Euclid's Lemma

▸ Start

Start

Euclid's Lemma:

▸ Start

Euclid's Lemma:

Let

Start

Euclid's Lemma:

Let a

Start

Euclid's Lemma:

Let a and

▸ Start

Euclid's Lemma:

Let a and b

▸ Start

Euclid’s Lemma:

Let a and b and

Start

Euclid's Lemma:

Let a and b and c

Start

Euclid’s Lemma:

Let a and b and c be

Start

Euclid's Lemma:

Let a and b and c be given integers.

Start

Euclid's Lemma:

Let a and b and c be given integers. If

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b

Start

Euclid’s Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c is divisible by

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c is divisible by a.

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c is divisible by a.

$$a|bc$$

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c is divisible by a.

$$a|bc \text{ and}$$

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c is divisible by a.

$$a|bc \text{ and } gcd(a, b) = 1$$

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c is divisible by a.

$$a|bc \text{ and } gcd(a,b) = 1 \Rightarrow$$

Start

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1 , then c is divisible by a.

$$a|bc \text{ and } gcd(a, b) = 1 \Rightarrow a|c$$

First

Euclid's Lemma:

Let a and b and c be given integers. If bc is divisible by a and the greatest common divisor of a and b is 1, then c is divisible by a.

$$a|bc \text{ and } gcd(a,b) = 1 \Rightarrow a|c$$ proof

First

First

$\exists x,$

First

$\exists x,\ y$

Euclid's Lemma

First

$\exists x,\ y \in$

▸ First

$\exists x,\ y \in \mathbb{Z}$

First

$\exists x,\ y \in \mathbb{Z}$ such that

Euclid's Lemma

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that 1

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 =$

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax$

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax +$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because$

Euclid's Lemma

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

c

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a,b) = 1)$

$c =$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a, b) = 1)$

$c = 1$

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c$

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a, b) = 1)$

$c = 1 \times c =$

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)$

Euclid's Lemma

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c$

Euclid's Lemma

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c =$

Euclid's Lemma

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by\ (\because gcd(a, b) = 1)$

$c = 1 \times c = (ax + by)c = acx$

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx +$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by\ (\because gcd(a,b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by \ (\because gcd(a, b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

a

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a,b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$

Euclid's Lemma

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ (

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ ($\because$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ ($\because a$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ ($\because a|$

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a, b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ $(\because a|ac$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ ($\because a|ac,$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a, b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ $(\because a|ac,\ a$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ ($\because a|ac,\ a|$

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a, b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ ($\because a|ac,\ a|bc$

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a,b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ $(\because a|ac,\ a|bc)$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ ($\because gcd(a,b) = 1$)

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ ($\because a|ac,\ a|bc$)

$\therefore$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by$ $(\because gcd(a, b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)$ $(\because a|ac,\ a|bc)$

$\therefore a$

Euclid's Lemma

▸ First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by\ (\because gcd(a, b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)\ (\ \because a|ac,\ a|bc)$

$\therefore a|$

Euclid's Lemma

First

$\exists x,\ y \in \mathbb{Z}$ such that $1 = ax + by\ (\because gcd(a,b) = 1)$

$c = 1 \times c = (ax + by)c = acx + bcy$

$a|(acx + bcy)\ (\because a|ac,\ a|bc)$

$\therefore a|c$