Rings and Things

Daniel H. Luecking

March 6, 2024

Modular arithmetic (aka "clock" arithmetic).

In the twenty-four hour system of telling time the hours go from 0 at midnight to 23 at one hour before midnight.

Modular arithmetic (aka "clock" arithmetic).

In the twenty-four hour system of telling time the hours go from 0 at midnight to 23 at one hour before midnight. Suppose the current time is 20 and my shift ends in 8 hours, then at the end of my shift the time won't be 28 but rather 4.

Modular arithmetic (aka "clock" arithmetic).

In the twenty-four hour system of telling time the hours go from 0 at midnight to 23 at one hour before midnight. Suppose the current time is 20 and my shift ends in 8 hours, then at the end of my shift the time won't be 28 but rather 4. This gives us a system where $20\ `+\text{'}\ 8 = 4$.
Similarly, $17\ `+\text{'}\ 7 = 0$.

In higher mathematics we study systems that consist of a set on which one or more binary operations are defined. The above description gives us a set, namely $\{0, 1, 2, 3, \ldots, 23\}$ and an operation '$+$'.

Modular arithmetic (aka "clock" arithmetic).

In the twenty-four hour system of telling time the hours go from 0 at midnight to 23 at one hour before midnight. Suppose the current time is 20 and my shift ends in 8 hours, then at the end of my shift the time won't be 28 but rather 4. This gives us a system where $20 \text{ `}+\text{' } 8 = 4$. Similarly, $17 \text{ `}+\text{' } 7 = 0$.

In higher mathematics we study systems that consist of a set on which one or more binary operations are defined. The above description gives us a set, namely $\{0, 1, 2, 3, \ldots, 23\}$ and an operation '$+$'. The operation is analogous to addition, but is not the usual operation of addition of integers. Let us call it $\hat{+}$ (temporarily). Its formal definition is

For any x and y in $\{0, 1, 2, \ldots, 23\}$, let $x \mathbin{\hat{+}} y = (x + y) \bmod 24$.

To make sense of this we need to know what mod means.

If k and n is are positive integers then there exist unique positive integers q and r where $0 \leq r < n$ and

$$k = qn + r$$

If k and n is are positive integers then there exist unique positive integers q and r where $0 \leq r < n$ and

$$k = qn + r$$

The number q is called the integer quotient of dividing k by n and r is the remainder. Then, by definition $k \bmod n$ is the remainder r. Some authors and most computer languages use '$\%$' instead of 'mod': $k \,\%\, n = r$.

If k and n is are positive integers then there exist unique positive integers q and r where $0 \leq r < n$ and

$$k = qn + r$$

The number q is called the integer quotient of dividing k by n and r is the remainder. Then, by definition $k \bmod n$ is the remainder r. Some authors and most computer languages use '$\%$' instead of 'mod': $k \,\%\, n = r$.

For example, Since $28 = 1 \cdot 24 + 4$, then for $k = 28$ and $n = 24$ we have $28 \bmod 24 = 4$. Similarly. $71 = 2 \cdot 24 + 23$ so $71 \bmod 24 = 23$ and $72 \bmod 24 = 0$.

If k and n is are positive integers then there exist unique positive integers q and r where $0 \leq r < n$ and

$$k = qn + r$$

The number q is called the integer quotient of dividing k by n and r is the remainder. Then, by definition $k \bmod n$ is the remainder r. Some authors and most computer languages use '$\%$' instead of 'mod': $k \,\%\, n = r$.

For example, Since $28 = 1 \cdot 24 + 4$, then for $k = 28$ and $n = 24$ we have $28 \bmod 24 = 4$. Similarly. $71 = 2 \cdot 24 + 23$ so $71 \bmod 24 = 23$ and $72 \bmod 24 = 0$.

By definition, we always have $0 \leq k \bmod n \leq n - 1$. We can obtain $k \bmod m$ by second grade divison: To find, for example $68 \bmod 9 = 5$ we say "9 goes into 68 seven times (for 63) with a remainder of 5." Here's an example computing $721 \bmod 101 = 14$:

```
          7 R 14
     ____________
101 | 721
      707
      ---
       14
```

We can do modular arithmetic in any 'base': Define $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and define 'addition' on $\mathbb{Z}_n$ by $x \hat{+} y = (x + y) \bmod n$.

We can do modular arithmetic in any 'base': Define $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and define 'addition' on $\mathbb{Z}_n$ by $x \hat{+} y = (x + y) \bmod n$. We can also define multiplication this way: $x \hat{\cdot} y = (xy) \bmod n$. The xy is ordinary multiplication.

We can do modular arithmetic in any 'base': Define $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and define 'addition' on $\mathbb{Z}_n$ by $x \hat{+} y = (x + y) \bmod n$. We can also define multiplication this way: $x \hat{\cdot} y = (xy) \bmod n$. The xy is ordinary multiplication.

So in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ we have $5 \hat{+} 4 = 3$ (because $9 \bmod 6 = 3$) and $4 \hat{\cdot} 5 = 2$ (because $20 \bmod 6 = 2$).

We can do modular arithmetic in any 'base': Define $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and define 'addition' on $\mathbb{Z}_n$ by $x \mathbin{\hat{+}} y = (x + y) \bmod n$. We can also define multiplication this way: $x \mathbin{\hat{\cdot}} y = (xy) \bmod n$. The xy is ordinary multiplication.

So in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ we have $5 \mathbin{\hat{+}} 4 = 3$ (because $9 \bmod 6 = 3$) and $4 \mathbin{\hat{\cdot}} 5 = 2$ (because $20 \bmod 6 = 2$). For small values of n one can find $k \bmod n$ by subtracting n from k (repeatedly, if necessary) until a nonnegative number less than n is obtained.

We can do modular arithmetic in any 'base': Define $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and define 'addition' on $\mathbb{Z}_n$ by $x \hat{+} y = (x + y) \bmod n$. We can also define multiplication this way: $x \hat{\cdot} y = (xy) \bmod n$. The xy is ordinary multiplication.

So in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ we have $5 \hat{+} 4 = 3$ (because $9 \bmod 6 = 3$) and $4 \hat{\cdot} 5 = 2$ (because $20 \bmod 6 = 2$). For small values of n one can find $k \bmod n$ by subtracting n from k (repeatedly, if necessary) until a nonnegative number less than n is obtained. For example, to get $20 \bmod 6$: $20 - 6 = 14$ (too big), $14 - 6 = 8$ (too big), $8 - 6 = 2$ (okay).

These operations ($\hat{+}$ and $\hat{\cdot}$) on $\mathbb{Z}_n$ share a lot of the algebraic properties of addition and multiplication of integers.

We can do modular arithmetic in any 'base': Define $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and define 'addition' on $\mathbb{Z}_n$ by $x \hat{+} y = (x + y) \bmod n$. We can also define multiplication this way: $x \hat{\cdot} y = (xy) \bmod n$. The xy is ordinary multiplication.

So in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ we have $5 \hat{+} 4 = 3$ (because $9 \bmod 6 = 3$) and $4 \hat{\cdot} 5 = 2$ (because $20 \bmod 6 = 2$). For small values of n one can find $k \bmod n$ by subtracting n from k (repeatedly, if necessary) until a nonnegative number less than n is obtained. For example, to get $20 \bmod 6$: $20 - 6 = 14$ (too big), $14 - 6 = 8$ (too big), $8 - 6 = 2$ (okay).

These operations ($\hat{+}$ and $\hat{\cdot}$) on $\mathbb{Z}_n$ share a lot of the algebraic properties of addition and multiplication of integers. It is usual to write $\mathbb{Z}$ for the set of all integers (positive negative and 0).

There is a concept called *congruence*. It uses the notation

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

We can do modular arithmetic in any 'base': Define $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and define 'addition' on $\mathbb{Z}_n$ by $x \hat{+} y = (x + y) \bmod n$. We can also define multiplication this way: $x \hat{\cdot} y = (xy) \bmod n$. The xy is ordinary multiplication.

So in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ we have $5 \hat{+} 4 = 3$ (because $9 \bmod 6 = 3$) and $4 \hat{\cdot} 5 = 2$ (because $20 \bmod 6 = 2$). For small values of n one can find $k \bmod n$ by subtracting n from k (repeatedly, if necessary) until a nonnegative number less than n is obtained. For example, to get $20 \bmod 6$: $20 - 6 = 14$ (too big), $14 - 6 = 8$ (too big), $8 - 6 = 2$ (okay).

These operations ($\hat{+}$ and $\hat{\cdot}$) on $\mathbb{Z}_n$ share a lot of the algebraic properties of addition and multiplication of integers. It is usual to write $\mathbb{Z}$ for the set of all integers (positive negative and 0).

There is a concept called *congruence*. It uses the notation

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

This means that $a - b$ is evenly divisible by n. The notation we will are using: $a = (b \bmod n)$ or $a = (b \,\%\, n)$ means two things

$$a \equiv b \pmod{n} \quad \text{and} \quad 0 \leq a < n\,.$$

A *ring* is a set R along with two binary operations (traditionally the symbols $+$ and $\cdot$ are used) that satisfy the following properties.

A *ring* is a set R along with two binary operations (traditionally the symbols $+$ and $\cdot$ are used) that satisfy the following properties.

C1 If x and y are in R then $x + y$ is in R.

C2 If x and y are in R then $x \cdot y$ is in R.

A *ring* is a set R along with two binary operations (traditionally the symbols $+$ and $\cdot$ are used) that satisfy the following properties.

C1 If x and y are in R then $x + y$ is in R.

C2 If x and y are in R then $x \cdot y$ is in R.

A1 If x and y are in R then $x + y = y + x$.

A2 If x, y and z are in R then $(x + y) + z = x + (y + z)$.

A *ring* is a set R along with two binary operations (traditionally the symbols $+$ and $\cdot$ are used) that satisfy the following properties.

- C1 If x and y are in R then $x + y$ is in R.
- C2 If x and y are in R then $x \cdot y$ is in R.

- A1 If x and y are in R then $x + y = y + x$.
- A2 If x, y and z are in R then $(x + y) + z = x + (y + z)$.
- A3 There exists a special element 0 in R satisfying $x + 0 = x$ for every x in R. This element is called the 'zero' of R.
- A4 If x is in R there is an associated element in R called the negative of x and written $-x$ that satisfies $x + -x = 0$.

A *ring* is a set R along with two binary operations (traditionally the symbols $+$ and $\cdot$ are used) that satisfy the following properties.

C1 If x and y are in R then $x + y$ is in R.

C2 If x and y are in R then $x \cdot y$ is in R.

A1 If x and y are in R then $x + y = y + x$.

A2 If x, y and z are in R then $(x + y) + z = x + (y + z)$.

A3 There exists a special element 0 in R satisfying $x + 0 = x$ for every x in R. This element is called the 'zero' of R.

A4 If x is in R there is an associated element in R called the negative of x and written $-x$ that satisfies $x + -x = 0$.

A5 If x, y and z are in R then $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

A *ring* is a set R along with two binary operations (traditionally the symbols $+$ and $\cdot$ are used) that satisfy the following properties.

- C1 If x and y are in R then $x + y$ is in R.
- C2 If x and y are in R then $x \cdot y$ is in R.

- A1 If x and y are in R then $x + y = y + x$.
- A2 If x, y and z are in R then $(x + y) + z = x + (y + z)$.
- A3 There exists a special element 0 in R satisfying $x + 0 = x$ for every x in R. This element is called the 'zero' of R.
- A4 If x is in R there is an associated element in R called the negative of x and written $-x$ that satisfies $x + -x = 0$.
- A5 If x, y and z are in R then $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- A6 If x, y and z are in R then $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

A *ring* is a set R along with two binary operations (traditionally the symbols $+$ and $\cdot$ are used) that satisfy the following properties.

- C1 If x and y are in R then $x + y$ is in R.
- C2 If x and y are in R then $x \cdot y$ is in R.

- A1 If x and y are in R then $x + y = y + x$.
- A2 If x, y and z are in R then $(x + y) + z = x + (y + z)$.
- A3 There exists a special element 0 in R satisfying $x + 0 = x$ for every x in R. This element is called the 'zero' of R.
- A4 If x is in R there is an associated element in R called the negative of x and written $-x$ that satisfies $x + -x = 0$.
- A5 If x, y and z are in R then $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- A6 If x, y and z are in R then $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

The sets $\mathbb{Z}_n$ with the operations of 'addition modulo n' and 'multiplication modulo n' are all examples of rings. Notice that in $\mathbb{Z}_{24}$ we saw that $17 \mathbin{\hat{+}} 7 = 0$. By part A4, that means that $-17 = 7$ and $-7 = 17$.

There are a number of other properties that can be proved from A1–A6.

There are a number of other properties that can be proved from A1–A6. For example.

- There is only one element that satisfies A3. In fact if any elements of R satisfy $x + y = x$ then y must be zero.

There are a number of other properties that can be proved from A1–A6. For example.

- There is only one element that satisfies A3. In fact if any elements of R satisfy $x + y = x$ then y must be zero.
- For any x in R, $0 \cdot x = 0 = x \cdot 0$.

There are a number of other properties that can be proved from A1–A6. For example.

- There is only one element that satisfies A3. In fact if any elements of R satisfy $x + y = x$ then y must be zero.
- For any x in R, $0 \cdot x = 0 = x \cdot 0$.
- There is only one negative for any element x in R. That is, if $x + y = 0$, then $y = -x$.

There are a number of other properties that can be proved from A1–A6. For example.

- There is only one element that satisfies A3. In fact if any elements of R satisfy $x + y = x$ then y must be zero.
- For any x in R, $0 \cdot x = 0 = x \cdot 0$.
- There is only one negative for any element x in R. That is, if $x + y = 0$, then $y = -x$.
- Laws of signs: $-0 = 0$, $-(-x) = x$, $x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$ and $(-x) \cdot (-y) = x \cdot y$.

There are a number of other properties that can be proved from A1–A6. For example.

- There is only one element that satisfies A3. In fact if any elements of R satisfy $x + y = x$ then y must be zero.
- For any x in R, $0 \cdot x = 0 = x \cdot 0$.
- There is only one negative for any element x in R. That is, if $x + y = 0$, then $y = -x$.
- Laws of signs: $-0 = 0$, $-(-x) = x$, $x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$ and $(-x) \cdot (-y) = x \cdot y$.
- We can extend A1 and A2 to any number of elements. That is $x_1 + x_2 + \cdots + x_n$ gives the same result however they are grouped or reordered.

There are a number of other properties that can be proved from A1–A6. For example.

- There is only one element that satisfies A3. In fact if any elements of R satisfy $x + y = x$ then y must be zero.
- For any x in R, $0 \cdot x = 0 = x \cdot 0$.
- There is only one negative for any element x in R. That is, if $x + y = 0$, then $y = -x$.
- Laws of signs: $-0 = 0$, $-(-x) = x$, $x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$ and $(-x) \cdot (-y) = x \cdot y$.
- We can extend A1 and A2 to any number of elements. That is $x_1 + x_2 + \cdots + x_n$ gives the same result however they are grouped or reordered.
- A5 can be extended to any number of elements: how they are grouped does not change the result of the multiplication.

There are a number of other properties that can be proved from A1–A6. For example.

- There is only one element that satisfies A3. In fact if any elements of R satisfy $x + y = x$ then y must be zero.
- For any x in R, $0 \cdot x = 0 = x \cdot 0$.
- There is only one negative for any element x in R. That is, if $x + y = 0$, then $y = -x$.
- Laws of signs: $-0 = 0$, $-(-x) = x$, $x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$ and $(-x) \cdot (-y) = x \cdot y$.
- We can extend A1 and A2 to any number of elements. That is $x_1 + x_2 + \cdots + x_n$ gives the same result however they are grouped or reordered.
- A5 can be extended to any number of elements: how they are grouped does not change the result of the multiplication.
- A6 applies to any length of the sum:

$$x \cdot (y_1 + y_2 + \cdots + y_n) = x \cdot y_1 + x \cdot y_2 + \cdots + x \cdot y_n$$

  and the same for multiplying on the right.

Some rings have additional properties

In the definition of a ring we required $x + y = y + x$ but **did not require** $x \cdot y = y \cdot x$.

Some rings have additional properties

In the definition of a ring we required $x + y = y + x$ but **did not require** $x \cdot y = y \cdot x$. The reason for this is that matrices are very important in mathematics and matrix multiplication doesn't satisfy this.

Some rings have additional properties

In the definition of a ring we required $x + y = y + x$ but **did not require** $x \cdot y = y \cdot x$. The reason for this is that matrices are very important in mathematics and matrix multiplication doesn't satisfy this.

We also note that for the ring of all integers $(\mathbb{Z}, +, \cdot)$ the only way one gets $x \cdot y = 0$ is if either $x = 0$ or $y = 0$.

Some rings have additional properties

In the definition of a ring we required $x + y = y + x$ but **did not require** $x \cdot y = y \cdot x$. The reason for this is that matrices are very important in mathematics and matrix multiplication doesn't satisfy this.

We also note that for the ring of all integers $(\mathbb{Z}, +, \cdot)$ the only way one gets $x \cdot y = 0$ is if either $x = 0$ or $y = 0$. However, this is not true for all rings. For example, in $\mathbb{Z}_6$ we have $2 \cdot 3 = 0$ as well as $4 \cdot 3 = 0$. (From now on I will use normal $+$ and $\cdot$ for the operations in any $\mathbb{Z}_n$.)

Some rings have additional properties

In the definition of a ring we required $x + y = y + x$ but **did not require** $x \cdot y = y \cdot x$. The reason for this is that matrices are very important in mathematics and matrix multiplication doesn't satisfy this.

We also note that for the ring of all integers $(\mathbb{Z}, +, \cdot)$ the only way one gets $x \cdot y = 0$ is if either $x = 0$ or $y = 0$. However, this is not true for all rings. For example, in $\mathbb{Z}_6$ we have $2 \cdot 3 = 0$ as well as $4 \cdot 3 = 0$. (From now on I will use normal $+$ and $\cdot$ for the operations in any $\mathbb{Z}_n$.)

The ring of integers has a special element, the number 1, that satisfies $1 \cdot x = x$ for every element x.

Some rings have additional properties

In the definition of a ring we required $x + y = y + x$ but **did not require** $x \cdot y = y \cdot x$. The reason for this is that matrices are very important in mathematics and matrix multiplication doesn't satisfy this.

We also note that for the ring of all integers $(\mathbb{Z}, +, \cdot)$ the only way one gets $x \cdot y = 0$ is if either $x = 0$ or $y = 0$. However, this is not true for all rings. For example, in $\mathbb{Z}_6$ we have $2 \cdot 3 = 0$ as well as $4 \cdot 3 = 0$. (From now on I will use normal $+$ and $\cdot$ for the operations in any $\mathbb{Z}_n$.)

The ring of integers has a special element, the number 1, that satisfies $1 \cdot x = x$ for every element x. This not always true: the set of even integers with the usual operations of addition and multiplication is a ring, but has no such element.

Definition

Let $(R, +, \cdot)$ be a ring

- if every pair of elements in R satisfies $x \cdot y = y \cdot x$ we call R a *commutative ring*

Definition

Let $(R, +, \cdot)$ be a ring

- if every pair of elements in R satisfies $x \cdot y = y \cdot x$ we call R a *commutative ring*
- If there exists an element $u \neq 0$ of R that satisfies $u \cdot x = x = x \cdot u$ for every x in R, then u is called a *unity* or a *multiplicative identity* (or just 'the identity') and we say R is a *ring with unity*.

Definition

Let $(R, +, \cdot)$ be a ring

- if every pair of elements in R satisfies $x \cdot y = y \cdot x$ we call R a *commutative ring*
- If there exists an element $u \neq 0$ of R that satisfies $u \cdot x = x = x \cdot u$ for every x in R, then u is called a *unity* or a *multiplicative identity* (or just 'the identity') and we say R is a *ring with unity*.
- An element $x \neq 0$ of a commutative ring R is called a *proper zero divisor* if there is another element $y \neq 0$ such that $x \cdot y = 0$.

Definition

Let $(R, +, \cdot)$ be a ring

- if every pair of elements in R satisfies $x \cdot y = y \cdot x$ we call R a *commutative ring*
- If there exists an element $u \neq 0$ of R that satisfies $u \cdot x = x = x \cdot u$ for every x in R, then u is called a *unity* or a *multiplicative identity* (or just 'the identity') and we say R is a *ring with unity*.
- An element $x \neq 0$ of a commutative ring R is called a *proper zero divisor* if there is another element $y \neq 0$ such that $x \cdot y = 0$.

Definition

Let $(R, +, \cdot)$ be a ring with unity u. If x is in R and there is an element y in R such that $x \cdot y = u = y \cdot x$ we call y the *multiplicative inverse* of x. In that case we say that x is a *unit* (or *is invertible*) and we call its multiplicative inverse x^{-1}.

Examples

The rings $\mathbb{Z}_n$ are all commutative rings and rings with unity. The unity is the element 1.

Examples

The rings $\mathbb{Z}_n$ are all commutative rings and rings with unity. The unity is the element 1. If n is prime (cannot be factored into a product of smaller numbers) then $\mathbb{Z}_n$ has no proper zero divisors.

Examples

The rings $\mathbb{Z}_n$ are all commutative rings and rings with unity. The unity is the element 1. If n is prime (cannot be factored into a product of smaller numbers) then $\mathbb{Z}_n$ has no proper zero divisors.

It can be shown that a ring has at most one unity.

Examples

The rings $\mathbb{Z}_n$ are all commutative rings and rings with unity. The unity is the element 1. If n is prime (cannot be factored into a product of smaller numbers) then $\mathbb{Z}_n$ has no proper zero divisors.

It can be shown that a ring has at most one unity.

In $\mathbb{Z}_6$ we have 1 for the unity. The elements 1 and 5 are units: since $1 \cdot 1 = 1$ and $5 \cdot 5 = 1$ it follows that each is its own multiplicative inverse.

In $\mathbb{Z}_{15}$ we have units 2 and 8 (inverses of each other), 7 and 13 (inverses of each other) and also 1, 4, 11 and 14 (each is its own inverse).

The simplest ring is $\{0\}$, with the operations defined $0+0=0$ and $0 \cdot 0 = 0$. It it trivially commutative, has no proper zero divisors, and has no unity.

The simplest ring is $\{0\}$, with the operations defined $0 + 0 = 0$ and $0 \cdot 0 = 0$. It it trivially commutative, has no proper zero divisors, and has no unity.

The next simplest might be $\mathbb{Z}_2$. In applications, 0 often represents 'false' and 1 represents 'true'. Then multiplication represents the AND operation and addition represents XOR (the 'exclusive or' operation).

The simplest ring is $\{0\}$, with the operations defined $0 + 0 = 0$ and $0 \cdot 0 = 0$. It it trivially commutative, has no proper zero divisors, and has no unity.

The next simplest might be $\mathbb{Z}_2$. In applications, 0 often represents 'false' and 1 represents 'true'. Then multiplication represents the AND operation and addition represents XOR (the 'exclusive or' operation). This is a commutative ring with unity with no proper zero divisors.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Addition and multiplication tables for $\mathbb{Z}_2$

The set of units in a ring is a useful system of its own that has the following properties

The set of units in a ring is a useful system of its own that has the following properties

Theorem

If R is a ring with unity u then

1. *the unity u is always a unit and is its own inverse;*

The set of units in a ring is a useful system of its own that has the following properties

Theorem

If R is a ring with unity u then

1. *the unity u is always a unit and is its own inverse;*
2. *if x is a unit so are $-x$ and x^{-1}: the inverse of $-x$ is $-x^{-1}$ and the inverse of x^{-1} is x.*

The set of units in a ring is a useful system of its own that has the following properties

Theorem

If R is a ring with unity u then

1. *the unity u is always a unit and is its own inverse;*
2. *if x is a unit so are $-x$ and x^{-1}: the inverse of $-x$ is $-x^{-1}$ and the inverse of x^{-1} is x.*
3. *if x and y are units then so is $x \cdot y$: the inverse of $x \cdot y$ is $y^{-1} \cdot x^{-1}$.*

The set of units in a ring is a useful system of its own that has the following properties

Theorem

If R is a ring with unity u then

1. *the unity u is always a unit and is its own inverse;*
2. *if x is a unit so are $-x$ and x^{-1}: the inverse of $-x$ is $-x^{-1}$ and the inverse of x^{-1} is x.*
3. *if x and y are units then so is $x \cdot y$: the inverse of $x \cdot y$ is $y^{-1} \cdot x^{-1}$.*

Proof: If u is the unity then $u \cdot u = u$.

The set of units in a ring is a useful system of its own that has the following properties

Theorem

If R is a ring with unity u then

1. *the unity u is always a unit and is its own inverse;*
2. *if x is a unit so are $-x$ and x^{-1}: the inverse of $-x$ is $-x^{-1}$ and the inverse of x^{-1} is x.*
3. *if x and y are units then so is $x \cdot y$: the inverse of $x \cdot y$ is $y^{-1} \cdot x^{-1}$.*

Proof: If u is the unity then $u \cdot u = u$.

If we multiply $(-x) \cdot (-x^{-1})$ we get $x \cdot x^{-1} = u$ (law of signs). The other order is similar.

If x and y are units consider $(x \cdot y) \cdot (y^{-1} \cdot x^{-1})$.

If x and y are units consider $(x \cdot y) \cdot (y^{-1} \cdot x^{-1})$. Regroup this as

$$\begin{aligned}(x \cdot (y \cdot y^{-1})) \cdot x^{-1} &= (x \cdot u) \cdot x^{-1} \\ &= x \cdot x^{-1} = u.\end{aligned}$$

If x and y are units consider $(x \cdot y) \cdot (y^{-1} \cdot x^{-1})$. Regroup this as

$$\begin{aligned}(x \cdot (y \cdot y^{-1})) \cdot x^{-1} &= (x \cdot u) \cdot x^{-1} \\ &= x \cdot x^{-1} = u.\end{aligned}$$

Similar steps show that $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = u$. QED

If x and y are units consider $(x \cdot y) \cdot (y^{-1} \cdot x^{-1})$. Regroup this as

$$\begin{aligned}(x \cdot (y \cdot y^{-1})) \cdot x^{-1} &= (x \cdot u) \cdot x^{-1} \\ &= x \cdot x^{-1} = u.\end{aligned}$$

Similar steps show that $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = u$. QED

Some examples: we saw that in $\mathbb{Z}_{15}$, 7 is invertible and $7^{-1} = 13$. Therefore 13 is invertible with $13^{-1} = 7$.

If x and y are units consider $(x \cdot y) \cdot (y^{-1} \cdot x^{-1})$. Regroup this as

$$\begin{aligned}(x \cdot (y \cdot y^{-1})) \cdot x^{-1} &= (x \cdot u) \cdot x^{-1} \\ &= x \cdot x^{-1} = u.\end{aligned}$$

Similar steps show that $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = u$. QED

Some examples: we saw that in $\mathbb{Z}_{15}$, 7 is invertible and $7^{-1} = 13$. Therefore 13 is invertible with $13^{-1} = 7$. Also, -7 is invertible and $(-7)^{-1} = 8^{-1} = 2 = -13 = -7^{-1}$.

If x and y are units consider $(x \cdot y) \cdot (y^{-1} \cdot x^{-1})$. Regroup this as

$$\begin{aligned}(x \cdot (y \cdot y^{-1})) \cdot x^{-1} &= (x \cdot u) \cdot x^{-1} \\ &= x \cdot x^{-1} = u.\end{aligned}$$

Similar steps show that $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = u$. QED

Some examples: we saw that in $\mathbb{Z}_{15}$, 7 is invertible and $7^{-1} = 13$. Therefore 13 is invertible with $13^{-1} = 7$. Also, -7 is invertible and $(-7)^{-1} = 8^{-1} = 2 = -13 = -7^{-1}$. Finally, as an example of inverses of products $7 \cdot 4 = 13$ is invertible and $4^{-1} \cdot 7^{-1} = 4 \cdot 13 = 7 = 13^{-1}$.

If x and y are units consider $(x \cdot y) \cdot (y^{-1} \cdot x^{-1})$. Regroup this as

$$\begin{aligned}(x \cdot (y \cdot y^{-1})) \cdot x^{-1} &= (x \cdot u) \cdot x^{-1} \\ &= x \cdot x^{-1} = u.\end{aligned}$$

Similar steps show that $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = u$. QED

Some examples: we saw that in $\mathbb{Z}_{15}$, 7 is invertible and $7^{-1} = 13$. Therefore 13 is invertible with $13^{-1} = 7$. Also, -7 is invertible and $(-7)^{-1} = 8^{-1} = 2 = -13 = -7^{-1}$. Finally, as an example of inverses of products $7 \cdot 4 = 13$ is invertible and $4^{-1} \cdot 7^{-1} = 4 \cdot 13 = 7 = 13^{-1}$.

We can do repeated multiplications as well: the inverse of $8 \cdot 13 \cdot 13 = 2$ is $7 \cdot 7 \cdot 2 = 8$.