CS1231: Discrete Structures

Tutorial 8

Li Wei

Department of Mathematics
National University of Singapore

25 March, 2019

Quick Review

- Euclidean Algorithm.

  Inverse of a modulo m.
- RSA Cryptosystem.
- **Principle of Mathematical Induction** To prove $\forall n \geqslant 0(P(n))$, we complete two steps:
  - ✍ Base Case: Verify that $P(0)$ is true. (That is, start with the least n.)
  - ✍ Inductive Step: Show that for all $k \geqslant 0$

    $P(0) \wedge P(1) \wedge \cdots \wedge P(k) \xrightarrow{\text{using various rules of inference}} P(k+1)$.

Menu

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: .

Step 1. $n = 1537$ with digits. I is separated into blocks of length ((the number of digits of n) -1) = .

Step 2. Let M be each block and $C = M^e$ **Mod** $n =$.

- $M =$. Then .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with digits. I is separated into blocks of length ((the number of digits of n) -1) $=$.

Step 2. Let M be each block and $C = M^e$ **Mod** $n =$.

- $M =$. Then .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.
Step 0. Translate HELP into a number I: 08051216.
Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) = .

Step 2. Let M be each block and
$C = M^e$ **Mod** $n =$.

- $M =$. Then .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

Step 2. Let M be each block and

$C = M^e$ **Mod** $n =$.

- $M =$. Then .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and

$C = M^e$ **Mod** $n =$.

- $M =$. Then .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M =$. Then .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.
Step 0. Translate HELP into a number I: 08051216.
Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and
$C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.
Step 0. Translate HELP into a number I: 08051216.
Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and
$C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C =$.
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** 1537 .
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) $-1) = 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M =$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.
Step 0. Translate HELP into a number I: 08051216.
Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and
$C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C =$.
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.
Step 0. Translate HELP into a number I: 08051216.
Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and
$C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C = 051^{47}$ **Mod** 1537 .
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.
Step 0. Translate HELP into a number I: 08051216.
Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and
$C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C = 051^{47}$ **Mod** $1537 = 419$.
- $M =$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C = 051^{47}$ **Mod** $1537 = 419$.
- $M = 216$. Then .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C = 051^{47}$ **Mod** $1537 = 419$.
- $M = 216$. Then $C =$.

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and
$C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C = 051^{47}$ **Mod** $1537 = 419$.
- $M = 216$. Then $C = 216^{47}$ **Mod** 1537 .

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C = 051^{47}$ **Mod** $1537 = 419$.
- $M = 216$. Then $C = 216^{47}$ **Mod** $1537 = 1456$.

The encrypted message is

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc.

Step 0. Translate HELP into a number I: 08051216.

Step 1. $n = 1537$ with 4 digits. I is separated into blocks of length ((the number of digits of n) -1) $= 3$.

$$08 \quad 051 \quad 216$$

Step 2. Let M be each block and $C = M^e$ **Mod** $n = M^{47}$ **Mod** 1537.

- $M = 08$. Then $C = 08^{47}$ **Mod** $1537 = 814$.
- $M = 051$. Then $C = 051^{47}$ **Mod** $1537 = 419$.
- $M = 216$. Then $C = 216^{47}$ **Mod** $1537 = 1456$.

The encrypted message is

$$814 \quad 419 \quad 1456$$

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\mod (p-1)(q-1) = (29-1) \times (53-1) = 1456$. Using the Euclidean algorithm, we have

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\bmod (p-1)(q-1) = (29-1) \times (53-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned} 1456 &= \underline{47} \times 30 + \underline{46} \\ \underline{47} &= \underline{46} \times 1 + 1 \end{aligned}$$

Now backward

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\bmod (p-1)(q-1) = (29-1) \times (53-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned} 1456 &= \underline{47} \times 30 + \underline{46} \\ \underline{47} &= \underline{46} \times 1 + 1 \\ &\quad \text{Now backward} \\ 1 &= \end{aligned}$$

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\mathrm{mod}\ (p-1)(q-1) = (29-1) \times (53-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned} 1456 &= \underline{47} \times 30 + \underline{46} \\ \underline{47} &= \underline{46} \times 1 + 1 \\ &\quad \text{Now backward} \\ 1 &= \underline{47} - \underline{46} \\ &= \end{aligned}$$

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\mathrm{mod}\ (p-1)(q-1) = (29-1) \times (53-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned} 1456 &= \underline{47} \times 30 + \underline{46} \\ \underline{47} &= \underline{46} \times 1 + 1 \\ & \quad \text{Now backward} \\ 1 &= \underline{47} - \underline{46} \\ &= \underline{47} - (1456 - \underline{47} \times 30) \\ &= \end{aligned}$$

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\mathrm{mod}\ (p-1)(q-1) = (29-1) \times (53-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned}
1456 &= \underline{47} \times 30 + \underline{46} \\
\underline{47} &= \underline{46} \times 1 + 1 \\
& \quad \text{Now backward} \\
1 &= \underline{47} - \underline{46} \\
&= \underline{47} - (1456 - \underline{47} \times 30) \\
&= 47 \times 31 - 1456
\end{aligned}$$

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\mathrm{mod}\ (p-1)(q-1) = (29-1) \times (53-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned}
1456 &= \underline{47} \times 30 + \underline{46} \\
\underline{47} &= \underline{46} \times 1 + 1 \\
&\ \text{Now backward} \\
1 &= \underline{47} - \underline{46} \\
&= \underline{47} - (1456 - \underline{47} \times 30) \\
&= 47 \times 31 - 1456 \\
d &=
\end{aligned}$$

RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(ii) Decrypt the message obtained in (i)

$$814 \quad 419 \quad 1456$$

We need to need the inverse d of $e = 47$ $\mathrm{mod}\ (p-1)(q-1) = (29-1)\times(53-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned}
1456 &= \underline{47} \times 30 + \underline{46} \\
\underline{47} &= \underline{46} \times 1 + 1 \\
&\quad \text{Now backward} \\
1 &= \underline{47} - \underline{46} \\
&= \underline{47} - (1456 - \underline{47} \times 30) \\
&= 47 \times 31 - 1456 \\
d &= 31.
\end{aligned}$$

The decryption formula is thus $M = C^{31}$ **Mod** 1537.

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C =$. Then $M = \quad ^{31}$ **Mod** $1537 =$.
- $C =$. Then $M = \quad ^{31}$ **Mod** $1537 =$.
- $C =$. Then $M = \quad ^{31}$ **Mod** $1537 =$.

Then I is

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 =$.
- $C =$. Then $M = \quad ^{31}$ **Mod** $1537 =$.
- $C =$. Then $M = \quad ^{31}$ **Mod** $1537 =$.

Then I is

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 = 8$.
- $C = \quad$. Then $M = \quad ^{31}$ **Mod** $1537 = \quad$.
- $C = \quad$. Then $M = \quad ^{31}$ **Mod** $1537 = \quad$.

Then I is

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 = 8$.
- $C = 419$. Then $M = 419^{31}$ **Mod** $1537 = \quad$.
- $C = \quad$. Then $M = \quad {}^{31}$ **Mod** $1537 = \quad$.

Then I is

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 = 8$.
- $C = 419$. Then $M = 419^{31}$ **Mod** $1537 = 051$.
- $C = \quad$. Then $M = \quad ^{31}$ **Mod** $1537 = \quad$.

Then I is

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 = 8$.
- $C = 419$. Then $M = 419^{31}$ **Mod** $1537 = 051$.
- $C = 1456$. Then $M = 1456^{31}$ **Mod** $1537 =$.

Then I is

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 = 8$.
- $C = 419$. Then $M = 419^{31}$ **Mod** $1537 = 051$.
- $C = 1456$. Then $M = 1456^{31}$ **Mod** $1537 = 216$.

Then I is

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 = 8$.
- $C = 419$. Then $M = 419^{31}$ **Mod** $1537 = 051$.
- $C = 1456$. Then $M = 1456^{31}$ **Mod** $1537 = 216$.

Then I is

$$8 \quad 051 \quad 216$$

Back into English:

The message obtained in (i)

$$814 \quad 419 \quad 1456$$

$M = C^{31}$ **Mod** 1537.

- $C = 814$. Then $M = 814^{31}$ **Mod** $1537 = 8$.
- $C = 419$. Then $M = 419^{31}$ **Mod** $1537 = 051$.
- $C = 1456$. Then $M = 1456^{31}$ **Mod** $1537 = 216$.

Then I is

$$8 \quad 051 \quad 216$$

Back into English: HELP

2. Let a and b be positive integers and d is the smallest positive integer that can be written in the form $as + bt$, where $t, s \in \mathbb{Z}$. Prove that $d = \gcd(a, b)$.

Prove that d is a divisor of a.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $a = dq + r$, $0 \leqslant r < d$. (Division Algorithm)
3. $\therefore$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore$ (From 3.)
5. $\therefore$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

2. Let a and b be positive integers and d is the smallest positive integer that can be written in the form $as + bt$, where $t, s \in \mathbb{Z}$. Prove that $d = \gcd(a, b)$.

Prove that d is a divisor of a.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $a = dq + r$, $0 \leqslant r < d$. (Division Algorithm)
3. $\therefore a = (au + bv)q + r = a(uq) + b(vq) + r$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore$ (From 3.)
5. $\therefore$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

2. Let a and b be positive integers and d is the smallest positive integer that can be written in the form $as + bt$, where $t, s \in \mathbb{Z}$. Prove that $d = \gcd(a, b)$.

Prove that d is a divisor of a.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $a = dq + r$, $0 \leqslant r < d$. (Division Algorithm)
3. $\therefore a = (au + bv)q + r = a(uq) + b(vq) + r$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore r = a(1 - uq) + b(-vq)$ (From 3.)
5. $\therefore$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

2. Let a and b be positive integers and d is the smallest positive integer that can be written in the form $as + bt$, where $t, s \in \mathbb{Z}$. Prove that $d = \gcd(a, b)$.

Prove that d is a divisor of a.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $a = dq + r$, $0 \leqslant r < d$. (Division Algorithm)
3. $\therefore a = (au + bv)q + r = a(uq) + b(vq) + r$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore r = a(1 - uq) + b(-vq)$ (From 3.)
5. $\therefore r = 0$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

2. Let a and b be positive integers and d is the smallest positive integer that can be written in the form $as + bt$, where $t, s \in \mathbb{Z}$. Prove that $d = \gcd(a, b)$.

Prove that d is a divisor of a.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $a = dq + r$, $0 \leqslant r < d$. (Division Algorithm)
3. $\therefore a = (au + bv)q + r = a(uq) + b(vq) + r$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore r = a(1 - uq) + b(-vq)$ (From 3.)
5. $\therefore r = 0$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore d|a$ (From 5)

Prove that d is a divisor of b.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $b = dp + w$, $0 \leqslant w < d$. (Division Algorithm)
3. $\therefore$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore$ (From 3.)
5. $\therefore$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

Prove that d is a divisor of b.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $b = dp + w$, $0 \leqslant w < d$. (Division Algorithm)
3. $\therefore b = (au + bv)p + w = a(up) + b(vp) + w$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore$ (From 3.)
5. $\therefore$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

Prove that d is a divisor of b.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $b = dp + w$, $0 \leqslant w < d$. (Division Algorithm)
3. $\therefore b = (au + bv)p + w = a(up) + b(vp) + w$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore w = a(1 - up) + b(-vp)$ (From 3.)
5. $\therefore$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

Prove that d is a divisor of b.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $b = dp + w$, $0 \leqslant w < d$. (Division Algorithm)
3. $\therefore b = (au + bv)p + w = a(up) + b(vp) + w$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore w = a(1 - up) + b(-vp)$ (From 3.)
5. $\therefore w = 0$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore$ (From 5)

Prove that d is a divisor of b.

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $b = dp + w$, $0 \leqslant w < d$. (Division Algorithm)
3. $\therefore b = (au + bv)p + w = a(up) + b(vp) + w$ (Substitute the expression of d in 1 to the equation in 2.)
4. $\therefore w = a(1 - up) + b(-vp)$ (From 3.)
5. $\therefore w = 0$ (From 2,4 and d is the smallest integer that can be written in the form $as + bt$)
6. $\therefore d|b$ (From 5)

We have proved that d is a common divisor of a and b. How to prove it is the greatest common divisor?

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $c|a$ and $c|b$ and $c > 0$ (That is, c is any common divisor of a and b.)
3. $\therefore$
4. $\therefore$
5. $\therefore$
6. $\therefore$

We have proved that d is a common divisor of a and b. How to prove it is the greatest common divisor?

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $c|a$ and $c|b$ and $c > 0$ (That is, c is any common divisor of a and b.)
3. $\therefore c|(au + bv)$
4. $\therefore$
5. $\therefore$
6. $\therefore$

We have proved that d is a common divisor of a and b. How to prove it is the greatest common divisor?

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $c|a$ and $c|b$ and $c > 0$ (That is, c is any common divisor of a and b.)
3. $\therefore c|(au + bv)$
4. $\therefore c|d$
5. $\therefore$
6. $\therefore$

We have proved that d is a common divisor of a and b. How to prove it is the greatest common divisor?

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $c|a$ and $c|b$ and $c > 0$ (That is, c is any common divisor of a and b.)
3. $\therefore c|(au + bv)$
4. $\therefore c|d$
5. $\therefore c \leqslant d$
6. $\therefore$

We have proved that d is a common divisor of a and b. How to prove it is the greatest common divisor?

1. Suppose $d = au + bv$. (By the given condition.)
2. Suppose $c|a$ and $c|b$ and $c > 0$ (That is, c is any common divisor of a and b.)
3. $\therefore c|(au + bv)$
4. $\therefore c|d$
5. $\therefore c \leqslant d$
6. $\therefore d$ is the greatest common divisor.

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n =$, LHS $=$, and RHS $=$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant$. In particular $P(k)$ is True, where $P(k)$ says

Now for the case $k+1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $=$, and RHS $=$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

Now for the case $k + 1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i =$, and RHS $=$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

Now for the case $k + 1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 =$, and RHS $=$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

Now for the case $k + 1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $=$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

Now for the case $k+1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 =$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

Now for the case $k+1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

Now for the case $k+1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k+1$:

LHS

$=$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k + 1$:

LHS

$= \sum_{i=1}^{k+2} i2^i =$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k+1$:

LHS

$= \sum_{i=1}^{k+2} i2^i =$ $\qquad\qquad\qquad + \sum_{i=1}^{k+1} i2^i =$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \dots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k+1$:

LHS

$= \sum_{i=1}^{k+2} i2^i = (k+2)2^{k+2} + \sum_{i=1}^{k+1} i2^i = (k+2)2^{k+2} +$

(by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k + 1$:

LHS

$= \sum_{i=1}^{k+2} i2^i = (k+2)2^{k+2} + \sum_{i=1}^{k+1} i2^i = (k+2)2^{k+2} + k2^{k+2} + 2$ (by $P(k)$)

$=$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k + 1$:

LHS

$= \sum_{i=1}^{k+2} i2^i = (k+2)2^{k+2} + \sum_{i=1}^{k+1} i2^i = (k+2)2^{k+2} + k2^{k+2} + 2$ (by $P(k)$)

$= (2k+2)2^{k+2} + 2 =$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \dots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k+1$:

LHS

$= \sum_{i=1}^{k+2} i2^i = (k+2)2^{k+2} + \sum_{i=1}^{k+1} i2^i = (k+2)2^{k+2} + k2^{k+2} + 2$ (by $P(k)$)

$= (2k+2)2^{k+2} + 2 = (k+1)2^{k+3} + 2 =$

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, LHS $= \sum_{i=1}^{0+1} i2^i = 1 \times 2^1 = 2$, and RHS $= 0 \times 2^{0+2} + 2 = 2$.

Inductive step: Assume that it's true for $0, \ldots k$, where $k \geqslant 0$. In particular $P(k)$ is True, where $P(k)$ says

$$\sum_{i=1}^{k+1} i2^i = k2^{k+2} + 2$$

Now for the case $k + 1$:

LHS

$= \sum_{i=1}^{k+2} i2^i = (k+2)2^{k+2} + \sum_{i=1}^{k+1} i2^i = (k+2)2^{k+2} + k2^{k+2} + 2$ (by $P(k)$)

$= (2k+2)2^{k+2} + 2 = (k+1)2^{k+3} + 2 =$ RHS (changing forms)

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n =$, then and .
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant$, so $\Rightarrow 7^k - 1 =$
Now consider the case $k + 1$.

$=$
$=$ ( ) (use $P(k)$)
$=$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then and .

Inductive step: Assume that the result holds for $0, \dots k$, where $k \geqslant 0$, so $\Rightarrow 7^k - 1 =$

Now consider the case $k + 1$.

$=$

$= \ (\qquad)$ (use $P(k)$)

$=$ (calculation) $=$ (changing forms)

$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 =$ and .
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $\Rightarrow 7^k - 1 =$
Now consider the case $k + 1$.

$=$
$= \; (\quad)$ (use $P(k)$)
$=$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 =$ and .
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $\Rightarrow 7^k - 1 =$
Now consider the case $k + 1$.

$=$
$= \quad (\quad)$ (use $P(k)$)
$=$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and .
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $\Rightarrow 7^k - 1 =$
Now consider the case $k + 1$.

$=$

$= \quad (\qquad)$ (use $P(k)$)

$=$ (calculation) $=$ (changing forms)

$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $\Rightarrow 7^k - 1 =$
Now consider the case $k + 1$.

$=$
$= \;(\qquad)$ (use $P(k)$)
$=$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 =$
Now consider the case $k + 1$.

$=$
$= \quad (\qquad\qquad)$ (use $P(k)$)
$=$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 = 6q$ for some $q \in \mathbb{Z}$.
Now consider the case $k + 1$.

$=$

$=$ ( ) (use $P(k)$)

$=$ (calculation) $=$ (changing forms)

$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 = 6q$ for some $q \in \mathbb{Z}$.
Now consider the case $k + 1$.

$7^{k+1} - 1$

$=$

$= \;(\qquad\qquad)$ (use $P(k)$)

$=$ (calculation) $=$ (changing forms)

$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \dots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 = 6q$ for some $q \in \mathbb{Z}$.
Now consider the case $k + 1$.
$7^{k+1} - 1$
$= 7(7^k) - 1$
$= 7(\qquad) - 1$ (use $P(k)$)
$=$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 = 6q$ for some $q \in \mathbb{Z}$.
Now consider the case $k + 1$.
$7^{k+1} - 1$
$= 7(7^k) - 1$
$= 7(6q + 1) - 1$ (use $P(k)$)
$=$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 = 6q$ for some $q \in \mathbb{Z}$.
Now consider the case $k + 1$.
$7^{k+1} - 1$
$= 7(7^k) - 1$
$= 7(6q + 1) - 1$ (use $P(k)$)
$= 42q + 6$ (calculation) $=$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 = 6q$ for some $q \in \mathbb{Z}$.
Now consider the case $k + 1$.
$7^{k+1} - 1$
$= 7(7^k) - 1$
$= 7(6q + 1) - 1$ (use $P(k)$)
$= 42q + 6$ (calculation) $= 6(7q + 1)$ (changing forms)
$\Rightarrow$.

(b) $6 \mid (7^n - 1) \quad \forall n \in \mathbb{Z}^*$.

Idea. **Base Case**: If $n = 0$, then $7^n - 1 = 7^0 - 1 = 0$ and $6 \mid 0$.
Inductive step: Assume that the result holds for $0, \ldots k$, where $k \geqslant 0$, so $6 \mid (7^k - 1) \Rightarrow 7^k - 1 = 6q$ for some $q \in \mathbb{Z}$.
Now consider the case $k + 1$.
$7^{k+1} - 1$
$= 7(7^k) - 1$
$= 7(6q + 1) - 1$ (use $P(k)$)
$= 42q + 6$ (calculation) $= 6(7q + 1)$ (changing forms)
$\Rightarrow 6 \mid (7^{k+1} - 1)$.

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n =$, LHS $=$

RHS $=$

$\Rightarrow$

Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant$, so Now consider the case $k+1$. Thus

$$
\begin{aligned}
\text{RHS} &= \\
&= \\
&\geqslant && \text{[by } P(k)\text{]} \\
&= && \text{[by calculation]} \\
\text{LHS} &=
\end{aligned}
$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $=$

RHS $=$

$\Rightarrow$

Inductive step: Assume that the result holds for $2, \dots k$, where $k \geqslant 2$, so Now consider the case $k+1$. Thus

$$
\begin{aligned}
\text{RHS} &= \\
&= \\
&\geqslant && \text{[by } P(k)\text{]} \\
&= && \text{[by calculation]} \\
\text{LHS} &=
\end{aligned}
$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $=$
$\Rightarrow$

Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so Now consider the case $k+1$. Thus

$$\begin{aligned}
\text{RHS} &= \\
&= \\
&\geqslant && [\text{by } P(k)] \\
&= && [\text{by calculation}] \\
\text{LHS} &=
\end{aligned}$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$

RHS $= (1+x)^2 =$

$\Rightarrow$

Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so Now consider the case $k+1$. Thus

$$\begin{aligned} \text{RHS} &= \\ &= \\ &\geqslant && \text{[by } P(k)\text{]} \\ &= && \text{[by calculation]} \\ \text{LHS} &= \end{aligned}$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$

Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so Now consider the case $k+1$. Thus

$$
\begin{aligned}
\text{RHS} &= \\
&= \\
&\geqslant && \text{[by } P(k)\text{]} \\
&= && \text{[by calculation]} \\
\text{LHS} &=
\end{aligned}
$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \dots k$, where $k \geqslant 2$, so Now consider the case $k+1$. Thus

RHS $=$

$=$

$\geqslant$ [by $P(k)$]

$=$ [by calculation]

LHS $=$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so $1 + kx \leqslant (1+x)^k$. Now consider the case $k+1$. Thus

$$\begin{aligned} \text{RHS} &= \\ &= \\ &\geqslant && \text{[by } P(k)\text{]} \\ &= && \text{[by calculation]} \\ \text{LHS} &= \end{aligned}$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so $1 + kx \leqslant (1+x)^k$. Now consider the case $k+1$. Thus

$$
\begin{array}{rcll}
\text{RHS} & = & (1+x)^{k+1} & \\
 & = & & \\
 & \geqslant & & [\text{by } P(k)] \\
 & = & & [\text{by calculation}] \\
\text{LHS} & = & &
\end{array}
$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so $1 + kx \leqslant (1+x)^k$. Now consider the case $k+1$. Thus

$$\begin{array}{rcll} \text{RHS} & = & (1+x)^{k+1} & \\ & = & (1+x)(1+x)^k & \\ & \geqslant & (1+x) & \text{[by } P(k)\text{]} \\ & = & & \text{[by calculation]} \\ \text{LHS} & = & & \end{array}$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so $1 + kx \leqslant (1+x)^k$. Now consider the case $k+1$. Thus

$$\begin{array}{rcll}
\text{RHS} & = & (1+x)^{k+1} & \\
& = & (1+x)(1+x)^k & \\
& \geqslant & (1+x)(1+kx)[\text{by } P(k)] & \\
& = & & [\text{by calculation}] \\
\text{LHS} & = & &
\end{array}$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so $1 + kx \leqslant (1+x)^k$. Now consider the case $k+1$. Thus

$$\begin{array}{rcl} \text{RHS} & = & (1+x)^{k+1} \\ & = & (1+x)(1+x)^k \\ & \geqslant & (1+x)(1+kx)[\text{by } P(k)] \\ & = & 1 + (k+1)x + kx^2[\text{by calculation}] \\ \text{LHS} & = & \end{array}$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so $1 + kx \leqslant (1+x)^k$. Now consider the case $k+1$. Thus

$$\begin{array}{rcl} \text{RHS} & = & (1+x)^{k+1} \\ & = & (1+x)(1+x)^k \\ & \geqslant & (1+x)(1+kx)[\text{by } P(k)] \\ & = & 1 + (k+1)x + kx^2[\text{by calculation}] \\ \text{LHS} & = & 1 + (k+1)x \end{array}$$

$\Rightarrow$

(c) $1 + nx \leqslant (1+x)^n$ for each integer $n \geqslant 2$ and for real numbers $x > -1$.

Idea. **Base step:** $n = 2$, LHS $= 1 + 2x$
RHS $= (1+x)^2 = 1 + 2x + x^2$
$\Rightarrow$ LHS $\leqslant$ RHS
Inductive step: Assume that the result holds for $2, \ldots k$, where $k \geqslant 2$, so $1 + kx \leqslant (1+x)^k$. Now consider the case $k+1$. Thus

$$\begin{array}{rcl} \text{RHS} & = & (1+x)^{k+1} \\ & = & (1+x)(1+x)^k \\ & \geqslant & (1+x)(1+kx)[\text{by } P(k)] \\ & = & 1 + (k+1)x + kx^2[\text{by calculation}] \\ \text{LHS} & = & 1 + (k+1)x \end{array}$$

$\Rightarrow$ LHS$\leqslant$RHS

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.

Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n =$

Idea. Inductive step: Now assume that it's true for all $n =$, where $k \geqslant$. Then $k + 1 \geqslant$

$$\begin{aligned} h_{k+1} &= \\ &\leqslant \quad + \quad + \quad [\text{ by } P(0), \ldots P(k)] \\ &= \quad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\ &\leqslant \quad [\text{Noth that} \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0$,
Idea. Inductive step: Now assume that it's true for all
$n =$, where $k \geqslant$. Then $k + 1 \geqslant$

$$\begin{aligned} h_{k+1} &= \\ &\leqslant \quad + \quad + \quad [\text{ by } P(0), \ldots P(k)] \\ &= \quad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\ &\leqslant \quad [\text{Noth that} \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1,$
Idea. Inductive step: Now assume that it's true for all
$n = 0, 1, 2, \ldots k$, where $k \geqslant$. Then $k + 1 \geqslant$

$$\begin{aligned} h_{k+1} &= \\ &\leqslant \quad + \quad + \quad [\text{ by } P(0), \ldots P(k)] \\ &= \quad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\ &\leqslant \quad [\text{Noth that} \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant$

$$\begin{aligned}
h_{k+1} &= \\
&\leqslant \quad + \quad + \quad [\text{ by } P(0), \ldots P(k)] \\
&= \quad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\
&\leqslant \quad [\text{Noth that}
\end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned} h_{k+1} &= \\ &\leqslant \qquad + \qquad + \qquad [\text{ by } P(0), \ldots P(k)] \\ &= \qquad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\ &\leqslant \qquad [\text{Noth that} \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned}
h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\
&\leqslant \quad + \quad + \quad [\text{ by } P(0), \ldots P(k)] \\
&= \quad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\
&\leqslant \quad [\text{Noth that}
\end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned} h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\ &\leqslant 3^k + \qquad + \qquad [\text{ by } P(0), \ldots P(k)] \\ &= \qquad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\ &\leqslant \qquad [\text{Noth that} \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned}
h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\
&\leqslant 3^k + 3^{k-1} + \qquad [\text{ by } P(0), \ldots P(k)] \\
&= \qquad (\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\
&\leqslant \qquad [\text{Noth that}
\end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned} h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\ &\leqslant 3^k + 3^{k-1} + 3^{k-2} [\text{ by } P(0), \ldots P(k)] \\ &= 3^{k+1}(\quad + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\ &\leqslant \qquad [\text{Noth that} \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned} h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\ &\leqslant 3^k + 3^{k-1} + 3^{k-2} [\text{ by } P(0), \ldots P(k)] \\ &= 3^{k+1}(\frac{1}{3} + \quad + \quad)[\text{ to compare with } 3^{k+1}] \\ &\leqslant \qquad [\text{Noth that} \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.

Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$

Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned}
h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\
&\leqslant 3^k + 3^{k-1} + 3^{k-2} [\text{ by } P(0), \ldots P(k)] \\
&= 3^{k+1}(\frac{1}{3} + \frac{1}{9} + \quad)[\text{ to compare with } 3^{k+1}] \\
&\leqslant \qquad [\text{Noth that}
\end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned} h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\ &\leqslant 3^k + 3^{k-1} + 3^{k-2} [\text{ by } P(0), \ldots P(k)] \\ &= 3^{k+1}(\frac{1}{3} + \frac{1}{9} + \frac{1}{27}) [\text{ to compare with } 3^{k+1}] \\ &\leqslant \qquad [\text{Noth that } \frac{1}{3} + \frac{1}{9} + \frac{1}{27} < 1]. \end{aligned}$$

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3$$

and

$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \text{ for } k \geqslant 3$$

Prove that $h_n \leqslant 3^n$ for all $n \geqslant 0$.
Idea. **Base Case**: Check that $h_n \leqslant 3^n$ for $n = 0, 1, 2$
Idea. Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geqslant 2$. Then $k + 1 \geqslant 3$

$$\begin{aligned} h_{k+1} &= h_k + h_{k-1} + h_{k-2} \\ &\leqslant 3^k + 3^{k-1} + 3^{k-2} [\text{ by } P(0), \ldots P(k)] \\ &= 3^{k+1}(\frac{1}{3} + \frac{1}{9} + \frac{1}{27}) [\text{ to compare with } 3^{k+1}] \\ &\leqslant 3^{k+1} [\text{Noth that } \frac{1}{3} + \frac{1}{9} + \frac{1}{27} < 1]. \end{aligned}$$

5. What's wrong with the following proof that $2^n = 1$ for all $n \in \mathbb{Z}^*$?

Basis step: $2^0 = 1$.

Inductive step: Assume that $2^j = 1$ for $j = 0, 1 \ldots, k$. Then

$$2^{k+1} = \frac{2^k \cdot 2^k}{2^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

5. What's wrong with the following proof that $2^n = 1$ for all $n \in \mathbb{Z}^*$?
Basis step: $2^0 = 1$.
Inductive step: Assume that $2^j = 1$ for $j = 0, 1 \ldots, k$. Then

$$2^{k+1} = \frac{2^k \cdot 2^k}{2^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

Answer. The inductive step is not valid for $k = 0$ because the denominator becomes $2^{k-1} = 2^{-1}$ and this is not covered by the induction hypothesis.

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 2$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 3$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 4$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value:

For $n = 2$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 3$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 4$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 3$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 4$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value:

For $n = 3$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 4$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 4$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value:

For $n = 4$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F

For $n = 4$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F

For $n = 4$, $2^n > n^2 + n$ says "$2^4 > 4^2 + 4$" Truth Value:

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F

For $n = 4$, $2^n > n^2 + n$ says "$2^4 > 4^2 + 4$" Truth Value: F

For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F

For $n = 4$, $2^n > n^2 + n$ says "$2^4 > 4^2 + 4$" Truth Value: F

For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value:

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F

For $n = 4$, $2^n > n^2 + n$ says "$2^4 > 4^2 + 4$" Truth Value: F

For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

For $n = 6$, $2^n > n^2 + n$ says " " Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F

For $n = 4$, $2^n > n^2 + n$ says "$2^4 > 4^2 + 4$" Truth Value: F

For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

For $n = 6$, $2^n > n^2 + n$ says "$2^6 > 6^2 + 6$" Truth Value:

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F
For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F
For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F
For $n = 4$, $2^n > n^2 + n$ says "$2^4 > 4^2 + 4$" Truth Value: F
For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T
For $n = 6$, $2^n > n^2 + n$ says "$2^6 > 6^2 + 6$" Truth Value: T

Guess. $2^n > n^2 + n$ for $n \geqslant$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.

Idea.

For $n = 1$, $2^n > n^2 + n$ says "$2^1 > 1^2 + 1$" Truth Value: F

For $n = 2$, $2^n > n^2 + n$ says "$2^2 > 2^2 + 2$" Truth Value: F

For $n = 3$, $2^n > n^2 + n$ says "$2^3 > 3^2 + 3$" Truth Value: F

For $n = 4$, $2^n > n^2 + n$ says "$2^4 > 4^2 + 4$" Truth Value: F

For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

For $n = 6$, $2^n > n^2 + n$ says "$2^6 > 6^2 + 6$" Truth Value: T

Guess. $2^n > n^2 + n$ for $n \geqslant 5$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n =$, $2^n > n^2 + n$ says " " Truth Value:

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant \quad}$. For $n =$, the LHS is

$$
\begin{aligned}
2^{k+1} &= \\
&> \\
&= \\
&= \\
&= \\
&=
\end{aligned}
$$

Note that $\underline{\qquad\qquad\qquad \text{is} \geqslant \qquad}$

$>$ = RHS

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says " " Truth Value:

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant \quad}$. For $n =$, the LHS is

$$2^{k+1} =$$
$$>$$
$$=$$
$$=$$
$$=$$
$$=$$

Note that ______ is $\geqslant$ ______

$>$ = RHS

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value:

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant \quad}$. For $n = \qquad$, the LHS is

$$2^{k+1} =$$

$$>$$

$$=$$

$$=$$

$$=$$

$$=$$

Note that $\underline{\qquad\qquad\qquad \text{is} \geqslant \quad}$

$>$ $\qquad\qquad$ = RHS

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant \quad}$. For $n =$, the LHS is

$$2^{k+1} =$$

$$>$$

$$=$$

$$=$$

$$=$$

$$=$$

Note that $\underline{\qquad\qquad\qquad \text{is} \geqslant \qquad}$

$$> \qquad\qquad\qquad = \text{RHS}$$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n =$ ______, the LHS is

$2^{k+1} =$

$>$

$=$

$=$

$=$

$=$

Note that ____________ is $\geqslant$ ______

$>$ ____________ $=$ RHS

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$
\begin{aligned}
2^{k+1} &= \\
&> \\
&= \\
&= \\
&= \\
&=
\end{aligned}
$$

Note that ______________ is $\geqslant$ ______

$>$ $= \text{RHS}$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$
\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(\qquad\quad) \\
&= \\
&= \\
&= \\
&=
\end{aligned}
$$

Note that $\underline{\qquad\qquad\qquad\qquad \text{is} \geqslant}$

$> \qquad\qquad\qquad\qquad = \text{RHS}$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$\begin{aligned} 2^{k+1} &= 2 \times 2^k \\ &> 2(k^2 + k) \\ &= \\ &= \\ &= \\ &= \end{aligned}$$

Note that ____________ is $\geqslant$ ______

$>$ $=$ RHS

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - \\
&= [(k+1)^2 + (k+1)] - \\
&= [(k+1)^2 + (k+1)] + \\
&= [(k+1)^2 + (k+1)] +
\end{aligned}$$

Note that ____________ is $\geqslant$ ____

$$> (k+1)^2 + (k+1) = \text{RHS}$$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - [(k+1)^2 + (k+1)] + \\
&= [(k+1)^2 + (k+1)] - \\
&= [(k+1)^2 + (k+1)] + \\
&= [(k+1)^2 + (k+1)] +
\end{aligned}$$

Note that __________ is $\geqslant$ __________

$$> (k+1)^2 + (k+1) = \text{RHS}$$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \dots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$
\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - [(k+1)^2 + (k+1)] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] - \qquad\qquad + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] + \\
&= [(k+1)^2 + (k+1)] +
\end{aligned}
$$

Note that $\underline{\qquad\qquad\qquad \text{is} \geqslant \qquad}$

$$> (k+1)^2 + (k+1) = \text{RHS}$$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$
\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - [(k+1)^2 + (k+1)] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] - [k^2 + 2k + 1 + k + 1] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] + \\
&= [(k+1)^2 + (k+1)] +
\end{aligned}
$$

Note that $\underline{\qquad\qquad\qquad \text{is} \geqslant \qquad}$

$$
> (k+1)^2 + (k+1) = \text{RHS}
$$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$
\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - [(k+1)^2 + (k+1)] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] - [k^2 + 2k + 1 + k + 1] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] + k^2 - k - 2 \\
&= [(k+1)^2 + (k+1)] +
\end{aligned}
$$

Note that $\underline{\qquad\qquad\qquad \text{is} \geqslant \qquad}$

$$> (k+1)^2 + (k+1) = \text{RHS}$$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$
\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - [(k+1)^2 + (k+1)] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] - [k^2 + 2k + 1 + k + 1] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] + k^2 - k - 2 \\
&= [(k+1)^2 + (k+1)] + k(k-1) - 2
\end{aligned}
$$

Note that $\underline{k(k-1) - 2 \text{ is } \geqslant \qquad\qquad}$

$$> (k+1)^2 + (k+1) = \text{RHS}$$

Prove $2^n > n^2 + n$ for all $n \geqslant 5$.

Base Case. For $n = 5$, $2^n > n^2 + n$ says "$2^5 > 5^2 + 5$" Truth Value: T

Inductive Step. Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $\underline{k \geqslant 5}$. For $n = k + 1$, the LHS is

$$\begin{aligned}
2^{k+1} &= 2 \times 2^k \\
&> 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - [(k+1)^2 + (k+1)] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] - [k^2 + 2k + 1 + k + 1] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] + k^2 - k - 2 \\
&= [(k+1)^2 + (k+1)] + k(k-1) - 2
\end{aligned}$$

Note that $\underline{k(k-1) - 2 \text{ is } \geqslant 18}$

$$> (k+1)^2 + (k+1) = \text{RHS}$$