Remarks on polynomial congruences in $\mathbb{Z}_m$

- Polynomial congruences in Ma135, need only:

  (1) make tables

  (2) Correct use of FlT or Cor 3.43

  - check prime modulus,
  - FlT for $[\ ]^{p-1}$, treat [x]=[0] separately
  - Cor 3.43 for $[\ ]^p$

- Advance questions

  In e.g.1, solve $[x]^2 - [3][x] + 2 = [0]$ –(*).

  [x]=[1] and [2] solves (*) in both $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

  - Is there a reason?

  Can we use $[x]^2 - [3][x] + 2 = ([x] - [1])([x] - [2])$?

- Ans: For all m, $s_1, \cdots, s_n$ solves

  $[0] = ([x] - [s_1])([x] - [s_2])...([x] - [s_n])$

  If m prime, no more solutions (Chp 4).

  Else, can miss some solutions.

  e.g. In $\mathbb{Z}_6$,

  $$[x]^2 - [3][x] + [2] = ([x] - [1])([x] - [2])$$
  $$= [x]^2 - [9][x] + [20] = ([x] - [5])([x] - [4]).$$

  Factorization not unique.