Modular Arithmetic: Two Hors d'Oeuvres

Charles H. Holbrow

September 21, 2023

1 Introduction

How this presentation came about.

Steve Isenberg sent me a link (`https://youtu.be/tRaq4aYPzCc?si=VNaZfuxxLVpo-DVh`)to the YouTube clip of Derek Muller's talk on p-adic numbers. He asked: Should we bring this to LCTG? Perhaps a joint presentation? After I watched it three times, I began to understand what Muller was talking about.

Then I made a list of subtopics that I thought we might need to explain before we could explain p-adic numbers. The list included

- different kinds of numbers and how they came to be:
  - natural numbers $\mathbb{N}$
  - integers which include negative numbers $\mathbb{Z}$
  - rational numbers $\mathbb{Q}$
  - real numbers $\mathbb{R}$
  - imaginary numbers
  - complex numbers $\mathbb{C}$
- different kinds of arithmetic
  - ordinal
  - algebra
  - calculus
  - vector algebra
  - complex variables
  - matrix algebra

    - tensor analysis
    - modular arithmetic
- Diophantine equations
    - Pythagorean triples
    - Chinese remainder theorem
    - modular arithmetic

We decided not do a talk on p-adics until we could figure out how to do it without all the overhead of other mathematics. “How about never? Is never good with you?” But maybe we should talk about some of the subtopics. And I volunteeered to talk briefly about modular arithmetic.

2 Modular Arithmetic

Modular arithmetic works with remainders from long division. For example, divide 2023 by 4. You get 505 and a remainder of 3. (Mathematicians call long division with a remainder Euclidean division.) After a while I’ll show you that such remainders can be added, subtracted, multiplied, and divided; they have an arithmetic all their own.

I use modular arithmetic recreationally. With it I can do some difficult calculations in my head. In particular I can verify by direct calculation the validity of a theorem by Fermat, sometimes called Fermat’s “little” theorem to distinguish it from his “last” theorem. I also use modular arithmetic to understand some interesting features of the base-10 number system.

Because this is a pot pourri, I am only going to give you a taste of modular arithmetic, a couple of hors d’ouevres, and leave the main meal for another time.

2.1 First Hors d’Oeuvre: Nines in Base Ten

A long time ago your teacher may have taught you to check your arithmetic by casting out nines. Accountants used to do this. If you did it, you were using modular arithmetic without knowing it.

Nines have interesting features. Let’s look at some of them. Take a number, say the one from your license plate or your birth year. My license number (with the letters removed) is 9616. Divide your number by 9. What’s the remainder? For my example, the remainder is 4. I did not actually do the division. I used a trick. In base-10 the remainder of any number divided by 9 is equal to the sum of the digits in the number, where you keep summing until you have only one digit left.

So what I did was sum

$$9 + 6 + 1 + 6 = 15 + 7 = 22 => 2 + 2 = 4$$

This 4 is the remainder if you divide 9616 by 9. You can do the long division

$$
\begin{array}{r}
1068\\
9\overline{)9616}\\
\underline{9}\\
061\\
\underline{54}\\
76\\
\underline{72}\\
4
\end{array}
$$

but if all you want to know is the remainder, summing the digits is much easier. And notice. As you sum the digits you can ignore the 9s or any combinations of digits that add to 9.

$$9 + 6 + 1 + 6 => 6 + 1 + 6 => 7 + 6 => 1 + 3 => 4$$

Instead of add 7 + 6, you can mentally take 2 from 6 and add it to 7 to make a 9 that you ignore, leaving 4.

Notice that this calculation does not depend on the order of the digits in the number. In other words, each of 9616, 9166, 9661, 6691, 6619, 6169, 6196, 6961,6916, 1669, 1696, 1966, when divided by 9 will have a remainder of 4.

This works for all integer numbers of any number of digits.

If the sum of the digits comes out equal to 9, that means the remainder is 0. When you're dividing by 9, a remainder of 9 means there is no remainder, and your number is exactly divisible by 9. Is your birth year divisible by 9? I discovered that mine is by adding its digits.

Here's another nice feature . If the remainder is 6 or 3, you know immediately that the original number is divisible by 3. Thus you can see at once that 201 is not a prime number; neither is 501.

2.2 Second Hors d'Oeuvre: Fermat and Primes

Around 1640 Pierre de Fermat showed that a prime number, e.g. 7, divided into any other number taken to a power equal to the prime less 1, in this case 6, will always have a remainder of 1. Put slightly differently, if you subtract 1 from the number to the power, the result will be exactly divisible by the prime.

$$\frac{3^6 - 1}{7} = \frac{729 - 1}{7} = 104 \text{ with remainder } 0.$$

Here's a general statement of Fermat's theorem:
Given a prime p and any number n coprime to p then the remainder of

$$\frac{n^{p-1}-1}{p} \text{ is } 0$$

Try this for $n = 2$; and for $n = 5$.

Coprime means that n must not have p as a factor. The modulus 7 and the number 10 are coprime, so $10^6 - 1$ is exactly divisible by 7. The numbers 5 and 10 have a factor 5 in common; they are not coprime, and $(10^4 - 1)$ is not exactly divisible by 5. The numbers 9 and 11 are coprime to 5. Show that $(9^4 - 1)$ and $(11^4 - 1)$ are each divisible by 5. [1]

Most alculations that confirm Fermat's theorem will require large numbers. $5^6 - 1 = 125^2 - 1 = 15624$ which is, indeed, divisible by 7. And you saw that 201 and 501 are not primes. What about 101? When you divide 2^{100} by 101, do you get a remainder of 1? 2^{100} is a number about 30 digits long. I can't handle that on paper, but with modular arithmetic I can do it in my head.

3 Modular Arithmetic

In elementary school you learned to do arithmetic first with integers, then with rational numbers, then with real numbers. You learned to add them, subtract them, multiply them, and divide them. The operations of addition, subtraction, multiplication, and division constitute an arithmetic. There are arithmetics for other objects such as vectors or matrices or complex numbers. There is also an arithmetic of the remainders generated by the familiar long division. This is modular arithmetic.

Some of the properties and ideas of modular arithmetic were known in classical antiquity, the middle ages, and later. In the early nineteenth century Carl Friedrich Gauss drew on these ideas and properties to create modular arithmetic. He made it into a powerful tool for solving certain kinds of problems. A key part of his work is his idea of modulus — a number that generates remainders. For a given modulus the remainders obey the rules of arithmetic.

As a concrete example take 7 as the modulus. Then every number is an integer multiple of 7 plus a remainder. For example, $437 = 62 * 7 + 3$. The remainder is 3. Gauss introduced a notation:

$$437 = 3 \text{ mod } 7$$

Any number divided by 7 will yield a remainder of 0 to 6. You may have seen this behavior represented as "clock" numbers. As you move along the number

[1] Fermat's theorem means that the 4th power of any number coprime to 5 must end in either a 1 or a 6. Obvious yet surprising.

line from 0 to 437, the sweep hand of the clock starts at 0 and advances to 1, to 2, . . . , to 6 and back to 0; it goes around 62 times and then advances to 3. You can have negative remainders. For these you read the clock counter clockwise. Thus for the example here, -1 would be the same as 6; -2 is the same as 5.

What is 156 mod 7?

$$156 = 2 \bmod 7$$

Here comes the arithmetic. What is the remainder you get when you add 156 and 437?

$$437 + 156 = 593 = (3 + 2) \bmod 7 = 5 \bmod 7$$

The remainders add.

What is the remainder when you subtract 156 from 437?

$$437 - 156 = 281 = (3 - 2) \bmod 7 = 1 \bmod 7$$

The remainders subtract.

What if you multiply the two numbers? You get 68172 which has a remainder of $2 \times 3 = 6$. The remainders multiply.

Division is tricky. Instead of dividing as you would with integers, you find the inverse of $156 = 2 \bmod 7$ and multiply 437 by that. The inverse is the number that when multiplied times the divisor (here 156) gives $1 \bmod 7$. It may not exist. For 156 the inverse is 4 because $4 \times 156 = 1 \bmod 7$. Then $4 \times 437 = 5 \bmod 7$. To compare this 5 to 3/2 convert the 3/2 to an integer by noting that 3 mod 7 is equivalent to 10 mod 7.. Then $10/2 = 5$ and in this sense the remainder of the quotient is the ratio of the remainders of the dividend and divisor. Alternatively, find the inverse of 2 and multiply that times 3.

In general given a modulus m and numbers $a_i = n_i \times m + b_i$ where n_i is an integer such that $b_i < m$.

$$\begin{array}{rcll} a_i &=& b_i \bmod m & \\ a_i + a_j &=& (b_i + b_j) \bmod m & \text{remainders add} \\ a_i - a_j &=& (b_i - b_j) \bmod m & \text{remainders subtract} \\ a_i \times a_j &=& (b_i \times b_j) \bmod m & \text{remainders multiply} \\ a_i \times a_j^{-1} &=& (b_i \times b_j^{-1}) \bmod m & \text{remainders divide but not like you expect} \end{array}$$

These relationships define modular arithmetic. To see why they hold consider the algebraic product of two numbers

$$(a_1 m + b_1)(a_2 m + b_2) = a_1 a_2 m^2 + a_1 m b_2 + a_2 m b_1 + b_1 b_2$$

Only the term $b_1 b_2$ is not exactly divisible by m. The remainder of the product is the product of the remainders of the two numbers. If it is greater than m, you divide by m and use that remainder. That is, you find $b_1 b_2 = b' \bmod m$.

4 Why 9s Are Special in Base 10

What about the 9s? A base ten number, for example 1776, uses place to designate powers of ten. That is,

$$1776 = 1 \times 10^3 + 7 \times 10^2 + 7 \times 10^1 + 6 \times 10^0$$

Because the remainder of a sum of numbers equals the sum of the individual numbers' remainders, you can find the remainder of 1776 mod 9 by performing the modulus operation on each term and adding the resulting set of remainders. But see what happens when the modulus is 9. Look at the first term, 1×10^3. This is 1×1000. Any power of 10 is 1 mod 9. This is so because any power of 10 less 1 is a string of 9s and therefore exactly divisible by 9;

$$10^n = 1 \bmod 9 \text{ for any value of } n$$

You can see that the modular value of each term in the representation of 1776 is the product of the modular value of the digit times the modular value of the multiplying power of 10 which is always 1. Then because remainders add, the sum of the digits is the remainder mod 9 for the entire number.

The value of 1776 mod 9 is the sum of its digits:

$$(1 + 7 + 7 + 6) \bmod 9 = (2 \times 10^1 + 1 \times 10^0) \bmod 9 = 3 \bmod 9.$$

The number 3 is the remainder you get when dividing 1776 by 9, and as was proved, it is the repeated sum of its digits.

Notice also that if the remainder is 3, then if instead of dividing by 9 you had divided by 3, there would have been no remainder. The remainder of 3 means 1776 is divisible by 3, and because 1776 is an even number, it is divisible by 2, so it is divisible by both 2 and 3, i.e., it is divisible by 6.

These properties exist because any power of 10 = 1 mod 9.

Suppose you were using a base six number system: 0, 1, 2, 3, 4, 5, 10, 11, 12,13, 14, 15, 20, 21, ... In this system the 5 would play the same role similar as 9 plays in the base 10 system. The base-6 sum of the digits would equal the remainder from division by 5_6.

5 Checking Fermat

Fermat showed that for any prime p and any number n that does not contain p as a factor, n taken to the power $(p - 1)$ will equal 1 mod p

$$n^{p-1} = 1 \bmod p$$

This is the same as saying that $(n^{p-1} - 1)$ is exactly divisible by p. For small values of p, say 2, 3, 5, or 7, it is easy to confirm the theorem by direct calculation.

$$\text{For } n = 2 \text{ and } p = 5; \text{ then } (2^4 - 1) = 15$$

which is divisible by 5. What if $n = 3$? Or $n = 7$? Try them and see.

But what if $p = 101$? Taking $n = 2$ you could calculate 2^{100}, subtract 1 and see if the answer is divisible by 101. The number 2^{100} has 30 digits. It is much easier to use modular arithmetic. Start by finding the modular value, i.e., the remainder, of $2^{10} = 1024$ divided by 101. It's 14. Because the remainder of a product is the product of the remainders, the remainder of $2^{10} \times 2^{10} = 2^{20}$ is $14 \times 14 = 196 = -6 \bmod 101$. So $2^{40} \bmod 101$ will be $-6 \times -6 = 36$ which is $36 \bmod 101$. Do this again to find $2^{80} \bmod 101$ is $1296 = -17 \bmod 101$. Now take the remainder of 2^{20} times the remainder of 2^{80} to get the remainder of $2^{100} = 102 \bmod 101$ which is $2^{100} = 1 \bmod 101$.

This result shows that 101 *could* be a prime number; it does not prove that it is prime. Fermat's theorem does not say that only prime numbers obey his theorem. There are non-primes that satisfy the relationship. A prime number *must* obey the relation, so if 2^{100} had not been $1 \bmod 101$ we would have known it was not prime.