CENG535 COMPUTATIONAL NUMBER THEORY

Homework #2

Tolga Gölbaşı
12400002006

1- Let I be a non-empty set of integers closed under addition.

I is closed only when its closed under multipication aswell.

$\forall x,y \in I \quad x.y=z \quad | z \in I \iff -a \in I \ \forall a \in I$

Assume I is closed under multipication $:\Rightarrow$ this will give us I is ideal

therefore $\forall az \in I$

If $z=-1$ $-a \in I$

Assume $-a \in I \ \forall a \in I$ $:\Rightarrow$ we know already for $b>0$

$ab = \underbrace{a+a+\dots+a}_{b \text{ times}}$ exists in I

If ab exists $-ab$ exists because of our assumption we can write it as

$-ab = a(-b)$ If we say $-b=c$ we can see

that $ac \in I$ when $c<0$

this will prove us that I is closed under multipication.

2- $\forall a,b,c \in \mathbb{Z}$

a) $\gcd(a,b) \overset{?}{=} \gcd(b,a)$

Theorem 1: For all $a,b \in \mathbb{Z}$ theres greatest common divison d of a and b, and moreover $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$

$a\mathbb{Z}+b\mathbb{Z} = b\mathbb{Z}+a\mathbb{Z} = d\mathbb{Z}$ therefore $\gcd(a,b)=\gcd(b,a)$

b) $\gcd(a,b)=|a| \overset{?}{\iff} a|b$;

Assume $\gcd(a,b)=|a| :\Rightarrow |a| \mid b$ If $a \in \mathbb{Z}^+$ $a|b$ ①

$|a| \mid a$ If $a \in \mathbb{Z}^-$ $-a|b \Rightarrow a|b$ ②

① and ② $a|b$

Assume $a|b :\Rightarrow$ $a|a$ and $a|b \Rightarrow \gcd(a,b)=|a|$

gcd of two numbers has to be positive

c) $\gcd(a,0) \overset{?}{=} \gcd(a,a) \overset{?}{=} |a|$ and $\gcd(a,1) \overset{?}{=} 1$

$\gcd(a,0) = d$

We know that $0 \nmid a$ from previous theorems

and $a | a$ this will give us $\gcd(a,0) = |a|$ ①

$\gcd(a,a) = d$

We know $a|a$ from previous theorems

$\gcd(a,a) = |a|$ ②

$1 \wedge 2 = \gcd(a,0) = \gcd(a,a) = |a|$

$\gcd(a,1) = d$

1 is divided only by itself. $1|1$ and 1 divides all integers

$\gcd(a,1) = 1$

d) $\gcd(ca, cb) \overset{?}{=} |c| . \gcd(a,b)$

3 - Show that for all integers a, b with $d := \gcd(a,b) = 0$ we have

$\gcd(a/d, b/d) = 1$

$d = 0$ If $d = 0$ then a, b should be 0 $0/0$

$\gcd(\underset{\text{undefined}}{0/0}, \underset{\text{undefined}}{0/0}) =$ undefined

4 - Let n be an integer. Show that if a, b are relatively prime integers, each of which divides n, then ab divides n.

If a, b relatively prime $\gcd(a,b) = 1$

If a, b divides n $ak = n$ $k \in \mathbb{Z}$

$ab \overset{?}{|} n$ If $b | n$ and $ak = n$ and $\gcd(a,b) = 1$ then

b / k $k = bt$ $a.b.t = n \Rightarrow a.b | n$

5- $gcd(a,b)=1 \overset{?}{\Leftrightarrow} \forall p \in P \; p \nmid a$ or $p \nmid b$

Assume $gcd(a,b)=1 :\Rightarrow$ only 1 divides both so primes not dividing them as well

$\forall p \in P \; p \nmid a$ or $p \nmid b :\Rightarrow$ If no primes divides both only 1 divides them $gcd(a,b)=1$

6- Let $a, b_1, \ldots, b_k$ be integers. Show that $gcd(a, b_1 \ldots b_k)=1 \overset{?}{\Leftrightarrow}$ $\underbrace{gcd(a,b_i)}_{=1}$ for $i=1,\ldots,k$.

Assume $gcd(a, b_1 \ldots b_k)=1 :\Rightarrow$ a cant divide any b_i for $i=1,\ldots,k$ therefore $gcd(a,b_i)=1$ for $i=1,\ldots,k$

Assume $gcd(a,b_i)=1$ for $i=1,\ldots,k :\Rightarrow$ a and b_i for $i=1,\ldots,k$ relative prime $d=b_1 \ldots b_k$ will be relative prime with a as well $gcd(a, b_1 \ldots b_k)=1$

7- Let p be a prime and k an integer, with $0<k<p$. Show that the binomal coefficent

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad \text{is divisible by } p$$

$$x \in \mathbb{Z} \quad \binom{p}{k} = \frac{p.(p-1)\ldots 1}{k.(k-1)\ldots 1.(p-k)(p-k-1)\ldots 1} = \frac{p.(p-1)\ldots(p-k+1)}{k(k-1)\ldots 1} = x$$

If $x \in \mathbb{Z}$ and $0<k<p$ and p is prime then $k! \nmid p$ therefore $k! \mid (p-1)\ldots(p-k+1)$ $\quad x = p.a \quad a \in \mathbb{Z} \Rightarrow p \mid x$

$$a = \frac{(p-1)\ldots(p-k+1)}{k(k-1)\ldots 1}$$

8- Let $a,b,c \in \mathbb{Z}$ such that $c|ab$ and $\gcd(a,c)=1$. Prove that $c|b$.

$c|ab$, $\gcd(a,c)=1$ $\Rightarrow$ $b/ as+ct=1$ for $s,t \in \mathbb{Z}$

$b.a.s+b.c.t=1.b$

If c divides ab then c divides $b.as$ therefore

$b.a.s+b.c.t=b$ divided by $c \Rightarrow c|b$

9- Let p be prime, and let $a,b \in \mathbb{Z}$. Then $p|ab$ implies that $p|a$ or $p|b$

$p|ab \Rightarrow ab=pk$ p has to divide one of a or b since pk is divided by p

10- Let $a_1,\dots,a_k$ be integers, and if p is a prime that divides the product $a_1,\dots,a_k$, then $p|a_i$ for some $i=1,\dots,k$

$p|a_1 \dots a_k \Rightarrow pk=a_1 \dots a_k$ Every number is products of prime numbers so we can write $a_1=p_1 \dots p_r$ $a_2=q_1 \dots q_r \dots$ and so on

$a_1 \dots a_k = p_1 \dots p_k q_1 \dots q_k \dots$

$pk=p.q'_1 \dots q'_k$

If $p q'_1 \dots q'_r = p_1 \dots p_k q_1 \dots q_r \dots$ then one of primes in $p_1 \dots p_k$ is p therefore $\exists a_i \in \mathbb{Z}$

If a_i has p as it is composite $a_i=p.p_1 \dots p_k$ then $p|a_i$