

**READING TO ACCOMPANY CSU-P MATH 319
NUMBER THEORY
SPRING TERM, 2014**

JONATHAN A. PORITZ *AFTER WISSAM RAJI*

2. CONGRUENCES

A congruence is nothing more than a statement about divisibility. The theory of congruences was introduced by Carl Friedreich Gauss, in his monumental *Disquisitiones Arithmeticae* (published in 1801, when he was 24).

We start by introducing congruences and their properties. We then present solutions to linear congruences which will serve as an introduction to the Chinese Remainder Theorem that follows.

2.1. Introduction to congruences. As we mentioned in the introduction, the theory of congruences was developed by Gauss at the beginning of the nineteenth century.

Definition 2.1. Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, we say that a **is congruent to b modulo n** if $n \mid (a - b)$, i.e., if $\exists k \in \mathbb{Z}$ such that $a = b + kn$. If a is congruent to b modulo n , we write $a \equiv b \pmod{n}$.

Example 2.2. $19 \equiv 5 \pmod{7}$. Similarly $2k + 1 \equiv 1 \pmod{2}$ which means every odd number is congruent to 1 modulo 2.

Congruence is much like equality in many ways. For example:

Theorem 2.3. Given $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then

(1) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Date: 17 February 2014 00:51 These notes are adapted by Jonathan Poritz from **An Introductory Course in Elementary Number Theory** by Wissam Raji, see www.saylor.org/books/. Both these notes and Raji's text are released under a Creative Commons **CC BY 3.0** license, see

<https://creativecommons.org/licenses/by/3.0/>



- (2) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
- (3) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.
- (4) If $a \equiv b \pmod{n}$, then $a - c \equiv b - c \pmod{n}$.
- (5) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.
- (6) If $c > 0$ and $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{nc}$.
- (7) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$.
- (8) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a - c \equiv b - d \pmod{n}$.
- (9) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.

Proof.

- (1) If $a \equiv b \pmod{n}$, then $n \mid (a - b)$. Thus $\exists k \in \mathbb{Z}$ such that $a - b = kn$. This implies $b - a = (-k)n$ and thus $n \mid (b - a)$. Consequently $b \equiv a \pmod{n}$.
- (2) Since $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, $n \mid (a - b)$ and $n \mid (b - c)$. As a result, there $\exists k, l \in \mathbb{Z}$ such that $a = b + kn$ and $b = c + ln$, which imply that $a = c + (k + l)n$. In other words, $a \equiv c \pmod{n}$.
- (3) Since $a \equiv b \pmod{n}$, $n \mid (a - b)$. So if we add and subtract c we get

$$n \mid ((a + c) - (b + c))$$

which means that

$$a + c \equiv b + c \pmod{n}.$$

- (4) Since $a \equiv b \pmod{n}$, $n \mid (a - b)$ so we can subtract and add c to get

$$n \mid ((a - c) - (b - c))$$

so

$$a - c \equiv b - c \pmod{n}.$$

- (5) If $a \equiv b \pmod{n}$, $n \mid (a - b)$. Thus there $\exists k \in \mathbb{Z}$ such that $a - b = kn$ and as a result $ac - bc = (kc)n$. Therefore

$$n \mid (ac - bc)$$

and hence

$$ac \equiv bc \pmod{n}.$$

- (6) If $a \equiv b \pmod{n}$, $n \mid (a - b)$. Thus there $\exists k \in \mathbb{Z}$ such that $a - b = kn$ and as a result

$$ac - bc = (k)cn.$$

Thus

$$nc \mid (ac - bc)$$

and hence

$$ac \equiv bc \pmod{nc}.$$

- (7) Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, $n \mid (a - b)$ and $n \mid (c - d)$. As a result, there $\exists k, l \in \mathbb{Z}$ such that $a - b = kn$ and $c - d = ln$. Note that

$$(a - b) + (c - d) = (a + c) - (b + d) = (k + l)n.$$

As a result,

$$n \mid ((a + c) - (b + d)),$$

hence

$$a + c \equiv b + d \pmod{n}.$$

- (8) If $a = b + kn$ and $c = d + ln$ for $k, l \in \mathbb{Z}$, we have

$$(a - b) - (c - d) = (a - c) - (b - d) = (k - l)n.$$

As a result,

$$n \mid ((a - c) - (b - d)),$$

hence

$$a - c \equiv b - d \pmod{n}.$$

- (9) $\exists k, l \in \mathbb{Z}$ such that $a - b = kn$ and $c - d = ln$ and thus $ca - cb = (ck)n$ and $bc - bd = (bl)n$. Note that

$$(ca - cb) + (bc - bd) = ac - bd = (kc - lb)n.$$

As a result,

$$n \mid (ac - bd),$$

hence

$$ac \equiv bd \pmod{n}.$$

□

Here is a technical result which will be useful later:

Theorem 2.4. *Given $a, b, c \in \mathbb{Z}$, if $a \mid c$, $b \mid c$, and a and b are relatively prime, then $ab \mid c$.*

Proof. By Corollary 1.27, we know $\exists m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Also, because of the divisibility hypotheses, we also know $\exists p, q \in \mathbb{Z}$ such that $c = pa$ and $c = qb$. Compute:

$$c = c \cdot 1 = c(ma + nb) = mca + ncb = mqba + npab = (mq + np)ab.$$

But this means $ab \mid c$, as desired. □

Examples 2.5.

- (1) $14 \equiv 8 \pmod{6}$ so $8 \equiv 14 \pmod{6}$.
- (2) Because $22 \equiv 10 \pmod{6}$ and $10 \equiv 4 \pmod{6}$, it is also true that $22 \equiv 4 \pmod{6}$.
- (3) $50 \equiv 20 \pmod{15}$ so $50 + 5 = 55 \equiv 20 + 5 = 25 \pmod{15}$.
- (4) $50 \equiv 20 \pmod{15}$ so $50 - 5 = 45 \equiv 20 - 5 = 15 \pmod{15}$.
- (5) $19 \equiv 16 \pmod{3}$ so $2(19) = 38 \equiv 2(16) = 32 \pmod{3}$.
- (6) $19 \equiv 16 \pmod{3}$ so $2(19) = 38 \equiv 2(16) = 32 \pmod{2 \cdot 3}$ or $38 \equiv 2(16) = 32 \pmod{6}$.
- (7) Because $19 \equiv 3 \pmod{8}$ and $17 \equiv 9 \pmod{8}$, we have $19 + 17 = 36 \equiv 3 + 9 = 12 \pmod{8}$.
- (8) Because $19 \equiv 3 \pmod{8}$ and $17 \equiv 9 \pmod{8}$, we have $19 - 17 = 2 \equiv 3 - 9 = -6 \pmod{8}$.
- (9) Because $19 \equiv 3 \pmod{8}$ and $17 \equiv 9 \pmod{8}$, we have $19(17) = 323 \equiv 3(9) = 27 \pmod{8}$.

Here is a result which at first seems very simple, but turns out to be immensely useful – so useful it has a name, “Euclid’s Lemma.”

Lemma 2.6. *Given $x, y, z \in \mathbb{Z}$, if $x \mid yz$ and $\gcd(x, y) = 1$ then $x \mid z$.*

Proof. From Corollary 1.27, we know $\exists m, n \in \mathbb{Z}$ such that $mx + ny = 1$. Multiplying by z , we get $mxz + nyz = z$. But we've assumed that $x \mid yz$, so $x \mid nyz$, and certainly $x \mid mxz$, so $x \mid mxz + nyz$, i.e., $x \mid z$. $\square$

We now present a theorem that will show one difference between equations and congruences: in equations, if we divide both sides of the equation by a non-zero number, equality holds. However, in congruences, this is not necessarily true. In other words, dividing both sides of a congruence by the same integer does not necessarily preserve the congruence.

Theorem 2.7.

- (1) Given $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$, define $d = \gcd(a, n) \in \mathbb{N}$. If $ab \equiv ac \pmod{n}$ then $b \equiv c \pmod{n/d}$.
- (2) In particular, if $\gcd(a, n) = 1$ then

$$b \equiv c \pmod{n} \iff ab \equiv ac \pmod{n}.$$

Proof. For Part 1, if $ab \equiv ac \pmod{n}$, then

$$n \mid (ab - ac) = a(b - c).$$

Hence $\exists k \in \mathbb{Z}$ such that $a(b - c) = kn$. Dividing both sides by d , we get $(a/d)(b - c) = k(n/d)$ or $(n/d) \mid (a/d)(b - c)$. Now, by Theorem 1.23, $\gcd(a/d, n/d) = 1$ so Euclid's Lemma tells us that $(n/d) \mid (b - c)$. Hence $b \equiv c \pmod{n/d}$.

For Part 2, the direction $\Rightarrow$ is part 5 of Theorem 2.3, while $\Leftarrow$ is a special case of Part 1. $\square$

Example 2.8. $38 \equiv 10 \pmod{7}$. Since $\gcd(2, 7) = 1$, we have $19 \equiv 5 \pmod{7}$.

One last technical result is worth stating clearly at this point:

Theorem 2.9. Given $n, d \in \mathbb{N}$ such that $d \mid n$, there are exactly d values $x \in \mathbb{Z}$, up to congruence modulo n , satisfying $x \equiv 0 \pmod{n/d}$.

Proof. Let $x_j = j(n/d)$ for $j = 0, \dots, (d - 1)$. Certainly each of these d values x_j is a multiple of n/d and so solves $x \equiv 0 \pmod{n/d}$. All we

must show, then, is that *every* solution x of $x \equiv 0 \pmod{n/d}$ is congruent, modulo n , to one of these x_j .

Let x be such a solution, so $\exists k \in \mathbb{Z}$ such that $x = k(n/d)$. Use the Division Algorithm for x divided by n , getting $x = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. But

$$r = x - qn = k(n/d) - qd(n/d) = (k - qd)(n/d)$$

so r is a multiple of (n/d) which lies in the range $[0, n)$. The only such multiples are the $x_0, \dots, x_{(d-1)}$ defined above; say $r = x_j$. Then $x = qn + r = qn + x_j \equiv x_j \pmod{n}$, so every solution x is congruent modulo n to exactly one of the d particular solutions $x_1, \dots, x_{(d-1)}$. $\square$

Exercises

- (1) Determine whether 3 and 99 are congruent modulo 7 or not.
- (2) Show that if x is an odd integer, then $x^2 \equiv 1 \pmod{8}$.
- (3) Show that if $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$ are such that $n \mid m$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.
- (4) Show that if $n, k \in \mathbb{N}$ and $\{a_1, \dots, a_k, b_1, \dots, b_k\} \subset \mathbb{Z}$ satisfy $a_i \equiv b_i \pmod{n}$ for $i = 1, 2, \dots, k$, then $\sum_{i=1}^k a_i \equiv \sum_{i=1}^k b_i \pmod{n}$.
- (5) For which $n \in \mathbb{N}$ is it true that $1 + 2 + \dots + (n-1) \equiv 0 \pmod{n}$?

2.2. Linear Congruences. Because congruence is analogous to equality, it is natural to ask about the analogues of linear equations, the simplest equations one can solve in algebra, but using congruence rather than equality. In this subsection, we discuss “linear congruences of one variable” and their solutions.

We start with a definition:

Definition 2.10. Given constants $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}$, a congruence of the form $ax \equiv b \pmod{n}$ where $x \in \mathbb{Z}$ is unknown is called a **linear congruence in one variable**.

If a linear congruence has one solution, then it has infinitely many:

Theorem 2.11. *Given constants $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}$, and a solution $x \in \mathbb{Z}$ to the linear congruence $ax \equiv b \pmod{n}$, any other $x' \in \mathbb{Z}$ satisfying $x' \equiv x \pmod{n}$ is also a solution of the same congruence.*

[Note: in the early history of number theory, before Gauss, one talked about

Definition 2.12. An algebraic equation whose constants and variables are all integers is called a **Diophantine equation**.

Then the modern linear congruence $ax \equiv b \pmod{n}$, for $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ is equivalent to the linear Diophantine equation $ax - ny = b$ in the two unknowns x and y .]

The following gives a fairly complete characterization of solutions of linear congruences:

Theorem 2.13. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ and consider the linear congruence*

$$ax \equiv b \pmod{n}.$$

Setting $d = \gcd(a, n)$, we have

- (1) *If $d \nmid b$, then the congruence has no solutions.*
- (2) *If $d \mid b$, then the congruence has exactly d solutions which are distinct modulo n .*

Proof. For Part 1, we prove its contrapositive. So assume the congruence has solutions, meaning $\exists x, k \in \mathbb{Z}$ such that $ax - b = kn$, or $ax - kn = b$. But since $d = \gcd(a, n)$ is a common divisor of a and n , it divides the linear combination $ax - kn = b$. Hence $d \mid b$.

Now for Part 2, assume $d \mid b$, so $\exists k \in \mathbb{Z}$ such that $kd = b$. But from Theorem 1.26 we know $\exists p, q \in \mathbb{Z}$ such that $d = pa + qn$. This means that $kpa + kqn = kd = b$ or, rearranging, $a(kp) - b = (-kq)n$. Hence $n \mid a(kp) - b$, i.e., $a(kp) \equiv b \pmod{n}$ and thus $x = kp$ is one solution to the linear congruence $ax \equiv b \pmod{n}$.

Finally, let us prove that there are the correct number of solutions, mod n , of the congruence equation. We have just seen that there is at least one

$x \in \mathbb{Z}$ satisfying $ax \equiv b \pmod{n}$. Let $y \in \mathbb{Z}$ be any other solution. Then $ax \equiv b \equiv ay \pmod{n}$. By part (2) of Theorem 2.7, $x \equiv y \pmod{n/d}$, or $\delta = y - x \equiv 0 \pmod{n/d}$. Now by Theorem 2.9, there are exactly d possibilities, modulo n , for this δ . Thus there are d solutions of $ax \equiv b \pmod{n}$ of the form $x + \delta$. $\square$

Remark 2.14. Notice that if $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ are relatively prime, then $\forall b \in \mathbb{Z}$ there is a unique solution modulo n to the equation $ax \equiv b \pmod{n}$.

Example 2.15. Let us find all the solutions of the congruence $3x \equiv 12 \pmod{6}$. Notice that $\gcd(3, 6) = 3$ and $3 \mid 12$. Thus there are three incongruent solutions modulo 6. Using the Euclidean algorithm to find the solution of the equation $3x - 6y = 12$ we get a solution $x_0 = 6$. Thus the three incongruent (modulo 6) solutions are given by $x_1 = 6 \pmod{6}$, $x_2 = 6 + 2 = 2 \pmod{6}$ and $x_3 = 6 + 4 = 4 \pmod{6}$.

As we mentioned in Remark 2.14, the congruence $ax \equiv b \pmod{n}$ for $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ has a unique (modulo n) solution if $\gcd(a, n) = 1$. This will allow us to talk about *modular inverses*.

Definition 2.16. Given $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, a solution to the congruence $ax \equiv 1 \pmod{n}$ for $(a, n) = 1$ is called the **inverse of a modulo n** . We denote such an inverse by a^{-1} , with the n to be understood from context.

Stating formally what was just recalled from Remark 2.14, we have

Corollary 2.17. *Given $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ which are relatively prime, the modular inverse a^{-1} exists and is unique modulo n .*

Example 2.18. The modular inverse 7^{-1} of 7 modulo 48 is 7. Notice that a solution of $7x \equiv 1 \pmod{48}$ is $x \equiv 7 \pmod{48}$.

Exercises

- (1) Find all solutions of $3x \equiv 6 \pmod{9}$.
- (2) Find all solutions of $3x \equiv 2 \pmod{7}$.
- (3) Find inverses modulo 13 of 2 and of 11.

- (4) Given $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, show that if a^{-1} is the inverse of a modulo n and b^{-1} is the inverse of b modulo n , then $a^{-1}b^{-1}$ is the inverse of ab modulo n .

2.3. The Chinese Remainder Theorem. In this subsection, we discuss solutions of systems of congruences having different moduli. An example of this kind of systems is the following: find a number that leaves a remainder of 1 when divided by 2, a remainder of 2 when divided by three and a remainder of 3 when divided by 5. We shall see that there is a systematic way of solving this kind of system.

The Chinese Remainder Theorem. Fix a $k \in \mathbb{N}$. Then given $b_1, \dots, b_k \in \mathbb{Z}$ and $n_1, \dots, n_k \in \mathbb{N}$, the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

has a solution $x \in \mathbb{Z}$ if the $n_1, n_2, \dots, n_k$ are pairwise relatively prime. The solution is unique modulo $N = n_1 n_2 \dots n_k$.

Proof. For $j = 1, \dots, k$, let $N_j = N/n_j$. Since the moduli n_j are pairwise relatively prime, $\gcd(N_j, n_j) = 1$ – after all, N_j is the product of all the moduli except n_j . Hence by Corollary 2.17, $\exists y_j = N_j^{-1}$ modulo n_j , satisfying $N_j y_j \equiv 1 \pmod{n_j}$. Consider now

$$x = \sum_{j=1}^k b_j N_j y_j$$

Since

$$N_j \equiv 0 \pmod{n_i} \quad \forall i \neq j,$$

we see that

$$x \equiv b_j N_j y_j \equiv b_j \pmod{n_j}.$$

Hence x is a solution to the system of congruences.

We have to show now that any two solutions are congruent modulo N . Suppose that x and y are both solutions of the system of congruences. Then $x \equiv b_j \equiv y \pmod{n_j}$, or $n_j \mid x - y$, for all $1 \leq j \leq k$. But then, since the moduli are pairwise relatively prime, using Theorem 2.4 k times (formally, this needs to be done by induction!), we can conclude that $N = n_1 \dots n_k \mid x - y$ or $x \equiv y \pmod{N}$. $\square$

Example 2.19. Solve the system

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}.$$

We have $N = 2 \cdot 3 \cdot 5 = 30$. Also

$$N_1 = 30/2 = 15, \quad N_2 = 30/3 = 10, \quad \text{and} \quad N_3 = 30/5 = 6.$$

So we have to solve now $15y_1 \equiv 1 \pmod{2}$ – a solution is $y_1 \equiv 1 \pmod{2}$. In the same way, we find that $y_2 \equiv 1 \pmod{3}$ and $y_3 \equiv 1 \pmod{5}$. Therefore

$$x = 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 = 53 \equiv 23 \pmod{30}.$$

Exercises

- (1) Find an integer that leaves a remainder of 2 when divided by either 3 or 5, but that is divisible by 4.
- (2) Find all integers that leave a remainder of 4 when divided by 11 and leaves a remainder of 3 when divided by 17.
- (3) Find all integers that leave a remainder of 1 when divided by 2, a remainder of 2 when divided by 3 and a remainder of 3 when divided by 5.
- (4) A band of 17 pirates steal some gold bars. When they try to divide the spoils equally, 3 bars are left over – so a fight breaks out, killing one. This immediately brings calm as they see if the gold can now be evenly shared. Unfortunately, there are now 10 bars left out, so they fight again. After the inevitable (single) further death, a perfect

division is now possible. What is the minimum number of gold bars the pirates could have started with? *[This is apparently an ancient Chinese problem.]*

2.4. Another Way to Work with Congruences: Equivalence Classes. In this subsection, we shall consider another way to work with congruences, based upon the following:

Definition 2.20. Let S be a set and $\cong$ a relation defined on S . (That is, $\forall x, y \in S$, the statement “ $x \cong y$ ” may be true or false.) If $\cong$ satisfies the following three properties, it is called an **equivalence relation**:

- *[Reflexivity]* $\forall x \in S, x \cong x$.
- *[Symmetry]* $\forall x, y \in S, x \cong y \Leftrightarrow y \cong x$.
- *[Transitivity]* $\forall x, y, z \in S, x \cong y$ and $y \cong z \Rightarrow x \cong z$.

If $\cong$ is an equivalence relation on the set S and $x \in S$, then the set $[x] = \{y \in S \mid y \cong x\} \subseteq S$ is called the **equivalence class of x** . We write $S/\cong$ for the set of equivalence classes in S . And if $\mathcal{C} \in S/\cong$, then any $r \in \mathcal{C}$ such that $\mathcal{C} = [r]$ is called a **representative of the equivalence class $\mathcal{C}$** .

Theorem 2.21. Let S be a set and $\cong$ an equivalence relation defined on S . Then

- (1) $\forall x \in S, x \in [x]$.
- (2) $\forall x, y \in S$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$, but not both.

Proof. (1): This is just the reflexivity of $\cong$.

(2): Suppose $z \in [x] \cap [y]$. This means $z \cong x$ and $z \cong y$, so by symmetry $y \cong z$ and by transitivity, $x \cong y$.

Now if $a \in [x]$ and $b \in [y]$, then $a \cong x$ and $b \cong y$. By transitivity, $a \cong x \cong y \cong b$. Thus $a \in [y]$ and, by symmetry, $b \cong x$ so $b \in [x]$.

Therefore $[x] \subseteq [y]$ and $[y] \subseteq [x]$, and thus $[x] = [y]$.

Since the above construction only relied on the existence of some element $z \in [x] \cap [y]$, we see that the only way we could fail to have $[x] = [y]$ is if $[x] \cap [y] = \emptyset$. □

Example 2.22. On the set $S = \{(n, m) \mid n, m \in \mathbb{Z}, m \neq 0\}$ we can define the relation $(a, b) \cong (c, d)$ if $ad = cb$. Then $S/\cong$ is nothing other than the rational numbers, $\mathbb{Q}$!

Now let us specialize the concept of equivalence class to the case of congruences:

Proposition 2.23. *Given $n \in \mathbb{N}$, the relation on $\mathbb{Z}$ defined by*

$$a \cong_n b \Leftrightarrow a \equiv b \pmod{n}$$

(which we shall write $a \cong b$ if the n is clear from context) is an equivalence relation.

Definition 2.24. Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, the equivalence class of a under the above equivalence relation is called the **congruence class of a mod n** and is written $[a]_n$ (or, by abuse of notation, merely $[a]$ if the n is understood from the context). The set of equivalence classes $\mathbb{Z}/\cong_n$ is called the **integers mod n** and is written $\mathbb{Z}/n\mathbb{Z}$ (or, by some authors, $\mathbb{Z}/n$ or $\mathbb{Z}_n$).

Theorem 2.25. *Given $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ has n elements, with representatives $0, \dots, n-1$ of these distinct equivalence classes. That is,*

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \dots, [n-1]_n\}.$$

Proof. Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, the Division Algorithm tells us there is a unique pair $q, r \in \mathbb{Z}$ such that $a = qn + r$ and $0 \leq r < n$. Note that $a \equiv r \pmod{n}$ or, equivalently, $a \in [r]$. Thus every $a \in \mathbb{Z}$ is an element of a unique equivalence class $[r]$ for $r \in \{0, \dots, n-1\}$. Since each such $r \in [r]$, uniquely!, the equivalence classes $[0], \dots, [n-1]$ are all distinct. $\square$

The remarkable thing about these $\mathbb{Z}/n\mathbb{Z}$ is that we can do much of the usual integer arithmetic in them; in fact, sometimes we can do a bit more than the usual.

Definition 2.26. Given $n \in \mathbb{N}$ and $\mathcal{C}, \mathcal{D} \in \mathbb{Z}/n\mathbb{Z}$, define $\mathcal{C} + \mathcal{D} = [a + b]$ and $\mathcal{C} \cdot \mathcal{D} = [a \cdot b]$ where a and b are any representatives of the congruence classes $\mathcal{C}$ and $\mathcal{D}$, respectively.

Theorem 2.27. *The operations $+$ and $\cdot$ on $\mathbb{Z}/n\mathbb{Z}$ are well-defined. That is, they are independent of the choices of representatives of the congruence classes.*

Proof. Say $n \in \mathbb{N}$ and $\mathcal{C}, \mathcal{D} \in \mathbb{Z}/n\mathbb{Z}$. Let $a, p, b, q \in \mathbb{Z}$ be such that $\mathcal{C} = [a] = [p]$ and $\mathcal{D} = [b] = [q]$. Then $p \equiv a \pmod{n}$ and $q \equiv b \pmod{n}$. But then Theorem 2.3 tells us that $a + b \equiv p + q \pmod{n}$ and $a \cdot b \equiv p \cdot q \pmod{n}$, so $[a + b] = [p + q]$ and $[a \cdot b] = [p \cdot q]$. This means that $\mathcal{C} + \mathcal{D}$ can be defined either as $[a + b]$ or as $[p + q]$ and it will be the same thing, as asserted, and likewise for $\mathcal{C} \cdot \mathcal{D}$. $\square$

These new operations are quite nice:

Theorem 2.28. *Given $n \in \mathbb{N}$, the addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$*

- (1) *are commutative and associative;*
- (2) *multiplication distributes over addition;*
- (3) *both operations have an identity – $[0]$ for addition and $[1]$ for multiplication;*
- (4) *every element of $\mathbb{Z}/n\mathbb{Z}$ has an additive inverse – the inverse of $[a]$ is $[-a]$ (or $[n - a]$, another name for the same thing); and*
- (5) *an element $[a] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse $[a]^{-1}$ if and only if $\gcd(a, n) = 1$; this inverse is unique when it exists.*

Proof. Left to the reader. Note the last point is basically Corollary 2.17 restated in the language of congruence classes. $\square$

We can also restate many of our other, earlier results beside just Corollary 2.17 in terms of congruence classes. Most of these shall be left to the reader, but here is one example:

Theorem 2.29. *Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, let $d = \gcd(a, n)$. Consider the equation*

$$[a] \cdot x = [b]$$

where $x \in \mathbb{Z}/n\mathbb{Z}$. Then

- (1) *If $d \nmid b$, there are no solutions.*

(2) If $d \mid b$, this equation has exactly d solutions in $\mathbb{Z}/n\mathbb{Z}$.

Proof. Left to the reader; this is really just Theorem 2.13 stated differently. $\square$

Exercises

(1) When the rational numbers $\mathbb{Q}$ are described as in Example 2.22, we define addition by $[(n, m)] + [(p, q)] = [(nq + mp, mq)]$ and multiplication by $[(n, m)] \cdot [(p, q)] = [(np, mq)]$, where $n, m, p, q \in \mathbb{Z}$ and neither m nor q is 0. Prove a version of Theorems 2.27 for this version of $\mathbb{Q}$.

What are the additive and multiplicative identities in this $\mathbb{Q}$? Does every element (or nearly every element) of $\mathbb{Q}$ have an additive and multiplicative inverse – if so, give a formula for those inverses; if not, why not?

- (2) Restate the Chinese Remainder Theorem in terms of congruence classes and *equations* in various $\mathbb{Z}/n\mathbb{Z}$'s rather than congruences.
- (3) Prove the statements in this section which have proofs “left to the reader.”
- (4) State and prove congruence class versions of any results about congruences from subsections 2.1 and 2.2 which do not have versions in this subsection.

2.5. Euler's ϕ function. Euler made the following definition, and it was good.

Definition 2.30. Given $n \in \mathbb{N}$,

$$\phi(n) = \# (\{m \in \mathbb{Z} \mid 0 \leq m < n \text{ and } \gcd(m, n) = 1\}) .$$

In other words, $\phi(n)$ counts the number of non-negative integers less than n which are relatively prime to n .

This is called **Euler's ϕ function**, or **Euler's totient function** (“totient” rhymes with “quotient”; this name was give to it by the English mathematician Sylvester).

Here's one thing it is good for:

Theorem 2.31. *Given $n \in \mathbb{N}$, $\phi(n)$ is the number of elements of $\mathbb{Z}/n\mathbb{Z}$ which are (multiplicatively) invertible.*

Proof. This is just Theorem 2.28 part (5) □

One quite surprising fact about Euler's totient function is that it is multiplicative, at least for relatively prime numbers:

Theorem 2.32. *Given $n, m \in \mathbb{Z}$, if $\gcd(n, m) = 1$ then $\phi(nm) = \phi(n)\phi(m)$.*

Proof. This is actually a nice application of the Chinese Remainder Theorem, as we shall see.

Fix $n, m \in \mathbb{N}$ which are relatively prime. For $k \in \mathbb{N}$, let

$$(\mathbb{Z}/k\mathbb{Z})^* = \{x \in \mathbb{Z}/k\mathbb{Z} \mid x \text{ is invertible}\}$$

so $\phi(k) = \#((\mathbb{Z}/k\mathbb{Z})^*)$. (This notation means “the number of things in the set $(\mathbb{Z}/k\mathbb{Z})^*$.”)

Now define the set of pairs

$$(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* = \{(a, b) \mid a \in (\mathbb{Z}/n\mathbb{Z})^* \text{ and } b \in (\mathbb{Z}/m\mathbb{Z})^*\}.$$

Notice that $\#((\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*) = \#((\mathbb{Z}/n\mathbb{Z})^*) \cdot \#((\mathbb{Z}/m\mathbb{Z})^*) = \phi(n)\phi(m)$, since each part of the pair is free to be whichever element it wants of the respective set, so the total number of pairs is the size of the first set times the size of the second. Therefore, if we can prove that $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ can be put into bijective correspondence with $(\mathbb{Z}/(nm)\mathbb{Z})^*$, then we will have

$$\phi(n)\phi(m) = \#((\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*) = \#((\mathbb{Z}/(nm)\mathbb{Z})^*) = \phi(nm)$$

as desired, since bijective sets have the same number of elements.

The correspondence is given by the function

$$\mathcal{F} : (\mathbb{Z}/(nm)\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* : [x]_{nm} \mapsto ([x]_n, [x]_m).$$

We must show $\mathcal{F}$ is well-defined, 1-1, and onto. Well-defined means that for some $[x]_{nm}$, if $y \in \mathbb{Z}$ is another representative of the congruence class

$[x]_{nm}$, then $([x]_n, [x]_m) = ([y]_n, [y]_m)$ so that $\mathcal{F}$ is defined only by the class $[x]_{nm}$, not by its choice of representative x . But this is easy, since $y \in [x]_{nm}$ means $y \cong_{nm} x$ so $\exists k \in \mathbb{Z}$ such that $y - x = k(nm) = (km)n = (kn)m$. These last two versions mean that $y \cong_n x$ and $y \cong_m x$, so $[x]_n = [y]_n$ and $[x]_m = [y]_m$, which means $\mathcal{F}$ is well-defined.

Now let us assume that $x, y \in \mathbb{Z}$ have $\mathcal{F}([x]_{nm}) = \mathcal{F}([y]_{nm})$, i.e., $[x]_n = [y]_n$ and $[x]_m = [y]_m$. That is, $z = x - y \in \mathbb{Z}$ solves the system

$$\begin{aligned} z &\equiv 0 \pmod{n} \\ z &\equiv 0 \pmod{m}. \end{aligned}$$

But $z = 0$ also solves this system, and the Chinese Remainder Theorem tells us that solutions of this system (which is an appropriate system for the CRT since $\gcd(n, m) = 1$) are unique modulo nm . Therefore, $x - y \equiv 0 \pmod{nm}$, so $x \equiv y \pmod{nm}$. Hence $[x]_{nm} = [y]_{nm}$, and thus $\mathcal{F}$ is 1-1.

Now, given any pair $([x]_n, [y]_m) \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$, consider the system of congruences

$$\begin{aligned} z &\equiv x \pmod{n} \\ z &\equiv y \pmod{m}, \end{aligned}$$

which system is again CRT-ready since $\gcd(n, m) = 1$. Therefore there exists a solution to this system, call it $z \in \mathbb{Z}$, and $\mathcal{F}([z]_{nm}) = ([x]_n, [y]_m)$. Thus $\mathcal{F}$ is onto as well. $\square$

Exercises

- (1) Compute $\phi(n)$ for $n = 2, 3, 5, 7, 11, 13, 17$. Make a general conjecture. Can you prove it?
- (2) Compute $\phi(n)$ for $n = 2, 4, 8, 16, 32, 64$. Make a conjecture about $\phi(2^k)$ for $k \in \mathbb{N}$. Prove it!