Discrete Mathematics & Mathematical Reasoning
Greatest Common Divisors

Colin Stirling

Informatics

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

$\gcd(36, 24) = 12$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

$\gcd(36, 24) = 12$

$\gcd(22, 9) = 1$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

$\gcd(36, 24) = 12$

$\gcd(22, 9) = 1$

Definition

The integers a and b are relatively prime (coprime) iff $\gcd(a, b) = 1$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

$\gcd(36, 24) = 12$

$\gcd(22, 9) = 1$

Definition

The integers a and b are relatively prime (coprime) iff $\gcd(a, b) = 1$

Although 9 and 22 are coprime they are both composite

Gcd by prime factorisations

Suppose that the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

Gcd by prime factorisations

Suppose that the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

Gcd by prime factorisations

Suppose that the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

$$\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

This number clearly divides a and b. No larger number can divide both a and b. Proof by contradiction and the prime factorisation of a postulated larger divisor.

Gcd by prime factorisations

Suppose that the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

$$\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

This number clearly divides a and b. No larger number can divide both a and b. Proof by contradiction and the prime factorisation of a postulated larger divisor.

Factorisation is a very inefficient method to compute gcd

Euclidian algorithm: efficient for computing gcd

Euclidian algorithm

```
algorithm gcd(x,y)
    if y = 0
    then return(x)
    else return(gcd(y,x mod y))
```

Euclidian algorithm: efficient for computing gcd

Euclidian algorithm

```
algorithm gcd(x,y)
    if y = 0
    then return(x)
    else return(gcd(y,x mod y))
```

The Euclidian algorithm relies on

$$\forall x, y \in \mathbb{Z}^+ \; (\mathrm{gcd}(x, y) = \mathrm{gcd}(y, x \bmod y))$$

Euclidian algorithm (proof of correctness)

Lemma

If $x = yq + r$, where x, y, q, and r are positive integers, then $\gcd(x, y) = \gcd(y, r)$. (Consider $r = x \bmod y$ and $q = x \operatorname{div} y$)

Euclidian algorithm (proof of correctness)

Lemma

If $x = yq + r$, where x, y, q, and r are positive integers, then $\gcd(x, y) = \gcd(y, r)$. (Consider $r = x \bmod y$ and $q = x \text{ div } y$)

Proof.

($\Rightarrow$) Suppose that d divides both x and y. Then d also divides $x - yq = r$. Hence, any common divisor of x and y must also be a common divisor of y and r.
($\Leftarrow$) Suppose that d divides both y and r. Then d also divides $yq + r = x$. Hence, any common divisor of y and r must also be a common divisor of x and y.
Therefore, $\gcd(x, y) = \gcd(y, r)$ $\square$

Gcd as a linear combination

Theorem (Bézout's theorem)

If x and y are positive integers, then there exist integers a and b such that $gcd(x, y) = ax + by$

Bézout's theorem: proof

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := e-gcd(y, x mod y)
     return((d, b, a - ((x div y) * b)))
```

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := e-gcd(y, x mod y)
     return((d, b, a - ((x div y) * b)))
```

- e-gcd$(24, 9)$

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := e-gcd(y, x mod y)
     return((d, b, a - ((x div y) * b)))
```

- e-gcd$(24, 9)$
- e-gcd$(22, 9)$

Bézout's theorem: proof

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := e-gcd(y, x mod y)
     return((d, b, a - ((x div y) * b)))
```

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := e-gcd(y, x mod y)
     return((d, b, a - ((x div y) * b)))
```

Correctness proof for computing Bézout coefficients

- Let $x = yq + r$ where $r = x \bmod y$ and $q = x \operatorname{div} y$
- So $r = x - yq$

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := e-gcd(y, x mod y)
    return((d, b, a - ((x div y) * b)))
```

Correctness proof for computing Bézout coefficients

- Let $x = yq + r$ where $r = x \bmod y$ and $q = x \operatorname{div} y$
- So $r = x - yq$
- If $d = ay + br$ then

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
   if y = 0
   then return(x, 1, 0)
   else
    (d, a, b) := e-gcd(y, x mod y)
    return((d, b, a - ((x div y) * b)))
```

Correctness proof for computing Bézout coefficients

- Let $x = yq + r$ where $r = x \bmod y$ and $q = x$ div y
- So $r = x - yq$
- If $d = ay + br$ then
  $d = ay + b(x - yq) = bx + (a - qb)y$

Bézout's theorem: proof

Extended Euclidian algorithm

```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := e-gcd(y, x mod y)
     return((d, b, a - ((x div y) * b)))
```

Correctness proof for computing Bézout coefficients

- Let $x = yq + r$ where $r = x \bmod y$ and $q = x \operatorname{div} y$
- So $r = x - yq$
- If $d = ay + br$ then
  $d = ay + b(x - yq) = bx + (a - qb)y$
- Base case $y = 0$: e-gcd$(x, y) = (x, 1, 0)$ and $x = 1 * x + 0 * y$

Further properties

Theorem

If a, b, c are positive integers such that $gcd(a, b) = 1$ and $a|bc$ then $a|c$

Further properties

Theorem

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$ then $a|c$

Proof.

Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that $sa + tb = 1$. So, $sac + tbc = c$. Assume $a|bc$. Therefore, $a|tbc$ and $a|sac$, so $a|(sac + tbc)$; that is, $a|c$. □

Further properties

Theorem

If a, b, c are positive integers such that $gcd(a, b) = 1$ and $a|bc$ then $a|c$

Proof.

Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that $sa + tb = 1$. So, $sac + tbc = c$. Assume $a|bc$. Therefore, $a|tbc$ and $a|sac$, so $a|(sac + tbc)$; that is, $a|c$. $\square$

Theorem

Let m be a positive integer and let a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

Further properties

Theorem

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$ then $a|c$

Proof.

Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that $sa + tb = 1$. So, $sac + tbc = c$. Assume $a|bc$. Therefore, $a|tbc$ and $a|sac$, so $a|(sac + tbc)$; that is, $a|c$. $\square$

Theorem

Let m be a positive integer and let a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

Proof.

Because $ac \equiv bc \pmod{m}$, it follows $m|(ac - bc)$; so, $m|c(a - b)$. By the result above because $\gcd(c, m) = 1$, it follows that $m|(a - b)$. $\square$