Congruences

Tuesday, June 29, 2021 1:23 AM

The set of integers is denoted by $\mathbb{Z}$. For $a, b \in \mathbb{Z}$, we say a divides b and write $a \mid b$ if $b = ak$ for some integer k. Suppose n is a non-zero integer. We say a is congruent to b modulo n and write $a \equiv b \pmod{n}$ or $a \overset{n}{\equiv} b$ if $n \mid a-b$.

Lemma. $\overset{n}{\equiv}$ is an equivalent relation over $\mathbb{Z}$.

Pf. Reflexive. For every $a \in \mathbb{Z}$, $a-a=0$ is a multiple of n as $n \cdot 0 = 0$. Hence $a \overset{n}{\equiv} a$.

Symmetric. $a \overset{n}{\equiv} b \Rightarrow n \mid a-b$

$\Rightarrow \exists\, k \in \mathbb{Z},\ a-b = nk$

$\Rightarrow b-a = n\underbrace{(-k)}_{\text{in } \mathbb{Z}}$

$\Rightarrow b \overset{n}{\equiv} a$.

Transitive. $a \overset{n}{\equiv} b \Rightarrow n \mid a-b \Rightarrow \exists\, k \in \mathbb{Z},\ a-b = nk$ (I)

$b \overset{n}{\equiv} c \Rightarrow n \mid b-c \Rightarrow \exists\, \ell \in \mathbb{Z},\ b-c = n\ell$ (II)

(I)+(II) $\Rightarrow (a-b)+(b-c) = nk+n\ell \Rightarrow a-c = n\underbrace{(k+\ell)}_{\text{in } \mathbb{Z}}$

$\Rightarrow a \overset{n}{\equiv} c$. ∎

Congruences

Tuesday, June 29, 2021 1:23 AM

As we have seen earlier, every equivalent relation gives us a partition and an equality function. For $a \in \mathbb{Z}$, the equivalence class of a with respect to $\overset{n}{\equiv}$ is called the mod-n residue class of a and it is denoted by $[a]_n$. By the results that we proved for equivalent relations we have that

- $\{[a]_n \mid a \in \mathbb{Z}\}$ is a partition of $\mathbb{Z}$ and
- $a \overset{n}{\equiv} b \iff [a]_n = [b]_n$.

The partition $\{[a]_n \mid a \in \mathbb{Z}\}$ is denoted by $\mathbb{Z}_n$ and it is called the set of integers modulo n. Notice that

$$b \in [a]_n \iff b \overset{n}{\equiv} a \iff n \mid b-a$$

$$\iff \exists k \in \mathbb{Z},\ b-a = nk$$

$$\iff \exists k \in \mathbb{Z},\ b = a+nk$$

$$\iff b \in \{a+nk \mid k \in \mathbb{Z}\} \text{ (arithmetic progression)}$$

To understand the set $\mathbb{Z}_n$ better, we recall the well-ordering principle and the long division. One of the important properties of positive integers is the well-ordering principle.

Congruences

Tuesday, June 29, 2021 1:23 AM

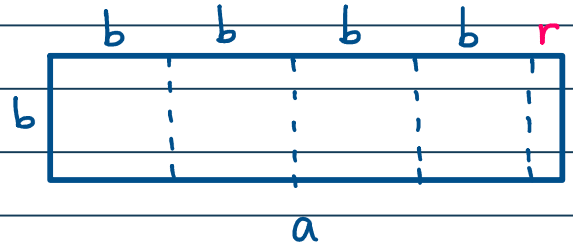
The well-ordering principle. Every non-empty subset of the set $\mathbb{Z}^{\geq 0}$ of non-negative integers has a minimum.

Using the well-ordering principle we can prove the division alg.

The division algorithm. For every $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$, there is a unique pair (q,r) of integers such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|.$$

Pictorial argument



For positive a and b we fold $b \times b$ squares till a rectangle smaller than $b \times b$ is remained (if any). So r is the smallest non-negative integer in the arithmetic progression $a - bk$.

Pf. Let $\sum := [a]_b \cap \mathbb{Z}^{\geq 0} = \{a + bk \mid k \in \mathbb{Z},\ a + bk \geq 0\}$.

Claim 1 $\sum$ is not empty.

Pf of Claim 1. Since $b \neq 0$, $|b| \geq 1$. Hence $|b|\,|a| \geq |a|$.

Therefore $\underbrace{|b|(|a|+1) + a}_{a \pm b(|a|+1)} \geq |a| + |b| + a \geq |b| > 0$

This shows that $[a]_b$ has a positive element.

By the above claim and the well-ordering principle, Σ has a minimum. Suppose r is the minimum of Σ. Then (I) $r = a - bq$ for some integer q.

Claim 2. $r < |b|$.

Pf of Claim 2. Suppose to the contrary that $r \geq |b|$. Then $r - |b| \geq 0$ and $r - |b| = a - bq - |b| = a - b(q \pm 1)$. Hence $r - |b| \in \Sigma$. This is a contradiction as $r - |b|$ is smaller than the minimum r of Σ.

By Claim 2, we obtain the existence of the pair (q, r) with

(I) $a = bq + r$ and $0 \leq r < |b|$.
($r \in \Sigma$; Claim 2)

Next we prove the uniqueness.

Suppose the pairs (q, r) and (q', r') satisfy the desired properties; that means $a = bq + r = bq' + r'$ and $0 \leq r, r' < |b|$. Then $b(q - q') = r' - r$. (II) Notice that $0 \leq r \Rightarrow r' - r \leq r' < |b|$ (III) and $0 \leq r' \Rightarrow r' - r \geq -r > -|b|$ (IV)

Division algorithm

Tuesday, June 29, 2021 1:23 AM

By (III) and (IV), we have $|r'-r|<|b|$. (I)

By (II), we obtain $|r'-r| = |b(q-q')| = |b||q-q'|$. (II)

By (I) and (II), $|b||q-q'|<|b|$ which implies that $|q-q'|<1$. Since $|q-q'|$ is a non-negative integer less than 1, it is 0. Thus $q=q'$. By (II),

$$r'-r = b(q-q') = 0, \text{ which implies } r=r'.$$

This shows the uniqueness. ∎

Suppose the pair (q,r) is given in the long division algorithm. Then q is called the quotient of a divided by b and r is called the remainder of a divided by b.

Using the long division algorithm we obtain that $\mathbb{Z}_n$ has n elements.

Proposition. Suppose n is an integer more than 1. Then

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

Pf. For every $a \in \mathbb{Z}$, by the long division algorithm, there are integers q, r such that $a = nq+r$ and $0 \le r < n$.

Congruence arithmetic

Tuesday, June 29, 2021 1:23 AM

$a = nq + r$ implies that $a \overset{n}{\equiv} r$. Hence $[a]_n = [r]_n$. Thus $[a]_n \in \{[0]_n, [1]_n, \ldots, [n-1]_n\}$. Next we show $[i]_n \neq [j]_n$ if $0 \leq i < j \leq n-1$. Suppose to the contrary $[i]_n = [j]_n$.

$$[i]_n = [j]_n \Rightarrow i \overset{n}{\equiv} j \Rightarrow n \mid i-j$$

$$\Rightarrow i - j = nq \text{ for some integer } q. \quad \text{(I)}$$

Notice that $0 \leq i < j < n$ implies $0 < i - j < n$. (II)

By (I) and (II), $0 < nq < n$. Then $0 < q < 1$ which is a contradiction as there is no integer more than 0 and less than 1. This completes the proof. ∎

The set of integers modulo n have arithmetic operations similar to the set of integers. This can be viewed as a generalization of the fact that

+	even	odd
even	even	odd
odd	odd	even

·	even	odd
even	even	even
odd	even	odd

No matter what even or odd numbers we pick the above tables hold. So we can simply view the above tables as

operations for the set of even numbers and the set of odd numbers.

Lemma. The following are well-defined operations on $\mathbb{Z}_n$:

$$[a]_n + [b]_n := [a+b]_n \quad \text{and} \quad [a]_n \cdot [b]_n := [a \cdot b]_n .$$

Before we go to the proof of this lemma, let's try to understand what it says. Notice that $[a]_n$ is a set and $a \in [a]_n$. We say a is a representative of this residue class. Recall that $[a]_n$ is the equivalency class of a with respect to the equivalent relation $\overset{n}{\equiv}$. From all the elements of $\mathbb{Z}$ that are in same class we are choosing a representative. We are doing the same for the residue class $[b]_n$. Then we are adding the chosen representatives in $\mathbb{Z}$, and next we are considering the residue class of the sum (or product) of these representatives. A priori it is not clear why these operations do not depend on the choice of the representatives. This is an extremely important process.

Congruence arithmetic

Tuesday, June 29, 2021 8:41 AM

We will be using the same idea later when we define factor groups. Whenever you are using a representative from a class and applying certain logic or operations to obtain a claim for the entire class, you have to be extra careful. You have to make sure that you are not "stereotyping" and your process is independent of the choice of a representative.

Pf of lemma. Suppose $[a]_n = [a']_n$ and $[b]_n = [b']_n$.

(we are choosing two representatives a and a', b and b' from each residue class) we have to show that

$$[a+b]_n = [a'+b']_n \quad \text{and} \quad [a\cdot b]_n = [a'\cdot b']_n.$$

$[a]_n = [a']_n \Rightarrow a \overset{n}{\equiv} a' \Rightarrow \exists\, k \in \mathbb{Z},\ a - a' = nk$ (I)

$[b]_n = [b']_n \Rightarrow b \overset{n}{\equiv} b' \Rightarrow \exists\, l \in \mathbb{Z},\ b - b' = nl$. (II)

(I) + (II) $\Rightarrow (a-a') + (b-b') = nk + nl = n(k+l)$

$\Rightarrow (a+b) - (a'+b') = n(\underbrace{k+l}_{\text{in } \mathbb{Z}})$

$\Rightarrow a+b \overset{n}{\equiv} a'+b'$

$\Rightarrow [a+b]_n = [a'+b']_n$.

Congruence arithmetic

Tuesday, June 29, 2021 12:06 PM

Next we want to show $[a\cdot b]_n = [a'\cdot b']_n$. Notice that

$$[a\cdot b]_n = [a'\cdot b']_n \iff a\cdot b \overset{n}{\equiv} a'\cdot b'$$

$$\iff a\cdot b - a'\cdot b' \text{ is a multiple of } n. \quad (I)$$

(We change one factor at a time. This is similar to how we show the product rule in calculus.)

$$\begin{aligned} a\cdot b - a'\cdot b' &= a\cdot b - a'\cdot b + a'\cdot b - a'\cdot b' \\ &= (a-a')\cdot b + a'\cdot(b-b') \\ &= (nk)\cdot b + a'\cdot(nl) \qquad (I),\ (II) \\ &= n\cdot(\underbrace{kb + a'l}_{\text{in } \mathbb{Z}}) \end{aligned}$$

Therefore $a\cdot b \overset{n}{\equiv} a'\cdot b'$, and so by (I), $[a\cdot b]_n = [a'\cdot b']_n$. ∎

Next we see that the above operations on $\mathbb{Z}_n$ satisfy associativity and distribution. Moreover $\mathbb{Z}_n$ has neutral elements with respect to both $+$ and $\cdot$. Every element has an additive inverse. Later we will see what elements have multiplicative inverse.

Congruence arithmetic

Tuesday, June 29, 2021 2:09 PM

Proposition. For every $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ we have

(Associative) $[a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n$

$[a]_n \cdot ([b]_n \cdot [c]_n) = ([a]_n \cdot [b]_n) \cdot [c]_n$

(Neutral element) $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$

$[a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$

(Additive inverse) $[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$

(Commutative) $[a]_n + [b]_n = [b]_n + [a]_n$

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

(Distributive) $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$

$([b]_n + [c]_n) \cdot [a]_n = [b]_n \cdot [a]_n + [c]_n \cdot [a]_n$

All the claims are straightfoward conclusions of similar properties for integers. Here we check just one of the distributive properties.

$[a]_n \cdot ([b]_n + [c]_n) = [a_n] \cdot [b+c]_n = [a \cdot (b+c)]_n = [a \cdot b + a \cdot c]_n$

$[a]_n \cdot [b]_n + [a]_n \cdot [c]_n = [a \cdot b]_n + [a \cdot c]_n = [a \cdot b + a \cdot c]_n$