Random Numbers

- Useful in many types of programs
  - Games
  - Simulations
  - Encryption keys
- Truly random numbers
  - Impossible to predict the next number
  - Aperiodic - there is not a repeating sequence

- Computers cannot generate truly random numbers through an algorithm alone

- Pseudo-random numbers
  - Generated by an algorithm together with an initial seed value
  - Efficient - fast to generate

Simple (but bad) pseudo-random algorithm:

```
value = seed
add = 11
repeat forever:
    value = value + add
    value = value % 10
    add = add + 1
```

seed = 4

value	add
4	11
5	12
7	13
0	14
4	15
9	16
5	17
2	18

seed = 5

value	add
5	11
6	12
8	13
1	14
5	15
0	16
6	17
3	18

- Truly random within a computer
    - Requires entropy from the world
        - User interaction - wiggle the mouse
        - Atmospheric noise
        - Radioactive decay
- Sometimes pseudo-random is good enough
    - Low-stakes games
    - Simulations that require efficiency

- Sometimes truly random is required
    - Generating encryption keys
    - High-stakes games