MAS114: Lecture 10

James Cranch

http://cranch.staff.shef.ac.uk/mas114/

2021–2022

Last time

Last time

We were talking about the *greatest common divisor* of two numbers, and how to calculate it.

Other ways

Other ways

Another way might be to work out all factors of one of the numbers (a, for example) and work out which of them are factors of b.

Other ways

Another way might be to work out all factors of one of the numbers (a, for example) and work out which of them are factors of b. That's also a pretty terrible way, because factorising numbers is hard work: it seems like a lot of work to find all factors of 123456789 still.

Other ways

Another way might be to work out all factors of one of the numbers (a, for example) and work out which of them are factors of b.
That's also a pretty terrible way, because factorising numbers is hard work: it seems like a lot of work to find all factors of 123456789 still.
We will see a much better way soon, but, first, let's spot some easy properties of greatest common divisors.

Properties of the gcd

Properties of the gcd

Remark

For all integers a and b, we have

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

because the definition is symmetric in a and b.

Properties of the gcd

Remark

For all integers a and b, we have

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

because the definition is symmetric in a and b.
Also, for all positive integers a, we have

$$\gcd(a, a) = a,$$

Properties of the gcd

Remark

For all integers a and b, we have

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

because the definition is symmetric in a and b.
Also, for all positive integers a, we have

$$\gcd(a, a) = a,$$

and

$$\gcd(a, 1) = 1,$$

Properties of the gcd

Remark

For all integers a and b, we have

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

because the definition is symmetric in a and b.
Also, for all positive integers a, we have

$$\gcd(a, a) = a,$$

and

$$\gcd(a, 1) = 1,$$

and

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

More properties of the gcd

More properties of the gcd

A slightly less obvious property is:

Proposition

Let a, b and k be integers. Then

$$\gcd(a, b) = \gcd(a + kb, b).$$

More properties of the gcd

A slightly less obvious property is:

Proposition

Let a, b and k be integers. Then

$$\gcd(a, b) = \gcd(a + kb, b).$$

Proof.

We'll show that the common divisors of a and b are the same as the common divisors of $a + kb$ and b.

More properties of the gcd

A slightly less obvious property is:

Proposition

Let a, b and k be integers. Then

$$\gcd(a, b) = \gcd(a + kb, b).$$

Proof.

We'll show that the common divisors of a and b are the same as the common divisors of $a + kb$ and b.
Suppose first that d is a common divisor of a and b; in other words, $d \mid a$ and $d \mid b$. Then we can write $a = md$ and $b = nd$ for some integers m and n. But then

$$a + kb = md + knd = (m + kn)d,$$

so $d \mid a + kb$, so d is a common divisor of $a + kb$ and b.

More properties of the gcd

A slightly less obvious property is:

Proposition

Let a, b and k be integers. Then

$$\gcd(a, b) = \gcd(a + kb, b).$$

Proof.

More properties of the gcd

A slightly less obvious property is:

Proposition

Let a, b and k be integers. Then

$$\gcd(a, b) = \gcd(a + kb, b).$$

Proof.

Similarly, if d is a common divisor of $a + kb$ and b, then we can write $a + kb = ld$ and $b = nd$. But then

$$a = a + kb - kb = ld - knd = (l - kn)d,$$

so $d \mid a$, so d is a common divisor of a and b.

More properties of the gcd

A slightly less obvious property is:

Proposition

Let a, b and k be integers. Then

$$\gcd(a, b) = \gcd(a + kb, b).$$

Proof.

Similarly, if d is a common divisor of $a + kb$ and b, then we can write $a + kb = ld$ and $b = nd$. But then

$$a = a + kb - kb = ld - knd = (l - kn)d,$$

so $d \mid a$, so d is a common divisor of a and b.
Since we've now proved that a and b have the same common divisors as $a + kb$ and b, it follows that they have the same *greatest* common divisor. □

Least common multiples

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\mathrm{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\mathrm{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\mathrm{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists (and is at most ab: we could find it by counting up from 1 to ab, stopping on the first common multiple).

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\mathrm{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists (and is at most ab: we could find it by counting up from 1 to ab, stopping on the first common multiple).

The last piece of terminology we might want is this:

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\mathrm{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists (and is at most ab: we could find it by counting up from 1 to ab, stopping on the first common multiple).

The last piece of terminology we might want is this:

Definition

Two integers a and b are said to be *coprime*, or *relatively prime*, if $\gcd(a, b) = 1$.

Division with remainder

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?
It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors.

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?
It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors. We can use it to make the numbers smaller; the question is, how?

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?
It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors. We can use it to make the numbers smaller; the question is, how? It turns out that this is something familiar to you all:

Division with Remainder

Division with Remainder

Proposition (Division with Remainder)

Let a and b be integers, with $b > 0$. One can write

$$a = qb + r$$

for integers q (the quotient) and r (the remainder) such that $0 \leqslant r < b$. □

Division with Remainder

Proposition (Division with Remainder)

Let a and b be integers, with $b > 0$. One can write

$$a = qb + r$$

for integers q (the quotient) and r (the remainder) such that $0 \leqslant r < b$. □

Remark

It is not too hard to prove this: one can do it with two inductions, for example, (one for the negative and one for the positive integers), but I won't do so here.

Division with Remainder

Proposition (Division with Remainder)

Let a and b be integers, with $b > 0$. One can write

$$a = qb + r$$

for integers q (the quotient) and r (the remainder) such that $0 \leqslant r < b$. □

Remark

It is not too hard to prove this: one can do it with two inductions, for example, (one for the negative and one for the positive integers), but I won't do so here.

Remark

It's reasonable to ask why we had to take $b > 0$. It's true for $b < 0$, too, we just have to say that the remainder r satisfies $0 \leqslant r < -b$ instead.

Computing GCDs

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example.

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 1 \times 70 + 56$. That means that

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 1 \times 70 + 56$. That means that

$$\begin{aligned} \gcd(126, 70) &= \gcd(56 + 1 \times 70, 70) \\ &= \gcd(56, 70) \\ &= \gcd(70, 56). \end{aligned}$$

Computing GCDs

That made the problem much smaller, and we can do the same trick repeatedly:

Computing GCDs

That made the problem much smaller, and we can do the same trick repeatedly:

$$\begin{aligned}\gcd(70, 56) &= \gcd(14 + 1 \times 56, 56) \\ &= \gcd(14, 56) \\ &= \gcd(56, 14).\end{aligned}$$

Computing GCDs

That made the problem much smaller, and we can do the same trick repeatedly:

$$\begin{aligned}\gcd(70, 56) &= \gcd(14 + 1 \times 56, 56) \\ &= \gcd(14, 56) \\ &= \gcd(56, 14).\end{aligned}$$

That's smaller still. Let's see what happens next:

Computing GCDs

That made the problem much smaller, and we can do the same trick repeatedly:

$$\begin{aligned}\gcd(70, 56) &= \gcd(14 + 1 \times 56, 56) \\ &= \gcd(14, 56) \\ &= \gcd(56, 14).\end{aligned}$$

That's smaller still. Let's see what happens next:

$$\begin{aligned}\gcd(56, 14) &= \gcd(0 + 14 \times 4, 14) \\ &= \gcd(0, 14) \\ &= 14.\end{aligned}$$

Computing GCDs

That made the problem much smaller, and we can do the same trick repeatedly:

$$\begin{aligned}\gcd(70, 56) &= \gcd(14 + 1 \times 56, 56) \\ &= \gcd(14, 56) \\ &= \gcd(56, 14).\end{aligned}$$

That's smaller still. Let's see what happens next:

$$\begin{aligned}\gcd(56, 14) &= \gcd(0 + 14 \times 4, 14) \\ &= \gcd(0, 14) \\ &= 14.\end{aligned}$$

As 56 is a multiple of 14, of course we get remainder 0, so we stop here: the greatest common divisor is 14.

Another example

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\gcd(556, 296)$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} & \gcd(556, 296) \\ = \ & \gcd(1 \times 296 + 260, 296) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} & \gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) &= \gcd(260, 296) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{gathered}\gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260)\end{gathered}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} &\gcd(556, 296) \\ &= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ &= \gcd(1 \times 260 + 36, 260) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{gathered}\gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ = \gcd(1 \times 260 + 36, 260) = \gcd(36, 260)\end{gathered}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{gathered}\gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ = \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36)\end{gathered}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} & \gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) &= \gcd(260, 296) = \gcd(296, 260) \\ = \gcd(1 \times 260 + 36, 260) &= \gcd(36, 260) = \gcd(260, 36) \\ = \gcd(7 \times 36 + 8, 36) & \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} &\gcd(556, 296) \\ &= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ &= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\ &= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{gathered}\gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ = \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\ = \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8)\end{gathered}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4) \\
&= \gcd(2 \times 4 + 0, 4)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4) \\
&= \gcd(2 \times 4 + 0, 4) = \gcd(0, 4)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4) \\
&= \gcd(2 \times 4 + 0, 4) = \gcd(0, 4) = 4.
\end{aligned}$$

Euclid's algorithm

Euclid's algorithm

Here's the general case:

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b)$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b)$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b)$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b) = \gcd(b, r),$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b) = \gcd(b, r),$$

and since $b \leqslant a$ and $r < b$ we've made our numbers smaller.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a \geqslant b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b) = \gcd(b, r),$$

and since $b \leqslant a$ and $r < b$ we've made our numbers smaller.
If we keep doing this repeatedly, we'll end up making one of the numbers zero and can stop (since $\gcd(d, 0) = d$).

Is this good?

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is.

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. One good answer (not very hard to prove) is that if you're trying to work out $\gcd(a, b)$ and $b \leqslant a$, then the number of steps you need is always less than five times the number of digits of b.

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. One good answer (not very hard to prove) is that if you're trying to work out $\gcd(a, b)$ and $b \leqslant a$, then the number of steps you need is always less than five times the number of digits of b. So working out $\gcd(123456789, 987654321)$ will take less than $5 \times 9 = 45$ divisions

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. One good answer (not very hard to prove) is that if you're trying to work out $\gcd(a, b)$ and $b \leqslant a$, then the number of steps you need is always less than five times the number of digits of b. So working out $\gcd(123456789, 987654321)$ will take less than $5 \times 9 = 45$ divisions (actually, this one takes a lot less than 45, if you try it).

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. One good answer (not very hard to prove) is that if you're trying to work out $\gcd(a, b)$ and $b \leqslant a$, then the number of steps you need is always less than five times the number of digits of b. So working out $\gcd(123456789, 987654321)$ will take less than $5 \times 9 = 45$ divisions (actually, this one takes a lot less than 45, if you try it). Compared with the other methods we discussed, this makes it seem really good.

Better yet

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n.

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b).

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b). This will be really useful later: I promise!

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b). This will be really useful later: I promise!
Let's see how this works with an example.

Better yet

Euclid's algorithm is in fact even more useful than it looks: using Euclid's algorithm, if we have $\gcd(a, b) = d$, that enables us to write d in the form $ma + nb = d$ for some integers m and n. (We say that we're writing it as a *linear combination* of a and b). This will be really useful later: I promise!

Let's see how this works with an example. We saw earlier that $\gcd(126, 70) = 14$, so we expect to be able to find integers m and n such that $126m + 70n = 14$.

The calculation

The calculation

Along the way we found that:

The calculation

Along the way we found that:

$$126 = 1 \times 70 + 56, \qquad (1)$$

The calculation

Along the way we found that:

$$126 = 1 \times 70 + 56, \quad (1)$$
$$70 = 1 \times 56 + 14. \quad (2)$$

Working through that backwards, we get that

The calculation

Along the way we found that:

$$126 = 1 \times 70 + 56, \qquad (1)$$
$$70 = 1 \times 56 + 14. \qquad (2)$$

Working through that backwards, we get that

$$14 = 1 \times 70 - 1 \times 56 \qquad \text{(using (2))}$$

The calculation

Along the way we found that:

$$\begin{aligned} 126 &= 1 \times 70 + 56, && (1) \\ 70 &= 1 \times 56 + 14. && (2) \end{aligned}$$

Working through that backwards, we get that

$$\begin{aligned} 14 &= 1 \times 70 - 1 \times 56 && \text{(using (2))} \\ &= 1 \times 70 - 1 \times (1 \times 126 - 1 \times 70) && \text{(using (1))} \end{aligned}$$

The calculation

Along the way we found that:

$$\begin{aligned} 126 &= 1 \times 70 + 56, && (1) \\ 70 &= 1 \times 56 + 14. && (2) \end{aligned}$$

Working through that backwards, we get that

$$\begin{aligned} 14 &= 1 \times 70 - 1 \times 56 && \text{(using (2))} \\ &= 1 \times 70 - 1 \times (1 \times 126 - 1 \times 70) && \text{(using (1))} \\ &= 2 \times 70 - 1 \times 126. \end{aligned}$$

Another calculation

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$556 = 1 \times 296 + 260, \qquad (3)$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$556 = 1 \times 296 + 260, \quad (3)$$

$$296 = 1 \times 260 + 36, \quad (4)$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3) \\ 296 &= 1 \times 260 + 36, && (4) \\ 260 &= 7 \times 36 + 8, && (5) \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3) \\ 296 &= 1 \times 260 + 36, && (4) \\ 260 &= 7 \times 36 + 8, && (5) \\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3) \\ 296 &= 1 \times 260 + 36, && (4) \\ 260 &= 7 \times 36 + 8, && (5) \\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$4 = 36 - 4 \times 8 \qquad \text{(using (6))}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3) \\ 296 &= 1 \times 260 + 36, && (4) \\ 260 &= 7 \times 36 + 8, && (5) \\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))} \\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))} \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3) \\ 296 &= 1 \times 260 + 36, && (4) \\ 260 &= 7 \times 36 + 8, && (5) \\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))} \\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))} \\ &= 29 \times 36 - 4 \times 260 \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3) \\ 296 &= 1 \times 260 + 36, && (4) \\ 260 &= 7 \times 36 + 8, && (5) \\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))} \\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))} \\ &= 29 \times 36 - 4 \times 260 \\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))} \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3) \\ 296 &= 1 \times 260 + 36, && (4) \\ 260 &= 7 \times 36 + 8, && (5) \\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))} \\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))} \\ &= 29 \times 36 - 4 \times 260 \\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))} \\ &= 29 \times 296 - 33 \times 260 \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260\\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))}\\ &= 29 \times 296 - 33 \times 260\\ &= 29 \times 296 - 33 \times (556 - 296) && \text{(using (3))} \end{aligned}$$

Another calculation

Similarly, when we calculated that $\gcd(556, 296) = 4$, we found that:

$$\begin{aligned} 556 &= 1 \times 296 + 260, && (3)\\ 296 &= 1 \times 260 + 36, && (4)\\ 260 &= 7 \times 36 + 8, && (5)\\ 36 &= 4 \times 8 + 4. && (6) \end{aligned}$$

This means that

$$\begin{aligned} 4 &= 36 - 4 \times 8 && \text{(using (6))}\\ &= 36 - 4 \times (260 - 7 \times 36) && \text{(using (5))}\\ &= 29 \times 36 - 4 \times 260\\ &= 29 \times (296 - 260) - 4 \times 260 && \text{(using (4))}\\ &= 29 \times 296 - 33 \times 260\\ &= 29 \times 296 - 33 \times (556 - 296) && \text{(using (3))}\\ &= 62 \times 296 - 33 \times 556. \end{aligned}$$