Today: HW4 discussion
& More (?)

Problem 2: Recall that

$$\gcd(a,b) = \max\{d \in \mathbb{Z} : d|a \ \& \ d|b\}.$$

On HW3, you showed that $\exists\, x,y \in \mathbb{Z}$ (not unique) such that

$$ax + by = d. \quad \text{(Bézout)}$$

By definition, since $d|a$ & $d|b$ we have $a = da'$ & $b = db'$ for some $a', b' \in \mathbb{Z}$. I claim that

$$\gcd(a',b') = 1$$
$$\text{"} \gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1 \text{"}$$

How to prove this? Let $e \in \mathbb{Z}$ be any common divisor of a' & b', say $a' = ea''$ & $b' = eb''$ where $a'', b'' \in \mathbb{Z}$.

We will show that $e \leq 1$.

To do this, observe:

$$ax + by = d$$

$$da'x + db'y = d$$

$$d(a'x + b'y) = d$$

$$a'x + b'y = 1$$

$$ea'' x + eb'' y = 1$$

$$e(a''x + b''y) = 1$$

$a''x + b''y$: some integer

$$e \mid 1.$$

$\Rightarrow e = \pm 1$

In other words, ± 1 are the only common divisors of a' & b'.

$\Rightarrow \gcd(a', b') = 1.$ ✓

Summary: If we cancel the gcd of two numbers, then they became "coprime"

Problem 3: When we proved unique prime factorization, we used the fact that for all $a, b, c \in \mathbb{Z}$:

$$a \mid bc \;\&\; \gcd(a,b) = 1 \implies a \mid c.$$

This is called "Euclid's Lemma." Now we will prove it.

Proof: Since $a \mid bc$ we have $ak = bc$ for some $k \in \mathbb{Z}$. Also, since $\gcd(a,b) = 1$ we have $ax + by = 1$ for some $x, y \in \mathbb{Z}$. It follows that

$$\begin{aligned} ax + by &= 1 \\ c(ax + by) &= c \\ acx + bcy &= c \\ acx + aky &= c \\ a(\underbrace{cx + ky}_{\text{some integer}}) &= c \implies a \mid c \end{aligned}$$

✓

Problem 4: Application of Euclid's Lemma, called "Rational Root Test." Consider

$$f(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x].$$

If $f(\alpha) = 0$ for some $\alpha \in \mathbb{Q}$, let's write α in lowest terms:

$$\alpha = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad \gcd(a,b) = 1.$$

Then $f(a/b) = 0$

$$c_n \left(\frac{a}{b}\right)^n + \cdots + c_1 \left(\frac{a}{b}\right) + c_0 = 0$$

$$c_n a^n + c_{n-1} a^{n-1} b + \cdots + \underline{c_1 a b^{n-1}} + c_0 b^n = 0$$

Pull $c_0 b^n$ to one side:

$$c_0 b^n = -c_n a^n + -c_{n-1} a^{n-1} b - \cdots - c_1 a b^{n-1}$$

$$= a \left[\underbrace{-c_n a^{n-1} - c_n a^{n-2} b - \cdots - c_1 b^{n-1}}_{\text{some integer.}} \right]$$

$\Rightarrow a \mid c_0 b^n$

Since $\gcd(a,b) = 1$, we also have $\gcd(a, b^n) = 1$ [think...], hence

$\underset{\text{Euclid}}{\Rightarrow} a \mid c_0$ ✓

A similar argument shows that

$$b \mid c_n .$$

□

So what?

Consider $f(x) = 4x^3 - 12x^2 + 11x - 3$.

What are the rational roots?

If $f(\frac{a}{b}) = 0$ for some $\gcd(a,b) = 1$, the RRT says that $a \mid 3$ & $b \mid 4$.

This leads to a small number of potential rational roots:

$$\frac{a}{b} \in \left\{ \pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{3}{2}, \pm \frac{1}{4}, \pm \frac{3}{4} \right\}.$$

By direct checking, we can show that

$1, \frac{1}{2}, \frac{3}{2}$ are actual roots.

Luckily, all three roots of $f(x)$ are rational, so we find

$$f(x) = (x-1)(x-\tfrac{1}{2})(x-\tfrac{3}{2})4 .$$

Note: This method does not help to find non-rational roots. //

Problem 5: Application. We will show

$$\cos\left(\frac{2\pi}{7}\right) \notin \mathbb{Q} .$$

TRICKY. Let $\omega = e^{2\pi i/7}$ so

$$\omega + \omega^{-1} = 2\cos\left(\frac{2\pi}{7}\right)$$

Call this $\alpha := \omega + \omega^{-1}$.

If we can show $\alpha \notin \mathbb{Q}$, it will follow that $\cos\left(\frac{2\pi}{7}\right) = \frac{\alpha}{2} \notin \mathbb{Q}$.

Strategy: Find a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Use RRT to show $f(x)$ has no rational roots. Hence $\alpha \notin \mathbb{Q}$.

$$
\begin{aligned}
1 &= 1 \\
\alpha &= \omega + 0 + \omega^{-1} \\
\alpha^2 &= \omega^2 + 0 + 2 + 0 + \omega^{-2} \\
\alpha^3 &= \omega^3 + 0 + 3\omega + 0 + 3\omega^{-1} + 0 + \omega^{-3}
\end{aligned}
$$

[Remark: $(\omega + \omega^{-1})^2 = \omega^2 + 2\omega\omega^{-1} + (\omega^{-1})^2$
$= \omega^2 + 2 + \omega^{-2}$.]

Recall: $1 + \omega + \omega^2 + \cdots + \omega^6 = 0$

$1 + \omega + \omega^2 + \omega^3 + \omega^{-3} + \omega^{-2} + \omega^{-1} = 0$.

Algorithm:

$\alpha^3 + \alpha^2 = (\omega^3 + \omega^{-3}) + 3\omega + 2 + 3\omega^{-1} + (\omega^2 + \omega^{-2})$

$\alpha^3 + \alpha^2 - 2\alpha = \checkmark + \omega + 2 + \omega^{-1} + \checkmark$

$\alpha^3 + \alpha^2 - 2\alpha - 1 =$ ✓ $= 0$

$$\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$$

$$f(\alpha) = 0$$

where $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Z}[x]$.

But this $f(x)$ has no rational roots. To see this, let

$$f\left(\frac{a}{b}\right) = 0, \quad \gcd(a,b) = 1$$

Then RRT: $b \mid 1$ & $a \mid 1$.

$$\Rightarrow \frac{a}{b} = \pm 1$$

But $f(1) \neq 0$

$f(-1) \neq 0$.

QED.

Skip Problem 6 for now.

Return to Fermat's problem:

$$x^4 + a^4 = 0.$$

$$x^4 = -a^4$$

$$\Rightarrow x = a\left(\frac{\pm 1 \pm i}{\sqrt{2}}\right).$$

Group roots into complex conj pairs:

$$x^4 + a^4 = \left(x - a\left(\frac{1+i}{\sqrt{2}}\right)\right)\left(x - a\left(\frac{1-i}{\sqrt{2}}\right)\right)$$

$$\cdot \left(x - a\left(\frac{-1+i}{\sqrt{2}}\right)\right)\left(x - a\left(\frac{-1-i}{\sqrt{2}}\right)\right)$$

$$= \left(x^2 - a\sqrt{2}\,x + a^2\right)\left(x^2 + a\sqrt{2}\,x + a^2\right)$$

It factors over $\mathbb{R}$!