Uncovering a Test for Divisibility by a Prime: A Journey of Mathematical Discovery

Murray L. Lauber

One of the joys of being a mathematics teacher is the excitement of being a student. Teaching concepts and solving problems with students provides many opportunities to see new relationships between concepts and to discover patterns that we have never noticed before.

This article has grown out of discoveries that I made over a fairly extended period of time teaching an introductory-level university course entitled Higher Arithmetic. Most of the students were in the humanities, and many planned to be elementary school teachers. My discoveries grew out of a particular topic—divisibility—but illustrate the discovery process that mathematics teachers engage in on a regular basis. The topic of divisibility was a part of a section of the course on number theory. In the textbook first employed, the authors presented or suggested ways of developing rules for divisibility by 2, 3, 4, 5, 6, 8 and 9, along with mathematical justification for some of these rules (Meserve 1981, 64–67). These rules and their justifications led me to wonder whether there was a general algorithm for divisibility by a prime. I could have searched for written sources to find the answer but was drawn by the appeal of discovering the rules for myself. Of course, I was far from alone in this kind of experience; the need to discover and the compulsion to generalize are at the heart of the study of mathematics.

There was another way in which I was far from alone. Although it is not often apparent, the process of mathematical discovery is typically somewhat convoluted. Characteristically, the textbook solution of a challenging mathematical problem misrepresents the process by editing out the convolution. The result is a tidied-up version of the solution in which sequential logic and efficient communication trump accurate representation of the process. The need to tidy up a solution is understandable but we should make our students aware that the process leading to a textbook solution is not always so tidy. The reader will benefit by knowing that, in favour of efficient communication, much of the convolution has been edited out of the following description of my journey of discovery.

Some Basic Rules for Divisibility

The following rules, along with the proof of the last one, illustrate how the process of discovery began.

A counting number n is divisible by

- 2 if and only if its last digit is divisible by 2;
- 3 if and only if the sum of the digits is divisible by 3;
- 4 if and only if the number represented by its last two digits is divisible by 4;
- 5 if and only if its last digit is 5 or a 0;
- 6 if and only of it is even and the sum of the digits is divisible by 3 (that is, it is divisible by both 2 and 3);
- 8 if and only if the number represented by its last three digits is divisible by 8;
- 9 if and only if the sum of the digits is divisible by 9.

The rule for divisibility by 7 is more complex and is often left out of such a list. The formulation of that rule was the beginning of my process of discovery. That rule and its proof will be given later. Because the rule for divisibility by 9 was instrumental in suggesting the structure of other rules and their proofs, it seems natural to begin with a proof of that rule. I have labelled it rule 1.

Rule 1: A counting number n is divisible by 9 if and only if the sum of its digits is divisible by 9.

The following proof for a four-digit number is dependent on the closure, commutative and associative properties of addition of counting numbers along with the distributive property of multiplication over addition.

Let $n = d_3d_2d_1d_0$ where d_3, d_2, d_1 and d_0 are its digits.

Then $n = 1{,}000d_3 + 100d_2 + 10d_1 + 1d_0$
$\Rightarrow n = (999 + 1)d_3 + (99 + 1)d_2 + (9 + 1)d_1 + 1d_0$
$\Rightarrow n = (999d_3 + 99d_2 + 9d_1) + (d_3 + d_2 + d_1 + d_0)$ **[1]**

1) To prove the *if* part of the theorem, we need to show that, if the sum of digits of n is divisible by 9 then n is also divisible by 9.
If the sum of n's digits is divisible by 9, then
$d_3 + d_2 + d_1 + d_0 = 9k$ for some $k \in N = \{1, 2, 3, . . .\}$
$\Rightarrow n = (999d_3 + 99d_2 + 9d_1) + 9k$ from equation [1]
$\Rightarrow n = 9(111d_3 + 11d_2 + d_1 + k)$
$\Rightarrow n$ is a multiple of 9, that is n is divisible by 9.

2) To prove the *only if* part of the theorem, we need to show that if n is divisible by 9 then the sum of its digits is also divisible by 9. Suppose that n is a multiple of 9, say $n = 9j$ for some $j \in N$. Then, from equation [1],
$9j = (999d_3 + 99d_2 + 9d_1) + (d_3 + d_2 + d_1 + d_0)$
$\Rightarrow 9j = 9(111d_3 + 11d_2 + 1d_1) + (d_3 + d_2 + d_1 + d_0)$
$\Rightarrow d_3 + d_2 + d_1 + d_0 = 9(111d_3 + 11d_2 + 1d_1) - 9j$
$\Rightarrow d_3 + d_2 + d_1 + d_0 = 9(111d_3 + 11d_2 + 1d_1 - j)$
$\Rightarrow$ the sum of the digits of n is a multiple of 9.

Once this and the other rules had been proven, some persistent exploration that made use of my knowledge of modular arithmetic (a topic that will be explored shortly) led to the following rule for divisibility by 7:

Rule 2: A counting number $n = d_t d_{t-1} d_{t-2} . . . d_2 d_1 d_0$ is divisible by 7 if and only if the following linear combination of its digits is divisible by 7:

$1d_0 + 3d_1 + 2d_2 + (-1d_3) + (-3d_4) + (-2d_5) + . . .$
$1d_6 + 3d_7 + 2d_8 + (-1d_9) + (-3d_{10}) + (-2d_{11}) + . . .$
. . . . . .
. . . . . .
. . . . . .

Note that the linear combination of digits begins with the last digit and that the coefficients of the linear combination repeat every six digits (the means by which these coefficients were determined will be described later).

Example: Determine whether $n = 88{,}580{,}723$ is divisible by 7.

Solution: According to Rule 2, n will be divisible by 7 if and only if
$1d_0 + 3d_1 + 2d_2 + (-1d_3) + (-3d_4) + (-2d_5) = 1d_6 + 3\,d_7$
is divisible by 7, that is, if
$(1 \times 3) + (3 \times 2) + (2 \times 7) + (-1 \times 0) + (-3 \times 8) + (-2 \times 5) + (1 \times 8) + (3 \times 8) = 21$ is divisible by 7.
According to the rule, because 21 is divisible by 7, 88,580,723 is also divisible by 7. The reader may use a calculator to verify the above result, but one of the advantages of Rule 2 is that it can be applied to numbers too large to input into your calculator.

The proof for Rule 2 drew on my knowledge of modular arithmetic. What follows is a brief overview of the concepts of modular arithmetic that are needed to discover and prove rules of divisibility.

Modular Arithmetic: A Tool for Exploring Divisibility Rules

Two integers, m and n, are said to be *congruent mod k* (Rosen 2003, 161–63) where k is a particular counting number is they differ by a multiple of k, that is $m - n = jk$ where $j \in Z = \{. . ., -2, -1, 0, 1, 2, . . .\}$. If this is the case, we write $m \equiv n(\text{mod } k)$. For example, 7 and 12 are congruent mod 5 because $12 - 7 = 1 \times 5$, a multiple of 5. Perhaps a more intuitive way of looking at this example is to say that 7 and 12 both have the same remainder, 2, when divided by 5. ($7 = 1 \times 5 + 2$ and $12 = 2 \times 5 + 2$). To extend the example, -3 is congruent to both 7 and 12 mod 5 because it also has a remainder of 2 when divided by 5 ($-3 = -1 \times 5 + 2$). In fact, modular arithmetic is often conceptualized as the arithmetic of remainders.

Using this idea, we can generate an infinite family of integers of which all members are congruent to 2 mod 5. That family is the set $\{. . ., -8, -3, 2, 7, 12, . . .\}$. It is easy to see that each of the numbers in this family will yield a remainder of 2 when divided by 5. We will say that each of these numbers and a *mod 5 equivalent of 2.*

Congruence mod 5 partitions the integers into five families of integers that are called *equivalence classes*:

$[0] = \{. . ., -10, -5, 0, 5, 10, . . .\}$
$[1] = \{. . ., -9, -4, 1, 6, 11, . . .\}$
$[2] = \{. . ., -8, -3, 2, 7, 12, . . .\}$
$[3] = \{. . ., -7, -2, 3, 8, 13, . . .\}$
$[4] = \{. . ., -6, -1, 4, 9, 14, . . .\}$

The term equivalence class is used because congruence mod k satisfies the three properties of an *equivalence relation* (Roman 1989, 141–48). More will be said about this shortly. [0] is referred to as the equivalence class associated with 0. Numbers in it are congruent to 0 mod 5. Numbers in [1], the equivalence class associated with 1, are each congruent to 1 mod 5; and so on. Note that the numbers in [0], that is, the numbers congruent to 0 mod 5, are all multiples of 5. In this analysis, $k = 5$, but analogous results can be obtained for any value of k. For example, $k = 12$ results in the "clock arithmetic," where 12 equivalence classes corresponding to the hours on a clock face, a analogy that is sometimes taught in the elementary school curriculum.

Exploration of the rule for divisibility by 7 will make use of congruence mod 7. In mod 7 arithmetic, the equivalence classes are

$[0] = \{. . ., -14, -7, 0, 7, 14, . . .\}$
$[1] = \{. . ., -13, -6, 1, 8, 15, . . .\}$
. . . .
. . . .
. . . .
$[6] = \{. . ., -15, -8, -1, 6, 13, . . .\}$

In mod k arithmetic, we often choose the non-negative numbers 0, 1, 2, . . . , (k-1) to be the representatives of the classes [0], [1], [2], . . ., [k - 1]. However, in developing rules for divisibility by a prime, these are not generally the most appropriate representatives. For example, in the test for divisibility by 7, the formulation of the rule is simpler if we use the numbers -3, -2, -1, 0, 1, 2, 3 as representatives of the classes. As well, as we shall see, the formulation of the rule for divisibility by 11 is far simpler if we use -1 rather than 10 as the representatives of the class [10] = {. . ., -23, -12, -1, 10, 21, 32, . . .}.

In devising the rule for divisibility by a prime p we will use mod p arithmetic with equivalence classes [0], [1], [2], . . . , [p - 1]. We will see that, in general, the formulation of the rule for divisibility by a prime p is simplest if we use the integers between _ 1/2 p and 1/2 p as the representatives of the classes rather than the non-negative integers 0, 1, 2, . . . , (p - 1).

Once useful property of modular arithmetic is that the result will be the same no matter if the remainders from addition or multiplication are determined before or after the operation. To put it more fornally, the mod k equivalent of the result of a calculation involving two or more counting numbers is the same if the mod k equivalent of each of the counting numbers is used in the calculation. For example, consider the product 28 × 6:

$28 \times 6 = 168 = 33 \times 5 + 3$
$\Rightarrow 28 \times 6 = 3 (\text{mod } 5)$

Now find the mod 5 equivalents before multiplying:

$28 = 5 \times 5 + 3 \Rightarrow 28 \Rightarrow 3 (\text{mod } 5)$, and
$6 = 1 \times 5 + 1 \Rightarrow 6 \equiv 1 (\text{mod } 5)$
Then $3 \times 1 = 3 \equiv 3 (\text{mod } 5)$, the same as the result above.

This example illustrates one of the properties of modular arithmetic. The following theorems describe the properties of congruence mod k that are useful in exploring and proving rules for divisibility.

Theorem 1: Suppose that a, b and c integers are that k is a particular counting number. Then the congruence mod k is:
a) reflexive: $a \equiv a (\text{mod } k)$
b) symmetric: $a \equiv b (\text{mod } k) \Rightarrow b \equiv a (\text{mod } k)$
c) transitive: $a \equiv b (\text{mod } k)$ and $b \equiv c (\text{mod } k) \Rightarrow a \equiv c (\text{mod } k)$;

A relation that is reflexive, symmetric and transitive is called an *equivalence relation.* Congruence mod k is a equivalent relation.

Proof of c): Suppose that $a \equiv b (\text{mod } k)$ and $b \equiv c (\text{mod } k)$

Then $a - b = ik$ and $b - c = jk$ for some $i, j \in Z$
$\Rightarrow a - c = (i + j)k,\ i + j \in Z$
$\Rightarrow a \equiv c (\text{mod } k)$

Theorem 1 c) says that if a and b differ by a multiple of k, and b and c differ by a multiple of k, then a and c will differ by a multiple of k. Or, to put it another way, a, b and c will each yield the same remainder when divided by k.

Theorem 2: Suppose $m, n \in Z$ with $m \equiv r_m (\text{mod } k)$ and $n \equiv r_n (\text{mod } k)$, r_m and $r_n \in Z$ with $0 \leq r_m < k$ and $0 \leq r_n < k$*. Then
a) $[m + n] \equiv [r_m + r_n] (\text{mod } k)$, and
b) $[m \times n] \equiv [r_m \times r_n] (\text{mod } k)$

Theorem 2 a) says that in computing a sum of two integers, the modular arithmetic can be done either before or after finding the sum; the result will be the same. Theorem 2 b) says the same thing about products. Theorem 2 a) can be extended to a sum with any number of items. Similarly, theorem 2 b) can be extended to a product with any number of factors, including a power, as in the corollary below. Taken together, theorems 2 a) and b) imply that in a calculation involving any combination of sums and products of integers, such as a polynomial, the modular arithmetic may be done either before or after doing the calculation. That is, the remainders may be found either before or after doing the calculations (see theorem 3 below). These results are important in an exploring and proving rules for divisibility. The proof of 2 a) is straightforward and is left to the reader.

Proof of 2 b): $m \equiv r_m (\text{mod } k)$ and $n \equiv r_n (\text{mod } k) \Rightarrow m = q_m k + r_m$ and $n = q_n k + r_n$, q_m, $q_n \in Z$. Then,

$$
\begin{aligned}
m \times n &= (q_m k + r_m)(q_n k + r_n) = q_m q_n k^2 + q_m r_n k + q_n r_m k + r_m r_n \\
&= (q_m q_n k + q_m r_n + q_n r_m)k + r_m r_n \\
&\equiv r_m r_n (\text{mod } k)
\end{aligned}
$$
$\Rightarrow m \times n \equiv r_m r_n (\text{mod } k)$

The symbols q_m and q_n are appropriate because they represent quotients, Equally appropriate are r_m and r_n, which represent remainders.

Corollary to theorem 2 b): $a \equiv b (\text{mod } k)$, $\Rightarrow a^n \equiv c^n (\text{mod } k)$ where n is any counting number

Proof: $a \equiv b\ (\text{mod } k) \Rightarrow a \times a \equiv b \times b (\text{mod } k)$

$$
\begin{aligned}
&\Rightarrow a^2 \equiv b^2 (\text{mod } k) \\
&\Rightarrow a^2 \times a \equiv b^2 \times b (\text{mod } k) \\
&\Rightarrow a^3 \equiv b^3 (\text{mod } k) \\
&\Rightarrow a^3 \times a \equiv b^3 \times b (\text{mod } k) \\
&\Rightarrow a^4 \equiv b^4 (\text{mod } k) \\
&\vdots
\end{aligned}
$$

Theorems 2 a) and b) and the above corollary lead to a m•re general theorem that has already been alluded to:

Theorem 3: Let $p(x)$ be a polynomial with integer coefficients and k be a counting number. Then, for integers a and b, $a \equiv b(\text{mod } k) \Rightarrow p(a) \equiv p(b)(\text{mod } k)$.

Theorem 3 says that in evaluating a polynomial mod k it does not matter which member of an equivalence class is used; the result will be the same for all members of the class. The theorem is proved formally in many texts (including Stark 1984, 61–65). The proof formalizes the following argument: the integers a and b are members of the same equivalence class and thus have the same remainder, r, when divided by k. In evaluating $p(a)$ and $p(b)$, x is replaced by a and b, respectively, in $p(x)$. Each evaluation consists of calculating sums and products. Thus, according to theorem 2, the remainders for each of $p(a)$ and $p(b)$ may be found either before or after calculating the sums and products. If the remainder r is found first, the result of the evaluation in both cases is $p(r)$. Thus, both $p(a)$ and $p(b)$ will be congruent to $p(r)$ and therefore congruent to each other.

Developing and Proving New Divisibility Rules

With these concepts from modular arithmetic, it is possible to prove the Rule 2 concerning divisibility by 7. The following is a proof for a 12-digit number n. It can easily be extended to numbers with more digits.

Let $n = d_{11}d_{10}d_9 \ldots d_2d_1d_0$
$\Rightarrow n = (d_{11} \times 10^{11}) + (d_{10} \times 10^{10}) + (d_9 \times 10^9) + (d_8 \times 10^8) + (d_7 \times 10^7) + (d_6 \times 10^6) + (d_5 \times 10^5) + (d_4 \times 10^4) + (d_3 \times 10^3) + (d_2 \times 10^2) + (d_1 \times 10^1) + (d_0 \times 10^0)$ **[2]**

Now $10^0 = 1 \equiv 1(\text{mod } 7)$,
$10^1 = 10 \equiv 3(\text{mod } 7)$ since $10 = 1 \times 7 + 3$,
$10^2 = 100 \equiv 2(\text{mod } 7)$ since $100 = 14 \times 7 + 2$,
$10^3 = 1{,}000 \equiv 6 \equiv -1(\text{mod } 7)$ since $1{,}000 = 143 \times 7 + (-1)$,
$10^4 = 10{,}000 \equiv -3(\text{mod } 7)$ since $10{,}000 = 1{,}429 \times 7 + (-3)$,
$10^5 = 100{,}000 \equiv -2(\text{mod } 7)$ since $100{,}000 = 14{,}286 \times 7 + (-2)$,
$10^6 = 1{,}000{,}000 \equiv 1(\text{mod } 7)$ since $1{,}000{,}000 = 142{,}858 \times 7 + 1$,
$10^7 = 10{,}000{,}000 \equiv 3(\text{mod } 7)$ since $10{,}000{,}000 = 1{,}000{,}000 \times 10 \equiv 3 \times 1(\text{mod } 7)$
[Theorem 2 b)]

It should be clear that this list repeats beginning at 10^6. Because n consists of sums of products in equation [2], we can apply theorem 2 to find the mod 7 equivalent of n by replacing the powers of 10 by their mod 7 equivalents. This will obtain

$\Rightarrow n = [(d_{11} \times -2) + (d_{10} \times -3) + (d_9 \times -1) + (d_8 \times 2) + (d_7 \times 3) + (d_6 \times 1) + (d_5 \times -2) + (d_4 \times -3) + (d_3 \times -1) + (d_2 \times 2) + (d_1 \times 3) + (d_0 \times 1)](\text{mod}7)$**
$\Rightarrow n = [(1d_0 + 3d_1 + 2d_2 + (-1d_3) + (-3d_4) + (-2d_5) + 1d_6 + 3d_7 + 2d_8 + (-1d_9) + (-3d_{10}) + (-2d_{11})](\text{mod}7)$ **[3]**

It is clear that n will be divisible by 7 if and only if $n \equiv 0(\text{mod } 7)$. Because n has a mod 7 equivalent that is equal to the linear combination of the digits in equation [3], it will be divisible by 7 if and only if that linear combination is divisible by 7.

This concludes the proof of rule 2 for a 12-digit number. This proof could be extended to a number with any length of digits. It should be clear why the mod 7 equivalents of the powers of 10 were chosen to be between -3 and 3 inclusive rather than between 0 and 6 inclusive.

Having discovered the rule for divisibility by 7, I was prepared to move on to other rules. But, as I reflected on the process the following facts struck me as having more than passing significance:

- $10^0 \equiv 1(\text{mod } 7)$
- $10^3 = 1{,}000 \equiv -1(\text{mod } 7)$
- $10^6 = 1{,}000{,}000 \equiv 1(\text{mod } 7)$
- $10^9 = 1{,}000{,}000{,}000 \equiv -1(\text{mod } 7)$

When I recognized that $1{,}000{,}000 = 1{,}000^2$, $1{,}000{,}000{,}000 = 1{,}000^3$ and so on, it occurred to me that a rule with a simpler formulation could be constructed if n were first written in base 1,000. For example, consider again $n = 88{,}580{,}723$. Then

$n = 88 \times 1{,}000^2 + 580 \times 1{,}000^1 + 723 \times 1{,}000^{\bullet}$
$\Rightarrow n \equiv [88 \times 1 + 580 \times -1 + 723 \times 1](\text{mod } 7)$
$\Rightarrow n \equiv [-231](\text{mod } 7) = [-33 \times 7 + 0](\text{mod } 7) \equiv 0(\text{mod } 7)$
Thus n is divisible by 7.

The above observations and example lead to another formulation of the rule for divisibility by 7.

Rule 2a: A number n is divisible by 7 if and only if, when it is expressed in base 1,000, the alternating sum of its digits beginning with the last digit is divisible by 7. Note that alternating sum is used here to mean that the signs of the digits are alternated between positive and negative. In base 1,000 a digit is typically a 3-digit base 10 number.***

The next step was to develop a rule for divisibility by 11. The exploration process was analogous to that used in developing the rule for divisibility by 7.

First, the mod 11 equivalents of the powers of 10 were found using theorem 1:

$10^0 = 1 \equiv 1(\text{mod } 11)$,
$10^1 = 10 \equiv -1(\text{mod } 11)$ since $10 = 1\times 11 + (-1)$,
$10^2 \equiv [(-1)^2](\text{mod } 11) \equiv 1(\text{mod } 11)$,
$10^3 = 1{,}000 \equiv [(-1)^3](\text{mod } 11) \equiv -1(\text{mod } 11)$,
$10^4 = 10{,}000 \equiv [(-1)^4](\text{mod } 11) \equiv 1(\text{mod } 11)$,
$10^5 = 10{,}000 \equiv [(-1)^5](\text{mod } 11) \equiv -1(\text{mod } 11)$

It is clear that the mod 11 equivalents of the powers of 10 alternate in the pattern 1, -1, 1, -1, . . . providing that -1 is used as the representative of the class {. . . , -23, -12, -1, 10, 21, . . .}.

The exploration described above leads to a simple rule for testing divisibility by 11:

Rule 3: A counting number *n* is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

As alluded to earlier, the simplicity of rule 3 is dependent on using -1 as the representative of the class {. . ., -23, -12, -1, 10, 21, . . .}. Because the above explanation of the development of the rule also contains the basic elements of its proof, no formal proof is included here. The following is an example of its application.

Determine whether n = 576,213,489,573 is divisible by 11.

Solution: $3 - 7 + 5 - 9 + 8 - 4 + 3 - 1 + 2 - 6 + 7 - 5 = -4 \equiv 7$ (mod 11). According to rule 3, *n* is not divisible by 11.

The techniques used in exploring rules for divisibility by 7 and 11 can be applied toward finding a rule for divisibility by 13, 17 or any prime. Much of that exploration is left for the reader. The next section deals, rather, with a theorem that describes a general algorithm for determining divisibility by any prime *p*.

A General Algorithm for Testing Divisibility by a Prime

Theorem 4: Suppose that $n = d_td_{t-1}d_{t-2} \ldots d_2d_1d_0$ is a counting number and *p* a prime with $n > p$. Then *n* is divisible by *p* if and only if $m = c_td_t + c_{t-1}d_{t-1} + c_{t-2}d_{t-2} + \ldots + c_1d_1 + c_0d_0$ is divisible by *p* where each $0 \leq i \leq t$, $c_i \equiv 10^i(\text{mod } p)$ and $-1/2p < c_i < 1/2p$.

Proof: It will be sufficient to prove than $n \equiv m(\text{mod } p)$

$n = (d_t\times 10^t) + (d_{t-1}\times 10^{t-1}) + \ldots + (d_i\times 10^i) + \ldots + (d_1\times 10^1) + (d_0\times 10^0)$

Note than $c_i \equiv 10^i(\text{mod } p) \Rightarrow 10^i \equiv c_i(\text{mod } p)$ [Theorem 1.b]

$\Rightarrow d_i\times 10^i \equiv d_i \times c_i (\text{mod} p)$ [Theorem 2.b]

$\Rightarrow (d_t \times c_1{}^t) + (d_{t-1}\times c_1{}^{t-1}) + \ldots + (d_1\times c_1{}^i) + \ldots + (d_1\times c_1{}^1) + (d_0\times c_1{}^0) \equiv (c_td_t + c_{t-1}d_{t-1} + c_{t-2}d_{t-2} + \ldots + c_1d_1 + c_0d_0)(\text{mod } p)$ [Theorem 2.a]

$\Rightarrow n \equiv m(\text{mod } p)$

As a final exercise in this exploration, apply theorem 4 to find a rule for divisibility by 13. In developing the rule, use $10^i \equiv c_1{}^i(\text{mod } p)$ to find the mod 13 equivalents of the powers of 10.

$10^0 = 1 \equiv 1(\text{mod } 13)$,
$10^1 = 10 \equiv -3(\text{mod } 13)$,
$10^2 \equiv (-3)^2(\text{mod } 13) \equiv 9(\text{mod } 13) \equiv -4,\text{mod } 13)$
$10^3 \equiv [(-3)^2\times(-3)](\text{mod } 13) \equiv [(-4) \times (-3)](\text{mod } 13)$
$\equiv 12(\text{mod } 13) \equiv -1(\text{mod } 13)$,
$10^4 \equiv [(-3)^3\times(-3)](\text{mod } 13) \equiv [(-1) \times (-3)](\text{mod } 13)$
$\equiv 3(\text{mod } 13)$,
$10^5 \equiv [(-3)^4\times (-3)](\text{mod } 13) \equiv [(3) \times (-3)](\text{mod } 13)$
$\equiv -9(\text{mod } 13) \equiv 4(\text{mod } 13)$,
$10^6 \equiv [(-3)^5(-3)](\text{mod } 13) \equiv [(4) \times (-3)](\text{mod } 13)$
$\equiv -12(\text{mod } 13) \equiv 1(\text{mod } 13)$,

. . . .
. . . .
. . . .

Now, suppose $n = d_td_{t-1}d_{t-2} \ldots d_{11}d_{10}d_9d_8d_7d_6d_5d_4d_3d_2d_1d_0$

$\Rightarrow n = (d_t\times 10^t) + (d_{t-1}\times 10^{t-1}) + (d_{t-2}\times 10^{t-2}) + \ldots + (d_{11}\times 10^{11}) + (d_{10}\times 10^{10}) + (d_9\times 10^9) + (d_8\times 10^8) + (d_7\times 10^7) + (d_6\times 10^6) + (d_5\times 10^5) + (d_4\times 10^4) + (d_3\times 10^3) + (d_2\times 10^2) + (d_1\times 10^1) + (d_0\times 10^0)$

Then, using the above mod 13 equivalents for the powers of 10, the following is obtained:

Rule 3: A counting number *n* is divisible by 13 if and only if *m* is divisible by 13 where

$m = [1d_0 = (-3d_1) + (-4d_2) + (-1d_3) + 3d_4 + 4d_5 + 1d_6 + (-3d_7) + (-4d_8) + (-1d_9) + 3d_{10} + 4\, d_{11} + \ldots]$

Example: Determine whether $n = 889{,}594{,}829{,}357$ is divisible by 13.

Solution: *n* will be divisible by 13 if and only if *m* is divisible by 13 where

$m = 1 \times 7 + (-3 \times 5) + (-4 \times 3) + (-1 \times 9) + 3 \times 2 + 4 \times 8 + 1 \times 4 + (-3 \times 9) + (-4 \times 5) + (=1 \times 9) + 3 \times 8 + 4 \times 8 = 13 \equiv 0(\text{mod } 13)$

$m \equiv 0(\text{mod } p) \Rightarrow m$ is divisible by 13
$\Rightarrow n$ is divisible by 13

Conclusion

The process of exploration described in this article began with some textbook rules for divisibility by 2, 3, 4, 5, 6, 8 and 9. Those rules lead to a search for rules for divisibility by other numbers like 7 and 11. The focus was on primes because it seemed that once the rules for divisibility by primes was uncovered, divisibility by a composite number could be tested using a combination of the rules for divisibility by primes. Uncovering the rules for divisibility by 7 and 11 was expedited by calling on the concepts of modular arithmetic. These concepts enabled the culmination of the exploration process, namely the formulation of a general algorithm for determining divisibility by a prime.

This process of exploration was particularly satisfying for a number of reasons:

1. There was the prospect of exploring many rules (because there are many primes that might be of interest) with the possibility of observing some general patterns.
2. The process naturally used the concepts of modular arithmetic and demonstrated a property that the concepts have in common with most mathematical concepts—their ability to expand our native brainpower.
3. The process satisfied a compulsion that has characterized most mathematical exploration over the past couple of centuries—the need to generalize. It lead to the determination of a general algorithm for testing divisibility by a prime.
4. The culmination in a general algorithm gave a feeling of completion to the process. Later, the thought hit me in an Archimedes moment that the algorithm could be made perfectly general. After the formulation and proof of the algorithm, it occurred to me that the properties of modular arithmetic that I had applied to the primes were equally applicable to composites. Therefore, the algorithm can be extended to composites and thus to all counting numbers. This even more general algorithm could be used to verify the rules for divisibility by 4, 6, 8 and 9, and to explore the patterns in the rules for divisibility by other composites.

This process of uncovering the rules for divisibility by a prime is illustrative of the many opportunities for mathematical exploration that teachers encounter. By taking advantage of these opportunities, we can sensitize our students to these opportunities and help them become more acquainted with the nature of mathematical discovery.

Notes

* The symbols rm and rn are used because they are the remainders when m and n, respectively, are divided by k. According to the division algorithm for counting numbers, the remainder r, when a counting number n (the dividend) is divided by another counting number d (the divisor), can be made to be a non-negative number less than d. In our case, the divisor is k so the remainder can be made to be less than k. The division algorithm can be extended to the integers Z.

** Alternatively, one could observe that $n = p(10)$, where $p(x) = d_{11}x^{11} + d_{10}x^{10} + d_9x^9 + \ldots + d_2x^2 + d_1x^1 + d_0x^0$, a polynomial. By theorem 3, since $10 \equiv 3 (\text{mod } 7)$, $p(10) \equiv p(3) (\text{mod } 7)$. The mod 7 equivalent of n could be evaluated by using $p(3)$ instead of $p(10)$. The reader can check that $3^0 \equiv 1 (\text{mod } 7)$, $3^1 \equiv 3 (\text{mod } 7)$, $3^2 \equiv 2 (\text{mod } 7)$, $3^3 \equiv -1 (\text{mod } 7)$, $3^4 \equiv -3 (\text{mod } 7)$, $3^5 \equiv -2 (\text{mod } 7)$ and so on. The result would be the same.

*** In a codified base 1,000 system we would need 1,000 different symbols to represent the numbers 0, 1, 2, . . . , 999. In such a theoretical system each digit would be represented by just one symbol.

Bibliography

Meserve, B. E., and M. A. Sobel. 1981. *Contemporary Mathematics*. 3rd ed. Englewood Cliffs, N.J.: Prentice-Hall.

Stark, H. M. 1984. *An Introduction to Number Theory*. Boston: MIT Press.

Roman, S. 1989. *An Introduction to Discrete Mathematics*. 2nd ed. Orlando, Fl.: Harcourt Brace.

Rosen, K. H. 2003. *Discrete Mathematics and Its Applications*. 5th ed. Boston: McGraw Hill.

Murray L. Lauber is an associate professor in the Augustana Faculty of the University of Alberta. He has taught a variety of courses, including precalculus, calculus, linear algebra, discrete mathematics and higher arithmetic at the university level and mathematics and physics at the high-school level. He has published a number of articles and has presented at workshops and conferences. He believes that mathematics is a potent tool for expanding the intellectual capacities of all students.