HW 5 due Friday, beginning of class.

Last time: "Modular Arithmetic"

Fix some $m \in \mathbb{Z}$, $m \neq 0$.

For all $a, b \in \mathbb{Z}$ define

$$a \underset{m}{\sim} b \iff m \mid (a-b) \quad \text{(Gauss, 1800)}$$

$$\mathbb{Z}_m := \left(\mathbb{Z}, +, \cdot, 0, 1, \underset{m}{\sim}\right)$$

is a ring. Every $n \in \mathbb{Z}$ has standard form

$$n \underset{m}{\sim} r, \quad r \text{ unique remainder of } n \text{ modulo } m.$$

Theorem: Given $a \in \mathbb{Z}_m$, $\exists\, b \in \mathbb{Z}_m$ such that $ab \underset{m}{\sim} 1$ if and only if $\gcd(a, m) = 1$.

e.g. Consider $5 \in \mathbb{Z}_7$. Since $\gcd(5,7) = 1$ we know $\exists\, x, y \in \mathbb{Z}$ with

$$5x + 7y = 1. \quad \text{(Bézout)}$$

Trial-and-error:

$5(3) + 7(-2) = 1$ ✓

$5(3) + \cancel{7}^{0}(-2) \overset{\sim}{7} 1$

$5 \cdot 3 \overset{\sim}{7} 1$ ✓

"$\frac{1}{5}$" $\overset{\sim}{7}$ 3. ///

Corollary: If $p \in \mathbb{Z}$ is prime then $\mathbb{Z}_p$ is a field.

In fact this construction generalizes to any "Euclidean Domain."

Example: Given $m(x) \in \mathbb{F}[x]$

$f(x) \tilde{m} g(x) \iff m(x) \mid [f(x) - g(x)]$

Get a ring

$\mathbb{F}[x]_m = (\mathbb{F}[x], +, \cdot, 0, 1, \tilde{m})$

If $p(x) \in \mathbb{F}[x]$ is a prime polynomial

then the ring $\mathbb{F}[x]_p$ is a field.

Cauchy construction of $\mathbb{C}$. (1847)

What is "i"?

Answer: formal symbol satisfying

$$i^2 = -1.$$

Cauchy gave a rigorous treatment of idea.

Definition: $\mathbb{C} := \mathbb{R}[x]_{x^2+1}$

Since $x^2+1 \in \mathbb{R}[x]$ is prime, we know that this $\mathbb{C}$ is a field.

Since $\deg(x^2+1) = 2$ we know every element of $\mathbb{C}$ has the form

$a+bx$ for some unique $a, b \in \mathbb{R}$.

Where is "i"?

[Aside: If $m(x) \in \mathbb{F}[x]$ has $\deg(m) = n$ then for all $f(x) \in \mathbb{F}[x]$ we

can write

$$f(x) \underset{m}{\sim} a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

for some unique $a_i \in \mathbb{F}$.

Proof: Uniqueness of remainder mod $m(x)$.]

Observe: $x^2 + 1 \underset{x^2+1}{\sim} 0$

$$x^2 \underset{x^2+1}{\sim} -1 .$$

The abstract symbol "x" is our version of "i".

Since $\mathbb{R}[x]_{x^2+1}$ is a field we know it is possible to divide by any nonzero element:

$$\frac{1}{a+bx} \underset{x^2+1}{\sim} c + dx$$

for some unique $c, d \in \mathbb{R}$.

Of course: $c = \dfrac{a}{a^2+b^2}$ & $d = \dfrac{-b}{a^2+b^2}$.

Another example:

$x^3-2 \in \mathbb{Q}[x]$ is prime, hence

$$\mathbb{Q}[x]_{x^3-2} = \{a+bx+cx^2 : a,b,c \in \mathbb{Q}\}/\sim_{x^3-2}$$

is a field. This means we can divide:

$$\frac{1}{a+bx+cx^2} \sim_{x^3-2} (?) + (?)x + (?)x^2$$

compute!

$$\frac{1}{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} = d + e\sqrt[3]{2} + f(\sqrt[3]{2})^2$$

exist & are unique.

Algorithm: Let

$$(a+bx+cx^2)(d+ex+fx^2) = 1+0x+0x^2.$$

Expand LHS.

Compute remainder mod x^3-2.

Equate coefficients

Get 3 (linear) equations in the
3 unknowns d, e, f.

Theorem guarantees unique solution.

My computer says

$$d = (b^2 - ac)/\Delta$$

$$e = (2a - bc)/\Delta$$

$$f = (c^2 - 2ab)/\Delta$$

where $\Delta = 4a^3 - 6abc + 2b^3 + c^3$.

Do not memorize!

This was Kronecker's idea (1880s)
because he did not believe in
irrational numbers. For him,
"$\sqrt[3]{2}$" is just an abstract symbol
"x" satisfying $x^3 \sim 2$.

$$x^3 - 2 \sim 0$$

So we should work modulo $x^3 - 2$.

The same idea can be used to create a root for any polynomial.

Kronecker's Theorem:

Given nonconstant $f(x) \in \mathbb{F}[x]$, there exists a field $\mathbb{E}$ and an element $\alpha \in \mathbb{E}$ such that

$$f(x) = (x - \alpha)\, g(x)$$

for some $g(x) \in \mathbb{E}[x]$.

Proof: "Pretend"

Let $f(x) = p(x)\, q(x)$ with $p(x) \in \mathbb{F}[x]$ prime. Let $\mathbb{E} = \mathbb{F}[x]_p$.

If $\deg(p) = n$ then every element of $\mathbb{E}$ looks like

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$$

for some unique $a_0, a_1, \cdots, a_{n-1} \in \mathbb{F}$.

I claim that

(1) $\mathbb{E} \supseteq \mathbb{F}$

(2) $\exists\, \alpha \in \mathbb{E}$ with $f(\alpha) = 0$.

Proof of (1): Let's just identify the element $a \in \mathbb{F}$ with

$$a + 0x + 0x^2 + \cdots + 0x^{n-1} \in \mathbb{E}.$$

"Sure, why not?" ///

Proof of (2): Let $\alpha := x$.

Then $f(\alpha) = f(x)$

$$= p(x)\,q(x) \underset{p}{\sim} 0.$$

"Sure, why not?" ///

Q.E.D.

This finally completes Laplace's proof of FTA.

☺

Moving On:

Kronecker's Idea of "Algebraic Field Extensions" also helps to solve the problem of "Impossible Geometric Constructions"

We prove the following problems cannot be solved with straightedge and compass:

- Double the Cube.
- Trisect the Angle.
- Construct Regular 7-gon.