Combinatorics Review

Daniel H. Luecking

Oct 24, 2022

You will be expected to solve two types. In the first type, some constant or expression is added to each term to produce the next term.

You will be expected to solve two types. In the first type, some constant or expression is added to each term to produce the next term. Some examples:

•
$$a_n = a_{n-1} + 7$$
, $a_0 = 4$. Solution: $a_n = 4 + 7n$.

You will be expected to solve two types. In the first type, some constant or expression is added to each term to produce the next term. Some examples:

•
$$a_n = a_{n-1} + 7$$
, $a_0 = 4$. Solution: $a_n = 4 + 7n$.

• $a_n = a_{n-1} + 3$, $a_0 = 1$. Solution: $a_n = 1 + 3n$.

You will be expected to solve two types. In the first type, some constant or expression is added to each term to produce the next term. Some examples:

•
$$a_n = a_{n-1} + 7$$
, $a_0 = 4$. Solution: $a_n = 4 + 7n$.

•
$$a_n = a_{n-1} + 3$$
, $a_0 = 1$. Solution: $a_n = 1 + 3n$.

These are called arithmetic progressions. Any recurrence relation of the form $a_n = a_{n-1} + d$, $a_0 = c$ (where d and c are constants) has the solution $a_n = c + dn$.

More generally, an expression can be added.

You will be expected to solve two types. In the first type, some constant or expression is added to each term to produce the next term. Some examples:

•
$$a_n = a_{n-1} + 7$$
, $a_0 = 4$. Solution: $a_n = 4 + 7n$.

• $a_n = a_{n-1} + 3$, $a_0 = 1$. Solution: $a_n = 1 + 3n$.

These are called arithmetic progressions. Any recurrence relation of the form $a_n = a_{n-1} + d$, $a_0 = c$ (where d and c are constants) has the solution $a_n = c + dn$.

More generally, an expression can be added.

•
$$a_n = a_{n-1} + 4n$$
, $a_0 = 3$. Solution: $a_n = 3 + 4 + 8 + \dots + 4n$, or $a_n = 3 + \sum_{k=1}^n 4k$.

You will be expected to solve two types. In the first type, some constant or expression is added to each term to produce the next term. Some examples:

•
$$a_n = a_{n-1} + 7$$
, $a_0 = 4$. Solution: $a_n = 4 + 7n$.

• $a_n = a_{n-1} + 3$, $a_0 = 1$. Solution: $a_n = 1 + 3n$.

These are called arithmetic progressions. Any recurrence relation of the form $a_n = a_{n-1} + d$, $a_0 = c$ (where d and c are constants) has the solution $a_n = c + dn$.

More generally, an expression can be added.

•
$$a_n = a_{n-1} + 4n$$
, $a_0 = 3$. Solution: $a_n = 3 + 4 + 8 + \dots + 4n$, or
 $a_n = 3 + \sum_{k=1}^n 4k$.
• $a_n = a_{n-1} + 3^{n-1}$, $a_0 = 2$. Solution:
 $a_n = 2 + 1 + 3 + 3^2 + \dots + 3^{n-1}$, or $a_n = 2 + \sum_{k=1}^n 3^{k-1}$.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \cdots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \dots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

For the second type, some constant or expression is multiplied by each term to produce the next term.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \cdots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

For the second type, some constant or expression is multiplied by each term to produce the next term. Some examples:

•
$$a_n = 3a_{n-1}$$
, $a_0 = 2$. Solution $a_n = (2)3^n$.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \dots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

For the second type, some constant or expression is multiplied by each term to produce the next term. Some examples:

•
$$a_n = 3a_{n-1}$$
, $a_0 = 2$. Solution $a_n = (2)3^n$.

•
$$a_n = 5a_{n-1}$$
, $a_0 = 4$. Solution $a_n = (4)5^n$.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \cdots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

For the second type, some constant or expression is multiplied by each term to produce the next term. Some examples:

•
$$a_n = 3a_{n-1}$$
, $a_0 = 2$. Solution $a_n = (2)3^n$

•
$$a_n = 5a_{n-1}$$
, $a_0 = 4$. Solution $a_n = (4)5^n$.

These are called geometric progressions. Any recurrence relation of the form $a_n = ra_{n-1}$, $a_0 = c$ (where r and c are constants) has the solution $a_n = c r^n$.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \dots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

For the second type, some constant or expression is multiplied by each term to produce the next term. Some examples:

•
$$a_n = 3a_{n-1}$$
, $a_0 = 2$. Solution $a_n = (2)3^n$

•
$$a_n = 5a_{n-1}$$
, $a_0 = 4$. Solution $a_n = (4)5^n$.

These are called geometric progressions. Any recurrence relation of the form $a_n = ra_{n-1}$, $a_0 = c$ (where r and c are constants) has the solution $a_n = c r^n$.

More generally, we can multiply by an expression.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \dots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

For the second type, some constant or expression is multiplied by each term to produce the next term. Some examples:

•
$$a_n = 3a_{n-1}$$
, $a_0 = 2$. Solution $a_n = (2)3^n$

•
$$a_n = 5a_{n-1}$$
, $a_0 = 4$. Solution $a_n = (4)5^n$.

These are called geometric progressions. Any recurrence relation of the form $a_n = ra_{n-1}$, $a_0 = c$ (where r and c are constants) has the solution $a_n = c r^n$.

More generally, we can multiply by an expression.

•
$$a_n = n^2 a_{n-1}$$
, $a_0 = 3$. Solution: $a_n = 3(1^2)(2^2)(3^2)\cdots(n^2)$.

If a recurrence relation has the form $a_n = a_{n-1} + f(n)$ for some expression f(n) and $a_0 = c$ is the initial condition, then the solution is $a_n = c + f(1) + f(2) + \cdots + f(n)$, or $a_n = c + \sum_{k=1}^n f(k)$.

For the second type, some constant or expression is multiplied by each term to produce the next term. Some examples:

•
$$a_n = 3a_{n-1}$$
, $a_0 = 2$. Solution $a_n = (2)3^n$

•
$$a_n = 5a_{n-1}$$
, $a_0 = 4$. Solution $a_n = (4)5^n$.

These are called geometric progressions. Any recurrence relation of the form $a_n = ra_{n-1}$, $a_0 = c$ (where r and c are constants) has the solution $a_n = c r^n$.

More generally, we can multiply by an expression.

•
$$a_n = n^2 a_{n-1}$$
, $a_0 = 3$. Solution: $a_n = 3(1^2)(2^2)(3^2)\cdots(n^2)$.

• $a_n = 4^n a_{n-1}, a_0 = 5$. Solution: $a_n = 5(4^1)(4^2)(4^3)\cdots(4^n)$.

Second order recurrence relations

Second order recurrence relations

We considered only constant coefficient linear recurrence relations. These we split into homogeneous versus nonhomogeneous:

Second order recurrence relations

We considered only constant coefficient linear recurrence relations. These we split into homogeneous versus nonhomogeneous:

• Homogeneous: $a_n + ba_{n-1} + ca_{n-2} = 0$.

Second order recurrence relations

We considered only constant coefficient linear recurrence relations. These we split into homogeneous versus nonhomogeneous:

- Homogeneous: $a_n + ba_{n-1} + ca_{n-2} = 0$.
- Nonhomogeneous: $a_n + ba_{n-1} + ca_{n-2} = f(n)$.

Second order recurrence relations

We considered only constant coefficient linear recurrence relations. These we split into homogeneous versus nonhomogeneous:

- Homogeneous: $a_n + ba_{n-1} + ca_{n-2} = 0$.
- Nonhomogeneous: $a_n + ba_{n-1} + ca_{n-2} = f(n)$.

We solve the homogeneous case by first solving the characteristic equation: $r^2 + br + c = 0$. What we do next depends on what the roots are.

An example is $a_n - a_{n-1} - 6a_{n-2} = 0$, $a_0 = 0$, $a_1 = 1$.

An example is $a_n - a_{n-1} - 6a_{n-2} = 0$, $a_0 = 0$, $a_1 = 1$.

The characteristic equation is $r^2 - r - 6 = 0$ or (r - 3)(r + 2) = 0.

An example is $a_n - a_{n-1} - 6a_{n-2} = 0$, $a_0 = 0$, $a_1 = 1$.

The characteristic equation is $r^2 - r - 6 = 0$ or (r - 3)(r + 2) = 0.

The solutions are r = 3 and r = -2. These give basic solutions 3^n and $(-2)^n$.

An example is $a_n - a_{n-1} - 6a_{n-2} = 0$, $a_0 = 0$, $a_1 = 1$.

The characteristic equation is $r^2 - r - 6 = 0$ or (r - 3)(r + 2) = 0.

The solutions are r = 3 and r = -2. These give basic solutions 3^n and $(-2)^n$.

The general solution is $a_n = C_1 3^n + C_2 (-2)^n$.

An example is $a_n - a_{n-1} - 6a_{n-2} = 0$, $a_0 = 0$, $a_1 = 1$.

The characteristic equation is $r^2 - r - 6 = 0$ or (r - 3)(r + 2) = 0.

The solutions are r = 3 and r = -2. These give basic solutions 3^n and $(-2)^n$.

The general solution is $a_n = C_1 3^n + C_2 (-2)^n$.

The initial conditions can be written:

$$a_0 = 0 = C_1 + C_2$$
 and $a_1 = 1 = 3C_1 - 2C_2$

An example is $a_n - a_{n-1} - 6a_{n-2} = 0$, $a_0 = 0$, $a_1 = 1$.

The characteristic equation is $r^2 - r - 6 = 0$ or (r - 3)(r + 2) = 0.

The solutions are r = 3 and r = -2. These give basic solutions 3^n and $(-2)^n$.

The general solution is $a_n = C_1 3^n + C_2 (-2)^n$.

The initial conditions can be written:

$$a_0 = 0 = C_1 + C_2$$
 and $a_1 = 1 = 3C_1 - 2C_2$

Solving these gives $C_1 = 1/5$ and $C_2 = -1/5$, and the completed solution is

$$a_n = (1/5)3^n - (1/5)(-2)^n.$$

An example is $a_n - 10a_{n-1} + 25a_{n-2} = 0$, $a_0 = 1$, $a_1 = 7$.

An example is $a_n - 10a_{n-1} + 25a_{n-2} = 0$, $a_0 = 1$, $a_1 = 7$.

The characteristic equation is $r^2 - 10r + 25 = 0$ or (r - 5)(r - 5) = 0.

An example is $a_n - 10a_{n-1} + 25a_{n-2} = 0$, $a_0 = 1$, $a_1 = 7$.

The characteristic equation is $r^2 - 10r + 25 = 0$ or (r - 5)(r - 5) = 0.

The solutions are r = 5 and r = 5. These give basic solutions 5^n and $n5^n$.

An example is $a_n - 10a_{n-1} + 25a_{n-2} = 0$, $a_0 = 1$, $a_1 = 7$.

The characteristic equation is $r^2 - 10r + 25 = 0$ or (r - 5)(r - 5) = 0.

The solutions are r = 5 and r = 5. These give basic solutions 5^n and $n5^n$. The general solution is $a_n = C_1 5^n + C_2 n5^n$.

An example is $a_n - 10a_{n-1} + 25a_{n-2} = 0$, $a_0 = 1$, $a_1 = 7$.

The characteristic equation is $r^2 - 10r + 25 = 0$ or (r - 5)(r - 5) = 0.

The solutions are r = 5 and r = 5. These give basic solutions 5^n and $n5^n$. The general solution is $a_n = C_1 5^n + C_2 n5^n$.

The initial conditions can be written:

$$a_0 = 1 = C_1$$
 and $a_1 = 7 = 5C_1 + 5C_2$

An example is $a_n - 10a_{n-1} + 25a_{n-2} = 0$, $a_0 = 1$, $a_1 = 7$.

The characteristic equation is $r^2 - 10r + 25 = 0$ or (r - 5)(r - 5) = 0.

The solutions are r = 5 and r = 5. These give basic solutions 5^n and $n5^n$. The general solution is $a_n = C_1 5^n + C_2 n5^n$.

The initial conditions can be written:

$$a_0 = 1 = C_1$$
 and $a_1 = 7 = 5C_1 + 5C_2$

Solving these gives $C_1 = 1$ and $C_2 = 2/5$, and the completed solution is

$$a_n = 5^n + (2/5)n5^n.$$

Case 3: there are two complex roots

An example is $a_n - 6a_{n-1} + 10a_{n-2} = 0$, $a_0 = 2$, $a_1 = 4$.

An example is $a_n - 6a_{n-1} + 10a_{n-2} = 0$, $a_0 = 2$, $a_1 = 4$. The characteristic equation is $r^2 - 6r + 10 = 0$.

An example is $a_n - 6a_{n-1} + 10a_{n-2} = 0$, $a_0 = 2$, $a_1 = 4$.

The characteristic equation is $r^2 - 6r + 10 = 0$.

The solutions are r = 3 + i and r = 3 - i. These give basic solutions $(3 + i)^n$ and $(3 - i)^n$.

An example is $a_n - 6a_{n-1} + 10a_{n-2} = 0$, $a_0 = 2$, $a_1 = 4$.

The characteristic equation is $r^2 - 6r + 10 = 0$.

The solutions are r = 3 + i and r = 3 - i. These give basic solutions $(3 + i)^n$ and $(3 - i)^n$.

The general solution is $a_n = C_1(3+i)^n + C_2(3-i)^n$.

An example is $a_n - 6a_{n-1} + 10a_{n-2} = 0$, $a_0 = 2$, $a_1 = 4$. The characteristic equation is $r^2 - 6r + 10 = 0$.

The solutions are r = 3 + i and r = 3 - i. These give basic solutions $(3 + i)^n$ and $(3 - i)^n$.

The general solution is $a_n = C_1(3+i)^n + C_2(3-i)^n$.

The initial conditions can be written:

$$a_0 = 2 = C_1 + C_2 \quad \text{and} \quad a_1 = 4 = (3+i)C_1 + (3-i)C_2$$

An example is $a_n - 6a_{n-1} + 10a_{n-2} = 0$, $a_0 = 2$, $a_1 = 4$. The characteristic equation is $r^2 - 6r + 10 = 0$.

The solutions are r = 3 + i and r = 3 - i. These give basic solutions $(3 + i)^n$ and $(3 - i)^n$.

The general solution is $a_n = C_1(3+i)^n + C_2(3-i)^n$.

The initial conditions can be written:

$$a_0 = 2 = C_1 + C_2 \quad \text{and} \quad a_1 = 4 = (3+i)C_1 + (3-i)C_2$$

Solving these gives $C_1 = 1 + i$ and $C_2 = 1 - i$, and the completed solution is

$$a_n = (1+i)(3+i)^n + (1-i)(3-i)^n.$$

Our method consists of (1) solving the corresponding homogeneous recurrence relation,

Our method consists of (1) solving the corresponding homogeneous recurrence relation, (2) finding a particular solution,

Our method consists of (1) solving the corresponding homogeneous recurrence relation, (2) finding a particular solution, (3) adding the two together,

Our method consists of (1) solving the corresponding homogeneous recurrence relation, (2) finding a particular solution, (3) adding the two together, and (4) applying the initial conditions.

Our method consists of (1) solving the corresponding homogeneous recurrence relation, (2) finding a particular solution, (3) adding the two together, and (4) applying the initial conditions.

We've already covered (1), while (3) and (4) are straightforward, so we'll concentrate on (2).

Our method consists of (1) solving the corresponding homogeneous recurrence relation, (2) finding a particular solution, (3) adding the two together, and (4) applying the initial conditions.

We've already covered (1), while (3) and (4) are straightforward, so we'll concentrate on (2).

If the right side is a polynomial, possibly times an nth power, then we expect there is a particular solution that is a polynomial of the same degree times the same nth power.

Our method consists of (1) solving the corresponding homogeneous recurrence relation, (2) finding a particular solution, (3) adding the two together, and (4) applying the initial conditions.

We've already covered (1), while (3) and (4) are straightforward, so we'll concentrate on (2).

If the right side is a polynomial, possibly times an nth power, then we expect there is a particular solution that is a polynomial of the same degree times the same nth power.

An example: $a_n - a_{n-1} - 6a_{n-2} = (4)2^n$, $a_0 = 1$, $a_1 = 2$.

$$a_n^{(h)} = C_1 3^n + C_2 (-2)^n.$$

$$a_n^{(h)} = C_1 3^n + C_2 (-2)^n.$$

Then we decide what a particular solution might look like.

$$a_n^{(h)} = C_1 3^n + C_2 (-2)^n.$$

Then we decide what a particular solution might look like. Since the right side is a constant times 2^n , we suppose one solution might be a constant times 2^n

$$a_n^{(h)} = C_1 3^n + C_2 (-2)^n.$$

Then we decide what a particular solution might look like. Since the right side is a constant times 2^n , we suppose one solution might be a constant times 2^n and so we put $a_n = A2^n$ into the recurrence relation and see what A will have to be:

$$A2^{n} - A2^{n-1} - 6A2^{n-2} = (4)2^{n} \implies -A = 4 \implies A = -4.$$

$$a_n^{(h)} = C_1 3^n + C_2 (-2)^n.$$

Then we decide what a particular solution might look like. Since the right side is a constant times 2^n , we suppose one solution might be a constant times 2^n and so we put $a_n = A2^n$ into the recurrence relation and see what A will have to be:

$$A2^{n} - A2^{n-1} - 6A2^{n-2} = (4)2^{n} \implies -A = 4 \implies A = -4.$$

This gives us the particular solution:

$$a_n^{(p)} = -(4)2^n.$$

The general solution is then $a_n = a_n^{(h)} + a_n^{(p)} = C_1 3^n + C_2 (-2)^n - (4) 2^n$.

$$a_0 = 1 = C_1 + C_2 - 4$$
 and $a_1 = 2 = 3C_1 - 2C_2 - 8$

$$a_0 = 1 = C_1 + C_2 - 4$$
 and $a_1 = 2 = 3C_1 - 2C_2 - 8$

This has solutions $C_1 = 4$ and $C_2 = 1$ for a completed solution:

$$a_n = (4)3^n + (-2)^n - (4)2^n.$$

$$a_0 = 1 = C_1 + C_2 - 4$$
 and $a_1 = 2 = 3C_1 - 2C_2 - 8$

This has solutions $C_1 = 4$ and $C_2 = 1$ for a completed solution:

$$a_n = (4)3^n + (-2)^n - (4)2^n.$$

A snag in the method

$$a_0 = 1 = C_1 + C_2 - 4$$
 and $a_1 = 2 = 3C_1 - 2C_2 - 8$

This has solutions $C_1 = 4$ and $C_2 = 1$ for a completed solution:

$$a_n = (4)3^n + (-2)^n - (4)2^n.$$

A snag in the method

Consider the recurrence relation $a_n - a_{n-1} - 2a_{n-2} = (3)2^n$, $a_0 = 0$, $a_1 = 1$.

$$a_0 = 1 = C_1 + C_2 - 4$$
 and $a_1 = 2 = 3C_1 - 2C_2 - 8$

This has solutions $C_1 = 4$ and $C_2 = 1$ for a completed solution:

$$a_n = (4)3^n + (-2)^n - (4)2^n.$$

A snag in the method

Consider the recurrence relation $a_n - a_{n-1} - 2a_{n-2} = (3)2^n$, $a_0 = 0$, $a_1 = 1$. If we tried the same particular solution: $a_n = A2^n$ the same process would give us 0A = 3, which is impossible for any A.

$$a_n^{(h)} = C_1 2^n + C_2 (-1)^n$$

shows that $A2^n$ is a solution of the homogeneous equation and so will always produce 0 and never $(3)2^n$.

$$a_n^{(h)} = C_1 2^n + C_2 (-1)^n$$

shows that $A2^n$ is a solution of the homogeneous equation and so will always produce 0 and never $(3)2^n$. In cases like this we multiply the proposed solution $A2^n$ by n and try $a_n = An2^n$.

$$a_n^{(h)} = C_1 2^n + C_2 (-1)^n$$

shows that $A2^n$ is a solution of the homogeneous equation and so will always produce 0 and never $(3)2^n$. In cases like this we multiply the proposed solution $A2^n$ by n and try $a_n = An2^n$.

Putting this in the recurrence relation gives

$$An2^{n} - A(n-1)2^{n-1} - 2A(n-2)2^{n-2} = (3)2^{n} \implies (3/2)A = 3$$

$$a_n^{(h)} = C_1 2^n + C_2 (-1)^n$$

shows that $A2^n$ is a solution of the homogeneous equation and so will always produce 0 and never $(3)2^n$. In cases like this we multiply the proposed solution $A2^n$ by n and try $a_n = An2^n$.

Putting this in the recurrence relation gives

$$An2^{n} - A(n-1)2^{n-1} - 2A(n-2)2^{n-2} = (3)2^{n} \implies (3/2)A = 3$$

This yelds A = 2 and so, $a_n^{(p)} = 2n2^n$. Then, the general solution is

$$a_n = C_1 2^n + C_2 (-1)^n + 2n2^n.$$

$$a_n^{(h)} = C_1 2^n + C_2 (-1)^n$$

shows that $A2^n$ is a solution of the homogeneous equation and so will always produce 0 and never $(3)2^n$. In cases like this we multiply the proposed solution $A2^n$ by n and try $a_n = An2^n$.

Putting this in the recurrence relation gives

$$An2^{n} - A(n-1)2^{n-1} - 2A(n-2)2^{n-2} = (3)2^{n} \implies (3/2)A = 3$$

This yelds A = 2 and so, $a_n^{(p)} = 2n2^n$. Then, the general solution is

$$a_n = C_1 2^n + C_2 (-1)^n + 2n2^n.$$

Applying the initial conditions to this:

$$a_0 = 0 = C_1 + C_2 + 0$$
 and $a_1 = 1 = 2C_1 - C_2 + 4$

we get $C_1 = -1$ and $C_2 = 1$ for a complete solution:

$$a_n = -2^n + (-1)^n + 2n2^n.$$

Computations in \mathbb{Z}_n

 \mathbb{Z}_n is the set $\{0, 1, \ldots, n-1\}$. We make it a ring by giving it two operations we call addition + and multiplication \cdot , defined as follows.

$$m+k = (m+k \bmod n)$$
 and $m \cdot k = (mk \bmod n)$

For example, in \mathbb{Z}_6 we have the following operation tables:

+	0	1	2	3	4	5		•	0	1	2	3	4	5
					4		-					0		
1	1	2	3	4	5	0		1	0	1	2	3	4	5
2	2	3	4	5	0	1		2	0	2	4	0	2	4
3	3	4	5	0	1	2		3	0	3	0	3	0	3
					2			4	0	4	2	0	4	2
5	5	0	1	2	3	4		5	0	5	4	3	2	1

If an element u in a ring R satisfies $u \cdot x = x \cdot u = x$ for all elements x in R, then u is called a *unity* and we say R is a ring *with unity*.

If an element u in a ring R satisfies $u \cdot x = x \cdot u = x$ for all elements x in R, then u is called a *unity* and we say R is a ring *with unity*. All \mathbb{Z}_n are rings with unity and 1 is the unity.

If an element u in a ring R satisfies $u \cdot x = x \cdot u = x$ for all elements x in R, then u is called a *unity* and we say R is a ring *with unity*. All \mathbb{Z}_n are rings with unity and 1 is the unity.

For a ring R with unity u, an element x is called a *unit* if there is an element y in R that satisfies $x \cdot y = y \cdot x = u$.

If an element u in a ring R satisfies $u \cdot x = x \cdot u = x$ for all elements x in R, then u is called a *unity* and we say R is a ring *with unity*. All \mathbb{Z}_n are rings with unity and 1 is the unity.

For a ring R with unity u, an element x is called a *unit* if there is an element y in R that satisfies $x \cdot y = y \cdot x = u$. We call y the *inverse of* x and denote it by x^{-1} .

In any ring -x is that element which when added to x produces 0. In \mathbb{Z}_6 , $2+4 = (6 \mod 6) = 0$ so -2 = 4. Similarly -5 = 1 and -3 = 3.

If an element u in a ring R satisfies $u \cdot x = x \cdot u = x$ for all elements x in R, then u is called a *unity* and we say R is a ring *with unity*. All \mathbb{Z}_n are rings with unity and 1 is the unity.

For a ring R with unity u, an element x is called a *unit* if there is an element y in R that satisfies $x \cdot y = y \cdot x = u$. We call y the *inverse of* x and denote it by x^{-1} .

In \mathbb{Z}_6 only the elements 1 and 5 are units with $1^{-1} = 1$ and $5^{-1} = 5$.

In any ring -x is that element which when added to x produces 0. In \mathbb{Z}_6 , $2+4 = (6 \mod 6) = 0$ so -2 = 4. Similarly -5 = 1 and -3 = 3.

If an element u in a ring R satisfies $u \cdot x = x \cdot u = x$ for all elements x in R, then u is called a *unity* and we say R is a ring *with unity*. All \mathbb{Z}_n are rings with unity and 1 is the unity.

For a ring R with unity u, an element x is called a *unit* if there is an element y in R that satisfies $x \cdot y = y \cdot x = u$. We call y the *inverse of* x and denote it by x^{-1} .

In \mathbb{Z}_6 only the elements 1 and 5 are units with $1^{-1} = 1$ and $5^{-1} = 5$. In \mathbb{Z}_7 , all the elements except 0 are units and

$$1^{-1} = 1, \quad 2^{-1} = 4, \quad 3^{-1} = 5, \quad 4^{-1} = 2, \quad 5^{-1} = 3, \quad 6^{-1} = 6.$$

You will be expected to do any computations in any of the rings \mathbb{Z}_n .

 $7+13+4\cdot 11 = 1+6 = 7$, or $4\cdot 7\cdot 3 = 9\cdot 3 = 8$, or -7 = 12, or $4^{-1} = 5$.

 $7+13+4\cdot 11 = 1+6 = 7$, or $4\cdot 7\cdot 3 = 9\cdot 3 = 8$, or -7 = 12, or $4^{-1} = 5$.

We know that an element k of \mathbb{Z}_n is a proper zero divisor if it is not 0 and $\gcd(n,k)>1.$

 $7+13+4\cdot 11 = 1+6 = 7$, or $4\cdot 7\cdot 3 = 9\cdot 3 = 8$, or -7 = 12, or $4^{-1} = 5$.

We know that an element k of \mathbb{Z}_n is a proper zero divisor if it is not 0 and gcd(n,k) > 1. That is, there is an integer larger than 1 that evenly divides both k and n.

 $7+13+4\cdot 11 = 1+6 = 7$, or $4\cdot 7\cdot 3 = 9\cdot 3 = 8$, or -7 = 12, or $4^{-1} = 5$.

We know that an element k of \mathbb{Z}_n is a proper zero divisor if it is not 0 and gcd(n,k) > 1. That is, there is an integer larger than 1 that evenly divides both k and n. All other elements, those that satisfy gcd(n,k) = 1, are units.

 $7+13+4\cdot 11 = 1+6 = 7$, or $4\cdot 7\cdot 3 = 9\cdot 3 = 8$, or -7 = 12, or $4^{-1} = 5$.

We know that an element k of \mathbb{Z}_n is a proper zero divisor if it is not 0 and gcd(n,k) > 1. That is, there is an integer larger than 1 that evenly divides both k and n. All other elements, those that satisfy gcd(n,k) = 1, are units.

For example, in \mathbb{Z}_{12} the proper zero divisors are 2, 3, 4, 6, 8, 9, 10 and the units are 1, 5, 7, 11. Notice that 0 is not in either list.

 $7+13+4\cdot 11 = 1+6 = 7$, or $4\cdot 7\cdot 3 = 9\cdot 3 = 8$, or -7 = 12, or $4^{-1} = 5$.

We know that an element k of \mathbb{Z}_n is a proper zero divisor if it is not 0 and gcd(n,k) > 1. That is, there is an integer larger than 1 that evenly divides both k and n. All other elements, those that satisfy gcd(n,k) = 1, are units.

For example, in \mathbb{Z}_{12} the proper zero divisors are 2, 3, 4, 6, 8, 9, 10 and the units are 1, 5, 7, 11. Notice that 0 is not in either list. You will be expected to be able to list these for any not-too-large \mathbb{Z}_n .

We have a formula for the number of units in \mathbb{Z}_n , if n can be completely factored into primes.

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

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

continuing through all the *different*, *prime* divisors p_1, p_2, \ldots of n.

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

continuing through all the *different*, *prime* divisors p_1, p_2, \ldots of n. For example, because $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$, the number of units in \mathbb{Z}_{2100} is

$$\phi(2100) = 2100 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) = \frac{(2100)(1)(2)(4)(6)}{(2)(3)(5)(7)} = 480$$

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

continuing through all the *different*, *prime* divisors p_1, p_2, \ldots of n. For example, because $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$, the number of units in \mathbb{Z}_{2100} is

$$\phi(2100) = 2100 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) = \frac{(2100)(1)(2)(4)(6)}{(2)(3)(5)(7)} = 480$$

The number of proper zero divisors is one less than everything else (because 0 is neither a unit nor a proper zero divisor). That is, $n - \phi(n) - 1$.

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

continuing through all the *different*, *prime* divisors p_1, p_2, \ldots of n. For example, because $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$, the number of units in \mathbb{Z}_{2100} is

$$\phi(2100) = 2100 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) = \frac{(2100)(1)(2)(4)(6)}{(2)(3)(5)(7)} = 480$$

The number of proper zero divisors is one less than everything else (because 0 is neither a unit nor a proper zero divisor). That is, $n - \phi(n) - 1$.

For \mathbb{Z}_{2100} there are 2100 - 480 - 1 = 1619 proper zero divisors.

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

continuing through all the *different*, *prime* divisors p_1, p_2, \ldots of n. For example, because $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$, the number of units in \mathbb{Z}_{2100} is

$$\phi(2100) = 2100 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) = \frac{(2100)(1)(2)(4)(6)}{(2)(3)(5)(7)} = 480$$

The number of proper zero divisors is one less than everything else (because 0 is neither a unit nor a proper zero divisor). That is, $n - \phi(n) - 1$.

For \mathbb{Z}_{2100} there are 2100 - 480 - 1 = 1619 proper zero divisors. You will be expected to do this for any \mathbb{Z}_n if I give you the factorization of n.

For example, find 101^{-1} in the ring \mathbb{Z}_{409} .

For example, find 101^{-1} in the ring \mathbb{Z}_{409} . The Euclidean algorithm gives

$$\begin{cases} 409 = 4(101) + 5\\ 101 = 20(5) + 1 \end{cases} \quad \text{or} \quad \begin{cases} n = 4k + r_1\\ k = 20r_1 + r_2 \end{cases}$$

where n = 409, k = 101, $r_1 = 5$ and $r_2 = 1$.

For example, find 101^{-1} in the ring \mathbb{Z}_{409} . The Euclidean algorithm gives

$$\begin{cases} 409 = 4(101) + 5\\ 101 = 20(5) + 1 \end{cases} \quad \text{or} \quad \begin{cases} n = 4k + r_1\\ k = 20r_1 + r_2 \end{cases}$$

where n = 409, k = 101, $r_1 = 5$ and $r_2 = 1$. Using $r_1 = n - 4k$ from the top equation in the bottom equation:

$$k = 20(n - 4k) + r_2$$

$$k = 20n - 80k + r_2.$$

For example, find 101^{-1} in the ring \mathbb{Z}_{409} . The Euclidean algorithm gives

$$\begin{cases} 409 = 4(101) + 5\\ 101 = 20(5) + 1 \end{cases} \quad \text{or} \quad \begin{cases} n = 4k + r_1\\ k = 20r_1 + r_2 \end{cases}$$

where n = 409, k = 101, $r_1 = 5$ and $r_2 = 1$. Using $r_1 = n - 4k$ from the top equation in the bottom equation:

$$k = 20(n - 4k) + r_2$$

$$k = 20n - 80k + r_2.$$

Solving for r_2 : $r_2 = 81k - 20n$.

For example, find 101^{-1} in the ring \mathbb{Z}_{409} . The Euclidean algorithm gives

$$\begin{cases} 409 = 4(101) + 5\\ 101 = 20(5) + 1 \end{cases} \quad \text{or} \quad \begin{cases} n = 4k + r_1\\ k = 20r_1 + r_2 \end{cases}$$

where n = 409, k = 101, $r_1 = 5$ and $r_2 = 1$. Using $r_1 = n - 4k$ from the top equation in the bottom equation:

$$k = 20(n - 4k) + r_2$$

$$k = 20n - 80k + r_2.$$

Solving for r_2 : $r_2 = 81k - 20n$. Putting the actual values back: 1 = 81(101) - 20(409). This tells us that, in the ring \mathbb{Z}_{409} , $1 = 81 \cdot 101$ and so $(101)^{-1} = 81$.