1 Basic Definitions

Definition 1 *The* translate of $m\mathbf{Z}$ by k *is the set of all integers that can be written as k plus a multiple of m:*

$$k + m\mathbf{Z} = \{\, k + im \,|\, i \in \mathbf{Z} \,\}.$$

Visualizing this subset of the integers, it is not hard to see that two translates either coincide completely or have no integer in common. Also, that any integer is in some translate. Hence, the collection of distinct translates partitions the integers and therefore gives rise to an equivalence relation.

To prove these statements formally we will make use of the properties of divisibility to give an alternative characterization of translates according to a divisibility criteria.

Definition 2 *For integer $a, b \in \mathbf{Z}$, a* divides *b, written $a \,|\, b$, if and only if there exists an integer $k \in \mathbf{Z}$ such that $ak = b$.*

The familiar property of divisibility that we shall use, but not prove is the following:

Theorem 1 *Suppose $a, b, c \in \mathbf{Z}$ are integers and c divides a and b. Then c divides all linear combinations of a and b, that is, for all $x, y \in \mathbf{Z}$, $c \,|\, (xa + yb)$.*

We now give an alternative definition for translates.

Theorem 2 *Two integers are in the same translate of $m\mathbf{Z}$ if and only if their difference is divisible by m. That is, for all $a, b \in \mathbf{Z}$, $a, b \in (k + m\mathbf{Z})$ for some integer k if and only if $m \,|\, (a - b)$.*

PROOF: Suppose $a, b \in (k + m\mathbf{Z})$. Then there are integers i_a, i_b such that,

$$a = k + i_a m, \quad b = k + i_b m.$$

Subtracting, $a - b = (i_a - i_b)m$, which is divisible by m.

Suppose now that we have $a, b \in \mathbf{Z}$ where $m \,|\, (a - b)$. Then there is an i such that $mi = a - b$, so, $a \in b + m\mathbf{Z}$. Obviously, $b \in b + m\mathbf{Z}$, so a and b are in the same translate. □

Theorem 3 *Given an $m \in \mathbf{Z}$, two translates $k_1 + m\mathbf{Z}$ and $k_2 + m\mathbf{Z}$ are either disjoint or identical, depending on whether m divides $k_1 - k_2$ or not, and the set of distinct translates covers all of $\mathbf{Z}$.*

PROOF: Suppose two translates $k_1 + m\mathbf{Z}$ and $k_2 + m\mathbf{Z}$ are not disjoint. Let z be an integer in both. So,

$$m \,|\, (z - k_1), \quad m \,|\, (k_2 - z),$$

and adding these two,

$$z - k_1 + (k_2 - z) = k_2 - k_1 \Rightarrow m \,|\, (k_2 - k_1).$$

So, if the translate are not disjoint, k_1 and k_2 are in the intersection. Take an arbitrary $z \in k_1 + m\mathbf{Z}$. It is in the same translate as k_2. So $m \,|\, (z - k_2)$, therefore $z \in k_2 + m\mathbf{Z}$. Likewise, any $z \in k_2 + m\mathbf{Z}$ is in $k_1 + m\mathbf{Z}$. This shows that the two translates are identical.

Conversely, if $m \,|\, (k_1 - k_2)$, then $k_1 \in k_2 + m\mathbf{Z}$, and the translates are not disjoint.

Every $z \in \mathbf{Z}$ is in some translate, namely $z \in z + m\mathbf{Z}$. □

Corollary 1 *If $k' \in k + m\mathbf{Z}$, then $k' + m\mathbf{Z} = k + m\mathbf{Z}$.*

Definition 3 *We say that two integer $a, b \in \mathbf{Z}$ are* congruent modulo m *if they are in the same translate of $m\mathbf{Z}$. This is written $a = b \pmod{m}$.*

Each translate is an *equivalence class*, it is the set of all integers which share equality under congruence modulo m. Typically, each equivalence class takes its name from the smallest non-negative integer in the class.

Theorem 4 *The set $\{0, 1, \ldots, m-1\}$ runs through all equivalence classes modulo m. That is, given any $z \in \mathbf{Z}$, there is exactly one r between 0 and $m-1$ for which $z = r \pmod{m}$.*

PROOF: Consider $z + m\mathbf{Z}$. This translate must contain one and only one integer r in the range $0 \leq r < m$. For if r' were the smallest non-negative integer in $z + m\mathbf{Z}$ and $r' \geq m$, then $r' - m$ would be non-negative and smaller than r'. And if there were two integer $0 \leq r \leq r' < m$ then $m \,|\, (r' - r)$ however $0 \leq r' - r < m$, so $r' - r$ must be zero. □

2 Arithmetic modulo m

Theorem 5 *Given an $m \in \mathbf{Z}$ and two translates $a + m\mathbf{Z}$ and $b + m\mathbf{Z}$, for any two a_1 and a_2 in $a + m\mathbf{Z}$ and b_1 and b_2 in $b + m\mathbf{Z}$,*

$$(a_1 + b_1) + m\mathbf{Z} = (a_2 + b_2) + m\mathbf{Z},$$

and

$$(a_1 b_1) + m\mathbf{Z} = (a_2 b_2) + m\mathbf{Z}.$$

PROOF: Write $a_1 = a_2 + i_a m$ and $b_1 = b_2 + i_b m$. Then,

$$\begin{aligned} a_1 + b_1 &= a_2 + b_2 + (i_a + i_b)m \\ &= a_2 + b_2 + i'm, \end{aligned}$$

Hence $(a_1 + b_1) \in (a_2 + b_2) + m\mathbf{Z}$, and the first equality holds. Likewise,

$$\begin{aligned} a_1 b_1 &= a_2 b_2 + (i_b a_2 + i_a b_2 + i_a i_b m)m \\ &= a_2 b_2 + i'' m, \end{aligned}$$

so the second equality holds. □

Hence a well-defined arithmetic can be defined for translates based on the arithmetic of integers.

Definition 4 *We define the sum of translates to be,*

$$\big(a + m\mathbf{Z}\big) + \big(b + m\mathbf{Z}\big) = (a + b) + m\mathbf{Z},$$

and their product to be,

$$\big(a + m\mathbf{Z}\big)\big(b + m\mathbf{Z}\big) = (ab) + m\mathbf{Z}.$$

By the previous theorem, this definition depends only on the translates, not the a and b used to describe the translate.

Translated into the language of congruences, we have the theorem,

Corollary 2 *If*

$$a_1 = a_2 \text{ and } b_1 = b_2 \pmod{m},$$

then

$$a_1 + b_1 = a_2 + b_2 \text{ and } a_1 b_1 = a_2 b_2 \pmod{m}.$$

Since the defined arithmetic is based on that of the integers, it inherits many properties from the integers. Addition modulo m is an associative and commutative operation, and for each translate T there is a unique translate $-T$, its *additive inverse*, for which $T + (-T) = 0 + m\mathbf{Z}$. Multiplication modulo m is also an associative and commutative operation which distributes over addition, that is, for three translates T_1, T_2 and T_3,

$$T_1(T_2 + T_3) = T_1 T_2 + T_1 T_3.$$

Having defined addition and multiplication modulo m, we next look at division. For the integers, one can only divide by 1 or -1. As for the rest, *fractions* are invented, where the inverse of i is $1/i$ for $i \neq 0$, being careful to discover and make all identifications, such as that $2/4$ is the same as $1/2$. For the integers modulo m the situation is different. If may happen that just taking the integer x modulo m creates a *multiplicative inverse* for that number, that is, an x^{-1} such that $x^{-1}x = xx^{-1} = 1$ modulo m. On the other hand, it may cause x to become a *divisors of zero*, that is, x is non-zero modulo m, however there is another number y, non-zero modulo y, such that $xy = 0$ modulo m. If it was the case that x^{-1} existed, we would have,

$$y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0,$$

so no inverse to x could exist or be created without forcing y to become 0.

In general, let us consider the solution for x to the equation,

$$ax = b \pmod{m}.$$

This means that ax is in $b + m\mathbf{Z}$, that is, that there exists an $i \in \mathbf{Z}$ such that,

$$ax = b + mi.$$

To this end, we look at all linear combinations of a and m.

Definition 5 *The set of linear combinations of two integers s and t is denoted $\langle\, s, t\,\rangle$,*

$$\langle\, s, t\,\rangle = \{\, is + jt \mid i, j \in \mathbf{Z}\,\}.$$

The existence of a solution x of the above equation is equivalent to whether or not $b \in \langle\, a, m\,\rangle$. There are some obvious and not so obvious facts about $\langle\, a, b\,\rangle$.

Theorem 6 *For all $a, b \in \mathbf{Z}$ integers,*

1. $\langle\, a, b\,\rangle = \langle\, b, a\,\rangle$.
2. $\langle\, -a, b\,\rangle = \langle\, a, b\,\rangle$.
3. $\langle\, a, b\,\rangle = \langle\, a - b, b\,\rangle$.
4. $\langle\, a, b\,\rangle = \langle\, b, r\,\rangle$ *where $a \geq b > 0$ and r is the remainder of $a \div b$.*

PROOF: The first two facts are the obvious ones. For the third, the computation,

$$ia + jb = ia - ib + (i + j)b = i(a - b) + (i + j)b,$$

implies that anything in $\langle\, a, b\,\rangle$ is in $\langle\, a - b, b\,\rangle$, and vice a versa. For $a \geq b > 0$, write $a = qb + r$ and apply Fact Three q times,

$$\langle\, a, b\,\rangle = \langle\, a - qb, b\,\rangle = \langle\, r, b\,\rangle = \langle\, b, r\,\rangle.$$

□

Definition 6 *Let $a, b \in \mathbf{Z}$ be integers. The set of* common divisors *of a and b is,*

$$\{\, c \in \mathbf{Z} \mid c \mid a \text{ and } c \mid b\,\}.$$

Except in the case when a and b are both zero, the largest element in the set of common divisors of a and b is called the greatest common divisor of a and b. *The greatest common divisor of zero and zero is defined to be zero.*

Theorem 7 *The set of all linear combinations of two integer a and b is the same as the set of all multiples of the greatest common divisor d of a and b,*

$$\langle\, a, b \,\rangle = d\mathbf{Z}.$$

PROOF: Starting from $\langle\, a, b \,\rangle$, use the above properties to arrange things so that $\langle\, a, b \,\rangle = \langle\, s_0, s_1 \,\rangle$ and $s_0 \geq s_1 \geq 0$. Let s_2 be the remainder of s_0 divided by s_1, in the case that s_1 is not zero, and repeat this process, getting a sequence of s_i such that $\langle\, s_{i-2}, s_{i-1} \,\rangle = \langle\, s_{i-1}, s_i \,\rangle$ and s_i is the remainder of s_{i-2} divided by s_{i-1}. This process must terminate when $s_j = 0$, in which case we have,

$$\langle\, a, b \,\rangle = \langle\, s_{j-1}, 0 \,\rangle = \left\{\, s_{j-1} i \,\middle|\, i \in \mathbf{Z} \,\right\}.$$

Since both a and b are in $s_{j-1}\mathbf{Z}$, they are multiples of s_{j-1}, so s_{j-1} is a common divisor of a and b. If c was any other common divisor of a and b, it would divide $xa + by$ for all $x, y \in \mathbf{Z}$, hence c divides anything in $\langle\, a, b \,\rangle$. But $s_{j-1} \in \langle\, a, b \,\rangle$, so $c \,|\, s_{j-1}$. Thus s_{j-1} is the greatest common divisor of a and b. □

Theorem 8 *In the previous theorem, let $A = \max(\,|\,a\,|, |\,b\,|\,)$. Then the length of the sequence of remainders $s_0, \ldots, s_j$ is bound by,*

$$j \leq 2 \log_2 A.$$

PROOF: Each two steps the larger value is lessened by at least half. That is,

$$\max(s_{i+3}, s_{i+2}) \leq \max(s_i, s_{i+1})/2.$$

This is already true after one step if $s_{i+1} \leq s_i/2$. So suppose $s_i/2 < s_{i+1} \leq s_i$. Then in the first step, s_{i+2} is calculated,

$$s_{i+2} = s_i - s_{i+1} < s_i/2,$$

and and in the second step s_{i+3} is calculated $s_{i+3} \leq s_{i+2}$.

Hence the number of pairs of steps cannot be longer than required to bring A to the minimum value attainable,

$$1 \leq A/(2^{j/2}).$$

Now take the log of both sides and solve for j. □

Therefore we also have an efficient method for calculating the greatest common divisor of a and b. Coming back to the original problem, we now have an efficient method to determine if there exists an x such that,

$$ax = b \pmod{m}.$$

We calculate the d such that $\langle\, a, m \,\rangle = d\mathbf{Z}$, and if $b \in d\mathbf{Z}$, that is if $d \,|\, b$, then there is a solution. Else there is no solution.

The algorithm for calculating d can be modified to also give the i and j such that $ai + jm = d$. In the case that d divides b, we multiply through by the k such that $dk = b$,

$$a(ki) + kjm = kd = b,$$

and so $b \in a(ki) + m\mathbf{Z}$,

$$a(ki) = b \pmod{m}.$$

We have not yet discussed the uniqueness of the solution, if it exists. If the greatest common divisor of a and m is 1, then the equation $ax = b$ has a solution for every possible b. Therefore, there are only enough elements to go around for one x to be a solution for each specific b. On the other hand, if the greatest common divisor is $d > 1$, then only m/d such equations have solutions, meanwhile for every x the multiplication ax must evaluate to something.

Suppose we have a solution $ax' = b$ (modulo m) where $\langle\, a, m \,\rangle = d\mathbf{Z}$. Then $x'' = x' + i(m/d)$ are also solutions for $i = 1, \ldots, d-1$, because,

$$ax'' = a(x' + i(m/d)) = ax' + ai(m/d) = ax' = b \pmod{m},$$

remarking that $m \mid ai(m/d)$. Furthermore, $i(m/d)$ are all unique modulo m, for $i = 0, \ldots, d-1$, so there are d solutions in this case.

Theorem 9 *In the integers modulo m, let a and b be integers, and d the greatest common divisor of a and m. Then the equation,*

$$ax = b \pmod{m}$$

has d solutions if $d \mid b$. Else there are no solutions.