MATH H113: Honors Introduction to Abstract Algebra

2016-01-25

- Euclidean Algorithm
- Partitions and equivalence relations

Proof of existence of gcd's

Euclidean algorithm:
Let $a, b \in \mathbb{Z}$ not both zero.
Step 1: If $b = 0$, then the answer is $|a|$.
Otherwise, let $r_0 = a$ and $r_1 = |b|$.
Then, for $n = 1, 2, 3, \ldots$ write $r_{n-1} = q_n r_n + r_{n+1}$ with $q_n, r_{n+1} \in \mathbb{Z}$ and $0 \leq r_{n+1} < r_n$.
When you reach $r_{n+1} = 0$, stop. The answer is r_n.

Example: compute $\gcd(2016, 98)$ where $r_0 = 2016, r_1 = 98$.
$2016 = 20 \times 98 + 56$
$98 = 1 \times 56 + 42$
$56 = 1 \times 42 + 14$
$42 = 3 \times 14 + 0$
Answer is 14.

Proof that the Euclidean algorithm actually gives you the gcd

Facts about the gcd:

i. If a and b are not both zero, then $\gcd(a, b) = \gcd(b, a)$. (From the definition, the common divisors are the same).
ii. The gcd only depends on the set of common divisors.
iii. If $a \neq 0$ then $\gcd(a, 0) = |a|$ because d is a common divisor iff $d \mid a$ ($d \mid 0$ always). So
    i. $d = |a|$ satisfies d is a common divisor ($|a| \mid a$)
    ii. If d' is a common divisor then $d' \mid a \therefore d' \mid |a| = d$
    iii. $|a| > 0$
iv. If a and b are not both zero, and if q is any integer, then $\gcd(a, b) = \gcd(a - qb, b)$
    If d is a common divisor of a and b, say $dx = a$ and $dy = b$; then $d(x - qy) = dx - ady = a - qb$, so $d \mid (a - qb)$ and $\therefore d$ is a common divisor of $a - qb$ and b.

Converse: $d \mid (a - qb)$ and $d \mid b \implies dz = a - qb$ and $dy = b$, $d(z + qy) = dz + qdy = a - qb + qb = a$, so $d \mid a$.
$\therefore$ d is a common divisor of a and b.
$\therefore$ the common divisors of a and b are the same as the common divisors of $a - qb$ and b.

v. $\gcd(a, b) = \gcd(a, -b)$

Back to the Euclidean algorithm:
If we end at Step 1 then the answer is correct by (iii).
Otherwise, $r_n = \gcd(r_n, 0) = \gcd(r_n, r_{n+1}) = \gcd(r_{n-1}, r_n) = \ldots = \gcd(r_1, r_0) = \gcd(|b|, a) = \gcd(|b|, a) = \gcd(a, b)$ by (iv) and (i). Because $n \mid b \iff n \mid (-b)$, so a and b have the same common divisors as a and $-b$.

Proposition:
If $d = \gcd(a, b)$ then there are integers x and y such that $d = ax + by$ (*d is a $\mathbb{Z}$-linear combination of a and b*).
Proof:
If you end at Step 1, then $d = (\pm 1)a$. Otherwise, follow the steps in the Euclidean algorithm to get x and y.

Back to the previous example:
$r_2 = 56 = 1 \times 2016 - 20 \times 98$
$r_3 = 42 = 98 - 56 = 98 - (1 \times 2016 - 20 \times 98) = 21 \times 98 - 1 \times 2016$
$r_4 = 14 = 56 - 1 \times 42 = 1 \times 2016 - 20 \times 98 - 1(21 \times 98 - 1 \times 2016) = 2 \times 2016 - 41 \times 98$

Remark:
You can also get gcds from the prime factorizations of $|a|$ and $|b|$.
In our example:
$2016 = 2^5 \times 3^2 \times 7$
$98 = 2^1 \times 3^0 \times 7^2$
$\gcd(2016, 98) = 2^1 \times 3^0 \times 7^1 = 14$
(take the smallest exponent for each prime).

Equivalence Relations

Definition:
A *relation* on a set A is a subset of $A \times A$.
If the subset is R, we may write aRb to mean $(a, b) \in R$, more often we write $a \sim b$.
Example: $\leq$ (when $A = \mathbb{R}$)
In that case $R = \{(a, b) \in \mathbb{R}^2 : a \leq b\}$.

Definition:
A relation $\sim$ on a set A is

- *reflexive* if $a \sim a$ for all $a \in A$

- *symmetric* if $a \sim b \implies b \sim a$ for all $a, b \in A$
- *transitive* if $(a \sim b \wedge b \sim c) \implies a \sim c$ for all $a, b, c \in A$

Definition:
An equivlance relation is a relation on a set that is reflexive, symmetric and transitive.
Example:
Let $f : A \to S$ be a function. Then the relation $\sim$ defined by $a \sim b$ iff $f(a) = f(b)$ is an equivalence relation on A.
Also $=$ on any set is an equivalence reltation
$\leq$ on $\mathbb{R}$ is *not* an equivalence relation.

Definition:
A *partition* of a set A is a collection of $\{A_i : i \in I\}$ of nonempty subsets of A such that: i. $\bigcup\limits_{i \in I} A_i = A$, and ii. $A_i \cap A_j = \emptyset$ for all $i, j \in I$ with $i \neq j$
Example:
$\{\{1,2,3\},\{4,5\},\{6\}\}$ is a partition of $\{1,2,3,4,5,6\}$
If $f : A \to B$ is surjective (onto), then $\{f^{-1}(b) : b \in B\}$ is a partition of A.

Equivalence relations and partitions are related by:
Definition:
Let $\sim$ be an equivalence relation on a set A, and let $a \in A$. Then the equivalence class of a is the subset $\bar{a} = \{b \in A : b \sim a\}$ of A.

Proposition:
Equivalence relations on a set A and partition of A are related:
$\{\text{equivalnce relations on } A\} \rightleftharpoons \{\text{partitions of } A\}$
bijective functions mutually inverse
$\sim \mapsto \{\bar{a} : a \in A\}$.
$p = \{A_i : i \in I\} \mapsto a \sim b$ if a and b lie in the same A_i