Lecture 2.2

Last time:

- There are infinitely many primitive Pyth. triples (a,b,c) corresponding to rational points $(x,y) = \left(\frac{a}{c}, \frac{b}{c}\right)$ on the unit circle

$$C: \ x^2 + y^2 = 1.$$

- Properties of the integers $\mathbb{Z}$ can be derived from the Axioms of Arithmetic.

- $d \mid n$ if $n = dk$ for some $k \in \mathbb{Z}$.

- $a \equiv b \pmod{d}$ if $d \mid (b-a)$.

- For $a, b \in \mathbb{N}$, $d = \gcd(a,b)$ if $d \mid a$, $d \mid b$ and $d \geq e$ for any $e \in \mathbb{N}$ such that $e|a$ and $e|b$.

The Division Algorithm

Theorem (Division Algorithm) For any $n, d \in \mathbb{N}$, there are unique $q, r \in \mathbb{Z}$ with $0 \leq r < d$ such that $n = dq + r$.

Think: $\frac{n}{d} = q + \frac{r}{d}$.

what about $d=1$?

Pf: Fix $d \geq 2$ and consider the set

$$S = \{ n \in \mathbb{N} \mid n = dq + r,\ q \in \mathbb{Z},\ 0 \leq r < d \}.$$

Then $1 \in S$: $1 = d \cdot 0 + 1$.

To induct, suppose $n \in S$, so that

$$n = dq + r \quad \text{for } q \in \mathbb{Z},\ 0 \leq r < d.$$

If $r + 1 = d$ then

$$n + 1 = dq + r + 1 = dq + d = d(q+1) + 0.$$

Otherwise $r + 1 < d$ and

$$n + 1 = dq + (r + 1)$$

with $q \in \mathbb{Z}$ and $0 \leq r + 1 < d$.

Exercise 1: Prove the uniqueness portion of the Theorem.

$\boxed{\text{Ex}}$

$$25 = 7 \cdot 3 + 4$$

$$33 = 11 \cdot 3 + 0$$

$$33 = 22 \cdot 1 + 11$$

This method of division lets us find greatest common divisors efficiently.

Lemma If $a, b, q, r \in \mathbb{Z}$ with

$$a = bq + r$$

then $\gcd(a,b) = \gcd(b,r)$.

Pf: Let $d = \gcd(a,b)$ and write

$$a = dj \quad \text{and} \quad b = dk, \quad j, k \in \mathbb{Z}.$$

Then

$$r = a - bq = dj - dkq$$

$$= d(j - kq)$$

so $d \mid r$.

If $e \mid b$ and $e \mid r$, say with

$$b = el \text{ and } r = em, \quad l, m \in \mathbb{Z},$$

then we have

$$\begin{aligned} a = bq + r &= elq + em \\ &= e(lq + m). \end{aligned}$$

This shows $e \mid a$, so $e \leq d$ since

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

Hence $d = \gcd(b, r)$. $\square$

$\boxed{\text{Theorem (Euclidean Algorithm)}}$ For any $a, b \in \mathbb{Z}$, not both 0, if $d = \gcd(a,b)$ then there is a sequence

$$
\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\ \vdots \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}
$$

with $r_n = d$.

Pf: Given such a sequence, the Lemma says

Lemma says

$$\begin{aligned} d = \gcd(a,b) &= \gcd(b, r_1) \\ &= \gcd(r_1, r_2) \\ &\;\vdots \\ &= \gcd(r_{n-1}, r_n) = r_n . \end{aligned}$$

To construct such a sequence, use the Division Algorithm in each step, so that

$$b > r_1 > r_2 > \cdots > r_{n-1} > r_n > 0.$$

There are only finitely many natural numbers less than b, so this process terminates in a finite number of

steps. $\square$

$\boxed{\text{Ex}}$ 1 $a = 112, \quad b = 96$

$112 = 96 \cdot 1 + 16$ ← $\gcd(112, 96)$

$96 = 16 \cdot 6 + 0$

2 $a = 162, \quad b = 31$

$162 = 31 \cdot 5 + 7$

$31 = 7 \cdot 4 + 3$

$7 = 3 \cdot 2 + 1$ ← $\gcd(162, 31)$

$3 = 1 \cdot 3 + 0$

So 162 and 31 are relatively

prime. (Faster proof: 31 is prime and $31 \nmid 162$.)

Notice that we can write

$$162x + 31y = 1$$

by rewriting 1 using the work above:

$$1 = 7 - 3 \cdot 2 = 7 - (31 - 7 \cdot 4) \cdot 2$$

$$= 7 \cdot 9 - 31 \cdot 2 = (162 - 31 \cdot 5) \cdot 9 - 31 \cdot 2$$

$$= 162 \cdot 9 - 31 \cdot 47.$$

Theorem For any $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ if and only if there are $x, y \in \mathbb{Z}$

with $ax + by = 1$.

Pf : ($\Rightarrow$) Suppose $\gcd(a,b) = 1$. By the Euclidean Algorithm, there is a sequence

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + 1$$

with $1 < r_{n-1} < r_{n-2} < \dots < r_1 < b$.

If $n = 1$, i.e. if $a = bq + 1$, then

$$1 = a - bq.$$

To induct, suppose the property holds for all a, b with a sequence of length N and $r_N = 1$.

Suppose a, b have a sequence of length $N+1$, with $r_{N+1} = 1$.

Then b and r_1 have a sequence of length N with smallest remainder 1, so by induction, for some $x', y' \in \mathbb{Z}$,

$$\begin{aligned} 1 &= bx' + r_1 y' \\ &= bx' + (a - bq_1)y' \end{aligned}$$

$= ay' + b(x' - q_1 y')$.

Setting $x = y'$ and $y = x' - q_1 y'$

gives us $ax + by = 1$.

($\Leftarrow$) If $ax + by = 1$ and $d \mid a$

and $d \mid b$, then d also divides

ax, by and therefore $ax + by$.

Therefore $d = 1$. $\square$

This says we can solve linear equations

of the form $ax + by = 1$ using

the Euclidean Algorithm.

Ex 3 Let's write

$$3x + 17y = 1$$

for some $x, y \in \mathbb{Z}$.

We know $\gcd(3,17) = 1$ because they're both prime, but explicitly:

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1 \leftarrow \gcd(3,17)$$

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

Working backwards,

$$1 = 3 - 2 \cdot 1 = 3 - (17 - 3 \cdot 5) \cdot 1$$

$$= 3 \cdot 6 - 17 \cdot 1$$

so $x = 6, \ y = -1.$

(4) Is it possible to write

$$34x + 255y = 1$$

for some $x, y \in \mathbb{Z}$? Let's compute $\gcd(34, 255)$:

$$255 = \overset{238}{34 \cdot 7} + 17 \qquad \gcd(34, 255)$$

$$34 = 17 \cdot 2 + 0.$$

Since the gcd is 17, no such $x, y \in \mathbb{Z}$ can be found.

5 How about $a = 1728$, $b = 1729$?

Notice $1729 = 1728 \cdot 1 + 1$

$1728 = 1 \cdot 1728 + 0$

So $\gcd(1728, 1729) = 1$ and it is possible to solve the linear equation:

$$-1728 + 1729 = 1.$$

$\boxed{\text{Corollary}}$ For any $n \in \mathbb{N}$, $\gcd(n, n+1) = 1$.

Pf: Same proof as 5. $\square$

Q: Does the Theorem have a converse? That is, if

$$ax + by = d$$

for some $x, y \in \mathbb{Z}$.

A: Definitely not! If

$$ax + by = 1$$

has a solution $x, y \in \mathbb{Z}$, then

$$ax' + by' = d$$

has a solution for all $d \geq 2$,

namely $x' = dx$ $y' = dy$

Next time: linear equations and the gcd.