Homework Assignment 1. U27565203 JAE HONG LEE

Problem 2, 7, 11, 14

Exercise 1.2)
Let $n$ be a composite integer. Show that there exists a prime $p$ dividing $n$, with $p \leq n^{1/2}$

Composite integer: if $n>1$ is not prime | Prime: positive integer $n$, 1 and $n$ are only divisor of $n$

$n$ is a composite integer that means there is a integer $>1$ divides $n$.

By the Fundamental theorem of arithmetic, every non-zero integer $n$ can be expressed as $n = \pm p_1^{e1} \cdots p_r^{er}$, where $p_1 \ldots p_r$ are distict primes and $e_1 \ldots e_r$ are positive integer.

we can say $n = p \cdot q$, $p$ and $q$ are divisor of $n$. Either $p$ or $q$ has to be prime since $n$ is a composite #. they can be both prime too

By the theorem of arithmetic, $n$ is composed with prime numbers. Let's say smallest prime of $p$ is $p'$, smallest prime of $q$ is $q'$. By Induction Axiom of natural number there is a smallest positive number is $p$ and $q$.

Let's $p'$ and $q'$ are both bigger than $n^{1/2}$, $p' > n^{1/2}$, $q' > n^{1/2}$
The multiplication $p'$ and $q'$ $p'q'$ has to be bigger than $n^{1/2} \times n^{1/2} = n$, But this is a contradition. so there exist a prime $p$ dividing $n$, with $p \leq n^{1/2}$

Problem 2. Show that The Theorem 1.5 in the textbook also holds for the interval $(x, x+b]$. Does it hold in general for the intervals $[x, x+b]$ or $(x, x+b)$?

Theorem 1.5 in the textbook is " Let $a, b \in \mathbb{Z}$ with $b > 0$, and let $x \in \mathbb{R}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $r \in [x, x+b)$.

Theorem 1.5 is derived from theorem 1.4 "Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$."

Let $x$ be any real number, and consider the interval $(x, x+b]$. This interval Also contains precisely $b$ integers, same as $[x, x+b)$, $\lceil x \rceil, \lceil x+1 \rceil, \ldots \lceil x \rceil + b - 1$. So Apply Theorem 1.4 "with $a - \lceil x \rceil$ in place of $a$, it works.

For $[x, x+b]$, it would not work. Since it lose uniquesness. Let's say $r \in [x, x+b]$ for any real number $x$. suppose that $a = bq + r$ and $a = bq' + r'$ where $r, r' \in [x, x+b]$ subtracting these two we get $r' - r = b(q - q')$ so $r' - r$ is a multiple of $b$. However $x \leq r' \leq x+b$, $x \leq r \leq x+b$ implies $a = bq + x$ and $a = bq + x + b$ are both right $a = bq + x + b$ means $a = b(q+1) + x$ so $q$ is not unique.

For $(x, x+b)$, it would not work. Let's say $r \in (x, x+b)$, $x$ be any real number this interval contains $b-1$ integers when $x \in \mathbb{Z}$, $x+1, \ldots, x+b-1$. It is equal to when $a$ divided by $b$, the remainder will fall into the range $(0, b-1)$. For example when $a = 5$, $b = 3$ the remainder $r$ will be 2 but it does not in $(0, b-1)$ which is $(0, 2)$ so it is false.

Problem 3 Let $n$ be an integer. Show that if $a, b$ are relatively prime integers each of which divides $n$, then $ab$ divides $n$.

$n$ is an integer $n \in \mathbb{Z}$ and $a, b$ are relatively prime integers, so $\gcd(a,b) = 1$.
each of $a, b$ divides $n$ so $a|n$, $b|n$. if $ab|n$ prove is done.

Since $\gcd(a,b) = 1$ $\quad as + bt = 1$ $\quad s, t \in \mathbb{Z}$ if we multiply both side by $n$ $\quad asn + btn = n$ $\quad ab$ divides $asn$ because $a$ divides $a$, $n$ is divided by $n$, $ab$ also divides $btn$ because $b$ divides $b$, and $a$ divides $n$.

So when $a, b$ are relatively prime, $a$ divides $n$, $b$ divides $n$ then $ab$ divides $n$.

Problem 4 Let $p$ be a prime and $k$ an integer, with $0 < k < p$. Show that the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ which is an integer is divisible by $p$.

From Appendix 2 "Binomial coefficient is $\binom{n}{k} := \frac{n!}{k!(n-k)!}$, $\binom{n}{n} = \binom{n}{0} = 1$

and for $0 < k < n$, we have pascal's identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ "

Since $p$ is a prime and $k$ is an integer $k \nmid p$ so $\gcd(k, p) = 1$.

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$ so we can say $\frac{p \times (p-1) \times (p-2) \times \cdots (1)}{k \times (k-1) \times (k-2) \cdots \times 1 \times (p-k) \times (p-k-1) \times \cdots 1}$ then this would be

$\frac{p \times (p-1) \times \cdots \times (p-k+1)}{k \times (k-1) \times (k-2) \times \cdots 1}$ since $(p-k)!$ would be a part of $p$, it can be removed.

When we multiply $k$ on the $\binom{p}{k}$, $k \cdot \binom{p}{k}$ would be $\frac{p \times (p-1) \times \cdots \times (p-k+1)}{(k-1) \times (k-2) \cdots \times 1}$

binomial coefficient $\binom{p}{k}$ is an integer so $k \times \binom{p}{k}$ would be also an integer

Since $k \times \binom{p}{k}$ is $\frac{p \times (p-1) \times \cdots (p-k+1)}{(k-1) \times (k-2) \times \cdots 1}$ it is divisible by $p$ so $p \mid k \cdot \binom{p}{k}$

Since $p$ and $k$ are relatively prime, $\binom{p}{k}$ is divisible by $p$.