The Rings $\mathbb{Z}_n$

Daniel H. Luecking

March 8, 2024

Product rings

If $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ are two rings then we can make a new ring out of $R_1 \times R_2 = \{(x, y) : x \in R_1 \text{ and } y \in R_2\}$,

Product rings

If $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ are two rings then we can make a new ring out of $R_1 \times R_2 = \{(x, y) : x \in R_1 \text{ and } y \in R_2\}$, by defining

$$(x, y) + (v, w) = (x + v, y + w) \quad \text{and} \quad (x, y) \cdot (v, w) = (x \cdot v, y \cdot w).$$

Product rings

If $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ are two rings then we can make a new ring out of $R_1 \times R_2 = \{(x, y) : x \in R_1 \text{ and } y \in R_2\}$, by defining

$$(x, y) + (v, w) = (x + v, y + w) \text{ and } (x, y) \cdot (v, w) = (x \cdot v, y \cdot w).$$

The zero of $R_1 \times R_2$ is $(0, 0)$. Note that $(x, 0) \cdot (0, w) = (0, 0)$, so $R_1 \times R_2$ almost always has proper zero divisors.

Matrix rings

If R is a ring and n is any positive integer we can create a new ring called $M_n(R)$ whose elements are all the $n \times n$ matrices whose entries are elements of R.

Product rings

If $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ are two rings then we can make a new ring out of $R_1 \times R_2 = \{(x, y) : x \in R_1 \text{ and } y \in R_2\}$, by defining

$$(x, y) + (v, w) = (x + v, y + w) \quad \text{and} \quad (x, y) \cdot (v, w) = (x \cdot v, y \cdot w).$$

The zero of $R_1 \times R_2$ is $(0, 0)$. Note that $(x, 0) \cdot (0, w) = (0, 0)$, so $R_1 \times R_2$ almost always has proper zero divisors.

Matrix rings

If R is a ring and n is any positive integer we can create a new ring called $M_n(R)$ whose elements are all the $n \times n$ matrices whose entries are elements of R. The zero of $M_n(R)$ is the matrix with all zero entries.

Product rings

If $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ are two rings then we can make a new ring out of $R_1 \times R_2 = \{(x, y) : x \in R_1 \text{ and } y \in R_2\}$, by defining

$$(x, y) + (v, w) = (x + v, y + w) \text{ and } (x, y) \cdot (v, w) = (x \cdot v, y \cdot w).$$

The zero of $R_1 \times R_2$ is $(0, 0)$. Note that $(x, 0) \cdot (0, w) = (0, 0)$, so $R_1 \times R_2$ almost always has proper zero divisors.

Matrix rings

If R is a ring and n is any positive integer we can create a new ring called $M_n(R)$ whose elements are all the $n \times n$ matrices whose entries are elements of R. The zero of $M_n(R)$ is the matrix with all zero entries. Even if R is commutative, $M_n(R)$ almost never is if $n > 1$. If R has a unity, then so does $M_n(R)$. $M_n(R)$ always has proper zero divisors when $n > 1$ unless $R = \{0\}$.

The rings $\mathbb{Z}_n$

We want to take a closer look at $\mathbb{Z}_n$ and answer some questions about it.

The rings $\mathbb{Z}_n$

We want to take a closer look at $\mathbb{Z}_n$ and answer some questions about it.

1. How can we tell which elements of $\mathbb{Z}_n$ are units?

The rings $\mathbb{Z}_n$

We want to take a closer look at $\mathbb{Z}_n$ and answer some questions about it.

1. How can we tell which elements of $\mathbb{Z}_n$ are units?
2. If k is a unit in $\mathbb{Z}_n$ how can we find its inverse?

The rings $\mathbb{Z}_n$

We want to take a closer look at $\mathbb{Z}_n$ and answer some questions about it.

1. How can we tell which elements of $\mathbb{Z}_n$ are units?
2. If k is a unit in $\mathbb{Z}_n$ how can we find its inverse?
3. How many units does $\mathbb{Z}_n$ have?

The rings $\mathbb{Z}_n$

We want to take a closer look at $\mathbb{Z}_n$ and answer some questions about it.

1. How can we tell which elements of $\mathbb{Z}_n$ are units?
2. If k is a unit in $\mathbb{Z}_n$ how can we find its inverse?
3. How many units does $\mathbb{Z}_n$ have?

Theorem

The nonzero elements in $\mathbb{Z}_n$ are either proper zero divisors or units. They are proper zero divisors when they have a factor in common with n (apart from 1) and units if they have no such common factor.

The rings $\mathbb{Z}_n$

We want to take a closer look at $\mathbb{Z}_n$ and answer some questions about it.

1. How can we tell which elements of $\mathbb{Z}_n$ are units?
2. If k is a unit in $\mathbb{Z}_n$ how can we find its inverse?
3. How many units does $\mathbb{Z}_n$ have?

Theorem

The nonzero elements in $\mathbb{Z}_n$ are either proper zero divisors or units. They are proper zero divisors when they have a factor in common with n (apart from 1) and units if they have no such common factor.

Definition

If k and n are two positive integers then a positive integer d is called a *common divisor* of k and n iff d evenly divides both k and n. The largest common divisor is denoted $\gcd(k, n)$.

The rings $\mathbb{Z}_n$

We want to take a closer look at $\mathbb{Z}_n$ and answer some questions about it.

1. How can we tell which elements of $\mathbb{Z}_n$ are units?
2. If k is a unit in $\mathbb{Z}_n$ how can we find its inverse?
3. How many units does $\mathbb{Z}_n$ have?

Theorem

The nonzero elements in $\mathbb{Z}_n$ are either proper zero divisors or units. They are proper zero divisors when they have a factor in common with n (apart from 1) and units if they have no such common factor.

Definition

If k and n are two positive integers then a positive integer d is called a *common divisor* of k and n iff d evenly divides both k and n. The largest common divisor is denoted $\gcd(k, n)$.

A common divisor is also called a *common factor*.

Example: 1, 2, 3 and 6 are the only common divisors of 24 and 90.

Example: 1, 2, 3 and 6 are the only common divisors of 24 and 90. The easiest way to see this is to completely factor both:

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$
$$90 = 2 \cdot 45 = 2 \cdot 3 \cdot 15 = 2 \cdot 3 \cdot 3 \cdot 5$$

Example: 1, 2, 3 and 6 are the only common divisors of 24 and 90. The easiest way to see this is to completely factor both:

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$
$$90 = 2 \cdot 45 = 2 \cdot 3 \cdot 15 = 2 \cdot 3 \cdot 3 \cdot 5$$

If we have factored both numbers down to primes, we can get the gcd by multiplying together the smallest power of all primes that appears in both. Thus $24 = 2^3 \cdot 3^1$ while $90 = 2^1 3^2 5^1$.

Example: 1, 2, 3 and 6 are the only common divisors of 24 and 90. The easiest way to see this is to completely factor both:

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$
$$90 = 2 \cdot 45 = 2 \cdot 3 \cdot 15 = 2 \cdot 3 \cdot 3 \cdot 5$$

If we have factored both numbers down to primes, we can get the gcd by multiplying together the smallest power of all primes that appears in both. Thus $24 = 2^3 \cdot 3^1$ while $90 = 2^1 3^2 5^1$. Since 2 appears in both factorizations with powers 2^1 and 2^3, the smaller is 2^1. Similarly, 3 appears as 3^1 and 3^2, with the smaller being 3^1. Then $\gcd(24, 90) = 2^1 \cdot 3^1 = 6$.

Example: 1, 2, 3 and 6 are the only common divisors of 24 and 90. The easiest way to see this is to completely factor both:

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$
$$90 = 2 \cdot 45 = 2 \cdot 3 \cdot 15 = 2 \cdot 3 \cdot 3 \cdot 5$$

If we have factored both numbers down to primes, we can get the gcd by multiplying together the smallest power of all primes that appears in both. Thus $24 = 2^3 \cdot 3^1$ while $90 = 2^1 3^2 5^1$. Since 2 appears in both factorizations with powers 2^1 and 2^3, the smaller is 2^1. Similarly, 3 appears as 3^1 and 3^2, with the smaller being 3^1. Then $\gcd(24, 90) = 2^1 \cdot 3^1 = 6$.

This method requires factoring completely both numbers. This can be rather difficult when the numbers are large. For example, finding $\gcd(37517, 75058)$ is not so easy by this method.

Example: 1, 2, 3 and 6 are the only common divisors of 24 and 90. The easiest way to see this is to completely factor both:

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$
$$90 = 2 \cdot 45 = 2 \cdot 3 \cdot 15 = 2 \cdot 3 \cdot 3 \cdot 5$$

If we have factored both numbers down to primes, we can get the gcd by multiplying together the smallest power of all primes that appears in both. Thus $24 = 2^3 \cdot 3^1$ while $90 = 2^1 3^2 5^1$. Since 2 appears in both factorizations with powers 2^1 and 2^3, the smaller is 2^1. Similarly, 3 appears as 3^1 and 3^2, with the smaller being 3^1. Then $\gcd(24, 90) = 2^1 \cdot 3^1 = 6$.

This method requires factoring completely both numbers. This can be rather difficult when the numbers are large. For example, finding $\gcd(37517, 75058)$ is not so easy by this method.

In fact, factoring large numbers is one of the hardest problems in computing (by 'large', I mean having thousands of bits in base 2).

The Euclidean Algorithm

Since computing gcd's is very important for applications, it is fortunate that there is a fast and easily programmable way to do it.

The Euclidean Algorithm

Since computing gcd's is very important for applications, it is fortunate that there is a fast and easily programmable way to do it.

Here is an example of finding a gcd by the *Euclidean algorithm*:

The Euclidean Algorithm

Since computing gcd's is very important for applications, it is fortunate that there is a fast and easily programmable way to do it.

Here is an example of finding a gcd by the *Euclidean algorithm*:

Finding $\gcd(195, 36)$. We try to divide 195 by 36. If this has no remainder we are done. But it has a remainder of 15:

$$195 = 5 \cdot 36 + 15$$

The Euclidean Algorithm

Since computing gcd's is very important for applications, it is fortunate that there is a fast and easily programmable way to do it.

Here is an example of finding a gcd by the *Euclidean algorithm*:

Finding $\gcd(195, 36)$. We try to divide 195 by 36. If this has no remainder we are done. But it has a remainder of 15:

$$195 = 5 \cdot 36 + 15$$

Any number that evenly divides both 195 and 36 must also evenly divide $15 = 195 - 5 \cdot 36$. So we try to find $\gcd(36, 15)$.

The Euclidean Algorithm

Since computing gcd's is very important for applications, it is fortunate that there is a fast and easily programmable way to do it.

Here is an example of finding a gcd by the *Euclidean algorithm*:

Finding $\gcd(195, 36)$. We try to divide 195 by 36. If this has no remainder we are done. But it has a remainder of 15:

$$195 = 5 \cdot 36 + 15$$

Any number that evenly divides both 195 and 36 must also evenly divide $15 = 195 - 5 \cdot 36$. So we try to find $\gcd(36, 15)$. If we divide 36 by 15:

$$36 = 2 \cdot 15 + 6$$

The Euclidean Algorithm

Since computing gcd's is very important for applications, it is fortunate that there is a fast and easily programmable way to do it.

Here is an example of finding a gcd by the *Euclidean algorithm*:

Finding $\gcd(195, 36)$. We try to divide 195 by 36. If this has no remainder we are done. But it has a remainder of 15:

$$195 = 5 \cdot 36 + 15$$

Any number that evenly divides both 195 and 36 must also evenly divide $15 = 195 - 5 \cdot 36$. So we try to find $\gcd(36, 15)$. If we divide 36 by 15:

$$36 = 2 \cdot 15 + 6$$

By the same argument, we need only find $\gcd(15, 6)$:

$$15 = 2 \cdot 6 + 3$$

The Euclidean Algorithm

Since computing gcd's is very important for applications, it is fortunate that there is a fast and easily programmable way to do it.

Here is an example of finding a gcd by the *Euclidean algorithm*:

Finding $\gcd(195, 36)$. We try to divide 195 by 36. If this has no remainder we are done. But it has a remainder of 15:

$$195 = 5 \cdot 36 + 15$$

Any number that evenly divides both 195 and 36 must also evenly divide $15 = 195 - 5 \cdot 36$. So we try to find $\gcd(36, 15)$. If we divide 36 by 15:

$$36 = 2 \cdot 15 + 6$$

By the same argument, we need only find $\gcd(15, 6)$:

$$15 = 2 \cdot 6 + 3$$

Finally, $\gcd(6, 3) = 3$ because 3 divides 6 evenly.

This tells us that
$3 = \gcd(6, 3) = \gcd(15, 6) = \gcd(36, 15) = \gcd(195, 36)$.

Here is the whole process condensed:

$$\begin{aligned} 195 &= 5 \cdot 36 + 15 \\ 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 \ \ + 3 \\ 6 &= 2 \cdot 3 \ \ + 0 \end{aligned}$$

This tells us that
$3 = \gcd(6,3) = \gcd(15,6) = \gcd(36,15) = \gcd(195,36)$.
Here is the whole process condensed:

$$
\begin{aligned}
195 &= 5 \cdot 36 + 15 \\
36 &= 2 \cdot 15 + 6 \\
15 &= 2 \cdot 6 \;\; + 3 \\
6 &= 2 \cdot 3 \;\; + 0
\end{aligned}
$$

This process for finding $\gcd(n,k)$, with $k < n$, is guaranteed to end in less than $2\log_2 n$ steps. This means it is very efficient.

This tells us that
$3 = \gcd(6, 3) = \gcd(15, 6) = \gcd(36, 15) = \gcd(195, 36)$.
Here is the whole process condensed:

$$\begin{aligned} 195 &= 5 \cdot 36 + 15 \\ 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 \;\; + 3 \\ 6 &= 2 \cdot 3 \;\; + 0 \end{aligned}$$

This process for finding $\gcd(n, k)$, with $k < n$, is guaranteed to end in less than $2\log_2 n$ steps. This means it is very efficient.

Theorem

An element k of $\mathbb{Z}_n$ is a unit if and only if $\gcd(n, k) = 1$. It is a proper zero divisor if and only if it is not zero and $\gcd(n, k) > 1$.

The second part is easy: Suppose $d > 1$ and evenly divides both n and k.

The second part is easy: Suppose $d > 1$ and evenly divides both n and k. That means there are positive integers m and j such that $n = md$ and $k = jd$. Then $km = (jd)m = jn$.

The second part is easy: Suppose $d > 1$ and evenly divides both n and k. That means there are positive integers m and j such that $n = md$ and $k = jd$. Then $km = (jd)m = jn$. That is, in the operations of the ring $\mathbb{Z}_n$ $k \cdot m = (km) \bmod n = (nj) \bmod n = 0$.

The second part is easy: Suppose $d > 1$ and evenly divides both n and k. That means there are positive integers m and j such that $n = md$ and $k = jd$. Then $km = (jd)m = jn$. That is, in the operations of the ring $\mathbb{Z}_n$ $k \cdot m = (km) \bmod n = (nj) \bmod n = 0$. Since $1 < m < n$ we see that m is a nonzero element of $\mathbb{Z}_n$ with $k \cdot m = 0$, so if k is not zero, it must be a proper zero divisor in $\mathbb{Z}_n$.

The second part is easy: Suppose $d > 1$ and evenly divides both n and k. That means there are positive integers m and j such that $n = md$ and $k = jd$. Then $km = (jd)m = jn$. That is, in the operations of the ring $\mathbb{Z}_n$ $k \cdot m = (km) \bmod n = (nj) \bmod n = 0$. Since $1 < m < n$ we see that m is a nonzero element of $\mathbb{Z}_n$ with $k \cdot m = 0$, so if k is not zero, it must be a proper zero divisor in $\mathbb{Z}_n$.

Let's illustrate the other half of the theorem. Consider finding the inverse of 7 in $\mathbb{Z}_{73}$. Lets first check that $\gcd(73, 7) = 1$:

$$\begin{aligned} 73 &= 10 \cdot 7 + 3 \\ 7 &= \ \ 2 \cdot 3 + 1 \\ 3 &= \ \ 3 \cdot 1 + 0 \end{aligned}$$

That is $\gcd(73, 7) = 1$.

There is a basic theorem in number theory that the gcd of n and k can always be written as a combination $an + bk$ with integers a and b.

There is a basic theorem in number theory that the gcd of n and k can always be written as a combination $an + bk$ with integers a and b. To see this for our example let's set $n = 73$, $k = 7$ and name the remainders $r_1 = 3$ and $r_2 = 1$. Then the set of equations is

$$\begin{aligned} n &= 10k \ + r_1 \\ k &= \ \ 2r_1 + r_2 \end{aligned}$$

There is a basic theorem in number theory that the gcd of n and k can always be written as a combination $an + bk$ with integers a and b. To see this for our example let's set $n = 73$, $k = 7$ and name the remainders $r_1 = 3$ and $r_2 = 1$. Then the set of equations is

$$\begin{aligned} n &= 10k \; + r_1 \\ k &= \; 2r_1 + r_2 \end{aligned}$$

We want to write r_2 as a combination of n and k. All we have to do is eliminate r_1 from the equations.

There is a basic theorem in number theory that the gcd of n and k can always be written as a combination $an + bk$ with integers a and b. To see this for our example let's set $n = 73$, $k = 7$ and name the remainders $r_1 = 3$ and $r_2 = 1$. Then the set of equations is

$$\begin{aligned} n &= 10k \ + r_1 \\ k &= \ \ 2r_1 + r_2 \end{aligned}$$

We want to write r_2 as a combination of n and k. All we have to do is eliminate r_1 from the equations. One way to do this is to solve the first equation for $r_1 = n - 10k$ and put this in the second equation:

$$k = 2(n - 10k) + r_2$$

There is a basic theorem in number theory that the gcd of n and k can always be written as a combination $an + bk$ with integers a and b. To see this for our example let's set $n = 73$, $k = 7$ and name the remainders $r_1 = 3$ and $r_2 = 1$. Then the set of equations is

$$\begin{aligned} n &= 10k \ + r_1 \\ k &= \ \ 2r_1 + r_2 \end{aligned}$$

We want to write r_2 as a combination of n and k. All we have to do is eliminate r_1 from the equations. One way to do this is to solve the first equation for $r_1 = n - 10k$ and put this in the second equation:

$$k = 2(n - 10k) + r_2$$

This leads to

$$k = 2n - 20k + r_2 \quad \text{or} \quad 21k - 2n = r_2$$

Since $r_2 = 1$, $k = 7$ and $n = 73$, this becomes $21(7) = 2(73) + 1$. This tells us that $21 \cdot 7 = 21(7) \bmod 73 = 1$. By definition, $7^{-1} = 21$ in $\mathbb{Z}_{73}$.

Since $r_2 = 1$, $k = 7$ and $n = 73$, this becomes $21(7) = 2(73) + 1$. This tells us that $21 \cdot 7 = 21(7) \bmod 73 = 1$. By definition, $7^{-1} = 21$ in $\mathbb{Z}_{73}$. We would check this by actually computing $21(7) = 147$, then dividing that by 73 to get a quotient of 2 and a remainder of 1.

Since $r_2 = 1$, $k = 7$ and $n = 73$, this becomes $21(7) = 2(73) + 1$. This tells us that $21 \cdot 7 = 21(7) \bmod 73 = 1$. By definition, $7^{-1} = 21$ in $\mathbb{Z}_{73}$. We would check this by actually computing $21(7) = 147$, then dividing that by 73 to get a quotient of 2 and a remainder of 1.

These types of calculation always allow one to find the inverse of an element k of $\mathbb{Z}_n$ if $\gcd(n, k) = 1$.

Since $r_2 = 1$, $k = 7$ and $n = 73$, this becomes $21(7) = 2(73) + 1$. This tells us that $21 \cdot 7 = 21(7) \bmod 73 = 1$. By definition, $7^{-1} = 21$ in $\mathbb{Z}_{73}$. We would check this by actually computing $21(7) = 147$, then dividing that by 73 to get a quotient of 2 and a remainder of 1.

These types of calculation always allow one to find the inverse of an element k of $\mathbb{Z}_n$ if $\gcd(n, k) = 1$.

Here's another example: Find the inverse of 34 in the ring $\mathbb{Z}_{371}$ (or else prove it has no inverse).

Here's the Euclidean algorithm:

$$\begin{aligned} 371 &= 10 \cdot 34 + 31 \\ 34 &= \ \ 1 \cdot 31 + 3 \\ 31 &= 10 \cdot 3 \ \ + 1 \end{aligned}$$

Since $r_2 = 1$, $k = 7$ and $n = 73$, this becomes $21(7) = 2(73) + 1$. This tells us that $21 \cdot 7 = 21(7) \bmod 73 = 1$. By definition, $7^{-1} = 21$ in $\mathbb{Z}_{73}$. We would check this by actually computing $21(7) = 147$, then dividing that by 73 to get a quotient of 2 and a remainder of 1.

These types of calculation always allow one to find the inverse of an element k of $\mathbb{Z}_n$ if $\gcd(n, k) = 1$.

Here's another example: Find the inverse of 34 in the ring $\mathbb{Z}_{371}$ (or else prove it has no inverse).

Here's the Euclidean algorithm:

$$\begin{aligned} 371 &= 10 \cdot 34 + 31 \\ 34 &= \ \ 1 \cdot 31 + 3 \\ 31 &= 10 \cdot 3 \ \ + 1 \end{aligned}$$

We can skip the division by 1 because the remainder will always be 0.

I like to write the modulus of our ring as n and the element we're testing as k, and then the remainders as r_1, r_2, etc.

I like to write the modulus of our ring as n and the element we're testing as k, and then the remainders as r_1, r_2, etc. The reason for this is to avoid multiplying the numbers together. That is, we do not want to write $371 = 340 + 31$ and lose sight of the element 34.

I like to write the modulus of our ring as n and the element we're testing as k, and then the remainders as r_1, r_2, etc. The reason for this is to avoid multiplying the numbers together. That is, we do not want to write $371 = 340 + 31$ and lose sight of the element 34. If we write this as $n = 10k + r_1$, we're not likely to lose the k. Doing that gives us

$$\begin{aligned} n &= 10k \ + r_1 \\ k &= \quad\ r_1 + r_2 \\ r_1 &= 10r_2 + r_3 \end{aligned}$$

I like to write the modulus of our ring as n and the element we're testing as k, and then the remainders as r_1, r_2, etc. The reason for this is to avoid multiplying the numbers together. That is, we do not want to write $371 = 340 + 31$ and lose sight of the element 34. If we write this as $n = 10k + r_1$, we're not likely to lose the k. Doing that gives us

$$\begin{aligned} n &= 10k \ + r_1 \\ k &= \quad\ r_1 + r_2 \\ r_1 &= 10r_2 + r_3 \end{aligned}$$

This time we need to eliminate r_1 and r_2 and leave r_3 as a combination of n and k.

I like to write the modulus of our ring as n and the element we're testing as k, and then the remainders as r_1, r_2, etc. The reason for this is to avoid multiplying the numbers together. That is, we do not want to write $371 = 340 + 31$ and lose sight of the element 34. If we write this as $n = 10k + r_1$, we're not likely to lose the k. Doing that gives us

$$\begin{aligned} n &= 10k \ + r_1 \\ k &= \quad\ r_1 + r_2 \\ r_1 &= 10r_2 + r_3 \end{aligned}$$

This time we need to eliminate r_1 and r_2 and leave r_3 as a combination of n and k. We can do this like before: put $r_1 = n - 10k$ into the second and third equations. Then use the second equation to get a formula for r_2 and put that in the third equation.

If you've had Linear Algebra you can rewrite this as

$$\begin{aligned} r_1 \qquad\qquad\qquad &= n - 10k \\ r_1 + \quad r_2 \qquad\quad &= k \\ -r_1 + 10r_2 + r_3 &= 0 \end{aligned}$$

If you've had Linear Algebra you can rewrite this as

$$\begin{aligned} r_1 \qquad\qquad\qquad &= n - 10k \\ r_1 + \quad r_2 \qquad\quad &= k \\ -r_1 + 10r_2 + r_3 &= 0 \end{aligned}$$

And then use Gaussian or Gauss-Jordan elimination.

If you've had Linear Algebra you can rewrite this as

$$\begin{aligned} r_1 \qquad\qquad\quad &= n - 10k \\ r_1 + \quad r_2 \qquad &= k \\ -r_1 + 10r_2 + r_3 &= 0 \end{aligned}$$

And then use Gaussian or Gauss-Jordan elimination. For example: subtract the first equation from the second and add it to the third:

$$\begin{aligned} r_1 \qquad\qquad\quad &= n - 10k \\ + \quad r_2 \qquad &= -n + 11k \\ + 10r_2 + r_3 &= n - 10k \end{aligned}$$

If you've had Linear Algebra you can rewrite this as

$$\begin{aligned} r_1 \quad\quad\quad\quad &= n - 10k \\ r_1 + \quad r_2 \quad\quad &= k \\ -r_1 + 10r_2 + r_3 &= 0 \end{aligned}$$

And then use Gaussian or Gauss-Jordan elimination. For example: subtract the first equation from the second and add it to the third:

$$\begin{aligned} r_1 \quad\quad\quad\quad &= n - 10k \\ + \quad r_2 \quad\quad &= -n + 11k \\ + 10r_2 + r_3 &= n - 10k \end{aligned}$$

Now subtract 10 times equation 2 from equation 3 to get

$$\begin{aligned} r_1 &= n - 10k \\ r_2 &= -n + 11k \\ r_3 &= 11n - 120k \end{aligned}$$

The last equation says that $1 = (-120)(34) + 11(371)$. This tells us that $(-120) \cdot 34 = 1$ in $\mathbb{Z}_{371}$. Thus $34^{-1} = -120 = 251$

The last equation says that $1 = (-120)(34) + 11(371)$. This tells us that $(-120) \cdot 34 = 1$ in $\mathbb{Z}_{371}$. Thus $34^{-1} = -120 = 251$

For Linear Algebra aficionados only: Use the augmented matrix

$$\left(\begin{array}{ccc|cc} r_1 & r_2 & r_3 & n & k \\ \hline 1 & 0 & 0 & 1 & -10 \\ 1 & 1 & 0 & 0 & 1 \\ -1 & 10 & 1 & 0 & 0 \end{array}\right)$$

The last equation says that $1 = (-120)(34) + 11(371)$. This tells us that $(-120) \cdot 34 = 1$ in $\mathbb{Z}_{371}$. Thus $34^{-1} = -120 = 251$

For Linear Algebra aficionados only: Use the augmented matrix

$$\left(\begin{array}{ccc|cc} r_1 & r_2 & r_3 & n & k \\ \hline 1 & 0 & 0 & 1 & -10 \\ 1 & 1 & 0 & 0 & 1 \\ -1 & 10 & 1 & 0 & 0 \end{array}\right)$$

and reduce it to echelon form

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -10 \\ 0 & 1 & 0 & -1 & 11 \\ 0 & 0 & 1 & 11 & -120 \end{array}\right)$$

The last equation says that $1 = (-120)(34) + 11(371)$. This tells us that $(-120) \cdot 34 = 1$ in $\mathbb{Z}_{371}$. Thus $34^{-1} = -120 = 251$

For Linear Algebra aficionados only: Use the augmented matrix

$$\left(\begin{array}{ccc|cc} r_1 & r_2 & r_3 & n & k \\ \hline 1 & 0 & 0 & 1 & -10 \\ 1 & 1 & 0 & 0 & 1 \\ -1 & 10 & 1 & 0 & 0 \end{array}\right)$$

and reduce it to echelon form

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -10 \\ 0 & 1 & 0 & -1 & 11 \\ 0 & 0 & 1 & 11 & -120 \end{array}\right)$$

Then read off $1 = 11n + (-120)k$.