1, 5, 7, 11, 13, 17\}$
By definition, the number of elements in $\mathbb{Z}_M^{\times}$ is $\varphi(M)$, since $\varphi(M)$ is "the number of numbers less than M that are coprime to M".

Q 3.0.3: -$gcd(6, 15) =?$
-Find the two non-zero numbers, a and b, in $\mathbb{Z}_{15}$ such that $[6a]_{15} = [6b]_{15} = 0$.
-$gcd(a, 15) =?$, $gcd(b, 15) =?$

Q 3.0.4: Show that if $a \in \mathbb{Z}_M$, but $a \notin \mathbb{Z}_M^{\times}$ (a is in the set $\{0, 1, 2, \cdots, M\}$, but $gcd(a, M) \neq 1$), then there's another number, b, such that $[ab]_M = 0$.

Q 3.0.5: Show that if $a \in \mathbb{Z}_M^{\times}$ and $b \in \mathbb{Z}_M^{\times}$, then $ab \in \mathbb{Z}_M^{\times}$.

Q 3.0.6: Show that if $a \in \mathbb{Z}_M^{\times}$, then a has an inverse.

So, if you look at the multiplicative table of just $\mathbb{Z}_6^{\times}$ (instead of the entire $\mathbb{Z}_6$ table above) you get:

$\times$	1	5
1	1	5
5	5	1

Not much left. But, every element has an inverse, there's no way to get a zero, and it's closed (you'll never get something other than 1 or 5).

Example: The multiplicative table for $\mathbb{Z}_{15}^{\times}$.

$\times$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Q 3.0.7: Construct the multiplication table for $\mathbb{Z}_7^{\times}$ and $\mathbb{Z}_8^{\times}$.

Q 3.0.8: For $\mathbb{Z}_5^{\times}$, $\mathbb{Z}_7^{\times}$, $\mathbb{Z}_8^{\times}$, and $\mathbb{Z}_{15}^{\times}$, multiply the numbers in the first row together, modulo the appropriate number, then do the same for every other row. What do you get? Notice a pattern?

Q 3.0.9: Show that every row in the multiplication table of $\mathbb{Z}_M^\times$ contains every number in $\mathbb{Z}_M^\times$. This is equivalent to showing that, for any x (row), and any z in $\mathbb{Z}_M^\times$, there's a y (column) such that $[xy]_M = [z]_M$.

-Give an equation for y in terms of x and z.

-Why isn't this true for $\mathbb{Z}_M$ in general?

Q 3.0.10: When P is prime, there are exactly two numbers in $\mathbb{Z}_P^\times$ that are their own inverse. One is "1". What is the other, in terms of P? You don't have to prove that it's unique, just find it.

Q 3.0.11: When we say that x is its own inverse in $\mathbb{Z}_M^\times$, that's the same as saying $[x^2]_M = 1$.

-What numbers are their own inverse in $\mathbb{Z}_{15}^\times$?

-What about in $\mathbb{Z}_{21}^\times$?

The fact that in you can multiply non-zero numbers together and still get zero causes a lot of difficulties. For example, addition and multiplication work in modular math, so we can say that $(x-1)(x+1) = x^2 - 1$ in any mod. No problem.

However, since $[ab]_M = [0]_M$ doesn't *necessarily* mean that either a or b are zero, $[(x-1)(x+1)]_M = [0]_M$ doesn't *necessarily* mean that $[x]_M = \pm 1$.

For example, $[4^2]_{15} = [1]_{15}$ and $[4^2 - 1]_{15} = [(4-1)(4+1)]_{15} = [(3)(5)]_{15} = [0]_{15}$. So, despite the fact that $4 \neq \pm 1$, 4 still solves $(x-1)(x+1) = 0$ in $\mathbb{Z}_{15}$.

Q 3.0.12: Using the ideas in the last paragraph, show that if $\mathbb{Z}_M^\times$ contains a number that is its own inverse, other than 1 and $M-1$ (which is the same as -1), then M is composite (is not prime).

3.1 Wilson's theorem

Q 3.1.1: $[(M-1)!]_M = ?$, when M is a composite (has two or more prime factors)? Prove it!

Note: $(M-1)! = 1 \cdot 2 \cdot 3 \cdots (M-1)$

Q 3.1.2: $[(P^k-1)!]_{P^k} = ?$, when P is prime and $k > 2$? Why is the $k = 2$ case different?

Q 3.1.3: $[(P-1)!]_P = ?$, when P is prime?
Hint: Consider the inverses.

Wilson's theorem states that $[(M-1)!]_M = -1$ if and only if M is prime.

Examples:
$[(4-1)!]_4 = [3!]_4 = [6]_4 = 2$
$[(5-1)!]_5 = [4!]_5 = [24]_5 = -1$
$[(6-1)!]_6 = [5!]_6 = [120]_6 = 0$
$[(7-1)!]_7 = [6!]_7 = [720]_7 = -1$

Q 3.1.4: Is Wilson's theorem a good tool for determining if a very, very large number is prime? Why or why not?

Q 3.1.5: If Wilson's theorem provides an absolute test of primality, then why do people still concern themselves with "finding large primes" or proving that particular large numbers are prime?

3.2 The divisor function

Q 3.2.1: You are given three letters: a, b, c.
-How many ways are there to select 0 letters?
-How many ways are there to select 1 letter?
-How many ways are there to select 2 letters?
-How many ways are there to select 3 letters?

Recall that as a shorthand for this operation we say, for example, three choose one, and we write it this way: $\binom{3}{1}$
This also gives us row #3 of Pascals triangle:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ \rightarrow & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

Q 3.2.2: The number 105 has 3 distinct prime factors: $105 = 3 \cdot 5 \cdot 7$.
-How many ways are there to select 0 prime factors? List the ways.
-How many ways are there to select 1 prime factors? List the ways.
-How many ways are there to select 2 prime factors? List the ways.
-How many ways are there to select 3 prime factors? List the ways.
-Use the information above to find all of the factors of 105.

A "divisor" of a number is another number that evenly divides it. For example, 3 is a divisor of 15, but 9 is not.

Q 3.2.3: How many divisors does $30 = 2 \cdot 3 \cdot 5$ have in all? What are they?

The number of divisors that a number, N, has is denoted "$d(N)$". For example, $d(10) = 4$, because 1, 2, 5, and 10 are all divisors of 10. $d(N)$ is called the "divisor function".

Q 3.2.4: How many distinct prime factors does 210 have? How many divisors does it have in all? That is, $d(210) =$?

Notice that when we have a prime factorization that includes single copies of each factor, the total number of factors is always a power of two:
$13 \rightarrow 2$ factors
$2 \cdot 3 \rightarrow 4$ divisors
$2 \cdot 3 \cdot 5 \rightarrow 8$ divisors
$5 \cdot 7 \cdot 11 \cdot 43 \rightarrow 16$ divisors

Q 3.2.5: How many factors would you expect each of the following numbers to have (based on their prime factorization)?

-15

-35

-165

-2310

This power-of-two pattern works because we can also think of each factor as a binary choice: either we include it or we dont. So, for each factor there are two choices:

Factorization of 11,935: $5 \cdot 7 \cdot 11 \cdot 31$

Ways to choose each factor: 2, 2, 2, 2

The total number of factors is the product of all of these choices, 2^4 or 16. On the other hand, when a numbers prime factorization includes multiple copies of a factor (such as $3^3 \cdot 5^2$), then the method above becomes a helpful way to organize the factors.

Q 3.2.6: In the factorization of 40, $2^3 \cdot 5$, how many different ways are there to choose a two? (Careful: We can choose no twos if we like!)

-How many ways are there to choose a five?

-How many factors are there altogether?

Q 3.2.7: If $d(N) = 2^k$, for some k, does that mean that N is the product of k primes? Prove it, or find a counter-example.

Q 3.2.8: How many divisors does each of the following have?

-45

-48

-100

-125

-150

Q 3.2.9: How many factors does each of the following numbers have? As you are working, think about why square numbers are the only ones that have an odd number of factors.

-25

-36

-81

-900

Q 3.2.10: Is there some number that has only 1 factor? 2 factors? What can you conclude about each of the following cases? What can we say about it for certain? Give

an example.

A number with exactly:

-1 factor:

-2 factors:

-3 factors:

-4 factors:

-5 factors:

-9 factors:

Q 3.2.11: What is the smallest number that has exactly 8 factors?

Q 3.2.12: What is the sum of all numbers between 1 and 10 that have an odd number of factors?

Q 3.2.13: What is the greatest number less than 50 that has an even number of factors?

Q 3.2.14: How many odd factors does 1800 have? How many square factors does it have?

Q 3.2.15: By considering the prime factorization of A and B, show that if $gcd(A, B) = 1$, then $d(AB) = d(A) \cdot d(B)$.

Q 3.2.16: The prime factorization of some general N can be written $N = (2^{e_2})\,(3^{e_3})\,(5^{e_5})\,(7^{e_7}) \cdots$
For example, if $N = 45 = 3^2 5$, then $e_2 = 0$, $e_3 = 2$, $e_5 = 1$.
Write a general formula for $d(N)$ in terms of e_2, e_3, e_5, ...

Q 3.2.17: -What 2-digit number has the largest number of divisors?
-What 3-digit number has the largest number of divisors?