Inductive Proofs

R To see if a property P holds of the elements of a finite set, one may, if the set is small, check the elements one by one. This is possible in principle even if the set is a large finite set. But if the set is infinite, then this is not possible at all. Therefore, we have to devise other methods of proof. If the set, in question, is the set of natural numbers, then the principle of mathematical induction gives us precisely such a method of proof.

The points to note that the natural numbers start at 0 and that each natural number has an immediate successor. Thus, if some property P holds of 0 and, if it is the case that, if the property P holds of $0, 1, 2, \ldots, n$, then P holds of the successor $n + 1$, then P holds of every natural number. Note that if P holds at 0, then by the principle of induction P holds at 1, if P holds at 0 and 1, then by the principle of induction P holds at 2, if P holds at 0, 1 and 2, then by the principle of induction P holds at 3, and so on.

The principle of induction is intimately connected with the idea of recursive definitions. Recursive definitions specify a family of objects indexed (for the moment) on the natural numbers where the $(n + 1)^{st}$ object of the family is determined by the members of the family from 0 to n. To prove that each member of such recursively defined families of objects have certain properties we use the method of induction. An efficient way to learn this material is to look at the examples and also to work out exercises.

We shall be concerned with the following three considerations:

Q Formulate a conjecture for the n^{th} term of a recursively defined sequence σ.

Q Formulate a conjecture for the sum $Sm(\sigma, n)$ of first n terms of a recursively defined sequence σ.

Q Prove that such conjectures are true using the method of induction.

T Principle of mathematical induction

$$\forall P \in \mathcal{P}(\mathbb{N}) \left(\frac{P(0) \quad \left(\frac{P(0) \quad P(1) \quad \cdots \quad P(n)}{P(n+1)}\right)}{\forall n \in \mathbb{N} \left(P(n) \right)} \right)$$

Recursive definitions

D Functions $\rho: \mathbb{N} \longrightarrow \mathbb{N}$ may be defined by recursion as folows:

Base Case(s)

(BC) (0) $\rho(0) \coloneqq r_0$

(1) $\rho(1) \coloneqq r_1$

(2) $\rho(2) \coloneqq r_2$

$\vdots$ $\vdots$

(b) $\rho(p) \coloneqq r_p$

Recursive Step

(RcS) $\forall n \in \mathbb{N}$ $\rho(p+n+1) \coloneqq \Phi\big((r_0, r_1, r_2, \cdots, r_B), n\big)$

R The following situation will concern us often:

There are two recursively defined functions $\varphi, \psi \in RcsFnc\left(\mathbb{N}, \mathbb{N}\right)$

and $\forall n \in \mathbb{N} \left(P(n) \coloneqq \left((\varphi(n)) R (\psi(n)) \right) \right)$, where $R \in \left\{ =, \ <, \ \leq, \ >, \ \geq \right\}$

R Properties of recursively defined functions are established by induction as follows:

R Suppose we want to prove that a function $\rho\colon \mathbb{N} \longrightarrow \mathbb{N}$ defined by recursion has a certain property P, that is, $P(\rho)$ is true.

T $$\forall P \in \mathcal{P}\big(Fnc(\mathbb{N},\mathbb{N})\big) \quad \left(\frac{\big(P(\rho)\big)(0) \quad \left(\frac{\big(P(\rho)\big)(0) \quad \big(P(\rho)\big)(1) \quad \cdots \quad \big(P(\rho)\big)(n)}{\big(P(\rho)\big)(n+1)}\right)}{\forall n{\in}\mathbb{N}\left(\Big(\big(P(\rho)\big)(n)\Big)\right)}\right)$$

E The example below illustrates how a recursive function may be used. We recall the recursive definition of the factorial function.

D The factorial function φ, is defined recursively as follows:

BC		$\varphi(0) \coloneqq 1$
RcS	$\forall n \in \mathbb{N}$	$\varphi(n+1) \coloneqq (n+1)\varphi(n)$

R Note that: $\forall n \in \mathbb{N}$, $\varphi(n) = n! \coloneqq \prod_{k\in 1..n} k$, but we are not using the notation $n!$ to conform to the conventions in this section.

To calculate $\varphi(1)$, we may use the recursive definition and proceed as follows. We shall repeatedly use Euclid's rule, namely: **equals substituted into equals yield equals**.

The first task is to match $\varphi(1)$ to the left or the right side of one of the defining equaitons. We shall show the match explicitly.

$$\varphi(1) = \varphi(0+1) = \Big(\varphi(n+1)\Big)\Big\langle n \quad \leftarrow \quad 0\Big\rangle$$

The above means that $\varphi(1)$ may be obtained by substituting 0 in the place of n in the expression $\Big(\varphi(n+1)\Big)$. Since $\varphi(n+1)$ is equal by definition to $(n+1)\varphi(n)$, we may, using Euclid's rule, substitute

0 in the expression $(n+1)\varphi(n)$ to obtain a new value $\varphi(n+1)$. This will reduce the argument of φ to 0 and this is to be used repeatedly to compute $\varphi(n)$. We record the process as follows.

$$
\begin{aligned}
& \varphi(1) \\
= \quad & \varphi(0+1) \\
= \quad & \left(\varphi(n+1)\right)\left\langle n \quad \leftarrow \; 0\right\rangle \\
= \quad & \left((n+1)\varphi(n)\right)\left\langle n \quad \leftarrow \; 0\right\rangle \\
= \quad & (0+1)\varphi(0) \\
= \quad & (1)1 && \left(\because \varphi(0) \coloneqq 1\right) \\
= \quad & 1
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
& \varphi(2) \\
= \quad & \varphi(1+1) \\
= \quad & \left(\varphi(n+1)\right)\left\langle n \quad \leftarrow \; 1\right\rangle \\
= \quad & \left((n+1)\varphi(n)\right)\left\langle n \quad \leftarrow \; 1\right\rangle \\
= \quad & (1+1)\varphi(1) \\
= \quad & (2)1 && \left(\because \varphi(1) \coloneqq 1\right) \\
= \quad & 2! \\
= \quad & 2
\end{aligned}
$$

Similarly, $\varphi(3)$

$$
\begin{aligned}
&= \varphi(2+1) \\
&= \Big(\varphi(n+1)\Big)\Big\langle n \quad \longleftarrow \; 2\Big\rangle \\
&= \Big((n+1)\varphi(n)\Big)\Big\langle n \quad \longleftarrow \; 2\Big\rangle \\
&= (2+1)\varphi(2) \\
&= (3)(2)1 && \Big(\because \varphi(2) \coloneqq (2)1\Big) \\
&= 3! \\
&= 6
\end{aligned}
$$

R This process of repeatedly 'running backwards' justifies the name recursion.

R The recursive scheme should be understood by reading the definition in words. There is a function $\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}$ whose output at the input 0 is 1, and to calculate its output at the input $n+1$, we need to multiply the current input, namely $n+1$, by the output at the immediately preceding number, namely, $\varphi(n)$.

E As a second example we consider the Fibonacci numbers which are defined recursively as follows.

$$
\begin{aligned}
&& \rho(0) &\coloneqq 0 \\
&& \rho(1) &\coloneqq 1 \\
\forall n \in \mathbb{N} && \rho(n+2) &\coloneqq \rho(n+1) + \rho(n)
\end{aligned}
$$

R The recursive scheme should be understood by reading the definition in words. There is a function $\rho\colon \mathbb{N} \longrightarrow \mathbb{N}$ whose output at the input 0 is 1 and at input 1 is 1. To calculate its output at the input $n+2$, we need to add the outputs at the two immediately preceding inputs, namely, $\rho(n+1)$ and $\rho(n)$.

We can record our calculation for $\rho(2)$ following the same bookkeeping scheme as before.

$$\begin{aligned}
& \rho(2) \\
= \quad & \rho(0+2) \\
= \quad & \Big(\rho(n+2)\Big)\Big\langle n \quad \leftarrow 0 \Big\rangle \\
= \quad & \Big(\rho(n+1)+\rho(n)\Big)\Big\langle n \quad \leftarrow 0 \Big\rangle \\
= \quad & \rho(0+1)+\rho(0) \\
= \quad & \rho(0+1)+\rho(0) \qquad\qquad \Big(\because \rho(0) \coloneqq 0, \rho(1) \coloneqq 1\Big) \\
= \quad & \rho(1)+\rho(0) \\
= \quad & 1+0 \\
= \quad & 1
\end{aligned}$$

Even without doing the calculation, one can immediately see that $\rho(3)=\rho(2)+\rho(1)=1+1$=2

Q Compute $\rho(10)$ recursively as shown earlier, by looking at the first 9 outputs, and also using a formula that you need to find.

Q $\exists n \in \mathbb{N}\Big(\rho(n)=123456789\Big) \qquad Y \qquad N \qquad Pf \qquad W$

Q Try to understand the following recursive scheme for the function $\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}$ by interpreting its meaning in a manner analogous to the one used for Fibonacci numbers. Then calculate the value of $\varphi(2), \varphi(3), \varphi(4)$, and $\varphi(5)$. Find a general formula for $\varphi(n)$.

$$\varphi(0) \coloneqq 1$$
$$\varphi(1) \coloneqq 2$$
$$\forall n \in \mathbb{N} \qquad \varphi(n+2) \coloneqq \left(\varphi(n+1)\right)\left(\varphi(n)\right)$$

Sequences

D A sequence σ of real numbers is defined to be a map

$$\sigma := n \longmapsto \sigma(n) : \mathbb{N} \longrightarrow \mathbb{R}$$

R $\sigma(n)$ is called the n^{th} term of the sequence.

R The sequence is better formalized as a family indexed on $\mathbb{N}$, a notion that does not require the specification of a target: $Tgt(\sigma)$; hence one also uses the notations below:

$$\sigma = (\sigma_n | n \in \mathbb{N}) = (\sigma(n) | n \in \mathbb{N})$$

in which one denotes $\sigma(n)$ by σ_n , that is: $\sigma_n := \sigma(n)$.

D Sums of initial segments of a sequence $(\sigma(n)|n \in \mathbb{N})$ is defined recursively as follows:

BC $\quad Sm(\sigma, 0) \quad := \quad \sum_{k=0}^{0} \sigma(k) \quad := \sigma(0)$

RcS $\quad \forall n \in \mathbb{N} \quad Sm(\sigma, n+1) := \quad Sm(\sigma, n) + \sigma(n+1)$

or equivalently,

$$\sum_{k=0}^{n+1} \sigma(k) \quad := \quad \sum_{k=0}^{n} \sigma(k) + \sigma(n+1)$$

E Find a recursive definition of the family $\left(n \middle| n \in \mathbb{N} \right)$.

Note that the terms of the sequence are: $0,1,2,3,\dots,n,n+1,\dots$. Each term is obtained by adding 1 to the previous one. Using this observation, we may define the the sequence recursively as follows:

BC $\quad \alpha(0) := 0$

RcS $\quad \forall n \in \mathbb{N} \quad \alpha(n+1) := \big(\alpha(n)\big) + 1$

E Find a recursive definition of the family $\left(2^n \middle| n \in \mathbb{N} \right)$.

Note that the terms of the sequence are: $2^0, 2^1, 2^2, 2^3, \dots, 2^n, 2^{n+1}, \dots$. Each term is obtained by multiplying the previous one by 2. Using this observation, we may define the the sequence recursively as follows:

BC $\qquad\qquad\qquad\qquad \beta(0) \coloneqq 1$

RcS $\qquad \forall n \in \mathbb{N} \qquad \beta(n+1) \coloneqq 2(\beta(n))$

E Find a recursive definition of the family $\left(n^2 \middle| n \in \mathbb{N}\right)$.

Note that the terms of the sequence are: $0^2, 1^2, 2^2, 3^2, \dots, n^2, (n+1)^2, \dots$. . Note that:

$$\forall n \in \mathbb{N} \qquad (n+1)^2 \coloneqq n^2 + 2n + 1$$

Using this observation, we may define the sequence recursively as follows:

BC $\qquad\qquad\qquad\qquad \gamma(0) \coloneqq 1$

RcS $\qquad \forall n \in \mathbb{N} \qquad \gamma(n+1) \coloneqq \gamma(n) + \ 2n + 1$

Q Find a recursive definition of the family $\left(n + 2 \middle| n \in \mathbb{N}\right)$.

Q Find a recursive definition of the family $\left(2n \middle| n \in \mathbb{N}\right)$.

Q Find a recursive definition of the family $\left(2n + 1 \middle| n \in \mathbb{N}\right)$.

Q Find a recursive definition of the family $\left(2n + 3 \middle| n \in \mathbb{N}\right)$.

Q Find a recursive definition of the family $\left(n(n + 1) \middle| n \in \mathbb{N}\right)$.

Q Find a recursive definition of the family $\left(n(2n + 1) \middle| n \in \mathbb{N}\right)$.

Q Find a recursive definition of the family $\left(n(n + 1)(n + 2) \middle| n \in \mathbb{N}\right)$.

Q Find a recursive definition of the family $\left(n^n \middle| n \in \mathbb{N}\right)$.

E Prove by induction that: $\quad \forall n \in \mathbb{N} \quad (2^n > n)$

We first recast the problem in terms of recursive functions.

Since we have already seen these examples, we recall (from previous examples) that the recursion:

BC $\alpha(0) \coloneqq 0$

RcS $\forall n \in \mathbb{N}$ $\alpha(n+1) \coloneqq \big(\alpha(n)\big) + 1$

defines the function $\alpha \coloneqq n \longmapsto n+1 : \mathbb{N} \longrightarrow \mathbb{N}$.

and that the recursion:

BC $\beta(0) \coloneqq 1$

RcS $\forall n \in \mathbb{N}$ $\beta(n+1) \coloneqq 2\big(\beta(n)\big)$

defines the function $\beta \coloneqq n \longmapsto 2^n : \mathbb{N} \longrightarrow \mathbb{N}$

The problem has now been recast as follows:

E Prove that: $\forall n \in \mathbb{N} \quad \Big(\beta(n) > \alpha(n)\Big)$

R We define: $\forall n \in \mathbb{N} \qquad P(n) \coloneqq \Big(\beta(n) > \alpha(n)\Big)$

We note that, upon replacing n with 0 on both sides, we get:

$$\frac{P(n) \coloneqq \Big(\beta(n) > \alpha(n)\Big)}{P(0) \coloneqq \Big(\beta(0) > \alpha(0)\Big)} \Big\langle n \longleftarrow 0 \Big\rangle$$

and, upon replacing n with 0 on both sides, we get:

$$\frac{P(n) \coloneqq \Big(\beta(n) > \alpha(n)\Big)}{P(0) \coloneqq \Big(\beta(n+1) > \alpha(n+1)\Big)} \Big\langle n \longleftarrow (n+1) \Big\rangle$$

E Prove that: $\forall n \in \mathbb{N} \left(\beta(n) > \alpha(n)\right)$

We recall that: $P(n) \coloneqq \left(\beta(n) > \alpha(n)\right)$

Hence, $P(0) \coloneqq \left(\beta(0) > \alpha(0)\right)$ and

$$P(n+1) \coloneqq \left(\beta(n+1) > \alpha(n+1)\right)$$

SPf BC

$$\frac{\begin{array}{cc} & \beta(0) \\ = & 1 \\ & \\ > & 0 \\ = & \alpha(0) \end{array}}{P(0)}$$

RcS

$$\frac{P(0) \quad P(1) \quad \cdots \quad P(n)}{\begin{array}{cll} & \beta(n+1) & \text{By recursive step of definition of } \beta \\ = & \beta(n) + \beta(n) & \text{Induction hypothesis } P(n) \\ > & \alpha(n) + \alpha(n) & n \geq 1 \\ \geq & \alpha(n) + 1 & \text{By recursive step of definition of } \alpha \\ = & \alpha(n+1) & \end{array}}$$

$$\overline{P(n+1)}$$

Hence $$\frac{P(0) \quad \left(\frac{P(0) \quad P(1) \quad \cdots \quad P(n)}{P(n+1)}\right)}{\forall n \in \mathbb{N} \left(P(n)\right)}$$

EPf

<u>Arithmetic Progression</u>

D Given $a, d \in \mathbb{R}$ we define an arithmetic progression recursively as follows:

BC		$\alpha(0)$	$\coloneqq$	a
RcS	$\forall n \in \mathbb{N}$	$\alpha(n+1)$	$\coloneqq$	$\alpha(n) + d$

R a and d are called the initial term and common difference respectively.

T $\forall n \in \mathbb{N}$

0	$\alpha(n)$	$\coloneqq$	$a + nd$
1	$Sm(\alpha, n)$	$\coloneqq$	$(n+1)a + \left(\frac{n(n+1)}{2}\right)d$

Both of these are proved by induction.

T0 $\forall n \in \mathbb{N}$ $\alpha(n) \coloneqq a + nd$

$$P(n) \coloneqq \Big(\alpha(n) = a + nd\Big)$$

Replacing n with 0,

$$\frac{P(n) \coloneqq \Big(\alpha(n) = a + nd\Big)}{P(0) \coloneqq \Big(\alpha(0) = a + (0)d\Big)} \Big\langle n \leftarrow 0 \Big\rangle$$

we obtain:

$$P(0) \coloneqq \Big(\alpha(0) = a + (0)d\Big)$$

Replacing n with $(n+1)$,

$$\frac{P(n) \coloneqq \Big(\alpha(n) = a + (n)d\Big)}{P(0) \coloneqq \Big(\alpha(n+1) = a + (n+1)d\Big)} \Big\langle n \leftarrow (n+1) \Big\rangle$$

we obtain:

$$P(n+1) \coloneqq \Big(\alpha(n+1) = a + (n+1)d\Big)$$

SPf

BC

$$\begin{array}{ll} & LS \\ = & \alpha(0) \\ = & a \\ = & a + 0(d) \\ = & RS \\ \hline & P(0) \end{array}$$

RcS

$$\dfrac{P(0) \quad P(1) \quad \cdots \quad P(n)}{\begin{array}{lll} & LS & \\ = & \alpha(n+1) & \\ = & \alpha(n) + d & \text{(by RcS of definition)} \\ = & a + nd + d & \\ & & \\ = & a + (n+1)d & \\ = & RS & \\ \hline & P(n+1) & \end{array}}$$

Hence $$\dfrac{P(0) \quad \left(\dfrac{P(0) \quad P(1) \quad \cdots \quad P(n)}{P(n+1)}\right)}{\forall n \in \mathbb{N} \left(P(n) \right)}$$

EPf

T1 $\quad \forall n \in \mathbb{N} \qquad Sm(\alpha, n) = (n+1)a + \left(\frac{n(n+1)}{2}\right) d$

SPf $\quad$ We define: $\quad \forall n \in \mathbb{N} \qquad P(n) \coloneqq \left(Sm(\alpha, n) = (n+1)a + \left(\frac{n(n+1)}{2}\right) d \right)$

Replacing n with 0:

$$\frac{P(n) \coloneqq \left(Sm(\alpha,n) = (n+1)a + \left(\frac{n(n+1)}{2}\right) d \right)}{P(0) \coloneqq \left(Sm(\alpha,0) = (0+1)a + \left(\frac{0(0+1)}{2}\right) d \right)} \langle n \leftarrow 0 \rangle$$

we obtain: $\quad P(0) \coloneqq \left(Sm(\alpha, 0) = (0+1)a + \left(\frac{0(0+1)}{2}\right) d \right)$

Replacing n with $(n+1)$:

$$\frac{P(n) \coloneqq \left(Sm(\alpha, n) = (n+1)a + \left(\frac{n(n+1)}{2}\right) d \right)}{P(n+1) \coloneqq \left(Sm(\alpha, n+1) = \big((n+1)+1\big)a + \left(\frac{(n+1)\big((n+1)+1\big)}{2}\right) d \right)} \langle n \leftarrow (n+1) \rangle$$

we obtain:

$$P(n+1) \coloneqq \left(Sm(\alpha, n+1) = \big((n+1)+1\big)a + \left(\frac{(n+1)\big((n+1)+1\big)}{2}\right) d \right)$$

SPf $\quad$ BC

LS

$= \quad Sm(\alpha, 0)$

$= \quad \alpha(0)$

$= \quad a$

$= \quad 1a + 0d$

$= \quad (0+1)a + \left(\frac{0(0+1)}{2}\right) d$

$= \quad RS$

$P(0)$

RcS $\quad P(0) \quad P(1) \quad \cdots \quad P(n)$

LS

$=$	$Sm(\alpha, n+1)$	(by RcS of definition)
$=$	$Sm(\alpha, n) + \alpha(n+1)$	$((\alpha(n) = a + nd)$
$=$	$Sm(\alpha, n) + a + (n+1)(d)$	(Induction hypothesis)
$=$	$(n+1)a + \left(\frac{n(n+1)}{2}\right) d + a + (n+1)(d)$	
$=$	$(n+1)a + a + \left(\frac{n(n+1)}{2}\right) d + (n+1)(d)$	
$=$	$\big((n+1)+1\big)a + (n+1)\left(\left(\frac{n}{2}\right) + 1\right)(d)$	
$=$	$\big((n+1)+1\big)a + (n+1)\left(\frac{n}{2} + \frac{2}{2}\right)(d)$	
$=$	$\big((n+1)+1\big)a + (n+1)\left(\frac{n+2}{2}\right)(d)$	
$=$	$\big((n+1)+1\big)a + (n+1)\left(\frac{(n+1)+1}{2}\right)(d)$	
$=$	$\big((n+1)+1\big)a + \left(\frac{(n+1)\big((n+1)+1\big)}{2}\right)(d)$	
$=$	RS	

$P(n+1)$

Hence $$\frac{P(0) \quad \left(\frac{P(0) \quad P(1) \quad \cdots \quad P(n)}{P(n+1)}\right)}{\forall n \in \mathbb{N} \left(P(n)\right)}$$

EPf

<u>Geometric Progression</u>

D Given $a \in \mathbb{R}$, $r \in \mathbb{R}\backslash\{1\}$, we define a geometric progression recursively as follows:

BC		$\gamma(0)$	$\coloneqq$	a
RcS	$\forall n \in \mathbb{N}$	$\gamma(n+1)$	$\coloneqq$	$\big(\gamma(n)\big)r$

R a and r are called the initial term and common ratio respectively.

T $\forall n \in \mathbb{N}$

0	$\gamma(n)$	$\coloneqq$	$a(r^n)$
1	$Sm(\gamma, n)$	$\coloneqq$	$a\left(\frac{1-r^{n+1}}{1-r}\right)$

Both of these are proved by induction.

T0 We define $\forall n \in \mathbb{N}$ $\gamma(n) \coloneqq a(r^n)$

We define $\forall n \in \mathbb{N}$ $P(n) \coloneqq \Big(\gamma(n) \coloneqq a(r^n)\Big)$

Replacing n with 0: $$\frac{P(n)\coloneqq\Big(\gamma(n)\coloneqq a(r^n)\Big)}{P(0)\coloneqq\Big(\gamma(0)\coloneqq a(r^0)\Big)}\Big\langle n \longleftarrow 0\Big\rangle$$

we obtain: $P(0) \coloneqq \Big(\gamma(0) \coloneqq a(r^0)\Big)$

Replacing n with $(n+1)$: $$\frac{P(n)\coloneqq\Big(\gamma(n)\coloneqq a(r^n)\Big)}{P(n+1)\coloneqq\Big(\gamma(n+1)=a(r^{n+1})\Big)}\Big\langle n \longleftarrow (n+1)\Big\rangle$$

we obtain: $P(n+1) \coloneqq \Big(\gamma(n+1) = a\big(r^{n+1}\big)\Big)$

SPf BC

$$
\begin{aligned}
& LS \\
= \quad & \gamma(0) \\
= \quad & a \\
= \quad & a(1) \\
= \quad & a(r^0) \\
= \quad & RS
\end{aligned}
$$

$$\frac{\qquad\qquad}{P(0)}$$

RcS

$$
\frac{P(0) \quad P(1) \quad \cdots \quad P(n)}{
\begin{aligned}
& LS \\
= \quad & \gamma(n+1) \\
= \quad & \big(\gamma(n)\big)r && \text{(by RcS of definition)} \\
= \quad & (a(r^n)r) \\
= \quad & a(r^{n+1}) \\
= \quad & RS
\end{aligned}
}
$$

$$\frac{\qquad\qquad}{P(n+1)}$$

Hence $$\frac{P(0) \quad \left(\frac{P(0) \quad P(1) \quad \cdots \quad P(n)}{P(n+1)}\right)}{\forall n \in \mathbb{N}\left(P(n)\right)}$$

EPf

T1 $\forall n \in \mathbb{N}$ $\quad Sm(\gamma, n) \quad \coloneqq \quad a\left(\frac{1-r^{n+1}}{1-r}\right)$

SPf We define: $\forall n \in \mathbb{N}$ $\quad P(n) \coloneqq \left(Sm(\gamma, n) \coloneqq \mathrm{a}\left(\frac{1-r^{n+1}}{1-r}\right)\right)$

Replacing n with 0:

$$\frac{P(n) \coloneqq \left(Sm(\gamma, n) \coloneqq \mathrm{a}\left(\frac{1-r^{n+1}}{1-r}\right)\right)}{P(0) \coloneqq \left(Sm(\gamma, 0) = \mathrm{a}\left(\frac{1-r^{0+1}}{1-r}\right)\right)} \left\langle n \leftarrow 0 \right\rangle$$

we obtain: $\quad P(0) \coloneqq \left(Sm(\gamma, n) \coloneqq \mathrm{a}\left(\frac{1-r^{n+1}}{1-r}\right)\right)$

Replacing n with $(n + 1)$:

$$\frac{P(n) \coloneqq \left(Sm(\gamma, n) \coloneqq a\left(\frac{1-r^{n+1}}{1-r}\right)\right)}{P(n+1) \coloneqq \left(Sm(\gamma, n+1) \coloneqq a\left(\frac{1-r^{(n+1)+1}}{1-r}\right)\right)} \left\langle n \leftarrow (n+1) \right\rangle$$

we obtain:

$$P(n+1) \coloneqq \left(Sm(\gamma, n+1) \coloneqq a\left(\frac{1-r^{(n+1)+1}}{1-r}\right)\right)$$

SPf BC $\quad LS$

$= \quad Sm(\gamma, 0)$

$= \quad \gamma(0) \qquad$ (BC of definition for $Sm(\gamma, 0)$)

$= \quad a$

$= \quad a(1)$

$= \quad a\left(\frac{1-r^{1}}{1-r^{1}}\right)$

$= \quad a\left(\frac{1-r^{0+1}}{1-r^{1}}\right)$

$= \quad RS$

$P(0)$

RcS $\dfrac{P(0) \quad P(1) \quad \cdots \quad P(n)}{LS}$

$= \quad Sm(\gamma, n+1)$ (by RcS of definition)

$= \quad Sm(\gamma, n) + \gamma(n+1)$ ($\gamma(n+1) = a(r^{n+1})$)

$= \quad Sm(\alpha, n) + a(r^{n+1})$ (Induction hypothesis)

$$= \quad a\left(\frac{1-r^{n+1}}{1-r}\right) + a(r^{n+1})$$

$$= \quad a\left(\left(\frac{1-r^{n+1}}{1-r}\right) + r^{n+1}\right)$$

$$= \quad a\left(\left(\frac{1-r^{n+1}}{1-r}\right) + r^{n+1}\left(\frac{1}{1}\right)\right)$$

$$= \quad a\left(\left(\frac{1-r^{n+1}}{1-r}\right) + r^{n+1}\left(\frac{1-r}{1-r}\right)\right)$$

$$= \quad a\left(\left(\frac{1-r^{n+1}}{1-r}\right) + \left(\frac{r^{n+1}-r^{n+2}}{1-r}\right)\right)$$

$$= \quad \frac{a}{1-r}\left(1 - \cancel{r^{n+1}} + \cancel{r^{n+1}} - r^{n+2}\right)$$

$$= \quad a\left(\frac{1-r^{(n+1)+1}}{1-r}\right)$$

$$= \quad RS$$

$$P(n+1)$$

Hence $$\dfrac{P(0) \quad \left(\dfrac{P(0) \quad P(1) \quad \cdots \quad P(n)}{P(n+1)}\right)}{\forall n \in \mathbb{N}\left(P(n)\right)}$$

EPf

R Arithmetic and Geometric Progressions are examples of recursively defined sequences.

R We note that a recursively defined sequence $\rho\colon \mathbb{N} \longrightarrow \mathbb{N}$ are also called recurrences.

Q Given a recursively defined sequence $\rho\colon \mathbb{N} \longrightarrow \mathbb{N}$ find formulas for:

0	$\rho(n)$
1	$Sm(\rho, n)$

R We deliberately do not define the word 'formula' and note that for certain forms of Φ it is possible to answer the preceding question. One may make the idea of a formula precise by specifying it as a member of a set of recursively defined terms. But we shall not take the time to do so here. We shall restrict ourselves to a certain simple form of Φ called a second-order recurrence with constant coefficients.

We recall that:

D Given $a, d \in \mathbb{R}$ we define an arithmetic progression recursively as follows:

BC		$\alpha(0)$	$\coloneqq$	a
RcS	$\forall n \in \mathbb{N}$	$\alpha(n+1)$	$\coloneqq$	$\alpha(n) + d$

R a and d are called the initial term and common difference respectively.

T $\forall n \in \mathbb{N}$

T0	$\alpha(n)$	$\coloneqq$	$a + nd$
T1	$Sm(\alpha, n)$	$\coloneqq$	$(n+1)a + \left(\frac{n(n+1)}{2}\right) d$

R We discuss a possible method for arriving at these conjectures.

We note that:

$$\alpha(0) = a = a = a + 0d$$

$$\alpha(1) = a + d = a + 1d$$

$$\alpha(2) = a + d + d = a + 2d$$

$$\alpha(3) = a + 2d + d = a + 3d$$

At this point one may be tempted to guess that

$$\alpha(n) = a + nd$$

R Note that this is just a conjecture; one still needs to prove that it is valid by using the method of induction. On IQ tests one is typically making conjectures. Since there are, in general, infinitely many possible conjectures, in mathematics one has strict criteria for distinguishing true assertions from false ones.

R In order to formulate a conjecture for $Sm(\alpha, n)$, we shall first add the numbers from 1 to 100 using a method invented by Gauss when he was only a child.

$$S = 1 + 2 + 3 + \cdots + n + \ \cdots + 98 + 99 + 100$$

$$S = 100 + 99 + 98 + \cdots + (101 - n) + \ \cdots + 3 + 2 + 1$$

In the second row, we have written the numbers backwards. Adding the two rows, we obtain:

$$2S = 101 + 101 + 101 + \cdots + 101 + \ \cdots + 101 + 101 + 101$$

because each of the 100 columns add up to 101.

Hence,

$$\begin{array}{ccc} 2S & = & 100 \times 101 \\ \div\, 2 & & \div\, 2 \\ \hline \frac{2S}{2} & = & \frac{100\times 101}{2} \\ \hline S & = & \frac{1}{2}\Big(100(100+1)\Big) \end{array}$$

R We may use the above technique to devise a conjecture for the sum of numbers from 1 to n, n being an indefinite natural number rather than the definite number 100. We proceed exactly as in the above.

$$S = 1 + 2 + 3 + \cdots + (n - 2) + (n - 1) + n$$

$$S = n + (n - 2) + (n - 1) + \cdots + 3 + 2 + 1$$

$$2S = (n + 1) + (n + 1) + (n + 1) + \cdots + (n + 1) + (n + 1) + (n + 1)$$

$2S$	$=$	$n(n+1)$
$\div 2$		$\div 2$
$\frac{2S}{2}$	$=$	$\frac{n(n+1)}{2}$
S	$=$	$\frac{n(n+1)}{2}$

R Our next task is to formulate a conjecture for $Sm(\alpha, n)$.

We make a table as shown below:

$$\alpha(0) = a + 0d$$
$$\alpha(1) = a + 1d$$
$$\alpha(2) = a + 2d$$
$$\alpha(3) = a + 3d$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$\alpha(n-1) = a + (n-1)d$$

Adding both sides we get: $\alpha(n) = a + nd \qquad \sum_{k=0}^{n} \alpha(k)$

$$\alpha(0) + \alpha(1) + \cdots \alpha(n) = (1 + 1 + \cdots + 1)a + (0 + 1 + \cdots + n)d$$

$$\sum_{k=0}^{n} \alpha(k) = (n+1)a + \left(\frac{n(n+1)}{2}\right) d$$

$$Sm(\alpha, n) = (n+1)a + \left(\frac{n(n+1)}{2}\right) d$$

R Note that these are just conjectures and they need to be proved using the method of induction.

R We next show similar techniques for the geometric progression.

We recall that:

D Given $a, r \in \mathbb{R}\backslash\{0\}$ we define a geometric progression recursively as follows:

BC		$\gamma(0)$	$:=$	a
RcS	$\forall n \in \mathbb{N}$	$\gamma(n+1)$	$:=$	$(\gamma(n))r$

R a and r are called the initial term and common ratio respectively.

T $\forall n \in \mathbb{N}$

0	$\gamma(n)$	$:=$	$a(r^n)$
1	$Sm(\gamma, n)$	$:=$	$a\left(\frac{1-r^{n+1}}{1-r}\right)$

R We discuss a possible method for arriving at these conjectures.

We note that:

$\gamma(0) = a = ar^0$

$\gamma(1) = (ar^0)r = ar^1$

$\gamma(2) = (ar^1)r = ar^2$

$\gamma(3) = (ar^2)r = ar^3$

At this point one may be tempted to guess that

$\alpha(n) = ar^n$

R Note that this is just a conjecture; one still needs to prove that it is valid by using the method of induction.

R Our next task is to formulate a conjecture for $Sm(\gamma, n)$ that we abbreviate as S.

We use the rules of inference for equational logic cleverly. These rules are as follows:

EL1 Equals added to equals yield equals.

EL2 Equals subtracted from equals yield equals.

EL3 Equals multiplied by equals yield equals.

EL4 Equals divided by non-zero equals yield equals.

EL5 Equals substituted into (replaced with) equals yield equals.

We write

$$
\begin{array}{lcl}
S & = & a + ar + ar^2 + \cdots + ar^n \\
\times(-r) & & \times(-r) \\
\hline
-rS & = & 0 - ar - ar^2 - \cdots - ar^n - ar^{n+1} \\
+S & = & +a + ar + ar^2 + \cdots + ar^n \\
\hline
(1-r)S & = & a + 0 + 0 + \cdots + 0 - ar^{n+1} \\
\div(1-r) & & \div(1-r) \\
\hline
\frac{(1-r)S}{(1-r)} & = & \frac{a - ar^{n+1}}{(1-r)} \\
\hline
S & = & a\left(\frac{1-r^{n+1}}{1-r}\right) = \left(\frac{a}{1-r}\right)(1 - r^{n+1})
\end{array}
$$

R Note that this is just a conjecture; one still needs to prove that it is valid by using the method of induction.

R You will get to try your hand at formulating conjectures on some problems on one of the exams.

D A second-order linear recurrence with constant co-efficients $c_0 . c_1, c_2 \in \mathbb{R}$ has the following form:

D Functions $\rho: \mathbb{N} \longrightarrow \mathbb{N}$ may be defined by recursion as folows:

(BC) (0) $\rho(0) \quad := r_0$

(1) $\rho(1) \quad := r_1$

(RcS) $\forall n \in \mathbb{N}$ $c_2\big(\rho(n+2)\big) := -c_1\big(\rho(n+1)\big) - c_0\big(\rho(n)\big)$

A To solve the above recurrence we use the following algorithm

0 Solve the quadratic equation: $c_2(x^2) + c_1(x) + c_0 = 0$

to find the roots: $r_1 = r - s$ and $r_2 = r + s$

where: $r := \frac{-c_1}{2c_2}$ $s := \frac{\sqrt{(c_1)^2 - 4(c_2)(c_0)}}{2c_2}$

Two cases arise:

1 $(c_1)^2 - 4(c_2)(c_0) \neq 0$, that is: $s \neq 0$

Hence there are two unequal roots: $r_1 = r - s \neq r_2 = r + s$

In this case assume that:

$$\forall n \in \mathbb{N} \qquad \rho(n) = k_1\left((r-s)^n\right) + k_2\left((r+s)^n\right)$$

2 $(c_1)^2 - 4(c_2)(c_0) = 0$, that is: $s \neq 0$

Hence there are two unequal roots: $r_1 = r_2 = r$

In this case assume that:

$$\forall n \in \mathbb{N} \qquad \rho(n) = k_1\left((r)^n\right) + k_2\left(n(r)^n\right)$$

R In each case, we use the base cases to get two equations for the unknown constants k_1 and k_2 and solve these linear equations to determine the values of k_1 and k_2.

10 $\forall n \in \mathbb{N}$ $$\rho(n) = k_1\left((r-s)^n\right) + k_2\left((r+s)^n\right)$$

Replacing n with 0, we obtain:

$$\frac{\dfrac{\rho(n) = k_1\left((r-s)^n\right) + k_2\left((r+s)^n\right)}{\rho(0) = k_1\left((r-s)^0\right) + k_2\left((r+s)^0\right)}\left\langle n \leftarrow 0\right\rangle}{\dfrac{r_0 = k_1(1) + k_2(1)}{r_0 = k_1 + k_2}}$$

Replacing n with 1, we obtain:

$$\frac{\dfrac{\rho(n) = k_1\left((r-s)^n\right) + k_2\left((r+s)^n\right)}{\rho(1) = k_1\left((r-s)^1\right) + k_2\left((r+s)^1\right)}\left\langle n \leftarrow 1\right\rangle}{r_1 = k_1(r-s) + k_2(r+s)}$$

We, therefore, we solve the following equations, to obtain:

$$\frac{\begin{array}{c}(1)k_1+(1)k_2=r_0 \\ (r-s)k_1+(r+s)k_2=r_1\end{array}}{k_1=\left(\frac{1}{2s}\right)\left(r_0(r+s)-r_1\right) \qquad k_2=\left(\frac{1}{2s}\right)\left(r_1-r_0(r-s)\right)}$$

Hence, if the two roots are distinct, that is, unequal, then

11 $\forall n \in \mathbb{N}$

$$\rho(n) = \left(\frac{r_0(r+s)-r_1}{2s}\right)\left((r-s)^n\right) + \left(\frac{r_1-r_0(r-s)}{2s}\right)\left((r+s)^n\right)$$

20 $\forall n \in \mathbb{N}$ $\rho(n) = k_1\left((r)^n\right) + k_2\left(n(r)^n\right)$

Replacing n with 0, we obtain:

$$\cfrac{\cfrac{\rho(n) = k_1\left((r)^n\right) + k_2\left(n(r)^n\right)}{\rho(0) = k_1\left(r^0\right) + k_2\left(0(r)^0\right)}\left\langle n \leftarrow 0\right\rangle}{\cfrac{r_0 = k_1(1) + k_2(0)}{r_0 = k_1}}$$

Replacing n with 1, we obtain:

$$\cfrac{\cfrac{\rho(n) = k_1\left((r)^n\right) + k_2\left(n(r)^n\right)}{\rho(1) = k_1\left((r)^1\right) + k_2\left(1(r)^1\right)}\left\langle n \leftarrow 1\right\rangle}{r_1 = k_1 r + k_2 r}$$

We, therefore, we solve the following equations, to obtain:

$$\cfrac{\begin{gathered}(1)k_1+(0)k_2=r_0\\(r)k_1+(r)k_2=r_1\end{gathered}}{k_1=r_0 \qquad k_2=\left(\frac{1}{r}\right)(r_1-rr_0)}$$

Hence, if the two roots are equal, then

21 $\forall n \in \mathbb{N}$

$$\rho(n) = (r_0)\left(r^n\right) + \left(\frac{r_1 - rr_0}{r}\right)\left(nr^n\right)$$

R You may use formulas 11 and 21 on exams.

Q Prove by induction that the solutions satisfy the recurrence.

R In the above, a certain form of the solution was assumed without any explanation whatsoever. This state of affairs is very unsatisfactory and the basis on which these methods rest can be properly understood only after one has studied linear algebra. You will get some explanation in Discrete Mathematics 2 (Math 263).

R Before one can prove something by induction, one must have some conjecture. One employs various heuristics for arriving at conjectures. Such methods have occurred to clever individuals in the past and cleverness cannot be taught. But these clever methods can be learnt.

Arithmetic

R Recurrent decimals provide examples geometric series.

F Every real number can be expressed as a decimal in base 10. A real number is rational if and inly if it can be expressed as a ratio of two whole numbers or integers and irrational otherwise. All rational numbers are either terminating decimals, or non-terminating decimals with a finite period of recurrence. Whether a decimal is terminating or non-terminating depends on the base and, therefore, is not an intrinsic property of a number. The only source of non-uniqueness of representation in base 10 is an infinite string of terminal 9's or an infinite string of terminal 0's; in base b, these are an infinite string of terminal $(b-1)'s$ or an infinte string of terminal 0's. Real numbers that are not rational are said to be irrational. Decimal representations of irrational numbers neither terminate nor exhibit any finite period of recurrence. Examples of irrational numbers are: $\sqrt{2}.\ \pi, e$. To find decimal representations for such numbers or combinations of such numbers can be quite difficult. There are some problems later in the section that touch on such issues. The subject of arithmetic is quite deep. We shall use the following notations for rational and irrational numbers.

R We write recurrent decimals by enclosing the recurrent string in parentheses to avoid confusion regarding what string recurs. To illustrate the above ideas, we prove the following theorem.

T $.(9) = 1$

SPf Define $x \coloneqq .(9)$ Note that the preceding means that

$$
\begin{aligned}
& x \\
= \quad & .(9) \\
= \quad & .9 + .09 + .009 + \cdots \\
= \quad & \tfrac{9}{10} + \tfrac{9}{100} + \tfrac{9}{1000} + \cdots \\
= \quad & \tfrac{9}{10}\left(1 + \tfrac{1}{10} + \left(\tfrac{1}{10}\right)^2 + \cdots\right)
\end{aligned}
$$

which exhibits x explicitly as a geometric series.

Note also that

$$x \quad = \quad .9 + .0(9)$$

$\times 10$		$\times 10$
$10x$	$=$	$9 + .(9)$
$10x$	$=$	$9 + x$
$-x$		$-x$
$9x$	$=$	9
$9x$	$=$	9
$\div 9$		$\div 9$
$\frac{9x}{9}$	$=$	$\frac{9}{9}$
x	$=$	1

EPf

Q Use the same technique to find the rational forms of $.12(3)$, $.1(23)$, and $.(123)$

Q Find recursive definitions from for the following numbers:

$a \coloneqq .(87)$

$b \coloneqq .(78)$

$c \coloneqq .78778777877778\cdots$

$d \coloneqq .778778777877778\cdots$

If $x, y \in \left\{a, b, c, d\right\}$, compute: $2x, x + y, x - y, x \times y, x \div y$

R We note that$\mathbb{R} = \mathbb{Q} \cup \left(\mathbb{R} \setminus \mathbb{Q}\right)$. Elements of $\mathbb{Q}$ are called rational while elements of V are called irrational. WE define the following two predicates for convenience.

D $\quad \forall r \in \mathbb{R}$, r is said to be rational and written $Rtnl\left(r \right) :\Leftrightarrow \left(r \in \mathbb{Q} \right)$

D $\quad \forall r \in \mathbb{R}$, r is said to be irrational and written $\cancel{Rtnl}\left(r \right) :\Leftrightarrow \left(r \notin \mathbb{Q} \right)$

T
$$Rtnl\left(r \right) \Leftrightarrow \left(\exists p, q \in \mathbb{Z} \left(\left(gcd(p,q) = \right) \wedge \left(r = \frac{p}{q} \right) \right) \right)$$

R The version of the above theorem that we use will have '$\exists p, q \in \mathbb{N}$' because we will deal with positive numbers. In essence, $r = \frac{p}{q}$ has the rational number r expressed in lowest terms, and, therefore, p and q do not have a common factor other than 1.

R We shall also need some other basic theorems about numbers.

T
$$\forall n, d \in \mathbb{N} \quad \exists!\, q \in 0..n \qquad \exists!\ r \in 0..(d-1) \left(n = qd + r \right)$$

R The above means that if one divides n by d there is exactly one quotient q which lies between 0 and n and exactly one remainder r that lies between 0 and $(d-1)$. Given $n, d \in \mathbb{N}$ the long division algorithm produces q and r.

T
$$\forall n, d \in \mathbb{N} \quad \exists!\, q \in 0..n \left(\frac{d|n}{\overline{n = dq}} \right)$$

R We use the above in the following form:

$$\forall n \in \mathbb{N}\ \exists!\, q \in 0..n \qquad \left(\frac{2|n}{n = 2q} \right)$$

R In my example I need the prime number 2. You will need to use a different prime depending on what number you have.

T $\quad \forall m, n, p \in \mathbb{N}\left(\dfrac{prm\,(p) \quad p|mn}{(p|m) \vee (p|n)}\right)$

T $\quad \forall n, p, l \in \mathbb{N}\left(\dfrac{prm\,(p) \quad p|n^l}{p|n}\right)$

R We establish below the irrationality of $\sqrt{2}$. This is a proof by contradiction. On one of the exams you have to establish the irrationality of a number made up from your J-number. You need to absorb this proof so that you may adopt it to your situation.

R The proof by contradiction. We assume the negation of the assertion that we wish to establish as true, namely, that $\sqrt{\mathbf{2}}$ **is irrational**. Therefore, we assume that $\sqrt{\mathbf{2}}$ **is not irrational**; this is equivalent to the assertion that $\sqrt{\mathbf{2}}$ **is rational**. We make logical deductions from this assumption and arrive at a contradiction that **2 divides 1**. Since we derive a contradiction our initial assumption, namely, that $\sqrt{2}$ is not irrational is false. Hence its negation is true. The negation reads: **it is not the case that** $\sqrt{\mathbf{2}}$ **is not irrational**, which is equivalent to the assertion that $\sqrt{\mathbf{2}}$ **is irrational**.

R The proof of irrationality of $\sqrt{2}$ is the most intricate proof that you will see in this class. It is crucial that you understand the deductive structure of the proof. The exam problem tests whether you have understood the proof and whether you can adapt it to your situation. This is not very difficult to do. But you may need to read the proof several times to completely understand its structure.

R In my example the prime that I need is 2. You will need to use a different prime number. It is best to use the smallest prime number that is a factor of the number under the radical.

R Your proof can be constructed essentially mechanically but it is important to do so slowly and carefully so that you understand exactly what is going on.

T $\cancel{Rtnl}\left(\sqrt{2}\right)$

SPf

$$\neg\left(\cancel{Rtnl}\left(\sqrt{2}\right)\right)$$

$$Rtnl\left(\sqrt{2}\right)$$

$$\exists!\, p, q \in \mathbb{N}\left(\left(gcd(p,q) = 1\right) \wedge \left(\sqrt{2} = \frac{p}{q}\right)\right)$$

$$\left(gcd(p,q) = 1\right) \quad \left(\sqrt{2} = \frac{p}{q}\right)$$

$$\sqrt{2} = \frac{p}{q}$$
$$(\quad)^2 \quad (\quad)^2$$

$$\left(\sqrt{2}\right)^2 = \left(\frac{p}{q}\right)^2$$

$$2 = \frac{p^2}{q^2}$$
$$\times\, q^2 \quad \times\, q^2$$

$$2q^2 = p^2$$

--- *

$$prm(2) \quad 2|p^2$$

$$2|p$$

$$\exists!\, r \in \mathbb{N}\left(p = 2r\right)$$

$$2q^2 = (2r)^2$$

$$2q^2 = 4r^2$$
$$\div\, 2 \quad \div\, 2$$

$$\frac{\begin{array}{c} 2q^2 = 4r^2 \\ \div 2 \quad \div 2 \end{array}}{\frac{2q^2}{2} = \frac{4r^2}{2}}$$

$$\frac{\frac{2q^2}{2} = \frac{4r^2}{2}}{q^2 = 2r^2}$$

$$\frac{q^2 = 2r^2}{2r^2 = q^2}$$

$$\frac{2r^2 = q^2}{prm(2) \quad 2|q^2}$$

$$\frac{prm(2) \quad 2|q^2}{2|q}$$

$$\frac{2|q}{2|p \quad 2|q}$$

$$\frac{2|p \quad 2|q}{2|(gcd(p,q))}$$

$$\frac{2|(gcd(p,q))}{2|(gcd(p,q)) \quad gcd(p,q) = 1}$$

$$\frac{2|(gcd(p,q)) \quad gcd(p,q) = 1}{2|1}$$

$$\frac{2|1}{\perp}$$

$$\frac{\perp}{\neg\left(\neg\left(\cancel{Rtnl}\left(\sqrt{2}\right)\right)\right)}$$

$$\frac{\neg\left(\neg\left(\cancel{Rtnl}\left(\sqrt{2}\right)\right)\right)}{\cancel{Rtnl}\left(\sqrt{2}\right)}$$

Epf

R The contradiction you will get will also be that some prime number divides 1. You will need to raise both sides to some power m that gets rid of the radical. Then you will get an equation of the form $nq^l = p^l$ for some number n. You should decompose n to find the prime factors of n. You should use the smallest prime factor of n.

R It is very important that you rewrite the proof in words as many times as necessary until you can directly look at the proof and read it in words.