Elementary Number Theory and Methods of Proof

CSE 215: Foundations of Computer Science

Stony Brook University

http://www.cs.stonybrook.edu/~liu/cse215

Number theory

- Properties of integers (whole numbers), rational numbers (integer fractions), and real numbers.
  - Determine the truth of mathematical statements.
- Example:

  Definition: For any real number x, the floor of x, $\lfloor x \rfloor$, is the largest integer that is less than or equal to x.

  $\lfloor 2.3 \rfloor = 2$; $\lfloor 12.99999 \rfloor = 12$; $\lfloor -1.5 \rfloor = -2$

  - For any real number x, is $\lfloor x-1 \rfloor = \lfloor x \rfloor - 1$? yes (true)
  - For any real numbers x and y, is $\lfloor x-y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$? no (false)
    - $\lfloor 2.0-1.1 \rfloor = \lfloor 0.9 \rfloor = 0$
    - $\lfloor 2.0 \rfloor - \lfloor 1.1 \rfloor = 2 - 1 = 1$

Number theory

- Proof example:
  - If x is a number with $5x + 3 = 33$, then $x = 6$

    <u>Proof:</u>

    If $5x + 3 = 33$, then $5x + 3 - 3 = 33 - 3$ since subtracting the same number from two equal quantities gives equal results.

    $5x + 3 - 3 = 5x$ because adding 3 to 5x and then subtracting 3 just leaves 5x, and also, $33 - 3 = 30$.

    Hence $5x = 30$.

    That is, x is a number which when multiplied by 5 equals 30.

    The only number with this property is 6.

    Therefore, if $5x + 3 = 33$ then $x = 6$.

Number theory introduction

- Properties of equality:

  (1) $A = A$

  (2) if $A = B$ then $B = A$

  (3) if $A = B$ and $B = C$, then $A = C$

- The set of all integers is closed under addition, subtraction, and multiplication.

  That is,

  sums, differences, and products of integers are integers.

Number theory introduction

- An integer n is **even** if, and only if, n equals twice some integer:

  n is even $\Leftrightarrow$ $\exists$ an integer k such that $n = 2k$

- An integer n is **odd** if, and only if, n equals twice some integer plus 1:

  n is odd $\Leftrightarrow$ $\exists$an integer k such that $n = 2k + 1$

- Reasoning examples:
  - Is 0 even? Yes, $0 = 2 \cdot 0$
  - Is -301 odd? Yes, $-301 = 2(-151) + 1$.
  - If a and b are integers, is $6a^2b$ even?

    Yes, $6a^2b = 2(3a^2b)$ and $3a^2b$ is an integer

    being a product of integers: 3, a, a, and b

Number theory introduction

- An integer n is **prime** if, and only if, $n>1$ and for all positive integers r and s, if $n=r \cdot s$, then either r or s equals n:

  n is prime ⇔ ∀ positive integers r and s, if $n = r \cdot s$ then either $r = 1$ and $s = n$, or $r = n$ and $s = 1$

- An integer n is **composite** if, and only if, $n>1$ and $n=r \cdot s$ for some integers r and s with $1 < r < n$ and $1< s < n$:

  n is composite ⇔ ∃ positive integers r and s such that $n = r \cdot s$ and $1 < r < n$ and $1 < s < n$

- Example: Is every integer greater than 1 either prime or composite?

  Yes. Let n be an integer > 1. There exist at least two pairs of integers: $r=n$ and $s=1$, and $r=1$ and $s=n$, such that $n= rs$. If there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n ($1 < r < n$ and $1<s< n$), then n is composite. Otherwise, it's prime.

Proving Existential Statements

- Existential statement: $\exists x \in D, Q(x)$

  is true if, and only if, $Q(x)$ is true for at least one x in D
- **Constructive proofs of existence:** find an x in D that makes $Q(x)$ true, or give a set of directions for finding such an x
- Examples:
  - $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers

    Proof: $n = 10 = 5+5 = 3+7$ where 5, 3 and 7 are prime numbers
  - $\exists$ an integer k such that $22r + 18s = 2k$ where r and s are integers

    Proof: Let $k = 11r + 9s$. k is an integer because it is a sum of products of integers. By distributivity of multiplication the equality is proved.

Proving Existential Statements

- **Nonconstructive proofs of existence:**

  the evidence for the existence of a value of x is guaranteed by an axiom or theorem

  the assumption that there is no such x leads to a contradiction

- Problem: gives no idea of what x is.

Disproving Universal Statements by Counterexample

- Disprove ∀x in D, if P(x) then Q(x)
  - The statement is false is equivalent to its negation is true.
  - The negation is: ∃x in D, P(x) ∧ ~Q(x)
- **Disproof by counterexample:**

  ∀x in D, if P(x) then Q(x) is false if we find an x in D for which P(x) is true and Q(x) is false

  - x is called a **counterexample**
- Example:

  Disprove ∀ real numbers a and b, if $a^2 = b^2$ then $a = b$.

  Counterexample: Let $a = 1$ and $b = -1$.

  $$a^2 = b^2 = 1, \text{ but } a \neq b$$

Proving Universal Statements

- Universal statement: $\forall x \in D$, if $P(x)$ then $Q(x)$
- **The method of exhaustion:**

  if D is finite or only a finite number of elements satisfy $P(x)$, then we can try all possibilities
- Example:
  - Prove $\forall n \in Z$, if n is even and $4 \leq n \leq 7$, then n can be written as a sum of two prime numbers.

  Proof:

  $4 = 2 + 2$ and

  $6 = 3 + 3$ ■

Proving Universal Statements

- **Method of generalizing from the generic particular:**

  suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property

  - no special assumptions about x that are not also true of all other elements of the domain

- **As in method direct proof:**

  1. Formalize the statement as: $\forall x \in D$, if P(x) then Q(x)
  2. Let x is a particular but arbitrarily chosen element of D for which the hypothesis P(x) is true
  3. Show that the conclusion Q(x) is true

Method of Direct Proof

- Example: prove that the sum of any two even integers is even
  1. Formalize: $\forall$ integers m, n, if m and n are even then $m + n$ is even
  2. Suppose m and n are any even integers

  Existential Instantiation: If the existence of a certain kind of object is assumed or has been deduced then it can be given a name

  Since m and n equal twice some integers, we give those integers names

  $m = 2r$ for some integer r and $n = 2s$ for some integer s

  $m + n = 2r + 2s = 2(r + s)$

  $r + s$ is an integer because the sum of any two integers is an integer, so $m + n$ is an even number
- The example can be formalized as a proved theorem

Common Mistakes

1. Arguing from examples: it is true because it's true in one particular case **– NO**
2. Using the same letter to mean two different things
3. Jumping to a conclusion **– NO,** we need a complete proof!
4. Circular reasoning: x is true because y is true since x is true
5. Confusion between what is known and what is still to be shown.

   What is known? Given hypothesis, axioms, proved theorems
6. Use of *any* rather than some. Any could mean *all* or *some.*
7. Misuse of *if*: when something is given, should use *because*

Disproving an Existential Statement

- The negation of an existential statement is universal

  To prove that an existential statement is false, we prove that its negation (a universal statement) is true.

- Example: disprove:

  There is a positive integer n s.t. $n^2 + 3n + 2$ is prime.

  The negation is:

  For all positive integers n, $n^2 + 3n + 2$ is not prime.

  Let n be any positive integer

  $n^2 + 3n + 2 = (n + 1)(n + 2)$

  where $n + 1 > 1$ and $n + 2 > 1$ because $n \geq 1$

  Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and thus is not prime.

Rational Numbers

- A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator

  r is rational $\Leftrightarrow \exists$integers a and b s.t. $r = a / b$ and $b \neq 0$

- Examples:

  $10/3, -5/39, 0.281 = 281/1000, 7 = 7/1,$

  $0 = 0/1, 0.12121212... = 12/99$

  - Every integer is a rational number: $n = n/1$

A Sum of Rationals Is Rational

- ∀ real numbers r and s, if r and s are rational then r + s is rational.

Proof:

Suppose r and s are particular but arbitrarily chosen real numbers such that r and s are rational

$r = a/b$ and $s = c/d$

for some integers a, b, c, and d, where $b \neq 0$ and $d \neq 0$

Then $r + s = a/b + c/d$

$= ad/bd + bc/bd$ (rewriting fractions with a common denominator)

$= (ad + bc)/bd$ (adding fractions with a common denominator)

And

$bd \neq 0$

Therefore, r + s is rational.

Deriving Additional Results about Even and Odd Integers

Prove:

if a is any even integer and b is any odd integer,

then $(a^2+b^2+1)/2$ is an integer

using the properties:

1. The sum, product, and difference of any two even integers are even.
2. The sum and difference of any two odd integers are even.
3. The product of any two odd integers is odd.
4. The product of any even integer and any odd integer is even.
5. The sum of any odd integer and any even integer is odd.
6. The difference of any odd integer minus any even integer is odd.
7. The difference of any even integer minus any odd integer is odd.

Group these:

1 2 for sum/diff =even, 5 6 7 for sum/diff=odd, 1 3 4 for product

Proof:

- Suppose a is any even integer and b is any odd integer.
- By property 1, a^2 is even.
- By property 3, b^2 is odd.
- By property 5, $a^2 + b^2$ is odd.
- By property 2, $a^2 + b^2 + 1$ is even.
- By definition of even, there exists an integer k such that

  $$a^2 + b^2 + 1 = 2k.$$

- By division with 2, $(a^2+b^2+1)/2 = k$, which is an integer.

Divisibility

- If n and d are integers and $d \neq 0$ then n **is divisible by** d if, and only if, n equals d times some integer

$$d \mid n \iff \exists \text{an integer } k \text{ s.t. } n = dk$$

  - n **is a multiple of** d
  - d **is a factor of** n
  - d **is a divisor of** n
  - d **divides** n
- Notation: $d \mid n$ (read "d divides n")
- Examples: 21 is divisible by 3, 32 is a multiple of −16,
  5 divides 40, 6 is a factor of 54, 7 is a factor of −7
  - Any nonzero integer k divides 0, because $0 = k \cdot 0$

A Positive Divisor of a Positive Integer

- For all integers a and b, if a and b are positive and a divides b, then $a \leq b$.

  Proof:

  - Suppose a and b are positive integers and a divides b
  - Then there exists an integer k such that $b = ak$
  - $1 \leq k$ because every positive integer is greater than or equal to 1
  - Multiplying both sides by a gives $a \leq ka = b$, since a is a positive number

Transitivity of Divisibility

- For all integers a, b, and c, if $a|b$ and $b|c$, then $a|c$

<u>Proof:</u>

- Since $a \mid b$, $b = ar$ for some integer r.
- Since $b \mid c$, $c = bs$ for some integer s.

Hence, $c = bs = (ar)s = a(rs)$

by the associative law for multiplication.

rs is an integer, so $a|c$

Counterexamples and Divisibility

- For all integers a and b, if $a \mid b$ and $b \mid a$ then a=b.

Counterexample:

Let $a = 2$ and $b = -2$.

Then $a \mid b$ since $2 \mid (-2)$ and $b \mid a$ since $(-2) \mid 2$,

but $a \neq b$ since $2 \neq -2$

Therefore, the statement is false.

Unique Factorization of Integers Theorem

- Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that:

$$n = p_1^{e1} p_2^{e2} p_3^{e3} \ldots p_k^{ek}$$

  and any other expression for n as a product of prime numbers is identical to this except for the order in which the factors are written.
  - proof is outlined in later chapters
- **Standard factored form:** $p_1 < p_2 < \cdots < p_k$
- Example: $360 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5^1$

The Quotient-Remainder Theorem

- Given any integer n and positive integer d, there exist unique integers q and r such that

  $$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

  - proof is outlined in later chapter/section
- n **div** d = the integer quotient obtained when n is divided by d
- n **mod** d = the nonnegative integer remainder obtained when n is divided by d.

  $$n \text{ div } d = q \quad \text{and} \quad n \text{ mod } d = r \quad \Leftrightarrow \quad n = dq + r$$

  $$n \text{ mod } d = n - d \cdot (n \text{ div } d)$$

- Examples: $d = 4$
  - $n = 54 = 52+2 = 4 \cdot 13 + 2$; hence $q = 13$ and $r = 2$
  - $n = -54 = -56 + 2 = 4 \cdot (-14) + 2$; hence $q = -14$ and $r = 2$

Method of Proof by Division into Cases

- To prove:

  If A_1 or A_2 or . . . or A_n, then C

  prove all of the following:

  If A_1, then C,

  If A_2, then C,

  …

  If A_n, then C.

  C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case

Parity

- The parity of an integer refers to whether the integer is even or odd

- Prove: consecutive integers have opposite parity

  - Case 1: The smaller of the two integers is even
  - Case 2: The smaller of the two integers is odd

Simple proof in both cases.

Representation of integers modulo 4

- Prove: any integer can be written in one of the four forms:

  $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$

<u>Proof:</u> By the quotient-remainder theorem to n with d =4:

$n = 4q + r$ and $0 \leq r < 4$

The only nonnegative remainders r less than 4 are 0, 1, 2, and 3

Hence:

$n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$

for some integer q

Absolute Value and the Triangle Inequality

- The **absolute value** of x is:

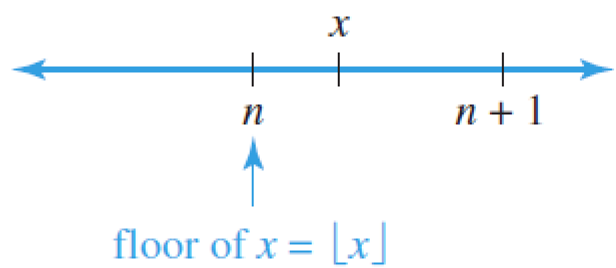
$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

- For all real numbers r, $-|r| \leq r \leq |r|$
  - Case 1 ($r \geq 0$): $|r| = r$
  - Case 2 ($r < 0$): $|r| = -r$, so, $-|r| = r$

Floor and Ceiling

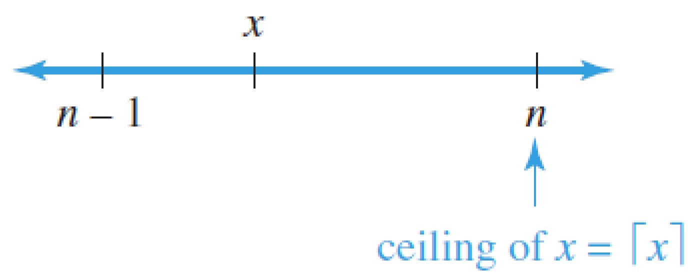
- The **floor** of a real number x, $\lfloor x \rfloor$, is a unique integer n such that $n \le x < n+1$:

  $\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \le x < n+1$



- The **ceiling** of a real number x, $\lceil x \rceil$, is a unique integer n such that $n-1 < x \le n$:

  $\lceil x \rceil = n \quad \Leftrightarrow \quad n-1 < x \le n$



Floor and Ceiling

- Examples:
  - $25/4 = 6.25$, where $6 < 6.25 < 7$

  $\lfloor 25/4 \rfloor = 6$

  $\lceil 25/4 \rceil = 7$

  - 0.999, where $0 < 0.999 < 1$

  $\lfloor 0.999 \rfloor = 0$

  $\lceil 0.999 \rceil = 1$

  - -2.01, where $-3 < -2.01 < -2$

  $\lfloor -2.01 \rfloor = -3$

  $\lceil -2.01 \rceil = -2$

Disproving A Property of Floor

- Disprove:

  For all real numbers x and y, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$

  Counterexample: $x = y = 1/2$

  $\lfloor x + y \rfloor = \lfloor 1 \rfloor = 1$

  $\lfloor x \rfloor + \lfloor y \rfloor = \lfloor 1/2 \rfloor + \lfloor 1/2 \rfloor = 0 + 0 = 0$

  Hence, $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$

Hints on how to reason about $\lfloor\rfloor$ & $\lceil\rceil$

$$2\frac{3}{5} = 2 + \frac{3}{5}$$

integer part (2) fractional part ($\frac{3}{5}$)

$$x = \lfloor x \rfloor + \text{fractional part of } x$$

$x + y = \lfloor x \rfloor + \lfloor y \rfloor +$ the sum of the fractional parts of x and y

$x + y = \lfloor x+y \rfloor +$ the fractional part of $(x + y)$

Counterexample: $x = y = 1/2$

the sum of the fractional parts of x and y $= 1$

the fractional part of $(x + y) = 0$

Proving a Property of Floor

- For all real numbers x and integers m, $\lfloor x+m \rfloor = \lfloor x \rfloor + m$

Suppose x is a particular but arbitrarily chosen real number,
m is a particular but arbitrarily chosen integer

$n = \lfloor x \rfloor \Leftrightarrow$ n is an integer and $n \leq x < n + 1$

add m: $n + m \leq x + m < n + m + 1$

so $\lfloor x+m \rfloor = n + m$

$= \lfloor x \rfloor + m$, since $n = \lfloor x \rfloor$

The Floor of n/2

- For any integer n,

$$\lfloor n/2 \rfloor = \begin{cases} n/2, & \text{if n is even} \\ (n-1)/2, & \text{if n is odd} \end{cases}$$

Suppose n is a particular but arbitrarily chosen integer

Case 1 (n is odd): $n = 2k + 1$ for some integer k

$\lfloor n/2 \rfloor = \lfloor (2k + 1)/2 \rfloor = \lfloor\ 2k/2 + 1/2 \rfloor = \lfloor k+1/2 \rfloor = \lfloor k \rfloor = k$

$(n - 1)/2 = (2k + 1 - 1)/2 = 2k/2 = k$

Case 2 (n is even): $n = 2k$ for some integer k

$\lfloor n/2 \rfloor = n/2 = k$

Division quotient and remainder

- If n is any integer and d is a positive integer,

  if $q = \lfloor n/d \rfloor$ and $r = n - d\lfloor n/d \rfloor$,

  then $n = dq + r$ and $0 \leq r < d$

  Proof: Suppose n is any integer, d is a positive integer

  $$dq + r = d\lfloor n/d \rfloor + (n - d\lfloor n/d \rfloor) = n$$

$q \leq n/d < q + 1$	by definition of floor
$dq \leq n < dq + d$	by multiplying all by d
$0 \leq n - dq < d$	by subtracting dq from all
$0 \leq r < d$	by substitution

Indirect Argument: Contradiction and Contraposition

- **Proof by Contradiction** (*reductio ad impossible* or *reductio ad absurdum*)
  - A statement is true or it is false but not both
  - Assume the statement is false
  - If the assumption that the statement is false leads logically to a contradiction, impossibility, or absurdity, then that assumption must be false
  - Hence, the given statement must be true

There Is No Greatest Integer

- Assumption: there is a greatest integer N

  $N \geq n$ for every integer n

- If there were a greatest integer, we could add 1 to it to obtain an integer that is greater

  $N + 1 > N$

- This is a contradiction, no greatest integer can exist (our initial assumption)

No Integer Can Be Both Even and Odd

- Suppose there is at least one integer n that is both even and odd

  $n = 2a$ for some integer a, by definition of even

  $n = 2b+1$ for some integer b, by definition of odd

  $$2a = 2b + 1$$

  $$2a - 2b = 1$$

  $$a - b = 1/2$$

  Since a and b are integers, the difference $a - b$ must also be an integer, a contradiction!

The Sum of a Rational Number and an Irrational Number

- The sum of any rational number and any irrational number is irrational

  $\forall$ real numbers r and s, if r is rational and s is irrational, then r + s is irrational

  Assume its negation is true:

  $\exists$ a rational number r and an irrational number s such that r + s is rational

  $r = a/b$ for some integers a and b with $b \neq 0$

  $r + s = c/d$ for some integers c and d with $d \neq 0$

  $s = c/d - a/b = (bc - ad)/bd$ with $bd \neq 0$

  This contradicts the supposition that it is irrational

Argument by Contraposition

- Logical equivalence between a statement and its contrapositive
- We prove the contrapositive by a direct proof and conclude that the original statement is true

$\forall x$ in D, if P(x) then Q(x)

Contrapositive: $\forall x$ in D, if Q(x) is false then P(x) is false

Prove the contrapositive by a direct proof

1. Suppose x is a (particular but arbitrarily chosen) element of D such that Q(x) is false
2. Show P(x) is false

Contraposition: the original statement is true

Contraposition Example

- If the Square of an Integer Is Even, Then the Integer Is Even

Contrapositive: For all integers n, if n is odd then n^2 is odd

Suppose n is any odd integer

$n = 2k + 1$ for some integer k, by definition of odd

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

$2k^2 + 2k$ is an integer

So n^2 is odd [This was to be shown]

Contradiction Example

- If the Square of an Integer Is Even, Then the Integer Is Even

Suppose the negation of the theorem:

There is an integer n such that n^2 is even and n is not even

Any integer is odd or even, by the quotient-remainder theorem

with $d = 2$ ➔ since n is not even it is odd

$n = 2k + 1$ for some integer k

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

➔ n^2 is odd

Contradiction: n^2 is both odd and even

The Irrationality of $\sqrt{2}$

$$c^2 = 1^2 + 1^2 = 2$$

$$c = \sqrt{2}$$

$$\frac{\text{length (diagonal)}}{\text{length (side)}} \quad \frac{c}{1} = \frac{\sqrt{2}}{1} = \sqrt{2}$$

- Suppose the negation: $\sqrt{2}$ is rational

  there exist 2 integers *m* and *n* with no common factors s.t. $\sqrt{2} = \dfrac{m}{n}$

  $m^2 = 2n^2$ implies that m^2 is even $\quad m = 2k$ for some integer k

  $m^2 = (2k)^2 = 4k^2 = 2n^2$

  $n^2 = 2k^2$ $\quad n^2$ is even, and so n is even

  both m and n have a common factor of 2 $\quad$ Contradiction

The set of all prime numbers is infinite

- **Proof (by contradiction):**

  Suppose the set of prime numbers is finite: some prime number p is the largest of all prime numbers:

  $$2, 3, 5, 7, 11, \ldots, p$$

  $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$

  $N > 1$ ➔ N is divisible by some prime number q in 2, 3,…,p

  q divides $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$, but not $(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p) + 1 = N$

  (also proved by contradiction)

  Contradiction!

Application: Algorithms

- A **variable** refers to a specific storage location in a computer's memory
- The **data type** of a variable indicates the set in which the variable takes its values: integers, reals, characters, strings, Boolean (the set {0, 1}) False, True
- **Assignment statement:** x := e x = e in py/da
- **Conditional statements:**

  if (condition) **then** s_1 **else** s_2 **if** cond: s_1

  else: s_2

The condition is evaluated by substituting the current values of all algorithm variables appearing in it and evaluating the truth or falsity of the resulting statement/expression

Application: Algorithms

$x := 5$	$x = r$
if $x > 2$	**if** $x > 2$:
then $y := x + 1$	$y = x+1$
else do	**else**:
$x := x - 1$	$x = x - 1$
$y := 3 \cdot x$	$y = 3 * x$
end do	

- the condition $x > 2$ is true, then $y := x + 1 = 6$

Iterative statements

while (condition)

[statements that make up the body of the loop]

end while

while cond:

stmt

i := 1, s := 0

while ($i \leq 2$)

s := s + i

i := i + 1

end while

Trace Table

Variable Name	Iteration Number	0	1	2
	i	1	2	3
	s	0	1	3

Iterative statements

for variable := initial expression to final expression

  [statements that make up the body of the loop]

next (same) variable

Trace Table

for i := 1 to 4

  x := i^2

next i

Variable Name		Iteration Number 0	1	2	3	4
	x		1	4	9	16
	i	1	2	3	4	5

```
for  i  in range(1,5):        1..4   SETL
  x = i**2
```

The Division Algorithm

- Given a nonnegative integer a and a positive integer d, find integers q and r that satisfy the conditions $a = dq + r$ and $0 \le r < d$

Input: *a* [a nonnegative integer], *d* [a positive integer]

Algorithm Body:

$r := a, q := 0$

while $(r \ge d)$

$\quad r := r - d$

$\quad q := q + 1$

end while

The greatest common divisor

- The greatest common divisor of two integers a and b (that are not both zero), gcd(a, b), is that integer d with the following properties:
  1. d is a common divisor of both a and b:

     $d \mid a$ and $d \mid b$

  2. For all integers c, if c is a common divisor of both a and b, then c is less than or equal to d:

     for all integers c, if $c \mid a$ and $c \mid b$, then $c \leq d$

- Examples:

  $$\gcd(72, 63) = \gcd(9 \cdot 8, 9 \cdot 7) = 9$$

  If r is a positive integer, then $\gcd(r, 0) = r$.

Euclidean Algorithm

- If a and b are any integers not both zero, and if q and r are any integers such that

$$a = bq + r,$$

then

$$\gcd(a, b) = \gcd(b, r).$$

(can be proved by proving

$$\gcd(a,b) \leq \gcd(b,r)$$

$$\gcd(a,b) \geq \gcd(b,r)$$

)

Euclidean Algorithm

- Given two integers A and B with A > B ≥ 0, this algorithm computes gcd(A, B)

Input: A, B [integers with $A > B \geq 0$]

Algorithm Body:

$a := A, b := B, r := B$

while $(b \neq 0)$ $b != 0$ in py/da

$r := a \bmod b$ $a \% b$

$a := b$

$b := r$

end while

$gcd := a$ Output: gcd [a positive integer]