# MATH 360 HOMEWORK 1 SOLUTIONS

① Euclidean Algorithm:

Line 1 $a = bq_1 + r_1$ $\quad 0 < r_1 < b$

Line 2 $b = r_1 q_2 + r_2$ $\quad 0 < r_2 < r_1$

Line 3 $r_1 = r_2 q_3 + r_3$ $\quad 0 < r_3 < r_2$

$\vdots$

Line k-1 $r_{k-3} = r_{k-2} q_{k-1} + r_{k-1}$ $\quad 0 < r_{k-1} < r_{k-2}$

Line k $r_{k-2} = r_{k-1} q_k + r_k$ $\quad 0 < r_k < r_{k-1}$

Line k+1 $r_{k-1} = r_k q_{k+1} + 0$

(Need To Prove) ← N.T.P two things to prove $r_k = \gcd(a,b)$

① $r_k \mid a$ and $r_k \mid b$

② If $r \mid a$ and $r \mid b$ then $r \leq r_k$

Proof ① Line k+1 $\Rightarrow r_k \mid r_{k-1}$.

Then since $r_{k-2} = r_{k-1} q_k + r_k$ (line k)

$r_k$ also divides $r_{k-2}$.

Then line k-1 $\Rightarrow r_k \mid r_{k-3}$

Continuing the process we get $r_k \mid b$

then $r_k \mid a$.

② Suppose $r \mid a$ and $r \mid b$.

Then $r \mid r_1$ because line 1 $\Rightarrow r_1 = a - bq_1$

Then similarly b/c $r \mid b$ and $r \mid r_1$ we get $r \mid r_2$

(because line 2 $\Rightarrow r_2 = b - r_1 q_2$)

Continuing this process we get that $r \mid r_k$ So $r \leq r_k$

By ① & ②, $r_k = \gcd(a,b)$.

② Euclid's lemma

$p$ is prime, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

Proof Suppose $p$ is prime $p \mid ab$ and $p \nmid a$

Need To Show ← N.T.S. $p \mid b$.

$p$ prime, $p \nmid a \Rightarrow \gcd(a,p) = 1$

$\Rightarrow \exists\, s,t \in \mathbb{Z}$ such that $1 = as + pt$

Then $b = bas + bpt$

Since $p \mid ab$ we have $p \mid bas$.

Obviously $p \mid bpt$

So, $p \mid bas + bpt \Rightarrow p \mid b$.

③ Ch. 0 #4

let $a = 7$, $b = 11$

$$\boxed{1 = 3.7 - 2 \cdot 11}$$

also

$$\boxed{1 = 8 \cdot 7 - 5 \cdot 11}$$

Ch 0 #8

$a, b, c \in \mathbb{Z}$ s.t $a \mid c$ and $b \mid c$.

If $\gcd(a,b) = 1$ show that $ab \mid c$.

Show if $\gcd(a,b) \neq 1$ then result doesn't hold.

Proof: Suppose $a \mid c$, $b \mid c$, $\gcd(a,b) = 1$ and $ab \nmid c$.

Then $\exists$ a prime $p$ s.t. $p \mid ab$ but $p \nmid c$. Since $\gcd(a,b) = 1$ by Euclid's lemma either $p \mid a$ or $p \mid b$

If $p \mid a$, since $p \nmid c$ we get $a \nmid c$.

If $p \mid b$ since $p \nmid c$ we get $b \nmid c$.

So, we can't have $ab \nmid c$.

Hence $ab \mid c$.

Ch 0 #16

$126 = 3 \times 34 + 24$

$34 = 1 \times 24 + 10$

$24 = 2 \times 10 + 4$

$10 = 2 \times 4 + 2$ gcd.

$4 = 2 \times 2 + 0$

$2 = 10 - 2 \times 4$

$= 10 - 2 \times (24 - 2 \times 10) = 5 \times 10 - 2 \times 24$

$= 5 \times (34 - 24) - 2 \times 24 = 5 \times 34 - 7 \times 24$

$= 5 \times 34 - 7 \times (126 - 3 \times 34)$

$$\boxed{2 = 26 \times 34 - 7 \times 126}$$

(4) Ch 0 #21

A set with $n$ elements has $2^n$ subsets for every $n \in \mathbb{Z}^+$

Proof by Induction.

initial case: $n=1$

Subsets of a set, with a single element are $\emptyset$ and the set itself so

For $n=1$, $\#\text{subsets} = 2^1 = 2$.

inductive hypothesis:

Assume a set with $n$ elements has $2^n$ subsets.

Suppose $A$ has $n+1$ elements,

Say: $A = \{a_1, a_2, \dots, a_n, a_{n+1}\}$

Consider $B = \{a_1, \dots, a_n\}$

By the inductive assumption $B$ has $2^n$ subsets.

Subsets of $B$ are obviously subsets of $A$. $A$ will have additional subsets which are obtained by including $a_{n+1}$ to each of the subsets of $B$.

So number of additional subsets will be $2^n$ as well.

Total number of subsets of $A$ is then $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$

(We used the first principle of induction) $\square$

Ch 0 # 28 $f_n$: $n$th Fibonacci number

$f_1 = f_2 = 1$

$f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$.

Show that $f_n < 2^n$ $\forall n$

Proof by Induction

initial case $n=3$

$f_3 = f_2 + f_1$

$= 1+1 < 8 = 2^3$

inductive hypothesis:

Assume $f_k < 2^k$ for all $k < n$.

second principle

Prove that $f_n < 2^n$.

$$f_n = f_{n-1} + f_{n-2}$$

By inductive assumption $f_{n-1} < 2^{n-1}$ and $f_{n-2} < 2^{n-2}$

So, $f_n < 2^{n-1} + 2^{n-2}$

b/c $2^{n-1} > 2^{n-2}$

$< 2^{n-1} + 2^{n-1}$

$= 2 \cdot 2^{n-1} = 2^n$.

So, $f_n < 2^n$

Ch 0 # 41 ISBN for our book: $\langle 0\ 6\ 1\ 8\ 5\ 1\ 4\ 7\ 1\ 6 \rangle$

dot product with $\langle 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 \rangle$ is $54 + 8 + 56 + 30 + 5 + 16 + 21 + 2 + 6$

mod 11 $-1 + 8 + 2 + 7 + 5 + 5 + (-1) + 2 + 6 = 0$

(5) $S = \mathbb{Z}$, $aRb$ iff $5 \mid a-b$.

i) reflexivity: Is $aRa$ $\forall a \in S$?

i.e. Does $5 \mid a-a$ $\forall a \in \mathbb{Z}$? yes

ii) symmetry If $aRb$ then is it true $bRa$ $\forall a,b \in S$?

$aRb \Rightarrow 5 \mid a-b \Rightarrow 5 \mid -(a-b) \Rightarrow 5 \mid b-a \Rightarrow bRa$

iii) transitivity If $aRb$ and $bRc$ then is $aRc$, $\forall a,b,c \in S$?

$aRb$ and $bRc \Rightarrow 5 \mid a-b$ and $5 \mid b-c \Rightarrow 5 \mid a-b+b-c \Rightarrow 5 \mid a-c \Rightarrow aRb$

So $R$ is an equivalence relation

equivalence classes:

$\bar{0} = \{a \in \mathbb{Z} \mid 5 \mid a-0\} = \{5k \mid k \in \mathbb{Z}\}$

$\bar{1} = \{a \in \mathbb{Z} \mid 5 \mid a-1\} = \{5k+1 \mid k \in \mathbb{Z}\}$

$\bar{2} = \{5k+2 \mid k \in \mathbb{Z}\}$ similar for $\bar{3}$ and $\bar{4}$.