MODULAR ARITHMETIC (SHORT VERSION)

KEITH CONRAD

1. Introduction

We will define the notion of congruent integers (with respect to a modulus) and develop some basic ideas of modular arithmetic, which lets us carry out algebraic calculations on integers with a systematic disregard for terms divisible by a certain number (called the modulus). This form of "reduced algebra" is essential background for the mathematics of computer science, coding theory, cryptography, primality testing, and much more.

2. Integer congruences

The following definition was introduced by Gauss in his *Disquisitiones Arithmeticae* (Arithmetic Investigations) in 1801.

Definition 2.1 (Gauss)**.** Let m be an integer. For $a, b \in \mathbf{Z}$, we write

$$a \equiv b \bmod m$$

and say "a is congruent to b modulo m" if $m \mid (a - b)$.

Example 2.2. Check $18 \equiv 4 \bmod 7$, $-20 \equiv 13 \bmod 11$, and $19 \equiv 3 \bmod 2$.

Remark 2.3. The parameter m is called the modulus, *not* the modulo. The symbol $\equiv$ in LaTeX is written as `\equiv`, but it is always pronounced "congruent," **never** "equivalent". (The LaTeX command `\cong` is for the congruence symbol $\cong$ in elementary geometry.)

We have $m \equiv 0 \bmod m$, and more generally $mk \equiv 0 \bmod m$ for any $k \in \mathbf{Z}$. In fact,

$$a \equiv 0 \bmod m \iff m \mid a,$$

so the congruence relation includes the divisibility relation as a special case: multiples of m are exactly the numbers that "look like 0" modulo m. Because multiples of m are congruent to 0 modulo m, we will see that working with integers modulo m amounts to systematically ignoring additions and subtractions by multiples of m in calculations.

Since $a \equiv b \bmod m$ if and only if $b = a + mk$ for some $k \in \mathbf{Z}$, adjusting an integer modulo m is the same as adding (or subtracting) multiples of m to it. Thus, if we want to find a positive integer congruent to $-18 \bmod 5$, we can add a multiple of 5 to -18 until we go positive. Adding 20 does the trick: $-18 + 20 = 2$, so $-18 \equiv 2 \bmod 5$ (check!).

There is a useful analogy between integers modulo m and angle measurements (in radians, say). In both cases, the objects involved admit *different representations*, *e.g.*, the angles 0, 2π, and -4π are the same, just as

$$2 \equiv 12 \equiv -13 \bmod 5.$$

Every angle can be put in "standard" form as a real number in the interval $[0, 2\pi)$. There is a similar convention for the "standard" representation of an integer modulo m using *remainders*, as follows.

Theorem 2.4. *Let $m \in \mathbf{Z}$ be a nonzero integer. For each $a \in \mathbf{Z}$, there is a unique r with $a \equiv r \bmod m$ and $0 \leq r < |m|$.*

Proof. Using division with remainder in $\mathbf{Z}$, there are q and r in $\mathbf{Z}$ such that

$$a = mq + r, \qquad 0 \leq r < |m|.$$

Then $m \mid (a - r)$, so $a \equiv r \bmod m$.

To show r is the unique number in the range $\{0, 1, \ldots, |m| - 1\}$ that is congruent to $a \bmod m$, suppose two numbers in this range work:

$$a \equiv r \bmod m, \quad a \equiv r' \bmod m,$$

where $0 \leq r, r' < |m|$. Then we have

$$a = r + mk, \quad a = r' + m\ell$$

for some k and ℓ in $\mathbf{Z}$, so the remainders r and r' have difference

$$r - r' = m(\ell - k).$$

This is a multiple of m, and the bounds on r and r' tell us $|r - r'| < |m|$. A multiple of m has absolute value less than $|m|$ only if it is 0, so $r - r' = 0$, which means $r' = r$. □

Example 2.5. Taking $m = 2$, every integer is congruent modulo 2 to exactly one of 0 and 1. Saying $n \equiv 0 \bmod 2$ means $n = 2k$ for some integer k, so n is even, and saying $n \equiv 1 \bmod 2$ means $n = 2k + 1$ for some integer k, so n is odd. We have $a \equiv b \bmod 2$ precisely when a and b have the *same parity*: both are even or both are odd.

Example 2.6. Every integer is congruent mod 4 to exactly one of 0, 1, 2, or 3. Congruence mod 4 is a refinement of congruence mod 2: even numbers are congruent to 0 or 2 mod 4 and odd numbers are congruent to 1 or 3 mod 4. For instance, $10 \equiv 2 \bmod 4$ and $19 \equiv 3 \bmod 4$.

Congruence mod 4 is related to Master Locks. Every combination on a Master Lock is a triple of numbers (a, b, c) where a, b, and c vary from 0 to 39. Each number has 40 choices, with $b \neq a$ and $c \neq b$ (perhaps $c = a$). This means the number of combinations could be up to 60840, but in fact the true number of combinations is a lot smaller: every combination has $c \equiv a \bmod 4$ and $b \equiv a + 2 \bmod 4$, so once some number in a combination is known the other two numbers are each limited to 10 choices (among the 40 numbers in $\{0, 1, \ldots, 39\}$ exactly 10 will be congruent to a particular value mod 4). Thus the real number of Master Lock combinations is $40 \cdot 10^2 = 4000$.

Example 2.7. Taking $m = 7$, every integer is congruent modulo 7 to exactly one of $0, 1, 2, \ldots, 6$. The choice is the remainder when the integer is divided by 7. For instance, $20 \equiv 6 \bmod 7$ and $-32 \equiv 3 \bmod 7$.

Definition 2.8. We call $\{0, 1, 2, \ldots, |m| - 1\}$ the *standard* representatives for integers modulo m.

In practice $m > 0$, so the standard representatives modulo m are $\{0, 1, 2, \ldots, m - 1\}$. In fact, congruence modulo m and modulo $-m$ are the same relation (just look back at the definition), so usually we never talk about negative moduli. Nevertheless, Theorem 2.4 is stated for any nonzero modulus m.

By Theorem 2.4, there are $|m|$ incongruent integers modulo m. Each integer is congruent modulo m to a standard representative, just like any fraction can be written in a reduced form. There are many other representatives, however, and this will be important!

3. Modular Arithmetic

When we add and multiply fractions, we can change their representation (that is, use a different numerator and denominator) and the results don't change. A similar idea occurs with addition and multiplication modulo m.

Theorem 3.1. *If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.*

Proof. By hypothesis, $a - b = mk$ and $b - c = m\ell$ for some integers k and ℓ. Adding the equations, $a - c = m(k + \ell)$ and $k + \ell \in \mathbf{Z}$, so $a \equiv c \bmod m$. □

This result is called transitivity of congruences. We will usually use it quite often.

The following theorem is the *key* algebraic feature of congruences in $\mathbf{Z}$: they behave well under addition and multiplication.

Theorem 3.2. *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then*

$$a + c \equiv b + d \bmod m \text{ and } ac \equiv bd \bmod m.$$

Proof. We want to show $(a + c) - (b + d)$ and $ac - bd$ are multiples of m. Write $a = b + mk$ and $c = d + m\ell$ for k and ℓ in $\mathbf{Z}$. Then

$$(a + c) - (b + d) = a - b + c - d = m(k + \ell),$$

so $a + c \equiv b + d \bmod m$. For multiplication,

$$\begin{aligned} ac - bd &= (b + mk)(d + m\ell) - bd \\ &= m(kd + b\ell + mk\ell), \end{aligned}$$

so $ac \equiv bd \bmod m$. □

Example 3.3. Check $11 \equiv 5 \bmod 6$, $-2 \equiv 4 \bmod 6$, and $11 \cdot (-2) \equiv 5 \cdot 4 \bmod 6$.

Example 3.4. What is the standard representative for $17^2 \bmod 19$? You could compute $17^2 = 289$ and then divide 289 by 19 to find a remainder of 4, so $17^2 \equiv 4 \bmod 19$. Another way is to notice $17 \equiv -2 \bmod 19$, so $17^2 \equiv (-2)^2 \equiv 4 \bmod 19$. That was quicker, and it illustrates the meaning of multiplication being independent of the choice of representative. Sometimes one representative can be more convenient than another.

Example 3.5. If we want to compute $10^4 \bmod 19$, compute successive powers of 10 but reduce modulo 19 *each time* the answer exceeds 19: using the formula $10^k = 10 \cdot 10^{k-1}$ and writing $\equiv$ for congruence modulo 19,

$$10^1 = 10,\ 10^2 = 100 \equiv 5,\ 10^3 \equiv 10 \cdot 5 = 50 \equiv 12,\ 10^4 \equiv 10 \cdot 12 = 120 \equiv 6.$$

Thus $10^4 \equiv 6 \bmod 19$. Theorem 3.2 says this kind of procedure leads to the right answer, since multiplication modulo 19 is independent of the choice of representatives, so we can always replace a larger integer with a smaller representative of it modulo 19 without affecting the results of (further) algebraic operations modulo 19.

Corollary 3.6. *If $a \equiv b \bmod m$ and $k \in \mathbf{Z}^+$ then $a^k \equiv b^k \bmod m$.*

Proof. This follows from the second congruence in Theorem 3.2 using induction on k. Details are left to the reader. □

Remark 3.7. Do **not** try to extend Corollary 3.6 to fractional exponents until you have much more experience in modular arithmetic. Extracting roots is *not* repeated multiplication, and extracting roots in modular arithmetic could be undefined or have unexpected behavior compared with your experience extracting roots in $\mathbf{R}$.

For example, in $\mathbf{R}$ all positive numbers are perfect squares, but $x^2 \equiv 2 \bmod 5$ has no solution (that is, no integer x satisfies that congruence). Positivity is really a meaningless concept mod m: every integer is congruent to a positive integer and a negative integer mod m (just add and subtract a suitably large multiple of m to the integer). There is no good notion of ordering mod m.

In $\mathbf{R}$ you know $x^2 = y^2 \Rightarrow x = \pm y$, but it is *false* that $a^2 \equiv b^2 \bmod m \Rightarrow a \equiv \pm b \bmod m$ in general. Consider $4^2 \equiv 1^2 \bmod 15$ with $4 \not\equiv \pm 1 \bmod 15$.

In $\mathbf{R}$ you are used to $x^3 = y^3 \Rightarrow x = y$. But $2^3 \equiv 1^3 \bmod 7$ and $2 \not\equiv 1 \bmod 7$.

When we add and multiply modulo m, we are carrying out *modular arithmetic*.

That addition and multiplication can be carried out on integers modulo m without having the answer change (modulo m) if we replace an integer by a congruent integer is similar to addition and multiplication of fractions being independent of the choice of numerator and denominator for the fractions, *e.g.*, $1/2 + 3/5 = 11/10$ and $2/4 + 9/15 = 66/60 = 11/10$.

Definition 3.8. The integers modulo m under addition and multiplication is written $\mathbf{Z}/(m)$.

Other notations you may meet for $\mathbf{Z}/(m)$ are $\mathbf{Z}_m$ and $\mathbf{Z}/m\mathbf{Z}$.

Example 3.9. Here are the elements of $\mathbf{Z}/(5)$:

$$\{\dots, -15, -10, -5, \mathbf{0}, 5, 10, 15, \dots\},$$
$$\{\dots, -14, -9, -4, \mathbf{1}, 6, 11, 16, \dots\},$$
$$\{\dots, -13, -8, -3, \mathbf{2}, 7, 12, 17, \dots\},$$
$$\{\dots, -12, -7, -2, \mathbf{3}, 8, 13, 18, \dots\},$$
$$\{\dots, -11, -6, -1, \mathbf{4}, 9, 14, 19, \dots\}.$$

These five sets each consist of all the integers congruent to each other modulo 5, so each set is called a *congruence class* (modulo 5). In practice we often use one representative from each congruence class to stand for the whole congruence class. In bold type is one set of representatives for the congruence classes modulo 5 – the choice 0, 1, 2, 3, and 4 – which is the standard one. Another set of representatives is 5, 6, -3, 18, and -6 (since $5 \equiv 0 \bmod 5$, $6 \equiv 1 \bmod 5$, $-3 \equiv 2 \bmod 5$, and so on).

Different integers in the same congruence class are like different real numbers representing the same angle, such as π and 3π. They're different ways of representing the "same thing". Just as π and 3π are not the same as real numbers but become "the same" in the setting of angles, we need to think this way about congruence classes: 1 and 6 are not the same in $\mathbf{Z}$ but they are the same when we think modulo 5.

4. Solving equations in $\mathbf{Z}/(m)$

In school you solve equations like $2x + 3 = 8$ or $x^2 - 3x + 1 = 0$ by the "rules of algebra": cancellation (if $a \neq 0$ and $ax = ay$ then $x = y$), equals plus equals are equal, and so on. This is in the setting of equations over the real numbers.

We can also try to solve polynomial equations in modular arithmetic, where we consider solutions to be different if they are incongruent. We will focus on the simplest case: a linear

congruence $ax \equiv b \bmod m$. Already in this case we will meet phenomena with no parallel in the case of a real linear equation (Examples 4.2 and 4.3 below).

Example 4.1. Let's try to solve $8x \equiv 1 \bmod 11$. If there is an answer, it can be represented by one of $0, 1, 2, \ldots, 10$, so we can just run through the possibilities:

$x \bmod 11$	0	1	2	3	4	5	6	7	8	9	10
$8x \bmod 11$	0	8	5	2	10	7	4	1	9	6	3

The only solution is 7 mod 11: $8 \cdot 7 = 56 \equiv 1 \bmod 11$. This means 7 and 8 are multiplicative inverses in $\mathbf{Z}/(11)$.

This problem concerns finding an inverse for 8 modulo 11. We can find multiplicative inverses for every nonzero element of $\mathbf{Z}/(11)$:

x	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10

Check in each case that the product of the numbers in each column is 1 in $\mathbf{Z}/(11)$.

Example 4.2. Find a solution to $8x \equiv 1 \bmod 10$. We run through the standard representatives for $\mathbf{Z}/(10)$, and find *no* answer:

x	0	1	2	3	4	5	6	7	8	9
$8x$	0	8	6	4	2	0	8	6	4	2

In retrospect, we can see *a priori* why there shouldn't be an answer. If $8x \equiv 1 \bmod 10$ for some integer x, then we can lift the congruence up to $\mathbf{Z}$ in the form

$$8x + 10y = 1$$

for some $y \in \mathbf{Z}$. But this is absurd: $8x$ and $10y$ are even, so the left side is a multiple of 2 but the right side is not.

Example 4.3. The linear congruence $6x + 1 \equiv 4 \bmod 15$ has three solutions! In the following table we can see the solutions are 3, 8, and 13:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$6x+1$	1	7	13	4	10	1	7	13	4	10	1	7	13	4	10

These examples show us that a linear congruence $ax \equiv b \bmod m$ may not behave like real linear equations: there could be no solutions or multiple solutions. In particular, taking $b = 1$, some nonzero elements of $\mathbf{Z}/(m)$ may have no multiplicative inverse.

The obstruction to inverting 8 in $\mathbf{Z}/(10)$ extends to other moduli in the following way.

Theorem 4.4. *For integers a and m, the following three conditions are equivalent:*

- *there is a solution x in $\mathbf{Z}$ to $ax \equiv 1 \bmod m$,*
- *there are solutions x and y in $\mathbf{Z}$ to $ax + my = 1$,*
- *a and m are relatively prime.*

Proof. Suppose $ax \equiv 1 \bmod m$ for some $x \in \mathbf{Z}$. Then $m \mid (1 - ax)$, so there is some $y \in \mathbf{Z}$ such that $my = 1 - ax$, so

$$ax + my = 1.$$

This equation implies a and m are relatively prime since any common factor of a and m divides $ax + my$. Finally, if a and m are relatively prime then by Bezout's identity (a consequence of back-substituting in Euclid's algorithm) we can write $ax + my = 1$ for some x and y in $\mathbf{Z}$ and reducing both sides mod m implies $ax \equiv 1 \bmod m$. □

This explains Example 4.2, since 8 and 10 have a common factor of 2. Similarly, we see at a glance that there is no solution to $3x \equiv 1 \bmod 15$ (common factor of 3) or $35x \equiv 1 \bmod 77$ (common factor of 7).

Example 4.5. Since $(8, 11) = 1$, 8 has a multiplicative inverse in $\mathbf{Z}/(11)$. We found it by an exhaustive search in Example 4.1, but now we can do it by a more systematic approach:

$$\begin{aligned} 11 &= 8 \cdot 1 + 3, \\ 8 &= 3 \cdot 2 + 2, \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 3 \cdot 2) \\ &= 3 \cdot 3 - 8 \\ &= 3 \cdot (11 - 8) - 8 \\ &= 3 \cdot 11 - 8 \cdot 4. \end{aligned}$$

Reducing the equation $1 = 3 \cdot 11 - 8 \cdot 4$ modulo 11,

$$8(-4) \equiv 1 \bmod 11.$$

The inverse of 8 in $\mathbf{Z}/(11)$ is -4, or equivalently 7.

To summarize: solving for x in the congruence $ax \equiv 1 \bmod m$ is equivalent to solving for integers x and y in the equation $ax + my = 1$ (be sure you see why!), and the latter equation can be solved without any guesswork by reversing Euclid's algorithm on a and m when $(a, m) = 1$. If Euclid's algorithm shows $(a, m) \neq 1$, then there is no solution.

In the real numbers, every nonzero number has a multiplicative inverse. This is not generally true in modular arithmetic: if $a \not\equiv 0 \bmod m$ it need not follow that we can solve $ax \equiv 1 \bmod m$. (For instance, $4 \not\equiv 0 \bmod 6$ and 4 mod 6 has no multiplicative inverse.) The correct test for invertibility in $\mathbf{Z}/(m)$ is $(a, m) = 1$, which is generally stronger than $a \not\equiv 0 \bmod m$. Although invertibility in $\mathbf{Z}/(m)$ is usually not the same as being nonzero in $\mathbf{Z}/(m)$, there is an important case when these two ideas agree: m is prime.

Corollary 4.6. *For a prime number p, an integer a is invertible in $\mathbf{Z}/(p)$ if and only if $a \not\equiv 0 \bmod p$.*

Proof. If $a \bmod p$ is invertible, then $(a, p) = 1$, so p does not divide a.

For the converse direction, suppose $a \not\equiv 0 \bmod p$. We show $(a, p) = 1$. Since (a, p) is a (positive) factor of p, and p is *prime*, (a, p) is either 1 or p. (The proof would break down here if p were not prime.) Since p does not divide a, $(a, p) \neq p$, so $(a, p) = 1$. Therefore the congruence $ax \equiv 1 \bmod p$ has a solution. □

The upshot of Corollary 4.6 is that our intuition from algebra over $\mathbf{R}$ carries over quite well to algebra over $\mathbf{Z}/(p)$: every nonzero number has a multiplicative inverse in the system. This is not true of $\mathbf{Z}/(m)$ for composite m, and that is why modular arithmetic in a composite modulus requires more care.

Why should we care about inverting integers in $\mathbf{Z}/(m)$? (By "inverting" we always mean "inverting multiplicatively.") One reason is its connection to inverting matrices with

entries in $\mathbf{Z}/(m)$. Given a square $n \times n$ matrix A with entries in $\mathbf{Z}/(m)$, your experience with linear algebra in $\mathbf{R}$ may suggest a matrix with entries in $\mathbf{Z}/(m)$ is invertible whenever its determinant is nonzero in $\mathbf{Z}/(m)$. But this is *false*.

Example 4.7. We work with matrices having entries in $\mathbf{Z}/(10)$. Let $A = \left(\begin{smallmatrix} 1 & 3 \\ 1 & 1 \end{smallmatrix}\right)$. The determinant of A is $-2 \equiv 8 \bmod 10$, so $\det A \not\equiv 0 \bmod 10$. However, there is no inverse for A as a mod 10 matrix. We can see why by contradiction. Suppose there is an inverse matrix, and call it B. Then $AB \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 10$. (Congruence of matrices means congruence of corresponding matrix entries on both sides.) Writing $B = \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$, we compute AB to get $\left(\begin{smallmatrix} x+3z & y+3t \\ x+z & y+t \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 10$. Then $x + 3z \equiv 1 \bmod 10$ and $x + z \equiv 0 \bmod 10$. The second congruence says $x \equiv -z \bmod 10$, and replacing x with $-z$ in the first congruence yields $2z \equiv 1 \bmod 10$. But that's absurd: $2z$ is even and 1 is odd, so $2z \not\equiv 1 \bmod 10$. (Said differently, if $2z \equiv 1 \bmod 10$ then $2z = 1 + 10y$ for some integer y, so $2z - 10y = 1$, but the left side is even and 1 is not even.)

As a real matrix, A is invertible and $A^{-1} = \left(\begin{smallmatrix} -1/2 & 3/2 \\ 1/2 & -1/2 \end{smallmatrix}\right)$. This inverse makes no sense if we try to reduce it modulo 10 (what is $1/2 \bmod 10$?!?), and that suggests there should be a problem if we try to invert A as a mod 10 matrix.

Let's look at determinants behave in modular arithmetic. Suppose $n \times n$ matrices A and B satisfy $AB \equiv I_n \bmod m$. Taking determinants of both sides tells us (by Theorem 3.2) that

$$(\det A)(\det B) \equiv 1 \bmod m,$$

so $\det A$ is *invertible* in $\mathbf{Z}/(m)$. Invertibility of $\det A$ in $\mathbf{Z}/(m)$ is usually a stronger condition than $\det A \not\equiv 0 \bmod m$. For instance, the 2×2 matrix A in Example 4.7 has determinant $8 \bmod 10$, which is not invertible. Thus the matrix A is not invertible mod 10. That sure is an easier way to see A is not invertible than the tedious matrix calculations in Example 4.7!

Example 4.8. Let $m = 14$ and $A = \left(\begin{smallmatrix} 1 & 4 \\ 3 & 2 \end{smallmatrix}\right)$ as a matrix with entries in $\mathbf{Z}/(14)$. The determinant of A is $2 - 12 = -10 \equiv 4 \bmod 14$, which is not invertible. Even though A has a nonzero determinant, there is no matrix inverse for A over $\mathbf{Z}/(14)$.

We now see that we have to be able to recognize invertible elements of $\mathbf{Z}/(m)$ before we can recognize invertible matrices over $\mathbf{Z}/(m)$, because an invertible matrix will have an invertible determinant. If we want to do linear algebra over $\mathbf{Z}/(m)$ then we need Euclid's algorithm (and Bezout's identity) to invert determinants.