MAS114: Lecture 10

James Cranch

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

2020–2021

Coprimality

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, it's going to turn out to be really useful to consider two numbers and compare their factors.

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, it's going to turn out to be really useful to consider two numbers and compare their factors.

Definition

Let a and b be integers. A *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$.

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, it's going to turn out to be really useful to consider two numbers and compare their factors.

Definition

Let a and b be integers. A *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$. The *greatest common divisor* of a and b, written $\gcd(a, b)$ (or sometimes as $\mathrm{hcf}(a, b)$ or sometimes even just (a, b) for short) is the largest common divisor of a and b.

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, it's going to turn out to be really useful to consider two numbers and compare their factors.

Definition

Let a and b be integers. A *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$. The *greatest common divisor* of a and b, written $\gcd(a, b)$ (or sometimes as $\operatorname{hcf}(a, b)$ or sometimes even just (a, b) for short) is the largest common divisor of a and b.

Remark

That definition probably just says that a greatest common divisor is what you'd expect it to be, given the name!

Warning!

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function.

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):*

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function.
There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every integer, and so will certainly be a common divisor.

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every integer, and so will certainly be a common divisor.
- *There may be lots of common divisors, but no largest one.*

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function.

There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every integer, and so will certainly be a common divisor.
- *There may be lots of common divisors, but no largest one.* For nonzero integers a, it's easy to see that if $d \mid a$ then $|d| \leqslant |a|$, which means we can't get arbitrarily large divisors

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every integer, and so will certainly be a common divisor.
- *There may be lots of common divisors, but no largest one.* For nonzero integers a, it's easy to see that if $d \mid a$ then $|d| \leqslant |a|$, which means we can't get arbitrarily large divisors. . . but $\gcd(0, 0)$ doesn't exist.

Finding GCDs

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important.

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we could just count down from $|a|$ and stop when we reach the first common divisor.

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we could just count down from $|a|$ and stop when we reach the first common divisor.

For example,

$$\gcd(9, 15) =$$

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we could just count down from $|a|$ and stop when we reach the first common divisor.

For example,

$$\gcd(9, 15) = 3$$

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we could just count down from $|a|$ and stop when we reach the first common divisor.
For example,

$$\gcd(9, 15) = 3$$

and

$$\gcd(-30, 42) =$$

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we could just count down from $|a|$ and stop when we reach the first common divisor.

For example,

$$\gcd(9, 15) = 3$$

and

$$\gcd(-30, 42) = 6.$$

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we could just count down from $|a|$ and stop when we reach the first common divisor.
For example,

$$\gcd(9, 15) = 3$$

and

$$\gcd(-30, 42) = 6.$$

This approach to finding greatest common divisors is pretty terrible:

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we could just count down from $|a|$ and stop when we reach the first common divisor.

For example,

$$\gcd(9, 15) = 3$$

and

$$\gcd(-30, 42) = 6.$$

This approach to finding greatest common divisors is pretty terrible: imagine being asked to find

$$\gcd(123456789, 987654321)$$

by this approach!

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* $\operatorname{lcm}(a, b)$ 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* $\text{lcm}(a, b)$ 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* $\operatorname{lcm}(a, b)$ 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

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

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

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

Another example

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

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

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

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

Another example

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

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

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

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