

Modular Arithmetic → wrap around result of arithmetic operation or conversion on integer type.

- Next number after the largest in an integer type is the smallest
  - ✓ (byte) 128 == (byte) (127+1) == (byte) -128
- Result of some arithmetic subexpression with Type T, an n-bit integer type,
  - ✓  $x$  = the real (mathematical) value of computation
  - ✓  $x' = x \text{ modulo } 2^n \rightarrow x' = x \text{ in the range of } T$
  - ✓ i.e.  $x - x'$  is a multiple of  $2^n \rightarrow x' = x - \text{a multiple of } 2^n$
- $a \equiv b \pmod{n} \rightarrow a - b = kn$  for some integer  $k \sim n = 2^{(\# \text{ of bits})}$  &  $b = a - kn$
- Binary operation  $a \text{ mod } n \rightarrow b$  such that  $a \equiv b \pmod{n}$  and  $0 \leq b < n$  for  $n > 0$
- Different from % operation
- Various facts ( $a' = a \text{ mod } n$ )
  - ✓  $a'' = a'$
  - ✓  $a' + b'' = (a' + b)' = a + b'$
  - ✓  $(a' - b')' = (a' + (-b'))' = (a - b)'$
  - ✓  $(a' \times b')' = a' \times b' = a \times b'$
  - ✓  $(a^k)' = ((a')^k)' = (a \times (a^{(k-1)}))'$  for  $k > 0$

### Modular Arithmetic and Bits

- Bit n, counting from 0 at the right, corresponds to  $2^n$
- Bits to the left of the vertical bars represents multiples of  $2^{(\# \text{ of bits})}$
- Arithmetic modulo  $2^{(\# \text{ of bits})} \rightarrow$  throwing away left of the vertical bar
- Representation for -1 → bits of 1s

### Bit twiddling

- Java allows handling integer types as sequences of bits w/o conversion
- Operations
  - a. Mask (&) → AND operation
  - b. Set (|) → OR operation
  - c. Flip (^) → XOR operation ~ true iff only one of bits is true
  - d. Flip all (~) → NOT operation
- Shifting
  - a. Left (<<) → append 0 at the left ~ equivalent to multiplying  $2^k$
  - b. Arithmetic Right (>>) → append 1 at the right ~ equivalent to dividing  $\text{low}(2^k)$  (i.e. rounded down)
  - c. Logical Right (>>>) → append 0 at the right ~ equivalent to ?????

Asymptotic analysis → Input bound

- Cost Measures (Time)
  - a. Dynamic statement counts of # of times statements are executed
  - b. Symbolic execution times → formulas for execution times as functions of input size ~ let us see the shape of the cost function
- Asymptotic behavior → growth of the function  $f(n)$  as  $n$  gets large
- Approximation ~ Behavior on small inputs and constant factors are pointless
- Asymptotic time unchanged by the constant factor
- No input → Works in a constant time
- Other than inputs are considered as constant

Order notation → produce families of functions w/ similarly behaved magnitudes

- Upper limits → Big Oh ( $O(g)$ ) - Express the upper bound of an algorithm's running time. ~ Measures the worst case (largest possible time)
- Lower limits → Omega ( $\Omega(g)$ ) → Express the lower bound of an algorithm's running time. ~ Measures the best case (smallest possible time)
- $\theta(g) = O(g) \cap \Omega(g)$  → set of functions bracketed in magnitude by two members of  $g$ 's family ~  $f$  is  $\theta(g(n))$  if  $g$  is an accurate characterization of  $f$  for large  $n$
- Theta bound → can be scaled so is both an upper and a lower bound of function
- Use order notation to specify bounds of functions
- At most  $N$  operations ~ Worst case time is  $N$  tests →  $O(N)$  &  $O(N^2)$ , since  $N \in O(N^2)$
- Average case analysis ~ calculate the expected time spent on a randomly chosen input - involves probabilistic arguments and often require assumptions about the distribution of inputs

Bubble sort → sort a list by repeatedly looping through the list and swapping adjacent items if they are out of order, until the entire sorting is complete.

$\Theta$  bound is a tight bound and applies when a function has the same  $\Omega$  and  $O$  bounds. For example, consider searching an array for a specific element. In the best case, we'll find the element immediately, so the best case will be  $\theta(1)$ . Meanwhile, the worst case will be  $\theta(n)$  since we're only considering inputs that will result in the worst case. As you can see, the best and worst cases have  $\theta$  bounds, but the runtime of the function as a whole would be  $\Omega(1)$  and  $O(n)$ .

For mathematical functions, there aren't any notion of "best" or "worst" case inputs. The input is just  $x$ : no subset of inputs  $x$  can make this function behave differently

Theta bound is a tight bound. All functions with higher or equal degree than the function of Theta bound can be the valid function of the Upper Bound (Big Oh) and all functions with lower or equal degree can be the valid function of the Lower Bound (Omega) ~ For  $f(x) = x^2$ ,  $\Omega(1)$ ,  $\Omega(\log x)$ ,  $\Omega(x)$  can be considered as simple lower asymptotic bounds

Sometimes we can't find a tight theta bound on a function's runtime. So, what we do is find the lower bound and upper bound of the function's runtime by Best and worst-case analysis.

$\text{Math.pow}(2,i) \rightarrow i \in \mathbb{N}$  where  $1 \leq i \leq 31$ . Otherwise, it's trivially true that none of them are actually equivalent to  $\text{Math.pow}(2, i)$  for 32-bit integers.

The worst and the best case runtime includes all bounds, not just  $\Theta$  bounds, but also the  $O$  and  $\Omega$  bounds. The "worst case" doesn't have to be unique. It can be the same as the "best case", if the runtime can be tightly bounded.