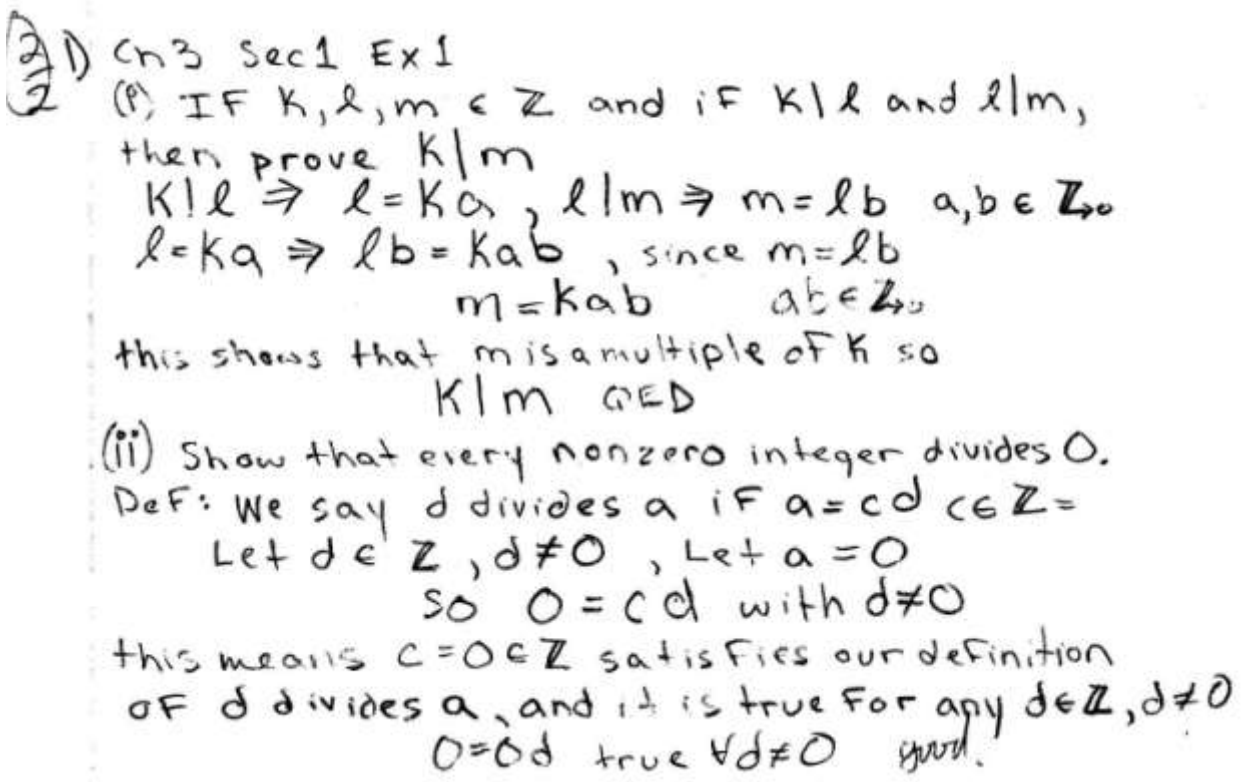
Homework 6

Solutions

1)



2 1) Ch 3 Sec 1 Ex 1

(i) If $k, \ell, m \in \mathbb{Z}$ and if $k \mid \ell$ and $\ell \mid m$, then prove $k \mid m$

$k \mid \ell \Rightarrow \ell = ka$, $\ell \mid m \Rightarrow m = \ell b$ $a, b \in \mathbb{Z}$

$\ell = ka \Rightarrow \ell b = kab$, since $m = \ell b$

$m = kab$ $ab \in \mathbb{Z}$

this shows that m is a multiple of k so

$k \mid m$ QED

(ii) Show that every nonzero integer divides 0.

Def: We say d divides a if $a = cd$ $c \in \mathbb{Z}$

Let $d \in \mathbb{Z}$, $d \neq 0$, Let $a = 0$

so $0 = cd$ with $d \neq 0$

this means $c = 0 \in \mathbb{Z}$ satisfies our definition of d divides a, and it is true for any $d \in \mathbb{Z}, d \neq 0$

$0 = 0d$ true $\forall d \neq 0$ good.

2)

(2) Suppose $n|A$ and $n|B$ ... is only a multiple of any positive integer, you restricted $x \in \mathbb{N}$, You want $0 \neq x \in \mathbb{Z}$

$A = an \quad B = bn \quad$ so $an = bn + C \quad a, b, n \in \mathbb{N}$

$an - bn = bn + C - bn$

$an - bn = C \Rightarrow n(a-b) = C$

$(a-b) \in \mathbb{N}$ because $A = B + C \quad (A, B, C \in \mathbb{N}) \Rightarrow$

$A \geq B \Rightarrow an \geq bn \Rightarrow a \geq b$

Since $C = n(a-b) \quad n|C$

Suppose $n|A$ and $n|C$

We can use argument identical to the above, since B and C are in arbitrary order

$n|A \wedge n|C \Rightarrow n|B$

suppose $n|B$ and $n|C$

$B = nb \quad b \in \mathbb{N} \qquad C = nc \quad c \in \mathbb{N}$

$A = B + C \Rightarrow A = nb + nc = n(b+c)$

$(b+c) \in \mathbb{N}$ as $b, c \in \mathbb{N}$ and $\mathbb{N}$ is closed under addition

so since $n \mid n(b+c)$, $n|A$ good.

3.1.5?

3)

3. $GCD(a,d)=k$, $k=ma-nd$ $m,n\in\mathbb{Z}_{>0}$

(2/2) We know $\exists c_1\in\mathbb{Z}$ s.t. $c_1k=a \Rightarrow \frac{a}{k}=c_1$

$\exists c_2\in\mathbb{Z}$ s.t. $c_2k=d \Rightarrow \frac{d}{k}=c_2$

So since $k=ma-nd$

$$\Rightarrow 1=\frac{ma-nd}{k}=\left(\frac{a}{k}\right)^m-\left(\frac{d}{k}\right)^n=c_1m-c_2n$$

$$\Rightarrow 1=c_1m-c_2n \quad (*)$$

Claim: $GCD(m,n)=1$

We know $GCD(m,n)\mid m$ and $GCD(m,n)\mid n$ and also multiples of m,n

$c_1,c_2\in\mathbb{Z}$ so $GCD(m,n)\mid mc_1-nc_2$ By #2, also divides their sum (substitute $*$)

$\Rightarrow GCD(m,n)\mid 1$

$\Rightarrow GCD(m,n)=1$ The only positive number to divide 1 is 1.

So m,n are relatively prime. ■

good.

4)

~~Ex. 4)~~ 3.1.7 Prove $r_3 < \frac{1}{2} r_1$

PROOF.

2/2

First, note that $r_3 < r_2$ as given

$\Rightarrow r_3 < r_2 \leq q_3 r_2$ since integer $q_3 > 0$

$\Rightarrow r_3 < q_3 r_2$

(since $q_3 = 0 \Rightarrow r_1 = r_3$ ⇒ violate division w/ remainder since $r_3 < r_1$)

$\Rightarrow \frac{1}{2} r_3 < \frac{1}{2}(q_3 r_2)$

$\Rightarrow \frac{1}{2} r_3 + \frac{1}{2} r_3 < \frac{1}{2} q_3 r_2 + \frac{1}{2} r_3$

$\Rightarrow r_3 < \frac{1}{2}(q_3 r_2 + r_3)$

$\Rightarrow r_3 < \frac{1}{2}(r_1)$ ✓

good.

5)

(2/2)

10. Prove $3 \mid n$ if 3 | the sum of n's digits.

=> let $n = n_n \cdots n_0$ where n_i is the digit in the i^{th} place.

$n = n_n \times 10^n + n_{n-1} \times 10^{n-1} + \cdots + n_0 \times 10^0$, want to show $3 \mid n$.

By hint: $3 \mid 10^i$ so $3c_i + 1 = 10^i$

So we can rewrite n as $n = n_n \times (3c_n + 1) + \cdots + n_0 \cdot (3c_0 + 1)$

$n = 3n_n c_n + n_n + \cdots + 3n_0 c_0 + n_0$

by writting again $n = 3n_n c_n + \cdots + 3n_0 c_0 + n_n + \cdots + n_0$

by distributive law $n = 3(n_n c_n + \cdots n_0 c_0) + (n_n + \cdots + n_0)$

So by Problem 2, Sec. 3.1 ; if $3 \mid 3(n_n c_n + \cdots + n_0 c_0)$

and $3 \mid 3(n_n c_n + \cdots + n_0 c_0)$

then $3 \mid n$.

qed

6)

11. Prove $9 \mid n$ if $9 \mid$ sum of n's digits

$\Rightarrow$ let $n = n_n \cdot 10^n + \cdots + n_0 10^0$

$9 \mid 10^i$ so $10^i = 9c_i + 1$ so we can rewrite n as

$n = n_n(9c_n + 1) + \cdots n_0(9c_0 + 1)$

$n = 9n_nc_n + n_n + \cdots 9n_0c_0 + n_0$ by the distributive law

$n = (9n_nc_n + \cdots + 9n_0c_0) + (n_n + \cdots + n_0)$ by commutativity.

$n = 9(n_nc_n + \cdots + n_0c_0) + (n_n + \cdots + n_0)$ by distributive law

Now by problem 2 in Sec 3.1 if $9 \mid n$ and $9 \mid 9(n_nc_n + \cdots + n_0c_0)$ then $9 \mid n_n + \cdots + n_0$ then

And similarly if $9 \mid 9(n_nc_n + \cdots + n_0c_0)$ and $9 \mid (n_n + \cdots + n_0)$ then $9 \mid n$.

7)

MATH 151
3/8/10

7a) Prove $GCD(n, n+1) = 1$. $\forall n \in \mathbb{Z}_{>0}$

let $k = GCD(n, n+1)$

$\Rightarrow k|n$ and $k|(n+1) \Rightarrow \exists c \in \mathbb{Z}$ s.t. $kc = n$, $\exists d \in \mathbb{Z}$ s.t. $kd = n+1 \Rightarrow kd = kc + 1$

We know $k|kd$ and $k|kc$ so by #2, $k|1$. good.

The only possible k is 1. ■

b) Let $k = GCD(n, n+2)$

$\Rightarrow k|n$ and $k|(n+2) \Rightarrow \exists c \in \mathbb{Z}$ s.t. $kc = n$, $\exists d \in \mathbb{Z}$ $kd = n+2 \Rightarrow kd = kc + 2$

Similarly we know $k|2$. Then the only candidates for k are 1 and 2.

The only way for n and $n+2$ to be divisible by 2 is if n is even

So $GCD(n, n+2) = \begin{cases} 1 & n \text{ odd} \\ 2 & n \text{ even} \end{cases}$ good ■

c) Let $g = GCD(n, n+k)$

$\Rightarrow g|n$ and $g|(n+k) \Rightarrow \exists c \in \mathbb{Z}$ s.t. $gc = n$, $\exists d \in \mathbb{Z}$ $gd = n+k \Rightarrow gd = gc + k$

$\Rightarrow g$ must divide k. by #2. so $g = gcd(n, k)$

So all divisors of k could be $GCD(n, n+k)$ ■

8)

8. §3.2 #3

Let a, b, c, be positive integers. Prove that if a is relatively prime to b and both a and b divide c, then ab divides c.

If $a \mid c$ then there exists a k such that $c = ak$. Since $b \mid c$, b must divide ak. Since b and a are relatively prime, b must divide k. Hence, $k = bm$ for some integer m. So,

$$\begin{aligned} c &= ak \\ &= abm \\ &= (ab)m \end{aligned}$$

We conclude that ab divides c. good.

9)

3.2, #4 (9) (2/2)

A.) Given: $a = p^3q^7r^3$, $b = p^6qs^4$

The gcd(a,b) is the number that contains all the prime factors common to both both a & b. $\Rightarrow$ $\gcd(a,b) = p^2q$

The lcm(a,b) is the smallest number that contains one of each prime factors (at least).

$\Rightarrow$ $\text{lcm}(a,b) = p^6q^7r^3s^4$

B.) Given: $\gcd(a,b) = k$, $\text{lcm}(a,b) = m$.

Let $a = k \cdot x$, $b = ky$, & $s = \frac{ab}{k}$. We have $\gcd(x,y) = 1$ from a previous problem. Now, a/m & b/m by definition. So, kxy/m.

Notice $kxy = s$, because $s = \frac{ab}{k} = \frac{kx \cdot ky}{k} = kxy$.

Thus, $s \leq m$. But both a,b divide s, so s is a common multiple of a,b. It follows that $m \leq s$, because $\text{lcm}(a,b) = m$. So, $s = m$.

But $s = m \Rightarrow m = \frac{ab}{k} \Rightarrow m \cdot k = ab$. Solved.

10)

SECTION 3.2

5) There are no three consecutive odd numbers that are primes other than 3, 5 & 7.

Let p_1, p_2, p_3 be three consecutive odd prime numbers where $p_1 > 3$. Note any whole number n, divided by three has three possible outcomes: $n = 3k+1$, $n = 3k+2$, or $n = 3k$, for some whole number k. Also note $p_2 = p_1 + 2$ & $p_3 = p_1 + 4$.

If $p_1 = 3k$ then $3 | p_1$ & p_1 is not prime.

If $p_1 = 3k+1$ then as $p_1 = p_2 - 2$ we have $p_2 - 2 = 3k+1 \Rightarrow p_2 = 3k+3 \Rightarrow p_2 = 3(k+1)$ thus $3 | p_2$ & p_2 is not prime.

If $p_1 = 3k+2$ then as $p_1 = p_3 - 4$ we have $p_3 - 4 = 3k+2 \Rightarrow p_3 = 3k+6 \Rightarrow p_3 = 3(k+2)$ thus $3 | p_3$ & p_3 is not prime.

Therefore for any prime number, p, at least one of the next two odd numbers must be divisible by 3 & 3, 5, 7 are the only three consecutive odd numbers that are prime