An Introduction to Proofs and the Mathematical Vernacular [1]

Martin V. Day
Department of Mathematics
Virginia Tech
Blacksburg, Virginia 24061
http://www.math.vt.edu/people/day/ProofsBook

Dedicated to the memory of my mother:
Coralyn S. Day, November 6, 1922 – May 13, 2008.

December 7, 2016

Lemma 4.12. *Suppose p is prime and divides a product of positive integers $a_1 \cdots a_m$. Then p divides a_i for some $1 \le i \le m$.*

Proof. We will prove the lemma by induction on m. First consider $m = 1$. Then by hypothesis p divides a_1, which is what we needed to show.

Next suppose the lemma is true for m and suppose p divides $a_1 \cdots a_{m+1}$. If p divides a_{m+1} then we are done. So suppose p does not divide a_{m+1}. Then, since the only (positive) divisors of p are 1 and p, it must be that $\gcd(p, a_{m+1}) = 1$. By applying Lemma 4.9 we conclude that p divides $a_1 \cdots a_m$. By the induction hypothesis it follows that p divides a_i for some $1 \le i \le m$. Thus the lemma holds for $m + 1$. This completes the proof. □

Now we can write a proof of uniqueness of prime factorizations.

Proof (Uniqueness in Theorem 4.11). Suppose there exists a natural number n with two different prime factorizations

$$p_1 \cdots p_s = n = q_1 \cdots q_r, \tag{4.4}$$

where $p_1 \le \cdots \le p_s$ are primes numbered in order and $q_1 \le \cdots \le q_r$ are also primes numbered in order. Since these two factorizations are different, either $s \ne r$ or $p_i \ne q_i$ for some i. Starting with (4.4) we can cancel all common factors and renumber the primes to obtain an equality

$$p_1 \cdots p_k = q_1 \cdots q_m, \tag{4.5}$$

in which none of the p_i appear among the q_i. Since the two factorizations in (4.4) were assumed different, there is at least one prime on each side of (4.5). In particular p_1 is a prime which divides $q_1 \cdots q_m$. By the lemma above, p_1 must divide one of the q_i. Since $p_1 \ne 1$ and $p_1 \ne q_i$ this contradicts the primality of q_i. This contradiction proves that different factorizations do not exist. □

Notice that we have used an "expository shortcut" by referring to a process of cancellation and renumbering but without writing it out explicitly. We are trusting that the reader can understand what we are referring to without needing to see it all in explicit notation. Just describing this in words is clearer than what we would get if we worked out notation to describe the cancellation and renumbering process explicitly.

Problem 4.18 Write a proof of the existence part of Theorem 4.11, namely that a prime factorization exists for each $n > 1$. [Hint: use strong induction, starting with $n = 2$. For the induction step, observe that either $n + 1$ is prime or $n + 1 = mk$ where both $2 \le m, k \le n$.]

FAexist

D The Integers Mod m

All our usual number systems are infinite, but there are finite number systems too! The most basic are the integers mod m, which we introduce in this section. We said "are" because for different choices of $m \in \mathbb{N}$ we will get different number systems. So bear in mind throughout this section that m is allowed to be any given positive integer.

Definition. We say $a, b \in \mathbb{Z}$ are *congruent modulo* m, and write $a \equiv_m b$ (or $a \equiv b \bmod m$) when $b - a$ is divisible by m.

Example 4.6. $3 \equiv 27 \bmod 8$, because $27 - 3 = 3 \cdot 8$. But $3 \not\equiv 27 \bmod 10$, because $27 - 3 = 24$ is not divisible by 10.

Lemma 4.13. *Congruence modulo m is an equivalence relation on $\mathbb{Z}$.*

Proof. For any $a \in \mathbb{Z}$, since $a - a = 0 = 0 \cdot m$ we see that $a \equiv_m a$, showing that $\equiv_m$ is reflexive. If $a \equiv_m b$, then $b - a$ is divisible by m. But then $a - b = -(b - a)$ is also divisible by m, so that $b \equiv_m a$. This shows that $\equiv_m$ is symmetric. For transitivity, suppose $a \equiv_m b$ and $b \equiv_m c$. Then $a - b$ and $b - c$ are both divisible by m. It follows that $a - c = (a - b) + (b - c)$ is also divisible by m, implying $a \equiv_m c$. □

Since $\equiv_m$ is an equivalence relation, we can define its equivalence classes according to Definition 3.8 on page 62. We abbreviate the notation for an equivalence class, writing $[n]_m$ rather than $[n]_{\equiv_m}$, and will refer to $[n]_m$ as a *congruence class* mod m.

Definition. Suppose m is a positive integer. The *integers modulo* m is the set $\mathbb{Z}_m$ of equivalence classes modulo m:

$$\mathbb{Z}_m = \{[n]_m : \ n \in \mathbb{Z}\}.$$

Back on page 63 we talked about the idea of defining new mathematical objects to be equivalence classes with respect to some equivalence relation. There we talked about considering an angle to be the set all real numbers which were "equivalent to each other as angles," i.e. an equivalence class of the relation $\oslash$ of Example 3.12. We are doing the same thing here using the relation $\equiv_m$: we take the set of all integers which are congruent to each other mod m and put them together as a set (congruence class); that set is a single element of $\mathbb{Z}_m$.

Example 4.7. A typical element of $\mathbb{Z}_8$ is

$$[27]_8 = \{\ldots, -13, -5, 3, 11, 19, 27, \ldots\}.$$

We can indicate the same equivalence class several ways, for instance $[27]_8 = [3]_8$. (We have several different ways of referring to the same real number as well, for instance $\frac{1}{2} = .5$.) We would say that 27 and 3 are both representatives of the equivalence class $[27]_8$. We can choose any representative of an equivalence class to identify it. But we often use the smallest nonnegative representative, which would be 3 in this example.

Whether we refer to it as $[27]_8$ or $[3]_8$ it is just one element of $\mathbb{Z}_8$. There are a grand total of 8 elements in $\mathbb{Z}_8$:

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}.$$

Every congruence class mod 8 is the same as one of these.

We have been saying that $\mathbb{Z}_m$ is a number system. That must mean there is a way to define addition and multiplication on the elements of $\mathbb{Z}_m$, i.e. there is a way to add and multiply congruence classes. The next example begins to explain.

Example 4.8. $3 \equiv_8 27$ and $5 \equiv_8 45$. Observe that

$$3 \cdot 5 \equiv_8 27 \cdot 45 \text{ and } 3 + 5 \equiv_8 27 + 45.$$

This example illustrates the fact that $\equiv_m$ "respects" the operations of multiplication and addition. The next lemma states this precisely.

Lemma 4.14. *Suppose $a \equiv_m a'$ and $b \equiv_m b'$. Then $a + b \equiv_m a' + b'$, $a \cdot b \equiv_m a' \cdot b'$, and $a - b \equiv_m a' - b'$.*

Proof. By hypothesis there exist $k, \ell \in \mathbb{Z}$ for which $a' = a + km$ and $b' = b + \ell m$. Then

$$a'b' = (a + km)(b + \ell m) = ab + (a\ell + bk + k\ell m)m,$$

which implies that $ab \equiv_m a'b'$. The proofs for addition and subtraction are similar. □

Here is how you should understand this. Suppose A and B are any two elements of $\mathbb{Z}_m$. (For example, $A = [3]_8$ and $B = [5]_8$.) We can add A and B in the following way: pick any element a of A and any element b of B. (For instance $a = 3$ and $b = 5$.) Form $a + b$ using ordinary arithmetic, and then take C to be the equivalence class of the result: $C = [a + b]_m$. (In our example, $C = [3 + 5]_8 = [0]_8$.) Then C is what we mean by $A + B$. What the lemma says is that the a and b that you picked don't matter; you will arrive at the same result C regardless. (For instance if we picked $a' = 27$ and $b' = 45$ instead, we would still get $C = [27 + 45]_8 = [72]_8 = [0]_8$.) The same procedue works for multiplication: $D = A \cdot B$ is $D = [a \cdot b]_m$.

Definition. Addition, multiplication, and negation are defined on $\mathbb{Z}_m$ by

$$\begin{aligned} [a]_m + [b]_m &= [a + b]_m, \\ [a]_m \cdot [b]_m &= [a \cdot b]_m, \\ -[a]_m &= [-a]_m. \end{aligned}$$

With this definition $\mathbb{Z}_m$ is a *finite* number system, and satisfies all the algebraic properties we listed in Section A.1:(A1)–(A5), (M1)–(M4), and (D). (There is no order relation, however.) This is called arithmetic *mod m* or simply *modular arithmetic*.

Example 4.9. Here are the addition and multiplication tables for $\mathbb{Z}_6$. (All the entries should really be surrounded by "$[\cdot]_6$" but we have left all these brackets out to spare our eyes from the strain.)

+	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

*	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	4	2
5	0	5	4	3	2	1

Notice that $[2]_6 \neq [0]_6$ and $[3]_6 \neq [0]_6$, but $[2]_6 \cdot [3]_6 = [0]_6$. In other words in $\mathbb{Z}_6$ two nonzero numbers can have zero as their product! (We have seen this happen before; see Problems 4.1 and the 2×2 matrices of Section A.3.)

There are many clever and creative things we can use modular arithmetic for.

Example 4.10. There do not exist positive integers a, b for which $a^2 + b^2 = 1234567$. A long, tedious approach would be to examine all possible pairs a, b with $1 \leq a, b < 1234567$. A faster way is to consider the implications modulo 4. If $a^2 + b^2 = 1234567$ were true then (mod 4),

$$[a]^2 + [b]^2 = [a^2 + b^2] = [1234567] = [3].$$

(For the last equality, observe that $1234567 = 1234500 + 64 + 3$, which makes it clear that $12345467 \equiv_4 3$.) Now in $\mathbb{Z}_4$, $[n]^2$ is always either $[0]$ or $[1]$. So there are four cases: $[a]^2 = [0]$ or $[1]$ and $[b]^2 = [0]$ or $[1]$. Checking the four cases, we find

$[a]^2$	$[b]^2$	$[a]^2 + [b]^2$
$[0]$	$[0]$	$[0]$
$[0]$	$[1]$	$[1]$
$[1]$	$[0]$	$[1]$
$[1]$	$[1]$	$[2]$

In no case do we find $[a]^2 + [b]^2 = [3]$. Thus $a^2 + b^2 = 1234567$ is not possible, no matter what the values of a and b.

In fact, we can turn this idea into a proposition. The proof is essentially the solution of the above example, so we won't write it out again.

Proposition 4.15. *If $c \equiv_4 3$, there do not exist integers a, b for which $a^2 + b^2 = c$.*

Problem 4.19 A natural question to ask about Example 4.10 is why we choose to use mod 4; why not some other m?

a) Show that in $\mathbb{Z}_6$ every $[n]$ occurs as $[a]^2 + [b]^2$ for some a and b. What happens if we try to repeat the argument of Example 4.10 in $\mathbb{Z}_6$ — can we conclude that $a^2 + b^2 = 1234567$ is impossible in that way?

b) For the argument of Example 4.10 to work in $\mathbb{Z}_m$, we need to use an m for which

$$\{[a]_m^2 + [b]_m^2 : \ a, b \in \mathbb{Z}\} \neq \mathbb{Z}_m.$$

This happens for $m = 4$ but not for $m = 6$. Can you find some values of m other than 4 for which this happens? [Hint: there are two values $m < 10$ other than $m = 4$ for which it works.]

expyth

Problem 4.20 Find values of $a, b, m \in \mathbb{N}$ so that $a^2 \equiv_m b^2$ but $a \not\equiv_m b$.

powne

Problem 4.21 Suppose $n \in \mathbb{N}$ is expressed in the usual decimal notation $n = d_k d_{k-1} \cdots d_1 d_0$, where each d_i is one of the digits $0, \ldots, 9$. You probably know that n is divisible by 3 if and only if $d_k + d_{k-1} + \cdots + d_1 + d_0$ is divisible by 3. Use $\mathbb{Z}_3$ to prove why this is correct. [Hint: The notation we use for the number one hundred twenty three, "n=123," does *not* mean $n = 1 \cdot 2 \cdot 3$. What *does* it mean? More generally what does "$n = d_k d_{k-1} \cdots d_1 d_0$" mean?] Explain why the same thing works for divisibility by 9.

div39

Problem 4.22 Along the same lines as the preceding problem, show that n is divisible by 11 if and only if the *alternating* sum of its digits $d_0 - d_1 + d_2 \cdots + (-1)^k d_k$ is divisible by 11.

div11

Problem 4.23 What is the remainder when $1^{99} + 2^{99} + 3^{99} + 4^{99} + 5^{99}$ is divided by 5? (From [17].)

pow99

Problem 4.24 What is the last digit of $2^{1000000}$? (Based on [9, #7 page 272])

TwoK

E Axioms and Beyond: Gödel Crashes the Party

We introduced a set of axioms for the integers in Section A.4. Axioms have been developed for many of the most basic mathematical systems, such as the natural numbers, the real numbers, set theory. (Russell's paradox showed that we need to be careful about what kinds of statements about sets we allow. To resolve this this requires developing a system of axioms for set theory.) If you take a modern algebra class you will see definitions of other types of algebraic systems (such as groups, rings and fields) in terms of axioms. In any of these settings, a set of axioms is a collection of basic properties from which all other properties can be derived and proven logically.

In the 1920s David Hilbert proposed that all of mathematics might be reduced to an appropriate list of axioms, from which everything mathematical could be then be derived in an orderly, logical way. This system of axioms should be complete, i.e. all true statements should be provable from it. It should also be consistent, i.e. there should be no contradictions that follow logically from the axioms. This would put all of mathematics on a neat and tidy foundation. By developing formal rules that govern logical arguments and deductions, so that proofs could be carried out mechanically, we would in principle be able to turn over all of mathematics to computers which would then determine all mathematical truth for us. In 1931 Kurt Gödel pulled the plug on that possibility. He showed that in *any* axiomatic system (provided it is at least elaborate enough to include $\mathbb{N}$) there are statements that can be neither proven nor disproven, i.e. whose truth or falsity *cannot* be logically established based on the axioms. (A good discussion of Gödel's brilliant proof is given in [21].) Gödel's result tells us that we can not pin our hopes on some ultimate set of axioms. There will always be questions which the axioms are not adequate to answer.

For instance suppose we consider the axioms for the integers as listed in Section A.4, but leave out the well-ordering principle. Now we ask if the well-ordering principle is true or false based on the other axioms. We know that $\mathbb{Z}$ satisfies the axioms and the well-ordering principle is true for $\mathbb{Z}$. That means it is impossible