Notes

August 29, 2014

last time assigned gcd stuff and assigned to read results

gcd definition

a, b not both 0, notation $\gcd(a, b) = (a, b)$

facts

1. gcd exists and is unique
   follows from assigned theorems.

   example

   $\gcd(6, 14) = 2$

2. the gcd of a and b is a linear combination of a and b. ie, there exist $m, n \in \mathbb{Z}$ such that $(a, b) = ma + nb$
   in fact $\gcd(a.b)$ is the smallest positive inegerthat is a linear combination of a and b

   $$\{ma + nb \mid m, n \in \mathbb{Z}\}$$

euclidean algorithm

$$(a, b) = (|a|, |b|)$$

we may assume that $a \geq b \geq 0$. $a = bq_1 + r_1$.

claim

$$\begin{aligned}
(a, b) &= (b, r_1) \\
d_1 = (a, b), &\quad d_2 = (b, r_1) \\
d_1|a &\rightarrow d_1|(bq_1 + r_1) \\
d_1|b &\rightarrow d_1|r_1 \\
&\rightarrow d_1|d2 \text{ because } d_2 = (b, r_1)
\end{aligned}$$

similarly show that $d2|d1$ hence d1=d2
now we see

$$a = bq_1 + r_1$$

$$\begin{aligned} b &= rq_2 + r_2 \\ r_1 &= r_2 q3 + r_3 \\ &\vdots \\ r_n &= \text{zero remainder because remainders are shrinking} \end{aligned}$$

so $(a, b) = (r_{n-1}, 0) = r_{n-1}$

example

find $(33, 9)$

$$\begin{aligned} 33 &= 9 * 3 + 6 \\ 9 &= 6 * 1 + 3 \\ 6 &= 3 * 2 + 0 \\ (33, 9) &= 33 & &= 9 - 1 * 6 \\ &= 9 - 1 * (33 - 3 * 9) \\ &= 9 - 1 * 33 + 3 * 9 \\ &= 4 * 9 + (-1) * 33 \end{aligned}$$

can also use euclidean algorithm to generate linear combination from gcd

1.2 prime numbers

definition

$p > 1$ is prime if the only positive divisors of p are 1 and p

$p > 1$ is prime if the only divisors of p are ± 1 and p

definition

we say that a and b are relatively prime if $\gcd(a, b) = 1$

proposition

let $p > 1, p \in \mathbb{Z}$ then p is prime iff the following property holds:

$a, b \in \mathbb{Z}$ and $p|ab$ then $p|a$ or $p|b$

only true if p is prime, $4 \not| 6 \cdot 6$

proof

assume p is prime. assume $p|ab$, then $(p, a) = 1$ or $(p, a) = p$. this is because the only divisor of p is p or 1.

case 1, $(p, a) = p$. then $p|a$ and we are done.

case 2, $(p, a) = 1$. then there exists $m, n \in \mathbb{Z}$ such that $mp + na = 1$.

$$\begin{aligned} mp + na &= 1 \\ bmp + bna &= b \\ & p|ab \rightarrow p|abp|bmp \end{aligned}$$

since $p|bmp$ and $p|bna$ therefore $p|b$

conversely

assume $\alpha|p$ with $\alpha > 0$. Nee to prove that $\alpha = 1$ or $\alpha = p$
$\alpha|p \to p = \alpha \cdot \beta$ with $\beta \in \mathbb{Z}$
by the property satisfied $p|\alpha or p|\beta$. if $p|\alpha$ since $\alpha|p$ we have $\alpha = p$. if $p|\beta$, since $\beta|p$ we have $\beta = p$
if $\beta = p$ then $\alpha = 1$