Chapter 4 roadmap:

- Subset proofs (week-before Wednesday)
- Set equality and emptiness proofs (week-before Friday)
- Conditional and biconditional proofs (last week Wednesday)
- Proofs about powersets (last week Friday)
- From theorems to algorithms (**Today**)
- (Start Chapter 5 relations next time)

Today: Two programming topics

- Hint on HW problem
- From theorems to algorithms
  - Greatest common divisor
  - Exponentiation
  - The quotient-remainder theorem
- Bull and cows

Lemma (4.13. Termination)

If $a \in \mathbb{N}$, then $gcd(a, 0) = a$.

Lemma (4.14. Progress)

If $a, b \in \mathbb{N}$, $q, r \in \mathbb{W}$, and $a = b \cdot q + r$, then $gcd(a, b) = gcd(b, r)$.

Ex 4.10.5 (rewritten). Consider the lemmas

Lemma (Invariant and termination.)

If $n, d \in \mathbb{N}$, then there exist unique $q, r \in \mathbb{W}$ such that $n = d \cdot q + r$ and $0 \leq r [< d]$.

Lemma (Progress.)

If $n, d \in \mathbb{N}$ and $q, r \in \mathbb{W}$, then $d \cdot q + r = d \cdot (q + 1) + (r - d)$.

Write a function `quotRem` that takes natural numbers `n` and `d` and computes the quotient and remainder of `n` divided by `d` using the lemmas above.

For next time:

Pg 177: 4.10.(3, 4, 6)
For exercise 4.10.3, name the function `pow`.
For exercise 4.10.4, name the function `mul`.
See Canvas for an important correction to Ex 4.10.6

Read carefully 5.1
Read 5.(2 & 3)
Take quiz