

The unique factorization theorem

In this activity we investigate unique factorization theorems.

Consider this proposition from Euclid's *Elements*:

Proposition 1 (IX.14). *If a number is the least that is measured by prime numbers, then it is not measured by any other prime number except those originally measuring it.*

Question 1 Explain what the proposition above is saying.

Question 2 Now consider Euclid's proof:

Let the number A be the least that is measured by the prime numbers B , C , and D . I say that A is not measured by any other prime number except B , C , or D . If possible, let it be measured by the prime number E , and let E not be the same as any one of the numbers B , C , or D .

Now, since E measures A , let it measure it according to F , therefore E multiplied by F makes A . And A is measured by the prime numbers B , C , and D . But, if two numbers multiplied by one another make some number, and any prime number measures the product, then it also measures one of the original numbers, therefore each of B , C , and D measures one of the numbers E or F . Now they do not measure E , for E is prime and not the same with any one of the numbers B , C , or D . Therefore they measure F , which is less than A , which is impossible, for A is by hypothesis the least number measured by B , C , and D . Therefore no prime number measures A except B , C , and D . Therefore, if a number is the least that is measured by prime numbers, then it is not measured by any other prime number except those originally measuring it.

Can you explain what this proof is saying?

Now let's consider a crazy set of numbers—all multiples of 3. Let's use the symbol $3\mathbb{Z}$ to denote the set consisting of all multiples of 3. As a gesture of friendship, I have written down the first 100 nonnegative integers in $3\mathbb{Z}$:

Author(s):

0	3	6	9	12	15	18	21	24	27
30	33	36	39	42	45	48	51	54	57
60	63	66	69	72	75	78	81	84	87
90	93	96	99	102	105	108	111	114	117
120	123	126	129	132	135	138	141	144	147
150	153	156	159	162	165	168	171	174	177
180	183	186	189	192	195	198	201	204	207
210	213	216	219	222	225	228	231	234	237
240	243	246	249	252	255	258	261	264	267
270	273	276	279	282	285	288	291	294	297

Question 3 Given any two integers in $3\mathbb{Z}$, will their sum be in $3\mathbb{Z}$? Explain your reasoning.

Question 4 Given any two integers in $3\mathbb{Z}$, will their difference be in $3\mathbb{Z}$? Explain your reasoning.

Question 5 Given any two integers in $3\mathbb{Z}$, will their product be in $3\mathbb{Z}$? Explain your reasoning.

Question 6 Given any two integers in $3\mathbb{Z}$, will their quotient be in $3\mathbb{Z}$? Explain your reasoning.

Definition 1. Call a positive integer **prime** in $3\mathbb{Z}$ if it cannot be expressed as the product of two integers both in $3\mathbb{Z}$.

As an example, I tell you that 6 is prime number in $3\mathbb{Z}$. You may object because $6 = 2 \cdot 3$, but remember—2 is not in $3\mathbb{Z}$!

Question 7 List all the prime numbers less than 297.

Question 8 Can you give some sort of algebraic characterization of prime numbers in $3\mathbb{Z}$?

Question 9 Can you find numbers that factor completely into prime numbers in two different ways? How many can you find?