Introduction to Number Theory

Kristian Guillaumier 04,05

http://webster.cs.um.edu.mt/kguil
kguil@cs.um.edu.mt

Number Theory

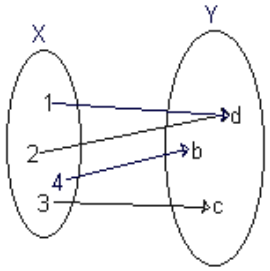
- Number theory is the branch of mathematics related to the study of positive numbers (called the Natural Numbers).
- Specifically the set:
  N = {1,2,3,4,5,…}
- Natural numbers are sometimes used to refer to both positive integers >= 1, or non-negative integers >=0.
- The set of natural numbers is said to be *countably infinite*.

Countablility

- Used to describe the size of a set.
- A set S is said to be countable if we have a surjective (onto) function:

  f : N→S

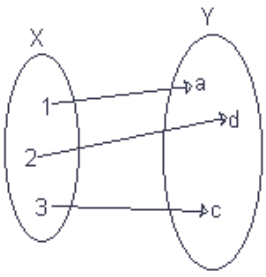
  (we can map all natural numbers to elements of S)



Countably Infinite

- A set is countably infinite if, apart from:

  f : N→S being surjective,
- f is bijective too (one-to-one and onto). I.e.:



Origins of Zero

- Natural numbers have been historically used for counting (“three pencils”) and ordering (“the 2nd smallest”).
- Zero was usually omitted from the natural numbers, but…
- A set-theoretical definition of natural numbers was developed and it was convenient to include zero (corresponding to the empty set).
- To be unambiguous if N includes zero, it can be written as N_0.

The Peano Axioms

- The Peano Axioms provide the precise definition of what is a natural number.
  - 0 is a natural number.
  - Every natural number n has a natural number successor denoted S(n).
  - No natural number n has S(n) = 0. I.e. 0 is not a successor of any natural number.
  - If n and m are natural numbers and n != m then S(n) != S(m).
  - If a set of numbers contains 0 and S(n), then n is in the set too. I.e. if a set contains 0 and also the successor to every number in the set than every number is in the set. (Induction).

Mathematical Induction

- Induction is a proof technique usually applied to natural numbers.
- In its simplest form induction behaves as follows:
  - Showing that a statement is true for n = 0,
  - Showing that if a statement is true for n=m, then it holds for n=m+1.
- An analogy is useful to understand this concept:
  - The first domino will fall.
  - Whenever a domino falls, the next one falls too.
  - This helps us conclude that ALL dominos will fall.

Example (1)

- Suppose we want to prove that:

$$0+1+2+\ldots+n = \frac{n(n+1)}{2}$$

- Proof:
  - Check for n = 0.
  - Clearly this is true. The sum of the first 0 natural numbers is 0 and 0.(0+1)/2 is 0 too.

Example (2)

- Assume the statement is true for n = m:

$$0+1+2+\ldots+m = \frac{m(m+1)}{2}$$

- Adding (m+1) to both sides yields:

$$0+1+2+\ldots+m+\mathbf{(m+1)} = \frac{m(m+1)}{2} + \mathbf{(m+1)}$$

Example (3)

- Lets apply some algebraic juggling to the RHS:

$$\frac{m(m+1)}{2} + (m+1) = \frac{m(m+1)}{2} + \frac{\mathbf{2}(m+1)}{\mathbf{2}}$$

$$= \frac{(m+2)(m+1)}{2} = \frac{(\mathbf{(m+1)} + 1)\mathbf{(m+1)}}{2}$$

Example (4)

- We have shown that:
  - Statement is true for m=0.
  - If statement is true for m then truth follows for m+1.

Properties of Natural Numbers

- The arithmetic addition and multiplication operators are closed for natural numbers.
  - Adding or multiplying any two natural numbers will yield another natural number.
- Arithmetic subtraction and division are not.

```
2 - 5 = -3
1 / 2 = 0.5
```

Preliminary (Monoid)

- A Monoid is a structure consisting of a set and a single binary operation
- (S,*) : S $\times$ S $\rightarrow$ S
- Such that:
  - It is associative: for all a, b, c in S:
    (a*b)*c = a*(b*c)
  - The identity element: there exists an element e such that:
    a*e = e*a = a

Definition of Addition

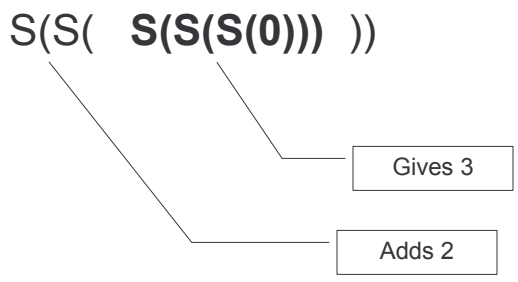
- Addition is defined as:
  - n + 0 = n
  - n + S(m) = S(n+m) for all n, m
- This definition makes (N, +) a commutative monoid with identity element 0.
  - Commutative: a+b = b+a

Explanation

- We know S(0) = 1.
- Consider 3 + 2:
  - We know that 3 = S(2) and 2 = S(1)…
  - So 3 + 2 is 3 + S(1) and also 3+S(S(0)).
  - From our rule:
    - 3+S(S(0))
    - = S(3 + S(0))
    - = S(S(3 + 0))
  - From the other rule, 3+0 = 0, so:
    - = S(S(3))
    - = S(4)
    - = 5

Further Explanation

- Another way to look at the example is:



Notes on Relations

- Let P and Q be sets.
- A relation between P and Q is a collection of ordered pairs (p,q) such that $p \in P$ and $q \in Q$.
- In other words, we are relating elements of the set P to those in set Q.
- Note that not necessarily all elements in P must be related to elements in Q.
- A relation between two sets is normally written P~Q.

Notes on Functions

- Let P and Q be sets.
- A function f from P to Q is a relation such that:
  - For each $p \in P$ there is one and only one associated $q \in Q$.
  - The set P is called the **Domain**.
  - The set Q is called the **Range**.

Notes on Equivalence Relations

- Let S be a set and r a relation between S and itself (S~S).
- r is an equivalence relation iff:
  - Every element in S is related to itself (reflexive: for example the >= or = functions but not >).
  - If the element a is related to b then b is related to a (Symetric: is_married_to).
  - If the element a is related to b and b is related to c, then a is related to c (transitive).

Notes on Partitions

- A partition of a set S is a number of non-empty subsets such that:
  - S is the union of all subsets.
  - The subsets are disjoint. I.e. if P and Q are sets, then $P \cap Q = \varnothing$.
- Each subset is called the **Part** of the partition.

Notes on Equivalence Classes

- The concept of relations, equivalence relations and partitions help us define the notion of Equivalence Classes.
- Consider:
  - The set C being the sets of all clothes.
  - The equivalence relation ~ defining ‘having the same colour’.
  - With the help of the equivalence relation we can partition the set C into parts having clothes of the same colour.
  - Now we have the equivalence class that is the part that contains red clothes.

Integers

- Set of integers is denoted by Z.
- Consider the set $N \times N$.
- Define a relation r saying that (a, b) is related to (c,d) if a+d = b+c.
- An integer n, -n or 0 is defined by considering the difference between the natural numbers a and b in (a, b) and all its equivalences. I.e.:
  - n: if a > b,
  - 0: if a = b,
  - -n if a < b.
- For example:
  - 0 = (0,0) = (1,1) = (2,2)…
  - 1 = (1,0) = (2,1) = (3,2)…
  - -3 = (0,3) = (1,4) = (2,5)…

Properties of Integers

- Closed under the operations of Addition, Multiplication and Subtraction (Unlike Natural Numbers).
- Associative: a + (b+c) = (a+b) + c
- Commutative: a + b = b + a
- Existence of Identity: a + 0 = 0 + a = a
- (Existence of) Inverse Elements: a + (-a) = 0
  - Note that there is no multiplicative inverse though.

Properties of Order

- Integers for a Totally Ordered Set:
  - A total order on a set S is a binary relation that is:
    - Antisymmetric: if a <= b and b <= a, then a = b.
    - Transitive: if a <= b and b <= c, then a <= c.
    - Total: either a <= b or b <= a.
- …but has no lower or upper bound.
- Ordering is: …-2 < -1 < 0 < 1 < 2…

Rational Numbers

- Rational numbers are the ratio between two integers.
- Rational numbers are demoted by Q.
- Can be written in an infinite number of forms: 1/2 = 2/4 = 3/6 = …
- Rational numbers are periodic:
  - 1/3 = 0.33333333…
  - 1/2 = 0.50000000…
- Note that irrational numbers cannot be expressed as a ratio between two integers.

Formal Construction of Q

- Defined as an ordered pair of integers (a,b) such that b != 0.
- Addition and multiplication between such pairs is defined as:
  - Addition: (a,b) + (c,d) = (ad + bc, bd).
  - Multiplication: (a,b) * (c,d) = (ac, bd).
- Remember that a rational can be written in an infinite number of ways (1/2 = 2/4…).
  - We need an equivalence relation to do this:
    - (a,b) ~ (c,d) iff ad = bc

Prime Numbers

- Natural numbers:
  - Greater than 1.
  - Whose divisors are one and itself.
- 2 is the only even prime numbers.

Composite Numbers

- Is a positive integer not prime and not equal to 1.
- So, n is a composite number if n = a $\times$ b, where a, b are natural numbers not equal to 1.
- Examples:
  - 1 (not prime/not composite, by defn).
  - 2 (prime/not composite).
  - 3 (prime/not composite).
  - 4 (not prime/composite, 4 = 2 $\times$ 2).
  - 15 (not prime/composite, 15 = 3 $\times$ 5).
  - …

Fundamental Theorem of Arithmetic

- Also known as the Unique Factorisation Theorem.
- Every positive integer greater than one can be written as a product of two prime numbers.
- Using this theorem we can view Primes are being the building blocks of positive integers.
  - $2 = 2^1$
  - $3 = 3^1$
  - $4 = 2^2$
  - $5 = 5^1$
  - $6 = 3^2$
  - $10 = 2 \times 5$
  - $60 = 2^2 \times 3 \times 5$
  - …

Proof (1)

- We need two prove two parts:
  - Every number can be written as a product of primes.
  - Any two representations for the same number are the same.

- Suppose a number CANNOT be written as a product of primes.
- Take the smallest such number and call it n.
- Clearly n cannot be prime because a prime is a product of itself.
- This means that $n = a \times b$ (i.e. n is composite).
- Therefore there must be a number D such that $1 < D < n$ and D divides n.
- Out of all the numbers that D can be, pick the smallest and call it D_s.
- Now, if D_s is composite, then it must have its own divisor F such that $1 < F < D_s$.
- This causes a problem because if F divides D_s, then it divides D also (which in turn divides n). This contradicts the minimality of D_s.
- In other words F must be prime.
- (Continued…)

Proof (2)

- Now we can write: $n = P \times n_1$.
- If n_1 is prime, then we are ready (n is written as a product of primes. If it is not,
- The same reasoning we applied for n above applies to n_1 here.
- This would make:
  - $n = P \times P' \times n_2$.
  - $n = P \times P' \times P'' \times n_3$.
  - Etc…
- The ever decreasing sequence $n > n_1 > n_2 > \ldots > 1$ cannot decrease for ever. At some point K must be a prime.
- So we get out prime representation:

$$n = P \times P' \times P'' \times P''' \times P'''' \times P''''' \times \ldots$$

Proof (3)

- To prove the second part (uniqueness) assume a number has two prime factorisations:
- $n = P_1 P_2 P_{3\ldots} P_r = Q_1 Q_2 Q_3 \ldots Q_s$
- Assume r <= s and the primes $P_1 P_2 P_{3\ldots} P_r$ and $Q_1 Q_2 Q_3 \ldots Q_s$ are written in order.
- Since the P sequence and the Q sequence yield n, then P_1 divides one of $Q_1 Q_2 Q_3 \ldots Q_s$ which are primes, so P_1 is equal to some Q_k. Also is is clear the $P_1 >= Q_1$.
- If we apply this reasoning starting from Q we get $Q_1 >= P_1$. So Q_1 must be equal to P_1.
- We can eliminate the common P and Q factors to get:
- $n = P_2 P_{3\ldots} P_r = Q_2 Q_3 \ldots Q_s$.
- If we go on eliminating all P's and Q's we get:
- $1 = Q_{r+1} Q_{r+2} Q_{r+3} \ldots Q_s$.
- Clearly all the remaining Q's must be 1 meaning that r = s and all P's and Q's are identical (i.e. a unique factorisation).

Greatest Common Divisor

- Once the prime factorisations for a number are known, finding their greatest common divisor is trivial:
- $6936 = \boldsymbol{2^3 \times 3} \times 17^2$
- $1200 = \boldsymbol{2^4 \times 3} \times 5^2$
- $GCD = 2^3 \times 3 = 24$

Euclid's Algorithm

- The algorithm is concerned with finding the Greatest Common Divisor between two numbers a and b.
- Written gcd(a,b).
- Pseudocode:

```
gcd(a,b)
{
  if (b == 0)
   return a;
  else
   return gcd(b, a mod b);
}
```

Coprimes (Relatively Prime)

- Two integers a, b are coprime (also called relatively prime) iff their GCD is 1.
- Examples:
  - 6 and 35 (coprime).
  - 6 and 27 (not coprime, divisible by 3).

Additive and Multiplicative Functions (1)

- An additive function is one such that when a and b are coprime (e.g. 6 and 35),
  $f(ab) = f(a) + f(b)$
- A function of completely additive if $f(ab) = f(a) + f(b)$ even when a and b are not coprime.
- An multiplicative function is one such that when a and b are coprime,
  $f(ab) = f(a) \times f(b)$
- A function of completely multiplicative if $f(1) = 1$ and $f(ab) = f(a) \times f(b)$ even when a and b are not coprime.

Additive and Multiplicative Functions (2)

- Remember the fundamental theorem says that any number can be represented by a product of (powers of) primes.
- Multiplicative fuctions have very interesting advantages because of this since:
- If, say, $n = P^a \times Q^b$, so $f(n) = f(P^a) \times f(Q^b)$.
- This can yield so significant computational efficiencies because the $f(P^a) \times f(Q^b)$ parts can be easier to compute then the f(n).