Week 1, lecture 2:
Euclid’s Algorithm
MA180/185/190 Algebra

Angela Carnevale

Introduction to Modular Arithmetic

Modular arithmetic

Prime numbers

Certain numbers with very few divisors hold a special place throughout mathematics (and everything else!).

Definition (prime number)

We say that a number $p \in \mathbb{N}$ with $p > 1$ is a **prime number** if its only positive divisors are 1 and p itself.

Coprime numbers

Definition (coprime numbers)

We say that two numbers a and b are **coprime** if their greatest common divisor is 1, that is if $\gcd(a, b) = 1$.

"2 does not divide 105"

Example.

- 105 and 64 are coprime.

Indeed, $64 = 2^6$ and $2 \nmid 105$

Coprime numbers

Definition (coprime numbers)

We say that two numbers a and b are **coprime** if their greatest common divisor is 1, that is if $\gcd(a, b) = 1$.

Example.

- 105 and 64 are coprime.
- What about 2023 and 64?

again 2023 is odd and 64 is divisible by 2 and its powers...

Coprime numbers

Definition (coprime numbers)

We say that two numbers a and b are **coprime** if their greatest common divisor is 1, that is if $\gcd(a, b) = 1$.

Example.

- 105 and 64 are coprime.
- What about 2023 and 64? And 2023 and 1700?

Remainder theorem

Theorem

Let $a, b \in \mathbb{Z}$, $b > 0$. There are unique integers q and r such that

$$a = bq + r$$

where $0 \leq r < b$.

Example.

- $a = 29$, $b = 7$

  here: $29 = 7 \cdot 4 + 1$ note $r = 1$ so $0 \leq r < b$

- If $b \mid a$ then $a = b \cdot q$ so $r = 0$ in that case

Remainder theorem

Theorem

Let $a, b \in \mathbb{Z}$, $b > 0$. There are unique integers q and r such that

$$a = bq + r$$

where $0 \leq r < b$.

Fact. If $a = bq + r$ as above, then $\gcd(a, b) = \gcd(b, r)$.

Example: $a = \overset{3\cdot 13}{\overset{\shortparallel}{39}}$, $b = \overset{3\cdot 5}{\overset{\shortparallel}{15}}$

$\gcd(39, 15) = 3$

$\wr$ ✓

$\gcd(15, 9) = 3$

Also, by the thm

$$\underset{a}{39} = \underset{b}{15} \cdot \underset{q}{2} + \underset{r}{9}$$

Remainder theorem

Theorem

Let $a, b \in \mathbb{Z}$, $b > 0$. There are unique integers q and r such that

$$a = bq + r$$

where $0 \le r < b$.

Fact. If $a = bq + r$ as above, then $\gcd(a, b) = \gcd(b, r)$.

why?

$$r = a - b\cdot q \underset{\substack{\uparrow \\ \text{since } d \mid a \\ d \mid b}}{=} d\cdot k - d\cdot m\cdot q = d\cdot(k - m\cdot q)$$

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

Euclid's algorithm

Combining the previous theorem and fact, we get an algorithm to compute the greatest common divisor of any two (positive) integers.

Example. Let's take again $a = 39$ and $b = 15$

We use the remainder theorem to write:

$$39 = 15 \cdot 2 + 9$$

We now apply the remainder theorem again, this time to b and r:

$15 = 9 \cdot 1 + 6$ and again...

$9 = 6 \cdot 1 + 3$ and again...

$6 = 3 \cdot 2 + 0$ The last non-zero remainder is $\gcd(39, 15)$

Euclid's algorithm: formally…

Let $a, b \in \mathbb{N}$ such $a \geq b$ and $b \neq 0$. We can assume $a > b$ (otherwise we simply have $\gcd(a, b) = a$.)

We can compute $\gcd(a, b)$ as follows:

- Use the Remainder theorem to write

$$a = bq + r \quad \text{with} \quad 0 \leq r < b.$$

- If $b = 0$ then $\gcd(a, b) = b$ and we are done. If $r \neq 0$ then repeat the procedure with b and r and so on.
- The last non-zero remainder is $\gcd(a, b)$.

Exercises

As an exercise, use Euclid's algorithm to compute the following:

- $\gcd(35, 65)$
- $\gcd(144, 360)$
- $\gcd(595, 2023)$

Applications: linear equations with integer solutions

One of our challenging problems from the beginning required that we find integer solutions to an equation with two variables and integer coefficients. That is, given some natural numbers a, b, c, we want to find $x, y \in \mathbb{Z}$ such that

$$ax + by = c.$$

It is natural to ask whether a solution to the above can be found and, if so, how many such solutions exist.

As it turns out, this is very much related to the $\gcd(a, b)$ and to Euclid's algorithm itself.

Euclid's algorithm…backwards

Say that we want to write the number 3 as a linear integer combination of 39 and 15. That is, we want to find $x, y \in \mathbb{Z}$ such that

$$39x + 15y = 3$$

Recall the steps done to compute $\gcd(39, 15)$ with Euclid's algorithm:

(here we stop at the last non-zero remainder)

$$\left.\begin{aligned} 39 &= 15 \cdot 2 + 9 \\ 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \end{aligned}\right\} \rightarrow$$

we can use each of these identities to write (at each step) the remainder as a combination of the other two numbers.

we start with 3 and at each step we (back) substitute the expression we get from the previous step:

Euclid's algorithm. . . backwards

$3 = 9 - 6\cdot 1$

here we now substitute an expression for 6 obtained from the previous step in Euclid's algorithm.

$$= 9 - (15 - 9\cdot 1) = 9 - 15 + 9 = 9\cdot 2 - 15$$

Note how instead of working out the products/sums, we keep the numbers 9 and 15 in the expression, so we can again use back-substitution to get an expression involving 15 and 39.

We now replace 9 with the corresponding expression from the first step of the algorithm:

$$= \overbrace{(39 - 15\cdot 2)}^{\text{this is the expression for 9 from the first step}}\cdot 2 - 15 =$$

← now we collect all the terms involving 15 and all those involving 39 together

$$= 39\cdot 2 - 15\cdot 5$$

So we can write $\boxed{3 = 39\cdot 2 - 15\cdot 5}$

Euclid's algorithm… backwards

Another example. First, let's compute gcd(105, 64). We have observed that they are coprime and we can now verify it by means of our algorithm.

$$105 = 64 \cdot 1 + 41$$

$$64 = 41 \cdot 1 + 23$$

$$41 = 23 \cdot 1 + 18$$

$$23 = 18 \cdot 1 + 5$$

$$18 = 5 \cdot 3 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + \underline{\underline{1}}$$

$$2 = 1 \cdot 2 + 0$$

Back substituting:

$$
\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3 \cdot 1) = 3 - 5 + 3 = 3 \cdot 2 - 5 \\
&= (18 - 5 \cdot 3) \cdot 2 - 5 = \\
&= 18 \cdot 2 - 5 \cdot 6 - 5 = 18 \cdot 2 + 5 \cdot (-7) \\
&= 18 \cdot 2 + (23 - 18) \cdot (-7) \\
&= 18 \cdot 2 - 23 \cdot 7 + 18 \cdot 7 = 18 \cdot 9 + 23 \cdot (-7) \\
&= (41 - 23) \cdot 9 + 23 \cdot (-7) = 41 \cdot 9 - 23 \cdot 9 - 23 \cdot 7 = 41 \cdot 9 + 23 \cdot (-16) \\
&= 41 \cdot 9 + (64 - 41) \cdot (-16) = 41 \cdot 25 + 64 \cdot (-16) \\
&= (105 - 64) \cdot 25 + 64 \cdot (-16) = 105 \cdot 25 + 64 \cdot (-41)
\end{aligned}
$$

So we can write 1 as an integer combination of 105 and 64 as follows:

$$1 = 105 \cdot 25 + 64 \cdot (-41)$$