Lecture 4: Divisibility and Greatest Common Divisor

Divisors

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.

Divisors

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.

Examples:

$$3|6 \quad \text{since} \quad 6 = 3 * 2;$$

Divisors

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.

Examples:

$$\begin{aligned} 3|6 &\quad \text{since} \quad 6 = 3 * 2; \\ 15|60 &\quad \text{since} \quad 60 = 15 * 4; \end{aligned}$$

Divisors

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.

Examples:

$$3|6 \quad \text{since} \quad 6 = 3 * 2;$$

$$15|60 \quad \text{since} \quad 60 = 15 * 4;$$

$$15 \nmid 25 \quad \text{since there is no } m \in \mathbb{Z} \text{ such that } 25 = 15 * m.$$

Divisors

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.

Examples:

$$3|6 \quad \text{since} \quad 6 = 3 * 2;$$

$$15|60 \quad \text{since} \quad 60 = 15 * 4;$$

$$15 \nmid 25 \quad \text{since there is no } m \in \mathbb{Z} \text{ such that } 25 = 15 * m.$$

In general, for any $n \in \mathbb{Z}$,

$$n|n, \quad -n|n, \quad 1|n, \quad \text{and } -1|n.$$

Divisors

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.
Examples:

$$3|6 \quad \text{since} \quad 6 = 3 * 2;$$
$$15|60 \quad \text{since} \quad 60 = 15 * 4;$$
$$15 \nmid 25 \quad \text{since there is no } m \in \mathbb{Z} \text{ such that } 25 = 15 * m.$$

In general, for any $n \in \mathbb{Z}$,

$$n|n, \quad -n|n, \quad 1|n, \quad \text{and } -1|n.$$

We often restrict to talking about numbers $n \in \mathbb{Z}_{>0}$, and list the divisors as the positive integers that divide n.

Divisors

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.

Examples:

$$3|6 \quad \text{since} \quad 6 = 3 * 2;$$

$$15|60 \quad \text{since} \quad 60 = 15 * 4;$$

$$15 \nmid 25 \quad \text{since there is no } m \in \mathbb{Z} \text{ such that } 25 = 15 * m.$$

In general, for any $n \in \mathbb{Z}$,

$$n|n, \quad -n|n, \quad 1|n, \quad \text{and } -1|n.$$

We often restrict to talking about numbers $n \in \mathbb{Z}_{>0}$, and list the divisors as the positive integers that divide n.

Example: the divisors of 12 are 1, 2, 3, 4, 6, and 12.

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

For example,

3 is a divisor of 30, but not 40;
4 is a divisor of 40, but not 30;
$1, 2, 5$, and 10 are all common divisors of 30 and 40.

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

For example,

$$3 \text{ is a divisor of } 30 \text{, but not } 40;$$
$$4 \text{ is a divisor of } 40 \text{, but not } 30;$$
$$1, 2, 5, \text{ and } 10 \text{ are all common divisors of } 30 \text{ and } 40.$$

The greatest common divisor of a and b, denoted $\gcd(a, b)$ is largest number that divides both a and b.

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

For example,

3 is a divisor of 30, but not 40;

4 is a divisor of 40, but not 30;

$1, 2, 5$, and 10 are all common divisors of 30 and 40.

The greatest common divisor of a and b, denoted $\gcd(a, b)$ is largest number that divides both a and b.

Example: $\gcd(30, 40) = 10$.

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

For example,

$$3 \text{ is a divisor of } 30, \text{ but not } 40;$$
$$4 \text{ is a divisor of } 40, \text{ but not } 30;$$
$$1, 2, 5, \text{ and } 10 \text{ are all common divisors of } 30 \text{ and } 40.$$

The greatest common divisor of a and b, denoted $\gcd(a, b)$ is largest number that divides both a and b.

Example: $\gcd(30, 40) = 10$.

Always, $\gcd(a, b) = \gcd(b, a)$.

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

For example,

3 is a divisor of 30, but not 40;

4 is a divisor of 40, but not 30;

$1, 2, 5$, and 10 are all common divisors of 30 and 40.

The greatest common divisor of a and b, denoted $\gcd(a, b)$ is largest number that divides both a and b.

Example: $\gcd(30, 40) = 10$.

Always, $\gcd(a, b) = \gcd(b, a)$.

If $b|a$, then $\gcd(a, b) = b$.

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

For example,

$$3 \text{ is a divisor of } 30 \text{, but not } 40;$$
$$4 \text{ is a divisor of } 40 \text{, but not } 30;$$
$$1, 2, 5, \text{ and } 10 \text{ are all common divisors of } 30 \text{ and } 40.$$

The greatest common divisor of a and b, denoted $\gcd(a, b)$ is largest number that divides both a and b.

Example: $\gcd(30, 40) = 10$.

Always, $\gcd(a, b) = \gcd(b, a)$.

If $b|a$, then $\gcd(a, b) = b$.

If $\gcd(a, b) = 1$, we say that a and b are relatively prime.

Common divisors

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e.

$$d|a \qquad \text{and} \qquad d|b.$$

For example,

3 is a divisor of 30, but not 40;
4 is a divisor of 40, but not 30;
1, 2, 5, and 10 are all common divisors of 30 and 40.

The greatest common divisor of a and b, denoted $\gcd(a, b)$ is largest number that divides both a and b.

Example: $\gcd(30, 40) = 10$.

Always, $\gcd(a, b) = \gcd(b, a)$.
If $b|a$, then $\gcd(a, b) = b$.
If $\gcd(a, b) = 1$, we say that a and b are relatively prime.

Example:

The divisors of 25 are 1, 5, and 25;
the divisors of 12 are 1, 2, 3, 4, 6, and 12;
so 25 and 12 are relatively prime (even though neither is prime).

Computing the greatest common divisor

Method 1: Compute all the divisors of a and b, and compare.

Computing the greatest common divisor

Method 1: Compute all the divisors of a and b, and compare.

VERY inefficient!

Computing the greatest common divisor

Method 1: Compute all the divisors of a and b, and compare.

VERY inefficient!

Method 2:

Compute the prime factorizations, and take their "intersection".

Computing the greatest common divisor

Method 1: Compute all the divisors of a and b, and compare.

VERY inefficient!

Method 2:

Compute the prime factorizations, and take their "intersection".

Example:

$$19500 = 2^2 * 3 * 5^3 * 13 \quad \text{and} \quad 440 = 2^3 * 5 * 11,$$

$$\text{so} \quad \gcd(19500, 400) = 2^2 * 5 = \boxed{20}.$$

In other words, $\gcd(a, b)$ will be the product over primes p to the highest power n such that $p^n|a$ and $p^n|b$.

Computing the greatest common divisor

Method 1: Compute all the divisors of a and b, and compare.

VERY inefficient!

Method 2:

Compute the prime factorizations, and take their "intersection".

Example:

$$19500 = 2^2 * 3 * 5^3 * 13 \quad \text{and} \quad 440 = 2^3 * 5 * 11,$$
$$\text{so} \quad \gcd(19500, 400) = 2^2 * 5 = \boxed{20}.$$

In other words, $\gcd(a, b)$ will be the product over primes p to the highest power n such that $p^n|a$ and $p^n|b$.

You try: compute the prime factorizations of $12, 30, 35$, and 84, and use them to compute

$$\gcd(12, 30), \quad \gcd(12, 35), \quad \gcd(12, 84), \quad \gcd(30, 35), \quad \gcd(30, 84),$$

Computing the greatest common divisor

Method 1: Compute all the divisors of a and b, and compare.

VERY inefficient!

Method 2:

Compute the prime factorizations, and take their "intersection".

Example:

$$19500 = 2^2 * 3 * 5^3 * 13 \quad \text{and} \quad 440 = 2^3 * 5 * 11,$$
$$\text{so} \quad \gcd(19500, 400) = 2^2 * 5 = \boxed{20}.$$

In other words, $\gcd(a, b)$ will be the product over primes p to the highest power n such that $p^n | a$ and $p^n | b$.

You try: compute the prime factorizations of $12, 30, 35$, and 84, and use them to compute

$$\gcd(12, 30), \quad \gcd(12, 35), \quad \gcd(12, 84), \quad \gcd(30, 35), \quad \gcd(30, 84),$$

Not computationally efficient either! (Prime factorization is computationally difficult/not possible without a list of primes.)

Method 3: The Euclidean algorithm.

Method 3: The Euclidean algorithm.

First, we'll need the division algorithm, which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Method 3: The Euclidean algorithm.

First, we'll need the division algorithm, which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Ex: if $a = 17, b = 5$

Method 3: The Euclidean algorithm.

First, we'll need the division algorithm, which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."
Ex: if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

Method 3: The Euclidean algorithm.

First, we'll need the division algorithm, which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Ex: if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

Ex: if $a = -17, b = 5$

Method 3: The Euclidean algorithm.

First, we'll need the division algorithm, which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Ex: if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

Ex: if $a = -17, b = 5$, then $q = -4$ and $r = 3$ since $-17 = 5 * (-4) + 2$.

Method 3: The Euclidean algorithm.

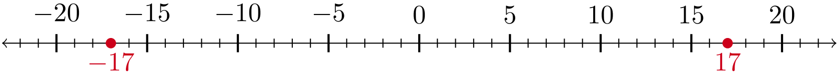
First, we'll need the division algorithm, which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Ex: if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

Ex: if $a = -17, b = 5$, then $q = -4$ and $r = 3$ since $-17 = 5 * (-4) + 2$.



Method 3: The Euclidean algorithm.

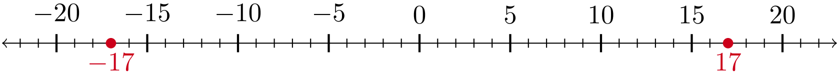
First, we'll need the division algorithm, which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Ex: if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

Ex: if $a = -17, b = 5$, then $q = -4$ and $r = 3$ since $-17 = 5 * (-4) + 2$.



Proof: (sketch) If a and b are the same sign, subtract b from a until the result is between 0 and $|b| - 1$. The result is r and the number of subtractions is q. If they're different signs, add b to a until the result is between 0 and $|b| - 1$. The result is r and the number of additions is $-q$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

And if $a_3 = 2, b_3 = 1$, then $q_3 = 2$ and $r_3 = 0$ since $2 = 2 * 1 + 0$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

And if $a_3 = 2, b_3 = 1$, then $q_3 = 2$ and $r_3 = 0$ since $2 = 2 * 1 + 0$.

Notice: $\gcd(17, 5) = 1$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

And if $a_3 = 2, b_3 = 1$, then $q_3 = 2$ and $r_3 = 0$ since $2 = 2 * 1 + 0$.

Notice: $\gcd(17, 5) = 1$.

Play this game again with new a and b:

1. Start with $a_1 = a$ and $b_1 = b$.
2. Compute the quotient q_i and remainder r_i in dividing a_i by b_i.
3. Repeat the division algorithm using $a_i = b_{i-1}$ and $b_i = r_{i-1}$.
4. Iterate until you get $r_n = 0$.
   Then compare $\gcd(a, b)$ with r_{n-1}.

You try: Do this process with $a = 30$, $b = 12$, and then with $a = 84$, $b = 30$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

And if $a_3 = 2, b_3 = 1$, then $q_3 = 2$ and $r_3 = 0$ since $2 = 2 * 1 + 0$.

Notice: $\gcd(17, 5) = 1$.

Play this game again with new a and b:

1. Start with $a_1 = a$ and $b_1 = b$.
2. Compute the quotient q_i and remainder r_i in dividing a_i by b_i.
3. Repeat the division algorithm using $a_i = b_{i-1}$ and $b_i = r_{i-1}$.
4. Iterate until you get $r_n = 0$.
   Then compare $\gcd(a, b)$ with r_{n-1}.

You try: Do this process with $a = 30$, $b = 12$, and then with $a = 84$, $b = 30$.

Claim: If n is the first time that $r_n = 0$, then $r_{n-1} = \gcd(a, b)$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

And if $a_3 = 2, b_3 = 1$, then $q_3 = 2$ and $r_3 = 0$ since $2 = 2 * 1 + 0$.

Notice: $\gcd(17, 5) = 1$.

Play this game again with new a and b:

1. Start with $a_1 = a$ and $b_1 = b$.
2. Compute the quotient q_i and remainder r_i in dividing a_i by b_i.
3. Repeat the division algorithm using $a_i = b_{i-1}$ and $b_i = r_{i-1}$.
4. Iterate until you get $r_n = 0$.
   Then compare $\gcd(a, b)$ with r_{n-1}.

You try: Do this process with $a = 30$, $b = 12$, and then with $a = 84$, $b = 30$.

Claim: If n is the first time that $r_n = 0$, then $r_{n-1} = \gcd(a, b)$.

Note that if $r = 0$ in the first step, then $b|n$, so $\gcd(a, b) = b$.

Spreadsheet functions

For a and integer and b a positive integer,

$$=\text{FLOOR}(a, b)$$

gives the largest multiple of b less or equal to a.

Namely, if $a = bq + r$, then $\text{FLOOR}(a, b) = bq$.

Spreadsheet functions

For a and integer and b a positive integer,

$$=\text{FLOOR}(a, b)$$

gives the largest multiple of b less or equal to a.

Namely, if $a = bq + r$, then FLOOR$(a, b) = bq$.

Example:

=FLOOR$(17, 5)$ returns 15,

=FLOOR$(-17, 5)$ returns -20,

=FLOOR$(17, -5)$ returns an error.

Spreadsheet functions

For a and integer and b a positive integer,

$$=\text{FLOOR}(a, b)$$

gives the largest multiple of b less or equal to a.

Namely, if $a = bq + r$, then FLOOR$(a, b) = bq$.

Example:

$=$FLOOR$(17, 5)$ returns 15,

$=$FLOOR$(-17, 5)$ returns -20,

$=$FLOOR$(17, -5)$ returns an error.

So to compute q and r such that $a = bq + r$,

$=$FLOOR$(a, b)/b$ returns q,

$=a-$FLOOR(a, b) returns r.

Why does $r_{n-1} = \gcd(a, b)$?

Why does $r_{n-1} = \gcd(a, b)$?

In general, our process looks like

$$
\begin{array}{ccccc}
a & = & b * q_1 & + & r_1 \\
b & = & r_1 * q_2 & + & r_2 \\
r_1 & = & r_2 * q_3 & + & r_3 \\
 & \vdots & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \quad \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 \quad \leftarrow r_n
\end{array}
$$

Why does $r_{n-1} = \gcd(a, b)$?

In general, our process looks like

$$
\begin{array}{rcccll}
a & = & b * q_1 & + & r_1 & \\
b & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
 & \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}
$$

To make everything look the same, let $r_{-1} = a$ and $r_0 = b$.

Why does $r_{n-1} = \gcd(a,b)$?

In general, our process looks like

$$
\begin{array}{ccccccl}
\overset{r_{-1}}{\cancel{a}} & = & \overset{r_0}{\cancel{b}} * q_1 & + & r_1 & & \\
\overset{r_0}{\cancel{b}} & = & r_1 * q_2 & + & r_2 & & \\
r_1 & = & r_2 * q_3 & + & r_3 & & \\
 & \vdots & & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow & \gcd(a,b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow & r_n
\end{array}
$$

To make everything look the same, let $r_{-1} = a$ and $r_0 = b$. So every line comes in the form

$$r_{i-2} = r_{i-1} * q_i + r_i.$$

Why does $r_{n-1} = \gcd(a, b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{ccccc}
r_{-1} & = & r_0 * q_1 & + & r_1 \\
r_0 & = & r_1 * q_2 & + & r_2 \\
r_1 & = & r_2 * q_3 & + & r_3 \\
 & \vdots & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \quad \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 \quad \leftarrow r_n
\end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{rcccll}
r_{-1} & = & r_0 * q_1 & + & r_1 & \\
r_0 & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
& \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}$$

Last line: $r_{n-2} = r_{n-1} q_n$.

Why does $r_{n-1} = \gcd(a,b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{rcccc} r_{-1} & = & r_0 * q_1 & + & r_1 \\ r_0 & = & r_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a,b)? \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n \end{array}$$

Last line: $r_{n-2} = r_{n-1} q_n$.

So

$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$

Why does $r_{n-1} = \gcd(a, b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{ccccccl}
r_{-1} & = & r_0 * q_1 & + & r_1 & & \\
r_0 & = & r_1 * q_2 & + & r_2 & & \\
r_1 & = & r_2 * q_3 & + & r_3 & & \\
 & \vdots & & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow & \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow & r_n
\end{array}$$

Last line: $r_{n-2} = r_{n-1} q_n$.

So

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} = (r_{n-1} q_n) q_{n-1} + r_{n-1}$$

Why does $r_{n-1} = \gcd(a,b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{ccccc}
r_{-1} & = & r_0 * q_1 & + & r_1 \\
r_0 & = & r_1 * q_2 & + & r_2 \\
r_1 & = & r_2 * q_3 & + & r_3 \\
 & \vdots & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a,b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}$$

Last line: $r_{n-2} = r_{n-1} q_n$.

So

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} = (r_{n-1} q_n) q_{n-1} + r_{n-1} = r_{n-1}(q_n q_{n-1} + 1).$$

Why does $r_{n-1} = \gcd(a,b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{ccccc} r_{-1} & = & r_0 * q_1 & + & r_1 \\ r_0 & = & r_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a,b)? \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n \end{array}$$

Last line: $r_{n-2} = r_{n-1}q_n$.

So

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} = (r_{n-1}q_n)q_{n-1} + r_{n-1} = r_{n-1}(q_nq_{n-1} + 1).$$

Then

$$r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$$

Why does $r_{n-1} = \gcd(a,b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{rcccl} r_{-1} & = & r_0 * q_1 & + & r_1 \\ r_0 & = & r_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \quad \leftarrow \gcd(a,b)? \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 \quad \leftarrow r_n \end{array}$$

Last line: $r_{n-2} = r_{n-1} q_n$.

So

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} = (r_{n-1} q_n) q_{n-1} + r_{n-1} = r_{n-1}(q_n q_{n-1} + 1).$$

Then

$$r_{n-4} = r_{n-3} q_{n-2} + r_{n-2} = r_{n-1}(q_n q_{n-1} + 1) q_{n-2} + r_{n-1} q_n$$

Why does $r_{n-1} = \gcd(a, b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{ccccl} r_{-1} & = & r_0 * q_1 & + & r_1 \\ r_0 & = & r_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \quad \leftarrow \gcd(a,b)? \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 \quad \leftarrow r_n \end{array}$$

Last line: $r_{n-2} = r_{n-1}q_n$.

So

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} = (r_{n-1}q_n)q_{n-1} + r_{n-1} = r_{n-1}(q_nq_{n-1} + 1).$$

Then

$$\begin{aligned} r_{n-4} = r_{n-3}q_{n-2} + r_{n-2} &= r_{n-1}(q_nq_{n-1} + 1)q_{n-2} + r_{n-1}q_n \\ &= r_{n-1}(q_nq_{n-1}q_{n-2} + q_{n-2} + 1). \end{aligned}$$

Why does $r_{n-1} = \gcd(a, b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{ccccc} r_{-1} & = & r_0 * q_1 & + & r_1 \\ r_0 & = & r_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a,b)? \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n \end{array}$$

Last line: $r_{n-2} = r_{n-1} q_n$.

So

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} = (r_{n-1} q_n) q_{n-1} + r_{n-1} = r_{n-1}(q_n q_{n-1} + 1).$$

Then

$$\begin{aligned} r_{n-4} = r_{n-3} q_{n-2} + r_{n-2} &= r_{n-1}(q_n q_{n-1} + 1) q_{n-2} + r_{n-1} q_n \\ &= r_{n-1}(q_n q_{n-1} q_{n-2} + q_{n-2} + 1). \end{aligned}$$

And so on...

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$84 = 30 * 2 + 24$$
$$30 = 24 * 1 + 6$$
$$24 = 6 * 4 + 0.$$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$84 = 30 * 2 + 24$$
$$30 = 24 * 1 + 6$$
$$24 = 6 * 4 + 0.$$

$r_{n-1} = 6$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$\begin{aligned} 84 &= 30 * 2 + 24 \\ 30 &= 24 * 1 + 6 \\ 24 &= 6 * 4 + 0. \end{aligned} \qquad r_{n-1} = 6$$

So

$$30 = 24 * 1 + 6$$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$84 = 30 * 2 + 24$$
$$30 = 24 * 1 + 6$$
$$24 = 6 * 4 + 0. \qquad r_{n-1} = 6$$

So

$$30 = 24 * 1 + 6 = (6 * 4) * 1 + 6$$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$84 = 30 * 2 + 24$$
$$30 = 24 * 1 + 6$$
$$24 = 6 * 4 + 0. \qquad r_{n-1} = 6$$

So

$$30 = 24 * 1 + 6 = (6 * 4) * 1 + 6 = 6(4 * 1 + 1) = 6 * 5$$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$84 = 30 * 2 + 24$$
$$30 = 24 * 1 + 6$$
$$24 = 6 * 4 + 0.$$

$$r_{n-1} = 6$$

So

$$30 = 24 * 1 + 6 = (6 * 4) * 1 + 6 = 6(4 * 1 + 1) = 6 * 5$$
$$84 = 30 * 2 + 24$$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$\begin{aligned} 84 &= 30 * 2 + 24 \\ 30 &= 24 * 1 + 6 \\ 24 &= 6 * 4 + 0. \end{aligned} \qquad r_{n-1} = 6$$

So

$$30 = 24 * 1 + 6 = (6 * 4) * 1 + 6 = 6(4 * 1 + 1) = 6 * 5$$

$$84 = 30 * 2 + 24 = (6 * 5) * 2 + (6 * 4)$$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$
\begin{aligned}
84 &= 30 * 2 + 24 \\
30 &= 24 * 1 + 6 \\
24 &= 6 * 4 + 0.
\end{aligned}
\qquad\qquad r_{n-1} = 6
$$

So

$$
\begin{aligned}
30 &= 24 * 1 + 6 = (6 * 4) * 1 + 6 = 6(4 * 1 + 1) = 6 * 5 \\
84 &= 30 * 2 + 24 = (6 * 5) * 2 + (6 * 4) = 6(5 * 2 + 4) = 6 * 24.
\end{aligned}
$$

Why does $r_{n-1} = \gcd(a, b)$?

Example: We saw

$$84 = 30 * 2 + 24$$
$$30 = 24 * 1 + 6$$
$$24 = 6 * 4 + 0. \qquad r_{n-1} = 6$$

So

$$30 = 24 * 1 + 6 = (6 * 4) * 1 + 6 = 6(4 * 1 + 1) = 6 * 5$$
$$84 = 30 * 2 + 24 = (6 * 5) * 2 + (6 * 4) = 6(5 * 2 + 4) = 6 * 24.$$

So 6 is a common divisor of 84 and 30.

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned}$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned}$$

$r_{n-1} = 4$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned} \qquad r_{n-1} = 4$$

So

$$28 = 8 * 3 + 4$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned} \qquad r_{n-1} = 4$$

So

$$28 = 8 * 3 + 4 = (4 * 2) * 3 + 4$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned} \qquad r_{n-1} = 4$$

So

$$28 = 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$100 = 36 * 2 + 28$$
$$36 = 28 * 1 + 8$$
$$28 = 8 * 3 + 4$$
$$8 = 4 * 2 + 0. \qquad r_{n-1} = 4$$

So

$$28 = 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7$$
$$36 = 28 * 1 + 8$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$
\begin{aligned}
100 &= 36 * 2 + 28 \\
36 &= 28 * 1 + 8 \\
28 &= 8 * 3 + 4 \\
8 &= 4 * 2 + 0.
\end{aligned}
\qquad r_{n-1} = 4
$$

So

$$28 = 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7$$

$$36 = 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2)$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned} \qquad r_{n-1} = 4$$

So

$$28 = 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7$$
$$36 = 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2) = 4(7 * 1 + 2) = 4 * 9$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned}$$

$$r_{n-1} = 4$$

So

$$\begin{aligned} 28 &= 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7 \\ 36 &= 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2) = 4(7 * 1 + 2) = 4 * 9 \\ 100 &= 36 * 2 + 28 \end{aligned}$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned}$$

$r_{n-1} = 4$

So

$$\begin{aligned} 28 &= 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7 \\ 36 &= 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2) = 4(7 * 1 + 2) = 4 * 9 \\ 100 &= 36 * 2 + 28 = (4 * 9) * 2 + (4 * 7) \end{aligned}$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$100 = 36 * 2 + 28$$
$$36 = 28 * 1 + 8$$
$$28 = 8 * 3 + 4$$
$$8 = 4 * 2 + 0. \qquad r_{n-1} = 4$$

So

$$28 = 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7$$
$$36 = 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2) = 4(7 * 1 + 2) = 4 * 9$$
$$100 = 36 * 2 + 28 = (4 * 9) * 2 + (4 * 7) = 4(9 * 2 + 7) = 4 * 25.$$

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned} \qquad r_{n-1} = 4$$

So

$$\begin{aligned} 28 &= 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7 \\ 36 &= 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2) = 4(7 * 1 + 2) = 4 * 9 \\ 100 &= 36 * 2 + 28 = (4 * 9) * 2 + (4 * 7) = 4(9 * 2 + 7) = 4 * 25. \end{aligned}$$

So 4 is a common divisor of 100 and 36.

From our spreadsheet, we can calculate that for $a = 100$, $b = 36$:

$$\begin{aligned} 100 &= 36 * 2 + 28 \\ 36 &= 28 * 1 + 8 \\ 28 &= 8 * 3 + 4 \\ 8 &= 4 * 2 + 0. \qquad\qquad r_{n-1} = 4 \end{aligned}$$

So

$$\begin{aligned} 28 &= 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7 \\ 36 &= 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2) = 4(7 * 1 + 2) = 4 * 9 \\ 100 &= 36 * 2 + 28 = (4 * 9) * 2 + (4 * 7) = 4(9 * 2 + 7) = 4 * 25. \end{aligned}$$

So 4 is a common divisor of 100 and 36.

You try: use the following computations, working backwards, to show that 2 is a common divisor of 100 and 26:

$$\begin{aligned} 100 &= 26 * 3 + 22 & 26 &= 22 * 1 + 4 \\ 22 &= 4 * 5 + 2 & 4 &= 2 * 2 + 0 \end{aligned}$$

Why does $r_{n-1} = \gcd(a, b)$?

Letting $r_{-1} = a$ and $r_0 = b$, and computing

$$
\begin{array}{rcccll}
r_{-1} & = & r_0 * q_1 & + & r_1 & \\
r_0 & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
 & \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}
$$

we can reverse this process to show that r_{n-1} is, at the very least, a *common divisor* to $a = r_{-1}$ and $b = r_0$.

Why does $r_{n-1} = \gcd(a, b)$?

Letting $r_{-1} = a$ and $r_0 = b$, and computing

$$
\begin{array}{rcccll}
r_{-1} & = & r_0 * q_1 & + & r_1 & \\
r_0 & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
 & \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}
$$

we can reverse this process to show that r_{n-1} is, at the very least, a *common divisor* to $a = r_{-1}$ and $b = r_0$.

Wait! How do we know we ever get 0??

Why does $r_{n-1} = \gcd(a, b)$?

Letting $r_{-1} = a$ and $r_0 = b$, and computing

$$\begin{array}{ccccc}
r_{-1} & = & r_0 * q_1 & + & r_1 \\
r_0 & = & r_1 * q_2 & + & r_2 \\
r_1 & = & r_2 * q_3 & + & r_3 \\
 & \vdots & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}$$

we can reverse this process to show that r_{n-1} is, at the very least, a *common divisor* to $a = r_{-1}$ and $b = r_0$.

Wait! How do we know we ever get 0??

The division algorithm ensures that each remainder is strictly smaller than the last, and always non-negative:

$$b = r_0 > r_1 > r_2 > \cdots \geqslant 0.$$

Why does $r_{n-1} = \gcd(a,b)$?

Letting $r_{-1} = a$ and $r_0 = b$, and computing

$$\begin{array}{rclcll}
r_{-1} & = & r_0 * q_1 & + & r_1 & \\
r_0 & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
& \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a,b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}$$

we can reverse this process to show that r_{n-1} is, at the very least, a *common divisor* to $a = r_{-1}$ and $b = r_0$.

Wait! How do we know we ever get 0??

The division algorithm ensures that each remainder is strictly smaller than the last, and always non-negative:

$$b = r_0 > r_1 > r_2 > \cdots \geqslant 0.$$

So since the r_i's are all *integers*, this process ends at some point.

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$.

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccc}
a & = & b * q_1 & + & r_1 \\
b & = & r_1 * q_2 & + & r_2 \\
r_1 & = & r_2 * q_3 & + & r_3 \\
 & \vdots & & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0
\end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccc} d\alpha & = & d\beta * q_1 & + & r_1 \\ b & = & r_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 \end{array}$$

Why does $r_{n-1} = \gcd(a,b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccc}
d\alpha & = & d\beta * q_1 & + & r_1 \\
b & = & r_1 * q_2 & + & r_2 \\
r_1 & = & r_2 * q_3 & + & r_3 \\
 & \vdots & & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0
\end{array}$$

so $r_1 = d(\alpha - \beta q_1)$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccl} d\alpha & = & d\beta * q_1 & + & r_1 \quad \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\ b & = & r_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 \end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccc} d\alpha & = & d\beta * q_1 & + & r_1 \\ d\beta & = & dm_1 * q_2 & + & r_2 \\ r_1 & = & r_2 * q_3 & + & r_3 \\ & \vdots & & & \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 \end{array} \qquad \text{so } r_1 = d(\alpha - \beta q_1) = dm_1$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{cccccl}
d\alpha & = & d\beta * q_1 & + & r_1 & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & \text{so } r_2 = d(\beta - m_1 q_2) \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
 & \vdots & & & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 &
\end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccccl}
d\alpha & = & d\beta * q_1 & + & r_1 & & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & & \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\
r_1 & = & r_2 * q_3 & + & r_3 & & \\
 & \vdots & & & & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & & \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & &
\end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccccl} d\alpha & = & d\beta * q_1 & + & r_1 & & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\ d\beta & = & dm_1 * q_2 & + & r_2 & & \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\ dm_1 & = & dm_2 * q_3 & + & r_3 & & \\ & \vdots & & & & & \\ r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & & \\ r_{n-2} & = & r_{n-1} * q_n & + & 0 & & \end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccccl}
d\alpha & = & d\beta * q_1 & + & r_1 & & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & & \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 & & \text{so } r_3 = \cdots = dm_3 \\
 & \vdots & & & & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & & \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & &
\end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccll}
d\alpha & = & d\beta * q_1 & + & r_1 & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 & \text{so } r_3 = \cdots = dm_3 \\
 & \vdots & & & & \\
dm_{n-3} & = & dm_{n-2} * q_{n-1} & + & r_{n-1} & \text{so } r_{n-1} = \cdots = dm_{n-1} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 &
\end{array}$$

Why does $r_{n-1} = \gcd(a,b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccll}
d\alpha & = & d\beta * q_1 & + & r_1 & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 & \text{so } r_3 = \cdots = dm_3 \\
 & \vdots & & & & \\
dm_{n-3} & = & dm_{n-2} * q_{n-1} & + & r_{n-1} & \text{so } \boxed{r_{n-1} = \cdots = dm_{n-1}} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 &
\end{array}$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccc l}
d\alpha & = & d\beta * q_1 & + & r_1 & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 & \text{so } r_3 = \cdots = dm_3 \\
 & \vdots & & & & \\
dm_{n-3} & = & dm_{n-2} * q_{n-1} & + & r_{n-1} & \text{so } \boxed{r_{n-1} = \cdots = dm_{n-1}} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 &
\end{array}$$

So d is a divisor of r_{n-1}.

Why does $r_{n-1} = \gcd(a,b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and} \quad b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccccl}
d\alpha & = & d\beta * q_1 & + & r_1 & \text{so} & r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & \text{so} & r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 & \text{so} & r_3 = \cdots = dm_3 \\
 & \vdots & & & & & \\
dm_{n-3} & = & dm_{n-2} * q_{n-1} & + & r_{n-1} & \text{so} & \boxed{r_{n-1} = \cdots = dm_{n-1}} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & &
\end{array}$$

So d is a divisor of r_{n-1}. In particular, since $r_{n-1} > 0$, we have

$$d | r_{n-1} \quad \textit{and} \quad d \leqslant r_{n-1}.$$

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and} \quad b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccccl}
d\alpha & = & d\beta * q_1 & + & r_1 & \text{so} & r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & \text{so} & r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 & \text{so} & r_3 = \cdots = dm_3 \\
 & \vdots & & & & & \\
dm_{n-3} & = & dm_{n-2} * q_{n-1} & + & r_{n-1} & \text{so} & \boxed{r_{n-1} = \cdots = dm_{n-1}} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & &
\end{array}$$

So d is a divisor of r_{n-1}. In particular, since $r_{n-1} > 0$, we have

$$d | r_{n-1} \quad \textit{and} \quad d \leqslant r_{n-1}.$$

In other words, r_{n-1} is a common divisor to a and b, *and* any other common divisor is less than or equal to r_{n-1}.

Why does $r_{n-1} = \gcd(a, b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{ccccl}
d\alpha & = & d\beta * q_1 & + & r_1 \quad \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 \quad \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 \quad \text{so } r_3 = \cdots = dm_3 \\
 & \vdots & & & \\
dm_{n-3} & = & dm_{n-2} * q_{n-1} & + & r_{n-1} \quad \text{so } \boxed{r_{n-1} = \cdots = dm_{n-1}} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0
\end{array}$$

So d is a divisor of r_{n-1}. In particular, since $r_{n-1} > 0$, we have

$$d | r_{n-1} \quad \textit{and} \quad d \leqslant r_{n-1}.$$

In other words, r_{n-1} is a common divisor to a and b, *and* any other common divisor is less than or equal to r_{n-1}. So $r_{n-1} = \gcd(a, b)$.

The Euclidean algorithm for computing the greatest common divisor of two positive numbers a and b is the process or successively dividing until just before you get a 0 divisor (like we just did).

The Euclidean algorithm for computing the greatest common divisor of two positive numbers a and b is the process or successively dividing until just before you get a 0 divisor (like we just did). Namely, we have the following theorem.

Theorem (Euclidean algorithm)

To compute the greatest common divisor of two positive integers a and b, let $r_{-1} = a$ and $r_0 = b$, and compute successive quotients and remainders

$$r_{i-2} = r_{i-1} q_i + r_i$$

for $i = 1, 2, 3, \ldots,$ until some remainder r_n is 0. The last nonzero remainder r_{n-1} is then the greatest common divisor of a and b.

This takes at most b steps (actually less), and is *much* more computationally efficient than the other methods.