Prime numbers:
if $p = ab$
then $a = \pm 1$ or $b = \pm 1$

don't consider ± 1 as primes
because they're units in $\mathbb{Z}$

Irred. polys:
if $f = gh$ then
$g = $ const or $h = $ const

don't consider
const. polynomials
as irred, bec. they're
units in $F[x]$

Unique factorization:
if F is a field and $f \in F[x]$
with $\deg f \geq 1$,
we can write it uniquely as a prod. of irreducibles

i.e. $f = g_1 g_2 \cdots g_n$ where g_i are all irred.

and if $f = h_1 h_2 \cdots h_m$ where h_j are irred

then $m = n$ and we can pair g_i's with h_j's
so that $g_i = \text{const} \cdot h_j$

Pf: existence is by induction on degree:
if $\deg f = 1$ then f is irred.

if $\deg f > 1$, either f is irred
or $f = gh$ with $\deg g \geq 1$
$\deg h \geq 1$
so $\deg g < \deg f$ and $\deg h < \deg f$.
by inductive hypothesis, can factor g and h.

uniqueness is also by induction on deg.
uses Euclid's lemma

if $f = g_1 \cdots g_n = h_1 \cdots h_m$ two factorizations

then $g_1 \mid h_1 h_2 \cdots h_n$

so $g_1 \mid$ some h_i

but h_i is irreducible, so $h_i = \text{const} \cdot g_1$

now cancel: $g_1 g_2 \cdots g_n = (\text{const}) \cdot h_1 \cdots h_i \cdots h_m$

and keep going till g's are used up. □

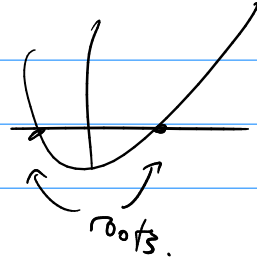
---

homework: uniqueness fails in $\mathbb{Z}_6[x]$

Thing we can do w/ polynomials that we can't with ints:
think about roots.

Def Let F be a field and $f \in F[x]$.
Then $c \in F$ is a <u>root</u> of f
if $f(c) = 0$

Claim: c is a root of f
iff $x - c \mid f$



One direction is easy:

if $x-c \mid f$,

write $f = (x-c)g$

so $f(c) = (c-c)\cdot g(c) = 0 \cdot g(c) = 0$

For the converse, divide f by $x-c$:

$f = (x-c)\cdot q + r$ where $\deg r < 1$

plug in $x=c$, get

$f(c) = (c-c)\cdot q(c) - r$ ← constant!

so $f(c) = r$

but c was a root of f, so $r=0$,

so $f = (x-c)q$. ∎

How to tell if a polynomial is irred?

(1) if $\deg f = 1$, yes,

(2) if $\deg f = 2$ or 3, reducible iff if has a root (homework)

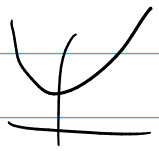
doesn't work for $\deg \geq 4$:

$x^4 + 5x^2 + 6 \in \mathbb{R}[x]$ has no roots in $\mathbb{R}$

but factors as $(x^2+2)(x^2+3)$

(3) if $F = \mathbb{C}$, only linear polys are irred.

any f of deg ≥ 1 has a root in $\mathbb{C}$
(fundamental thm. of algebra.)



got from $\mathbb{R}$ to $\mathbb{C}$ by noticing
that x^2+1 doesn't have a root in $\mathbb{R}$

throw that in call it i:
now every polynomial has a root?!

(4) $\mathbb{R}(x)$: see worksheet.

(5) in $\mathbb{Q}[x]$ it's complicated.

develop some tools:
Rational Root Thm.
Gauss's Lemma
Eisenstein's Criterion.

§3.3.