Notes

September 8, 2014

exercises

second part of chinese remainder theorem Section 1.3: exercises # 4, 6, 12, 18, 20, 24.

4.

$$
\begin{aligned}
20x \equiv 12 \mod 72 \\
\gcd(20, 12) = 4 \\
4|12 \\
ax = b + qn \\
20x = 12 + q7220 = 4a_1, 12 = 4b_1, 72 = 4m \\
a_1x = b_1 = qm \\
a_1x \equiv b_1 \mod m \\
5x \equiv 3 \mod 18 \\
ca_1 \equiv 1 \mod m \\
c5 \equiv 1 \mod 18 \\
55 = 18 * 3 + 1
\end{aligned}
$$

24. claim:remainder of integer when divided by 9.

proof:

$$
\begin{aligned}
n_0 \equiv r \mod 9 \\
n_0 = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + a_0 \\
a \equiv b \mod n \\
c \equiv d \mod n \\
ac \equiv bd \mod n \\
a \equiv b \mod n \to a^k \equiv b^k \mod n \\
10 \equiv 1 \mod 9 \\
10^k \equiv 1 \mod 9 \\
n_0 \equiv a_n + a_{n-1} + \cdots + a_0 \mod 9
\end{aligned}
$$

similar to 25

section 2.1

$f : S \longrightarrow T$ and S is domain, T is codomain.

$f' : S' \longrightarrow T'$

$f = f' \Leftrightarrow S = S', T = T'$ and $f(x) = f'(x) \forall x \in S$

The image of f is $f(s) = \{f(t) | x \in S\}$

example

$$f : R \to R$$
$$f(x) = x^2$$
$$\mathrm{Im} f = f(R) = [0, \infty)$$

one to one (injective functions) $f : S \to T$ $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

onto (surjective) $f : S \to T$ $f(S) = T$

one to one correspondences (bijective) satisfy both injective and surjective (one-to-one and onto)

inverse function $f : S \to T$ $f^{-1} : T \to S$. $f(f^{-1}(x)) = x \forall x \in T$ and $f^{-1}(f(x)) = x \forall x \in S$. defined iff f is bijective

section 2.2 equivalence relations

S set

an equivalence relation is a subset $R \subseteq S \times S$ with the properties

1. for all $x \in S$ we have that $(x, x) \in R$
2. $\forall x, y \in S$ if $(x, y) \in R$ then $(y, x) \in R$
3. $\forall x, y, z \in S$ if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$

notation

we write $a \sim b$ to indicate that $a, b \in R$

example

$$S = \mathbb{Z}$$
$$n \in \mathbb{Z}$$
$$n > 0$$

we say that $x \sim y$ iff

$$x \equiv y \mod n$$

example

$$S = \mathbb{R}$$

$x \sim y$ iff $x + y \geq 0$. is this equivalence? no $x + x$ might be negative

example

$$S = [0, \infty)$$

$x \sim y$ iff $x + y \geq 0$. is this equivalence? yes

note

equality is always equivalence relation, the trivial case

equivalence class

S is a set and is and equivalence relation. let $a \in S$, $[a] = \{x \in S | a \sim x\}$ where $[a]$ is equivalence class of a. $S/\sim$ is the set of all equivalence classes

example

$S = \mathbb{Z}$ and $\sim$ is the congruence modulo n, then the set $\mathbb{Z}/\sim$ has n elements: $[0], [1], \ldots, [n-1]$

observation

1. let $\sim$ be an equivalence relation on the set S. take two elements $a, b \in S$ then $a \sim b \Leftrightarrow [a] = [b]$
2. if $a \not\sim b$ then $[a] \cap [b] = \emptyset$
3. $S = \cup_{a \in S}[a]$. each element of S belongs to exactly one equivalence class. the equivalence classes form a partition of S.

   ### question

   if we have a partition of S, can we "naturally" define an equivalence on S? yes, two way relation $x \sim y$ iff x, y belong to the same subset of the partition.

observation

let $\sim$ be an equiv relation on S. then we can define a function $\pi : S \to S/\sim$. $\pi(x) = [x]$. aside (call $S/\sim$ factor set from now on). is this function surjective? $S/\sim$ is the set of all possible equiv classes, so π (the natural projection) is always surjective. it is injective iff every equiv classes has one element (itself) and is therefore the trivial equality relation.