# Math 4400
## Week 5 – Tuesday
### Roots of polynomials + modular arithmetic gone off the rails.

**Definition:** Let $R$ be a ring and let $f(x) \in R[x]$ be a polynomial with coefficients in $R$.
An element $r \in R$ is a <u>root</u> or <u>zero</u> of $f(x)$ if $f(r) = 0$.

**Example:** Let $f(x) = x^2 - 1$ (makes sense for any $R$).
$x^2 - 1 = (x-1)(x+1)$ so $1, -1$ are always roots.
If $R$ is a field, these are the only roots, <u>but</u> if $R = \mathbb{Z}/8\mathbb{Z}$ then:

$f(0) = 0^2 - 1 = -1$ not zero

$f(1) = 1^2 - 1 = 0$ ✓

$f(2) = 2^2 - 1 = 3$ and $0$.

$f(3) = 9 - 1 = 8 = 0$ ✓

$1, 3, 5, 7$ are all roots of $x^2 - 1$ in

$f(4) = 16 - 1 = -1 \neq 0$ $\qquad\qquad$ $\mathbb{Z}/8\mathbb{Z}$.

$f(5) = 25 - 1 = 24 = 0$ ✓

$f(6) = 36 - 1 = 3 \neq 0$.

$f(7) = 49 - 1 = 48 = 0$ ✓

$-1$

**Theorem:** If $\mathbb{K}$ is a field and $f(x) \in \mathbb{K}[x]$, then for any $a \in \mathbb{K}$,

$$f(a) = 0 \iff a \text{ is a root of } f \iff (x-a) \mid f(x).$$

this is the definition of a root.

i.e. $f(x) = (x-a)q(x)$ for some $q(x) \in \mathbb{K}[x]$.

**Corollary:** If $\mathbb{K}$ is a field and $f(x) \in \mathbb{K}[x]$, then $\#$ roots of $f(x)$ in $\mathbb{K}$ $\leq \deg f(x)$.

**Corollary:** If $\mathbb{K}$ is a field and $f(x) \in \mathbb{K}[x]$ is such that $\deg f \leq 3$, then $f$ is irreducible/prime in $\mathbb{K}[x]$ if and only if $f$ has no roots in $\mathbb{K}$.

**Recall:** If $p$ is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field. We will use the notation $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, and call it "the field with $p$ elements."

**Example:** Wilson's Theorem – if $p$ is prime, then $(p-1)! \equiv -1 \mod p$. ~ $n! = n(n-1)(n-2)\ldots(1)$. "$n$ Factorial."

E.g. $p=2$ $(2-1)! = 1! = 1$ $1 \equiv -1 \mod 2$ ✓.

$p=3$ $(3-1)! = 2! = 2\cdot 1 = 2$ $2 \equiv -1 \mod 3$ ✓.

$p=5$ $4! = 4\cdot 3\cdot 2\cdot 1 = 24$ $24 \equiv -1 \mod 5$. ✓

$p=7$ $6! = 720$ $720 \equiv -1 \mod 7$. ✓

Proof for $p>2$: $(p-1)! = (p-1)(p-2)\ldots(1)$

Multiplying together all of $\mathbb{F}_p^\times$ $((\mathbb{Z}/p\mathbb{Z})^\times)$.

Pair them up as $a, a^{-1}$

E.g. $p=7$ $6! = 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1$

$= 6\cdot \underbrace{(5\cdot 3)}_{1}\underbrace{(4\cdot 2)}_{1}$ in $\mathbb{F}_7$

$= 6$ $6$ is $-1$.

Pairing up eliminates all terms not equal to their own inverse. If $x = x^{-1} \iff x^2 = 1 \iff x^2 - 1 = 0 \iff$ a root of $x^2-1$. We know by Theorem/Corollaries only roots are $1$ and $-1$. So $(p-1)(p-2)\ldots 1 = -1\cdot 1 = -1$ in $\mathbb{Z}/p\mathbb{Z}$.

## Modular arithmetic in general rings:

**Definition:**

- If $R$ is a ring and $r \in R$, $a \equiv b \mod (r)$ means $r \mid (b-a)$ (i.e. $b - a = qr$ for some $q \in R$).

- $R/(r)$ is the set of congruence classes modulo $r$. It is a ring!

Example:

- $R = \mathbb{Z} \qquad r = 5$

  $R/(r) = \mathbb{Z}/(5) = \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$.

- $R = \mathbb{R}[x] \qquad r = x^2+1$.

  $\mathbb{R}[x]/(x^2+1)$. $\leftarrow$ elements have unique representatives

  $a + bx$. $\left( \text{E.g. } x^3 = x(x^2+1) - x \equiv -x \mod (x^2+1) \right)$.

  $a+bx + c+dx = (a+c) + (b+d)x$

  $(a+bx)(c+dx) = ac + (bc+ad)x + bdx^2 \quad x^2 \equiv -1$

  $= (ac-bd) + (bc+ad)x$.

Compare $a+bx \longleftrightarrow a+bi \in \mathbb{C}$.
You get same addition and multiplication laws.

i.e. $\mathbb{R}[x]/x^2+1 \cong \mathbb{C}$.

A field with 9 elements. ⚠ $\mathbb{Z}/9\mathbb{Z}$ has 9 elements but it is ~~not~~ a field.

Idea: repeat above, but use $\mathbb{F}_3$ instead of $\mathbb{R}$.

$\mathbb{F}_3[x] / (x^2+1)$ is a field!

Ring ✓ Can check by hand everything is invertible.

Representatives of the form

$a + bx \quad a, b \in \mathbb{F}_3.$

3 choices for a & 3 choices for b

so $\underset{=3\cdot 3}{9}$ choices total, so 9 elements!