Notes

August 27, 2014

chapters 1-5 in 420, chapter 6 in 421. chapter 1 should be review. one of the hardest, if not the hardest course. much new material. not necessary to solve all problems, but try and be able to discuss. will need to present solutions at least 3 times. assignments to be turned in will probably be selected from the group of problems that were assigned and discussed.

notation review

integers: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

natural numbers:$\mathbb{N} = \{0, 1, 2, 3, ...\}$ note this includes 0

divisibility $a, b \in \mathbb{Z}, b|a$ (b divides a) means $a = bc$ for some integer c

division algorithm

given two integers $a, b \in \mathbb{Z}$ where $b > 0$ there exists unique integers q and r such that $a = bq + r$ with $0 \leq r < b$

note that this is trivial without constraints on r because one can set $q = 0$ and $r = b$

proof

take $\mathcal{C} = \{a - bq \mid q \in \mathbb{Z}\}$

$\mathcal{C}^+ = \mathcal{C} \cap \mathbb{N}$

claim

$\mathcal{C}^+$ is non-empty. why?

if $a \geq 0$, then $a - b \cdot 0 \in \mathcal{C}^+$

if $a < 0$, then $a - b \cdot a = a(1 - b)$. $b > 0$ so $1 - b \leq 0$ so $a - ba \geq 0$

now take the *well ordering principle* (you can always find a smallest or least element of a subset of natural numbers)

let r be the smallest element of $\mathcal{C}^+$

$$r = a - bq$$

claim is that $r < b$

contradiction

assume $r \geq b$. then $r - b \geq 0$

$$\begin{aligned} r - b &= (a - bq) - b \\ &= a - b(q + 1) \in \mathcal{C} \end{aligned}$$

this means $r - b \in \mathcal{C}^+$ which is a contradiction because it is smaller than r which is supposed to be the smalled element in $\mathcal{C}^+$

we know that $r < b$ so there exists q, r with $a = bg + r$, $0 \leq r < b$.

to prove uniqueness, assume $a = bq_1 + r_1$ with $0 \leq r_1 < b$ and $a = bq_2 + r_2$ with $0 \leq r_2 < b$

prove 1 and 2 are the same, prove q get remainder for free.

subtract the two quantities

$$0 = b(q_1 - q_2) + (r_1 - r_2)$$

lets talk about r_1 and r_2. distance between r_1 and r_2 is at most b. draw it on a number line with r's between 0 and b to be convinced

$$\begin{aligned} r_2 - r_1 &= b(q_1 - q_2) \\ |r_2 - r_1| &= b\,|q_1 - q_2| \end{aligned}$$

since $|r_1 - r_2| < b$ the difference is zero and $r_1 = r_2$

gcd

greatest common divisor

definition

let $a, b \in \mathbb{Z}$ not both 0. we say that the positive integer d is the greatest common divisor of a and b if

1. $d|a$ and $d|b$ (always at least have one)
2. any other common divisor of a and b is also a divisor of d

   in other words, if $c|a$ and $c|b$ then $c|d$

uniqueness is implied by saying *the* greatest common divisor