The Rings $\mathbb{Z}_n$

Daniel H. Luecking

October 20, 2023

A couple of examples of finding inverses. Find the inverse of 100 in the ring $\mathbb{Z}_{711}$. Here's the Euclidean algorithm:

$$\begin{aligned} 711 &= 7(100) + 11 \\ 100 &= 9(11) \quad + 1 \end{aligned}$$

A couple of examples of finding inverses. Find the inverse of 100 in the ring $\mathbb{Z}_{711}$. Here's the Euclidean algorithm:

$$\begin{aligned} 711 &= 7(100) + 11 \\ 100 &= 9(11) \quad + 1 \end{aligned}$$

So $\gcd(711, 100) = 1$ and we know that 100 is invertible.

A couple of examples of finding inverses. Find the inverse of 100 in the ring $\mathbb{Z}_{711}$. Here's the Euclidean algorithm:

$$711 = 7(100) + 11$$
$$100 = 9(11) \ \ + 1$$

So $\gcd(711, 100) = 1$ and we know that 100 is invertible. With $n = 711$, $k = 100$, $r_1 = 11$ and $r_2 = 1$:

$$n = \ 7k + r_1$$
$$k = 9r_1 + r_2$$

A couple of examples of finding inverses. Find the inverse of 100 in the ring $\mathbb{Z}_{711}$. Here's the Euclidean algorithm:

$$711 = 7(100) + 11$$
$$100 = 9(11) \quad + 1$$

So $\gcd(711, 100) = 1$ and we know that 100 is invertible. With $n = 711$, $k = 100$, $r_1 = 11$ and $r_2 = 1$:

$$n = \ 7k + r_1$$
$$k = 9r_1 + r_2$$

we can eliminate r_1 by inserting its value $(n - 7k)$ in the second equation:

$$k = 9(n - 7k) + r_2 \ \text{ or } \ r_2 = 64k - 9n \ \text{ or } \ 1 = 64(100) - 9(711)$$

A couple of examples of finding inverses. Find the inverse of 100 in the ring $\mathbb{Z}_{711}$. Here's the Euclidean algorithm:

$$\begin{aligned} 711 &= 7(100) + 11 \\ 100 &= 9(11) \ \ + 1 \end{aligned}$$

So $\gcd(711, 100) = 1$ and we know that 100 is invertible. With $n = 711$, $k = 100$, $r_1 = 11$ and $r_2 = 1$:

$$\begin{aligned} n &= \ 7k + r_1 \\ k &= 9r_1 + r_2 \end{aligned}$$

we can eliminate r_1 by inserting its value $(n - 7k)$ in the second equation:

$$k = 9(n - 7k) + r_2 \quad \text{or} \quad r_2 = 64k - 9n \quad \text{or} \quad 1 = 64(100) - 9(711)$$

This tells us that $64 \cdot 100 = 1$ in $\mathbb{Z}_{711}$ so, $100^{-1} = 64$.

Lets take the same ring, $\mathbb{Z}_{711}$ and find the inverse of 101.

$$\begin{aligned} 711 &= \ \ 7(101) + 4 \\ 101 &= 25(4) \quad\ + 1 \end{aligned}$$

Lets take the same ring, $\mathbb{Z}_{711}$ and find the inverse of 101.

$$\begin{aligned} 711 &= \ \ 7(101) + 4 \\ 101 &= 25(4) \quad\ + 1 \end{aligned}$$

So $\gcd(711, 101) = 1$ and we know that 101 is invertible.

Lets take the same ring, $\mathbb{Z}_{711}$ and find the inverse of 101.

$$\begin{aligned} 711 &= \ \ 7(101) + 4 \\ 101 &= 25(4) \quad\ + 1 \end{aligned}$$

So $\gcd(711, 101) = 1$ and we know that 101 is invertible. We can eliminate the intermediate remainder 4 by substituting $4 = (711) - 7(101)$ into the second equation:

$$\begin{aligned} (101) &= 25((711) - 7(101)) + 1, \\ &= 25(711) - 175(101) + 1, \qquad\qquad \text{or} \\ 1 &= 176(101) - 25(711) \end{aligned}$$

Lets take the same ring, $\mathbb{Z}_{711}$ and find the inverse of 101.

$$\begin{aligned} 711 &= \;\; 7(101) + 4 \\ 101 &= 25(4) \quad\; + 1 \end{aligned}$$

So $\gcd(711, 101) = 1$ and we know that 101 is invertible. We can eliminate the intermediate remainder 4 by substituting $4 = (711) - 7(101)$ into the second equation:

$$\begin{aligned} (101) &= 25((711) - 7(101)) + 1, \\ &= 25(711) - 175(101) + 1, \qquad \text{or} \\ 1 &= 176(101) - 25(711) \end{aligned}$$

This tells us that $176 \cdot 101 = 1$ in $\mathbb{Z}_{711}$ so, $101^{-1} = 176$.

Counting units

Counting how many units $\mathbb{Z}_n$ has is the same as counting the number of integers k between 1 and n that satisfy $\gcd(n, k) = 1$.

Counting units

Counting how many units $\mathbb{Z}_n$ has is the same as counting the number of integers k between 1 and n that satisfy $\gcd(n, k) = 1$. This was first accomplished by $Euler$, who denoted the number by $\phi(n)$. Nowadays, ϕ is called *Euler's totient function* or the *Euler ϕ-function*.

Counting units

Counting how many units $\mathbb{Z}_n$ has is the same as counting the number of integers k between 1 and n that satisfy $\gcd(n, k) = 1$. This was first accomplished by $Euler$, who denoted the number by $\phi(n)$. Nowadays, ϕ is called *Euler's totient function* or the *Euler ϕ-function*.

That is, $\phi(n)$ is the number of units in $\mathbb{Z}_n$ or the number of k with $1 \leq k \leq n$ such that $\gcd(n, k) = 1$.

Counting units

Counting how many units $\mathbb{Z}_n$ has is the same as counting the number of integers k between 1 and n that satisfy $\gcd(n, k) = 1$. This was first accomplished by $Euler$, who denoted the number by $\phi(n)$. Nowadays, ϕ is called *Euler's totient function* or the *Euler ϕ-function*.

That is, $\phi(n)$ is the number of units in $\mathbb{Z}_n$ or the number of k with $1 \leq k \leq n$ such that $\gcd(n, k) = 1$.

If we know the prime factorization of n there is a relatively simple formula for $\phi(n)$. The first thing we remark is that if d evenly divides both k and n, then any prime factor of d also does so.

So, if we want to eliminate numbers with $\gcd(n, k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

So, if we want to eliminate numbers with $\gcd(n,k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

So, if we want to eliminate numbers with $\gcd(n, k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

c_1: divisible by p_1

c_2: divisible by p_2

c_3: divisible by p_3

So, if we want to eliminate numbers with $\gcd(n,k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

c_1: divisible by p_1

c_2: divisible by p_2

c_3: divisible by p_3

So we need to process an inclusion/exclusion problem:

So, if we want to eliminate numbers with $\gcd(n,k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

- c_1: divisible by p_1
- c_2: divisible by p_2
- c_3: divisible by p_3

So we need to process an inclusion/exclusion problem: $N = n$,

So, if we want to eliminate numbers with $\gcd(n, k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

c_1: divisible by p_1

c_2: divisible by p_2

c_3: divisible by p_3

So we need to process an inclusion/exclusion problem: $N = n$, $N(c_1) = n/p_1$,

So, if we want to eliminate numbers with $\gcd(n, k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

c_1: divisible by p_1

c_2: divisible by p_2

c_3: divisible by p_3

So we need to process an inclusion/exclusion problem: $N = n$, $N(c_1) = n/p_1$, $N(c_2) = n/p_2$,

So, if we want to eliminate numbers with $\gcd(n, k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

c_1: divisible by p_1

c_2: divisible by p_2

c_3: divisible by p_3

So we need to process an inclusion/exclusion problem: $N = n$, $N(c_1) = n/p_1$, $N(c_2) = n/p_2$, $N(c_3) = n/p_3$,

So, if we want to eliminate numbers with $\gcd(n, k) > 1$ we only need to test primes. In fact we only need to test primes that divide n.

Suppose p_1, p_2, p_3 are all the prime divisors of n. Then we want to count how many integers from 1 to n *do not* satisfy any of the following conditions

c_1: divisible by p_1

c_2: divisible by p_2

c_3: divisible by p_3

So we need to process an inclusion/exclusion problem: $N = n$, $N(c_1) = n/p_1$, $N(c_2) = n/p_2$, $N(c_3) = n/p_3$, So,

$$S_1 = n\left(\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3}\right).$$

Continuing: The numbers that satisfy both c_1 and c_2, those divisible by both p_1 and p_2 must be divisible by $p_1 p_2$

Continuing: The numbers that satisfy both c_1 and c_2, those divisible by both p_1 and p_2 must be divisible by $p_1 p_2$ and there are $N(c_1 c_2) = n/(p_1 p_2)$ of those.

Continuing: The numbers that satisfy both c_1 and c_2, those divisible by both p_1 and p_2 must be divisible by p_1p_2 and there are $N(c_1c_2) = n/(p_1p_2)$ of those. Similarly, $N(c_1c_3) = n/(p_1p_3)$, $N(c_2c_3) = n/(p_2p_3)$

Continuing: The numbers that satisfy both c_1 and c_2, those divisible by both p_1 and p_2 must be divisible by p_1p_2 and there are $N(c_1c_2) = n/(p_1p_2)$ of those. Similarly, $N(c_1c_3) = n/(p_1p_3)$, $N(c_2c_3) = n/(p_2p_3)$ and so,

$$S_2 = n\left(\frac{1}{p_1p_2} + \frac{1}{p_1p_3} + \frac{1}{p_2p_3}\right).$$

Continuing: The numbers that satisfy both c_1 and c_2, those divisible by both p_1 and p_2 must be divisible by p_1p_2 and there are $N(c_1c_2) = n/(p_1p_2)$ of those. Similarly, $N(c_1c_3) = n/(p_1p_3)$, $N(c_2c_3) = n/(p_2p_3)$ and so,

$$S_2 = n\left(\frac{1}{p_1p_2} + \frac{1}{p_1p_3} + \frac{1}{p_2p_3}\right).$$

and lastly

$$S_3 = n\left(\frac{1}{p_1p_2p_3}\right).$$

Continuing: The numbers that satisfy both c_1 and c_2, those divisible by both p_1 and p_2 must be divisible by $p_1 p_2$ and there are $N(c_1 c_2) = n/(p_1 p_2)$ of those. Similarly, $N(c_1 c_3) = n/(p_1 p_3)$, $N(c_2 c_3) = n/(p_2 p_3)$ and so,

$$S_2 = n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \frac{1}{p_2 p_3}\right).$$

and lastly

$$S_3 = n\left(\frac{1}{p_1 p_2 p_3}\right).$$

Putting these together

$$\begin{aligned} N(\overline{c_1}\,\overline{c_2}\,\overline{c_3}) &= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \frac{1}{p_3} + \frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \frac{1}{p_2 p_3} - \frac{1}{p_1 p_2 p_3}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \end{aligned}$$

All that was for 3 prime factors.

All that was for 3 prime factors. The formula for any number of primes is: if $p_1, p_2, \ldots$ are the different primes that divide n then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots = n\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right)\cdots$$

All that was for 3 prime factors. The formula for any number of primes is: if $p_1, p_2, \ldots$ are the different primes that divide n then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots = n\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right)\cdots$$

In particular, if p is a prime number then $\phi(p) = p(1 - 1/p) = p - 1$, $\phi(p^2) = p^2(1 - 1/p) = p(p-1)$, etc.

All that was for 3 prime factors. The formula for any number of primes is: if $p_1, p_2, \ldots$ are the different primes that divide n then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots = n\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right)\cdots$$

In particular, if p is a prime number then $\phi(p) = p(1 - 1/p) = p - 1$, $\phi(p^2) = p^2(1 - 1/p) = p(p - 1)$, etc.

Some examples. $90 = 2(3^2)5$ so the prime divisors are 2, 3, and 5.

All that was for 3 prime factors. The formula for any number of primes is: if $p_1, p_2, \ldots$ are the different primes that divide n then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots = n\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right)\cdots$$

In particular, if p is a prime number then $\phi(p) = p(1 - 1/p) = p - 1$, $\phi(p^2) = p^2(1 - 1/p) = p(p - 1)$, etc.

Some examples. $90 = 2(3^2)5$ so the prime divisors are 2, 3, and 5. Then

$$\begin{aligned}\phi(90) &= 90\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\\ &= 2(3^2)5\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\\ &= 3(1)(2)(4) = 24\end{aligned}$$

Another example: find $\phi(2200)$. Since $2200 = 2^3 5^2 11$ we get

$$\begin{aligned} \phi(2200) &= 2^3 5^2 11 \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{10}{11}\right) \\ &= 2^2 5(1)(4)(10) = 800. \end{aligned}$$

Another example: find $\phi(2200)$. Since $2200 = 2^3 5^2 11$ we get

$$\begin{aligned} \phi(2200) &= 2^3 5^2 11 \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{10}{11}\right) \\ &= 2^2 5(1)(4)(10) = 800. \end{aligned}$$

Two final examples: $\phi(100) = 100(1/2)(4/5) = 40$. From $1155 = 3(5)(7)(11)$ we have $\phi(1155) = 1155(2/3)(4/5)(6/7)(10/11) = 480$.

Another example: find $\phi(2200)$. Since $2200 = 2^3 5^2 11$ we get

$$\begin{aligned}\phi(2200) &= 2^3 5^2 11 \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{10}{11}\right) \\ &= 2^2 5(1)(4)(10) = 800.\end{aligned}$$

Two final examples: $\phi(100) = 100(1/2)(4/5) = 40$. From $1155 = 3(5)(7)(11)$ we have $\phi(1155) = 1155(2/3)(4/5)(6/7)(10/11) = 480$.

Counting proper zero divisors

Because every element of $\mathbb{Z}_n$ is either 0 or a unit or a proper zero divisor, there must be $n - \phi(n) - 1$ proper zero divisors.

Another example: find $\phi(2200)$. Since $2200 = 2^3 5^2 11$ we get

$$\begin{aligned}\phi(2200) &= 2^3 5^2 11 \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{10}{11}\right)\\ &= 2^2 5(1)(4)(10) = 800.\end{aligned}$$

Two final examples: $\phi(100) = 100(1/2)(4/5) = 40$. From $1155 = 3(5)(7)(11)$ we have $\phi(1155) = 1155(2/3)(4/5)(6/7)(10/11) = 480$.

Counting proper zero divisors

Because every element of $\mathbb{Z}_n$ is either 0 or a unit or a proper zero divisor, there must be $n - \phi(n) - 1$ proper zero divisors.

Since $\phi(90) = 24$, the ring $\mathbb{Z}_{90}$ has 24 units and $90 - 24 - 1 = 65$ proper zero divisors.

The ring $\mathbb{Z}_{2200}$ has $\phi(2200) = 800$ units and $2200 - 800 - 1 = 1399$ proper zero divisors.

The ring $\mathbb{Z}_{2200}$ has $\phi(2200) = 800$ units and $2200 - 800 - 1 = 1399$ proper zero divisors.
The ring $\mathbb{Z}_{100}$ has $\phi(100) = 40$ units and $100 - 40 - 1 = 59$ proper zero divisors.

The ring $\mathbb{Z}_{2200}$ has $\phi(2200) = 800$ units and $2200 - 800 - 1 = 1399$ proper zero divisors.
The ring $\mathbb{Z}_{100}$ has $\phi(100) = 40$ units and $100 - 40 - 1 = 59$ proper zero divisors.
The ring $\mathbb{Z}_{1155}$ has $\phi(1155) = 480$ units and $1155 - 480 - 1 = 674$ proper zero divisors.

The ring $\mathbb{Z}_{2200}$ has $\phi(2200) = 800$ units and $2200 - 800 - 1 = 1399$ proper zero divisors.
The ring $\mathbb{Z}_{100}$ has $\phi(100) = 40$ units and $100 - 40 - 1 = 59$ proper zero divisors.
The ring $\mathbb{Z}_{1155}$ has $\phi(1155) = 480$ units and $1155 - 480 - 1 = 674$ proper zero divisors.
The ring $\mathbb{Z}_{911}$ has $\phi(911) = 910$ units and $911 - 910 - 1 = 0$ proper zero divisors. (911 is prime so $\phi(911) = 911\left(1 - \frac{1}{911}\right) = 911 - 1 = 910$.)

One more way to create a new ring

One more way to create a new ring

Theorem

Suppose $(R, +.\cdot)$ *is a ring and* $(Y, +, \cdot)$ *is a set with operations of* $+$ *and* $\cdot$.

One more way to create a new ring

Theorem

Suppose $(R, +.\cdot)$ *is a ring and* $(Y, +, \cdot)$ *is a set with operations of* $+$ *and* $\cdot$*. If there is a function* h *from* R *to* Y *such that*

1. *For every pair* x, y *in* R*,* $h(x + y) = h(x) + h(y)$*.*

One more way to create a new ring

Theorem

Suppose $(R, +.\cdot)$ *is a ring and* $(Y, +, \cdot)$ *is a set with operations of* $+$ *and* $\cdot$*. If there is a function* h *from* R *to* Y *such that*

1. *For every pair* x, y *in* R*,* $h(x + y) = h(x) + h(y)$*.*
2. *For every pair* x, y *in* R*,* $h(x \cdot y) = h(x) \cdot h(y)$*.*

One more way to create a new ring

Theorem

Suppose $(R, +.\cdot)$ *is a ring and* $(Y, +, \cdot)$ *is a set with operations of* $+$ *and* $\cdot$*. If there is a function* h *from* R *to* Y *such that*

1. *For every pair* x, y *in* R*,* $h(x + y) = h(x) + h(y)$*.*
2. *For every pair* x, y *in* R*,* $h(x \cdot y) = h(x) \cdot h(y)$*.*
3. $Y = \{h(x) : x \in R\}$*. (We say* h *is 'onto' or 'surjective'.)*

One more way to create a new ring

Theorem

Suppose $(R, +.\cdot)$ *is a ring and* $(Y, +, \cdot)$ *is a set with operations of* $+$ *and* $\cdot$*. If there is a function* h *from* R *to* Y *such that*

1. *For every pair* x, y *in* R*,* $h(x + y) = h(x) + h(y)$*.*
2. *For every pair* x, y *in* R*,* $h(x \cdot y) = h(x) \cdot h(y)$*.*
3. $Y = \{h(x) : x \in R\}$*. (We say* h *is 'onto' or 'surjective'.)*

Then $(Y, +, \cdot)$ *is also a ring.*

One more way to create a new ring

Theorem

Suppose $(R, +.\cdot)$ *is a ring and* $(Y, +, \cdot)$ *is a set with operations of* $+$ *and* $\cdot$*. If there is a function* h *from* R *to* Y *such that*

1. *For every pair* x, y *in* R*,* $h(x+y) = h(x) + h(y)$*.*
2. *For every pair* x, y *in* R*,* $h(x \cdot y) = h(x) \cdot h(y)$*.*
3. $Y = \{h(x) : x \in R\}$*. (We say* h *is 'onto' or 'surjective'.)*

Then $(Y, +, \cdot)$ *is also a ring.*

An example of this is the function from $\mathbb{Z}$ to $\mathbb{Z}_n$ defined by $h(x) = x \bmod n$. Checking the three conditions of the theorem is not particularly difficult.

One more way to create a new ring

Theorem

Suppose $(R, +.\cdot)$ *is a ring and* $(Y, +, \cdot)$ *is a set with operations of* $+$ *and* $\cdot$*. If there is a function* h *from* R *to* Y *such that*

1. *For every pair* x, y *in* R*,* $h(x + y) = h(x) + h(y)$*.*
2. *For every pair* x, y *in* R*,* $h(x \cdot y) = h(x) \cdot h(y)$*.*
3. $Y = \{h(x) : x \in R\}$*. (We say* h *is 'onto' or 'surjective'.)*

Then $(Y, +, \cdot)$ *is also a ring.*

An example of this is the function from $\mathbb{Z}$ to $\mathbb{Z}_n$ defined by $h(x) = x \bmod n$. Checking the three conditions of the theorem is not particularly difficult.

Proving the theorem is maybe a little tricky but not particularly long. The first two conditions are the definition of h being a *homomorphism*.