⇒

MAST-332/COMP-367
Techniques in Symbolic Computation:
Lecture 1 Notes

Numbers, Equivalence Relations (Ch.1)

Different types of numbers that we know are the following:

natural numbers: $\mathbb{N} = \{1, 2, 3, ...\}$

integer numbers: $\mathbb{Z} = \{... -3, -2, -1, 0, 1, 2, 3, 4, ...\}$

rational numbers: $\mathbb{Q} = \left\{ ... -\frac{1}{7}, -\frac{2}{7}, ... \frac{3}{2}, 1 = \frac{3}{3}, -5 = -\frac{5}{1}, ..., \frac{m}{n} \ (n \neq 0), ... \right\}$:

real numbers: $\mathbb{R} = \left\{ -3.0, -2.7, -\sqrt{2} ..., 0, 1, e, 4.3, ... \frac{m}{n}, ... \right\}$:

complex numbers: $\mathbb{C} = \{a + i\,b : \ a, b \in \mathbb{R}, \ i^2 = -1\}$:

ALL these types are in the form of sets.

Subset relations: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Rational numbers as sets of pairs of integers, *equivalence classes.*

Rational numbers are fractions of integers, $\frac{a}{b}$. However, unlike integers, they have a property that two rational numbers may look formally different but be in fact be the same (i.e. equal to each other), such as $\frac{2}{4} = \frac{30}{60}$:

One can say that these two numbers are equal because $2 \cdot 60 = 4 \cdot 30 \ (= 120)$:
Or in general, that $\frac{a}{b} = \frac{c}{d}$ **iff** (*i.e.* **if and** *only* **if**) $a \cdot d = c \cdot b$ (and b,d $\neq 0$).

But this definition does not define rational numbers as ***distinct*** (i.e. *unique*) objects.

Thus, the definition of rational numbers must resolve this problem of ambiguity.

The problem has been solved (500-300 B.C.) by representing a rational number given by the ratio of two integers, $\frac{a}{b}$, in the form of ***sets*** of ordered pairs of integer numbers,

$S = \{(m, n) : m, n \in \mathbb{Z}, n \neq 0\}$ such that $a \cdot n = b \cdot m.$

In this case the rational number $\frac{a}{b}$ can be treated as a representative of that set S, such that we can write

$\frac{a}{b} = \{(m, n) \mid a \cdot n = b \cdot m\}$:

At the same time, any pair in that set is equally treated as representative of the entire set. Often we use as representatives the pair of numbers with the smallest possible absolute value of a . That is the reduced form of the rational number. Say , $(2, 4)$, $(1, 2)$ **and** $(5, 10)$, are in the same set, where the reduced rational number is $\frac{1}{2} = (1, 2)$.

This definition divides the set $S = \{(m, n)\}$ of all possible pairs of integers into distinct subsets with no common element between any two of such subsets. Thus, the subsets

$\frac{2}{3} = \left\{(m, n) \,\middle|\, 2 \cdot n = 3 \cdot m\right\}$ **and** $\frac{24}{36} = \left\{(m, n) \,\middle|\, 24 \cdot n = 36 \cdot m\right\}$:

are the same because for all (m,n) $2\,n = 3\,m$ **iff** $24\,n = 36\,m$:

This is an example of dividing a set into distinct ***equivalence classes***:

Equivalence relations and equivalence classes:

The definition of rational numbers in terms of sets $Q = \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$: is an example of dividing a set into ***equivalence classes.***

Definition: We say that a relation on a set S is an ***equivalence relation*** (~)
if for $\forall\ s \in S$ it satisfies the following properties:

(1): ***Reflexivity property***: $s \sim s$: (an element in S is equivalent to itself).

(2): ***Symmetry property***: **if** $s1 \sim s2$ **then** $s2 \sim s1$:

(3): ***Transitivity property***: **if** $s1 \sim s2$ **and** $s2 \sim s3$ **then** $s1 \sim s3$.

The equivalence relation divides the set S into equivalence classes with no common element between any two different classes. Two elements are equivalent if they are in the same equivalence class.

In case of rational numbers we say that the ordered pair $(a, b \neq 0) \in Q$ is equivalent to

$(c, d \neq 0) \in Q$ if $ad = bc$: This is an ***equivalence relation on Q***.

Let us check the equivalence relations on Q:

1. **Reflexivity:** $(a, b) \sim (a, b)$ because $a \cdot b = b \cdot a$:

2. **Symmetry**: if $(a, b) \sim (c, d)$ then by definition of this relation, $a \cdot d = b \cdot c$.
Because the product of two numbers is commutative, it follows that

$\Rightarrow \quad d \cdot a = c \cdot b \;\Rightarrow c \cdot b = d \cdot a$:

This means, again by the given definition of this relation, that $(c, d) \sim (a, b)$

3. Let us check the **transitivity**:

Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $a \cdot d = b \cdot c$ **and** $c \cdot f = d \cdot e$

$\Rightarrow$ (*multiply the* 1*st* **by** f) $a \cdot d \cdot f = b \cdot c \cdot f$ **and**
(*multiply the* 2*nd* **by** b) $b \cdot c \cdot f = b \cdot d \cdot e$

$\Rightarrow a \cdot d \cdot f = b \cdot d \cdot e \;\Rightarrow\; a \cdot d \cdot f - b \cdot d \cdot e = 0$:

Using commutativity of the product of two numbers, and distributivity of the product over the sum, we have $(a \cdot f - b \cdot e) \cdot d = 0$:
Because $d \neq 0$, $\Rightarrow a \cdot f - b \cdot e = 0 \;\Rightarrow a \cdot f = b \cdot e$:
Therefore by the definition given, $(\boldsymbol{a, b}) \sim (\boldsymbol{e, f})$:

Exercises (class):

Consider the following relations on $\mathbb{Z}$. In each case decide whether the relation is an equivalence relation or not. If yes, describe the partition of $\mathbb{Z}$, and if not determine which property(s) of the equivalence relation fails.

(1) $a \sim b$ **if** $ab \geq 0$:

(2) $a \sim b$ **if** $ab > 0$:

(3) $a \sim b$ **if** $(a - b)$ is divisible by 3.

(4) $a \sim b$ **if** $a \geq b$:

GCD, primes & Euclid's Algorithm (Ch.3)

Division Theorem & GCD (Ch. 3A , 3B)

Division Theorem: Given nonnegative integers $a > 0$ and $b > 0$, there exist integers $q \geq 0$ and $0 \leq r < a$ such that $b = q \cdot a + r$; for given a and b the numbers q and r are unique.

Proof :
Part 1: the Existence of q **and** r is based on the idea that in the set C of nonnegative numbers in the form $C = \{c = (b - n \cdot a) \geq 0 |\ n \in \mathbb{Z}+\}$, there should be the smallest nonnegative number $r = b - q \cdot a$, and this number also should be less than a because otherwise there would be number a number $r1 = r - a = b - (q + 1)a \geq 0$ in C smaller than r.

Part 2: Uniqueness of q **and** r :

Suppose
$b = q \cdot a + r$ **and** $b = s \cdot a + t$: *where*, $0 \leq r, t < a$:
and *let* $r \geq t$:
Then
$\Rightarrow b - b = 0 = (q - s) \cdot a + (r - t)$:
$\Rightarrow a \cdot (s - q) = (r - t)$:

Hence:
$0 \leq r - t \leq r < a$:

But then we have
$$0 \leq (s - q) = \frac{(r - t)}{a} < 1 :$$

Because (s-q) is an integer, the only possibility to satisfy this inequality is to assume
$(s - q) = 0 : \Rightarrow s = q$ **and** *also* $r = t$:
This proves uniqueness of the numbers q and r.

Examples:
for a=12 and b=27, $\Rightarrow 27 = 2 \cdot 12 + 3$.
for a=27 and b=12, $\Rightarrow 12 = 0 \cdot 27 + 12$:

We call a the ***divisor***, b the ***divident***, q the ***quotient***, and r the ***remainder*** of division of the divident b by the devisor a.

Definition 1: We say that an intiger $a \neq 0$ ***divides*** b (or else a is a ***divisor*** of b, or else a is a ***factor*** of b), if $b = a \cdot q$ for some integer q.

In other words, a divides b if the remainder of division of b by a is $r = 0$. The symbolic notation for "a divides b" is $a|b$.

Examples:

1. $45 = 3 \cdot 15 + 0 = 3 \cdot 15$, thus 15 divides 45 (and also 3 divides 45, because $45 = 15 \cdot 3$).

2. $33 = 2 \cdot 16 + 1$, and $1 (< 16)$ is the remainder of the division of 33 by 16. Therefore 16 does not divide 33. Also note that 1 is the remainder of division of 33 by 2, because $1 < 2$, so also 2 does not divide 33.

3. $36 = 3 \cdot 10 + 6$, and 6 is the remainder of the division of 36 by 10. So 10 does not divide 36.

4. However, 6>3, so 6 is ***not*** the remainder of division of 36 by 3. Therefore we cannot claim based on the equation above that 3 does not divide 36. In fact, the remainder of division of 36 by 3 is 0 because $36 = 12 \cdot 3$, so 3 is a divisor of 36.

Definition (terminology): saying "*a* is a ***divisor*** of *b*" is the same as saying " *a* is a ***factor*** of *b*".

Examples:

1. The divisors (factors) of 15 are 1, 3, 5 and 15.
2. The factors (divisors) of 24 are 1, 2, 3, 4, 6, 8, 12 and 24.
3. The divisors of 17 are 1 and 17.

Note that the number 1 and *a* are divisors of any integer *a*.

The concept of '*divisor*' can be extended to negative integers as well. Say,
$15 = 3 \cdot 5 = (-3) \cdot (-5) = (-1) \cdot (-15)$, so $-1, -3, -5, -15$ could be all considered as divisors of 15. By default, however, we will be considering in this course only positive divisors for natural numbers, unless specially stated otherwise.

Definition 2: An integer *a* is said to be a ***common divisor*** of integers *b* and *c* if *a* divides *b* and *a* divides *c,*
i.e. if $a|b$ **and** $a|c$.

Example:
Common divisors of *b*=45 $(=1 \cdot 3 \cdot 3 \cdot 5)$ and $c = 30$ $(= 1 \cdot 2 \cdot 3 \cdot 5)$ are the numbers 1, 3, 5 and 15.

The number 1 is a common divisor for any pair of integers *a* and *b,* therefore it does not represent a particular interest.

Definition 3: A number *d* is said to be the ***greatest common divisor*** (GCD) of integer numbers *b* and *c* if
(i) *d* is a common divisor of *b* and *c*, ***and***
(ii) no common divisor of *b* and *c* is larger than *d*:

We denote the g.c.d. of *b* and *c* by (b, c) (***not*** to be confused with similar notation for rational numbers). Thus, $(45, 30) = (30, 45) = 15$:

In Maple the command for GCD is *gcd* (*a,b*):

$gcd(30, 45);$

Definition 4: A number c is said to be a ***common multiple*** of a and b if both a and b divide c.

For example, both 45 and 30 are a common multiples of 5 and 3. The simplest example of common multiple of a and b is their product, $c = ab$.

The smallest of all common multiples of a and b is the ***least common multiple*** and is denoted LCM.

N.B.: the notations '[a,b]' or '(a,b)' can be used for denoting LCM or GCD in a text line in Maple, but should NOT be used in the Maple command line for LCM or GCD since [....] in Maple is identified with the object type '*list*', and '(....)' represents the type '*sequence*':

```
> whattype([a, b]);
  whattype((a, b));
```

list

exprseq **(2.1.2)**

Definition 5: A natural number a is ***prime*** if $a \geq 2$ and it cannot be factored to a product of smaller natural numbers. That is, the only two divisors of a are 1 and a itself.

Example: The first 10 prime numbers are

```
> seq(ithprime(i), i = 1 ..10);
```

2, 3, 5, 7, 11, 13, 17, 19, 23, 29 **(2.1.3)**

Definition 6: Two numbers a and b are ***coprime*** if $(a,b) = 1$.
In other words, they do not have common factors other than 1.

Example:
(a) The numbers 15 $(=3\cdot5)$ and 8 $(=2\cdot2\cdot2)$ both are composite but coprime to each other.
(b) $26=2\cdot13$ **and** $-25=-5^2$ are coprime.

Example: Show that two consequtive natural numbers, a **and** $b=(a+1)$, are coprime.

Proof: Assume that a and b are not coprime. Then there should exist some $m \geq 2$ such that $a = m\cdot a1$ **and** $b = m\cdot b1$ for some integers $a1, b1$. Then $1 = b - a = m\cdot b1 - m\cdot a1 = m\cdot(b1 - a1)$:
However, this would mean that $m \geq 2$ divides 1, which is impossible. So a and (a+1) are coprime.

Exercise (class)**:**
Find the greatest common divisor of
(1) 35 and 65 ;

(2) 135 and 156 ;

(3) 17017 and 19210;
Very problematic if using only a calculator, although it can be done quickly using Maple:

$$gcd(17017, 19210);$$
$$17 \qquad \textbf{(2.1.4)}$$

Euclid's Algorithm (Ch. 3C)

How GCD can be calculated effectively?
The answer is provided by the method called ***Euclid's algorithm***.

Consider two natural numbers, a **and** $b \geq a$.
If a divides b then obviously $(a, b) = a$ because there cannot be a number larger than a that divides it.
If a does ***not*** divide b then

$$b = a \cdot q_1 + r_1$$

where q_1 is the quotient and $0 < r_1 < a$.
If now we denote $(a, b) = m$, then $a = m \cdot a_1$ **and** $b = m \cdot b_1$, so that $m \cdot b_1 = m \cdot a_1 \cdot q_1 + r_1$ (while b_1**and** a_1 are coprime). But then $m \cdot (b_1 - a_1 \cdot q_1) = r_1$:
This implies that m should divide r_1 as well, i.e. $r_1 = m \cdot c$, *with some* $c \in \mathbb{Z}$.
At the same time, neither (r_1, a) **or** (r_1, b) could be larger than m, because assuming otherwise and using similar transformation we can show that that number would represent a common divisor of a and b exceeding m.

Thus, m must be the GCD of a and r_1, i.e. $m = (r_1, a)$, and if r_1 divides a, then $m = r_1$.

By applying the same procedure again, but now to significantly smaller numbers a and r_1, etc.,

$$a = r_1 \cdot q_2 + r_2 :$$
$$r_1 = r_2 \cdot q_3 + r_3 :$$
$$\ldots\ldots$$
$$r_{k-2} = r_{k-1} \cdot q_k + r_k :$$
$$r_{k-1} = r_k \cdot q_{k+1} + 0 :$$

we will come to some step k when the remainder r_k will divide r_{k-1}. This will correspond to

$r_k = m.$

Example:
(19210,17017) = ?

Solution:

$19210 = 17017 \cdot 1 + 2193$:

$17017 = 2193 \cdot 7 + 1666$:

$2193 = 1666 \cdot 1 + 527$:

$1666 = 527 \cdot 3 + 85$:

$527 = 85 \cdot 6 + 17$:

$85 = 17 \cdot 5 + 0$:

Thus, 17=(19210,17017).

Check:
$gcd(19210, 17017)$;

(2.2.1)

Exercise (class):,
Apply Euclid's algorithm to find (121,365).

Solution: