MAS114: Lecture 11

James Cranch

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

2020–2021

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

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

A general recipe

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

This is a decreasing sequence, and eventually we will get $a_k = 0$ for some k; we can't divide by zero, so we end the sequence there.

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

This is a decreasing sequence, and eventually we will get $a_k = 0$ for some k; we can't divide by zero, so we end the sequence there. We then have

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{k-1}, 0) = a_{k-1}.$$

A general recipe

In general, if we have positive integers a and b, with $a > b$, we can start defining a sequence $a_0, a_1, \ldots$ as follows:

- $a_0 = a$,
- $a_1 = b$,
- a_{n+2} is the remainder upon dividing a_n by a_{n+1}:

$$a_n = q_n a_{n+1} + a_{n+2}.$$

This is a decreasing sequence, and eventually we will get $a_k = 0$ for some k; we can't divide by zero, so we end the sequence there. We then have

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{k-1}, 0) = a_{k-1}.$$

Let's write $d = \gcd(a, b)$ for this.

A general recipe

A general recipe

Now, we have $a_{k-3} = q_{k-3}a_{k-2} + a_{k-1}$, so $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$, so we can write d as a linear combination of a_{k-3} and a_{k-2}.

A general recipe

Now, we have $a_{k-3} = q_{k-3}a_{k-2} + a_{k-1}$, so $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$, so we can write d as a linear combination of a_{k-3} and a_{k-2}.
We have $a_{k-4} = q_{k-4}a_{k-3} + a_{k-2}$, so $a_{k-2} = a_{k-4} - q_{k-4}a_{k-3}$, so substituting in we can write d as a linear combination of a_{k-4} and a_{k-3}.

A general recipe

Now, we have $a_{k-3} = q_{k-3}a_{k-2} + a_{k-1}$, so $a_{k-1} = a_{k-3} - q_{k-3}a_{k-2}$, so we can write d as a linear combination of a_{k-3} and a_{k-2}.
We have $a_{k-4} = q_{k-4}a_{k-3} + a_{k-2}$, so $a_{k-2} = a_{k-4} - q_{k-4}a_{k-3}$, so substituting in we can write d as a linear combination of a_{k-4} and a_{k-3}.
Proceeding in this way, we end up with d as a linear combination of a_0 and a_1: in other words, of a and b.

Bezout's Lemma

Bezout's Lemma

We've proved the following:

Bezout's Lemma

We've proved the following:

Proposition (Bezout's Lemma)

Let a and b be two integers with $\gcd(a, b) = d$.

Bezout's Lemma

We've proved the following:

Proposition (Bezout's Lemma)

Let a and b be two integers with $\gcd(a, b) = d$. Then there are integers m and n such that $ma + nb = d$. □

A better version

A better version

In fact, slightly more is true:

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

Proof.

The "if" part: We must prove that, if $d \mid e$, then we can write e as a linear combination of a and b.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

Proof.

The "if" part: We must prove that, if $d \mid e$, then we can write e as a linear combination of a and b.
However, since $d \mid e$, we can write $e = dk$ for some k. Also, by the above Proposition we can write $d = ma + nb$ for some m and n. But then

$$e = dk = (mk)a + (nk)b,$$

as required.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

Proof.

A better version

In fact, slightly more is true:

Proposition

Let a and b be two integers with $\gcd(a, b) = d$. Then, for an integer e, we can write e in the form $e = ma + nb$ if and only if $d \mid e$.

Proof.

The "only if" part: We must prove that if $e = ma + nb$, then $d \mid e$. But, since $d = \gcd(a, b)$ we have $d \mid a$ and $d \mid b$, and hence also $d \mid ma$ and $d \mid nb$, and therefore $d \mid ma + nb$ as required. □