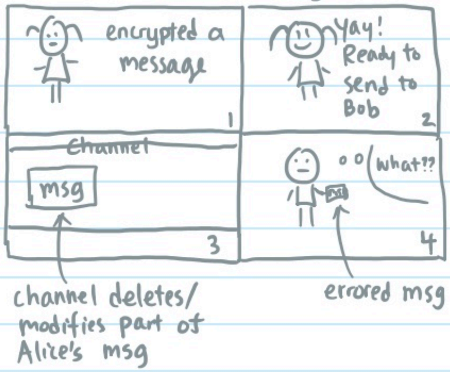
# Polynomials

motivation: we learned about how to encrypt our message using CRT.
How does Alice actually send messages to Bob?




Before learning about how to deal with those errors, let's learn about polynomials.
Tomorrow, we'll use polynomials as a tool to deal with erasure or general errors.

- 2 ways of uniquely determine a degree $d$ polynomial
  - using $d+1$ coefficients
  - using $d+1$ points
- a nonzero degree $d$ polynomial has at most $d$ roots.

Q2. Q3

Answer in $\mathbb{R}$. Answer in $GF(p)$.

(a) $p(x)$, $q(x)$ are two different nonzero polynomials with degrees $d_1$ and $d_2$.
What can you say about number of solutions of $p(x) = q(x)$?
That is the # roots of $p(x) - q(x)$. Thus at most $\max\{d_1, d_2\}$
At most $\max\{d_1, d_2\}$ with the same reasoning.
How about $p(x) \cdot q(x) = 0$?
That is # roots of $p(x) \cdot q(x)$. Thus at most $d_1 + d_2$.
At most $d_1 + d_2$ with the same reasoning.

(b) Show that if $f(x) = x^2 + ax + b$ has exactly one root, then $a^2 = 4b$.
$f$ has one root $\Rightarrow f(x) = (x-c)g(x)$
$x^2$ has coefficient $1 \Rightarrow f(x) = (x-c)(x-d) \Rightarrow c = d$
$\Rightarrow f(x) = (x-c)^2 \Rightarrow a = -2c.\ b = c^2 \Rightarrow a^2 = 4b$
All operation still holds, so same proof.

(c) min # real roots that a polynomial $p$ with degree $d$ can have?
Does the answer depend on $d$?
$d$ is even : min # roots is 0
$d$ is odd : min # roots is 1
$d$ is even: min # roots is 0 e.g. $x^2+1 \pmod 3$
$d$ is odd: min # root is 0 e.g. $x^3+x+1 \pmod 5$

## Lagrange interpolation

motivation: translate from points representation to coefficients representation

e.g. Q4.

Find the lowest degree polynomial $P(x)$ that passes through the points $(1,4), (2,3), (5,0)$ modulo 7.

**Sol:** [ Idea: we want to find basis $\Delta_1, \Delta_2, \Delta_3$ such that

$$P(x) = 4\,\Delta_1(x) + 3\,\Delta_2(x) + 0\cdot\Delta_3(x).$$

That is, $\Delta_1(1)=1, \quad \Delta_1(2)=0, \quad \Delta_1(5)=0$

$\Delta_2(1)=0, \quad \Delta_2(2)=1, \quad \Delta_3(5)=0$

$\Delta_3(1)=0. \quad \Delta_3(2)=0, \quad \Delta_3(5)=1$ ]

$$\Delta_1(x) \equiv (x-2)(x-5)\left((1-2)(1-5)\right)^{-1} \equiv (x^2-7x+10)\cdot 4^{-1} \equiv 2x^2+6 \pmod 7$$

$$\Delta_2(x) \equiv (x-1)(x-5)\left((2-1)(2-5)\right)^{-1} \equiv (x^2-6x+5)\cdot(-3)^{-1} \equiv 2x^2+2x+3 \pmod 7$$

$$p(x) \equiv 4\Delta_1(x) + 3\Delta_2(x) \equiv 14x^2+6x+33 \equiv 6x+5 \pmod 7$$