CISC 102 (Fall 20)
Homework #7: Number Theory (30 Points)

Student Name/ID: Amy Brons / 20252295

1. (2 pts)
   Let a be any integer > 1. Prove that a and $a+1$ are relatively prime.
   Assume that they are not prime.
   Therefore for integer $k, k \neq 1$ And therefore we can have the following:
   $k * n = a(n \neq 1)$
   $k + q = a + 1(q \neq r)$
   If we subtract we can get:
   $k * (q - n) = 1$
   However this can only be true if $k = 1$ and if $q - n = 1$.
   $\therefore a$ and $a+1$ must be relatively prime.

2. (4 pts)
   Let a, b and c be integers
   Prove the following:

   (a) $2ab \leq a^2 + b^2$ (Hint: consider $(a-b)^2$)
   We should use this formula to start:
   $(a-b)^2 = a^2 - 2ab + b^2$
   We can then determine:
   $a^2 - 2ab + b^2 \geq 0$
   Now we can add $2ab$ to both sides:
   $2ab \leq a^2 + b^2$
   $\therefore$ this is proved.

   (b) $ab + ac + bc \leq a^2 + b^2 + c^2$
   (Hint: consider $(a-b)^2 + (b-c)^2 + (c-a)^2$)
   We can determine that $0 \leq (a-b)^2$
   We can determine that $0 \leq (b-c)^2$
   We can determine that $0 \leq (c-a)^2$
   Now can plug these in:
   $0 = 0 + 0 + 0 \leq (a-b)^2 + (b-c)^2 + (c-a)^2$
   Now we can use this formula: $(a-b)^2 = a^2 - 2ab + b^2$
   $0 \leq a^2 - 2ab + b^2 + b^2 - 2bc + c^2 + c^2 - 2ac + a^2$
   We can add $2ab + 2bc + 2ac$ to each side:

$2ab + 2bc + 2ac \leq 2a^2 + 2b^2 + 2c^2$
Now divide by two:
$ab + bc + ac \leq a^2 + b^2 + c^2$
$\therefore$ this is proved.

3. (4 pts)
Prove the following statements:

(a) For any integer a there is an integer k such that one of the following is true:
$a = 5k$
$a = 5k + 1$
$a = 5k + 2$
$a = 5k + 3$
$a = 5k + 4$

For this answer we need to see what each question is asking us. For example $a = 5k$ requires that a be divisible by 5, and still be a full number. Therefore $\frac{a}{5} = k$. Therefore $\frac{a}{5} = k$. So here we can prove this true, if the integer a is still an integer when divided by 5.

For $a = 5k + 1$ we need to use an a integer that is divisible by 5, after subtracting 1.Therefore $\frac{a-1}{5} = k$. So here we can prove this true, if $a - 1$ is still an integer when divided by 5

For $a = 5k + 2$ we need to use an a integer that is divisible by 5, after subtracting 2. Therefore $\frac{a-2}{5} = k$. So here we can prove this true, if $a - 2$ is still an integer when divided by 5

For $a = 5k + 3$ we need to use an a integer that is divisible by 5, after subtracting 3. Therefore $\frac{a-3}{5} = k$.So here we can prove this true, if $a - 3$ is still an integer when divided by 5

For $a = 5k + 4$ we need to use an a integer that is divisible by 5, after subtracting 4. Therefore $\frac{a-4}{5} = k$.So here we can prove this true, if $a - 4$ is still an integer when divided by 5

Because $a = 5k + 5$ is another multiple of 5, we can see that any value a there is a integer k that satisfies one of the following. For examples:
a = 5 is satisfied by a= 5k, because it is divisible by 5.
a= 6 is satisfied by a = 5k+1 because we bring over the -1 and then it is divisible by 5.
a = 7 is satisfied by a = 5k +2 because we bring over the -2 and then it is divisible by 5.
a = 8 is satisfied by a = 5k +3 because we bring over the -3 and then it is divisible by 5.

a = 9 is satisfied by a = 5k +4 because we bring over the -4 and then it is divisible by 5.
And then we start back with a= 5k, because the value a=10 is already divisible by 5. Therefore this starts over every 5th integer for a.

(b) In any sequence of five consecutive integers, exactly one of them is a multiple of 5
In this sequence:
(a, a+1, a+2, a+3, a+4)
$a_k = 5q$
Because any number ending in 0 or 5 is divisible by 5, it is logical that in any sequence of five consecutive integers, one of them must end with this. There are no exceptions to this rule (ie: (1,2,3,4,5), (12,13,14,15,16)).
This logically follows that if there is at-least one integer that ends in a 0 or 5 in each sequence, there must be atleast one multiple of 5.
p = The integer ends in 0 or 5.
q = The integer is divisible by 5.
r = Ending in 0 or 5 means that the number is divisible by 5.
$p \wedge r \rightarrow q$
$\therefore$ In any sequence of five consecutive integers, exactly one of them is a multiple of 5.

4. (4 pts)
Prove the following statements:

(a) If $n > 1$ is composite, then n has a positive divisor d such that $d \leq \sqrt{n}$
If n is composite, by definition:
$n = ab$
Therefore this means that both a and b are divisors of n, and positive. This means that n has a positive divisor d that is less than or equal to $\sqrt{n}$. This is if $a \geq \sqrt{n}$ and $b \geq \sqrt{n}$ then $ab \geq \sqrt{n} * \sqrt{n} = n$, which is not true. Therefore it must be that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
$\therefore d \leq \sqrt{n}$

(b) If $n > 1$ is not divisible by any prime p where $p \leq \sqrt{n}$, then n is a prime number
$p \leq \sqrt{n}$
$p^2 \leq n$
If n is not divisible by p, where $p^2 \leq n$, then n is not prime.
Because prime numbers are only divisible by 1 and themselves, we can see that n is prime because $p^2 \leq n$ for 1 is $1^2 \leq n$ is correct because we defined $n > 1$
$\therefore$ if $n > 1$ is not divisible by any prime p where $p \leq \sqrt{n}$, then n is a prime number.

5. (4 pts)

Let a, b and m be positive integers.

(a) (a) Prove $gcd(m \cdot a, m \cdot b) = m \cdot gcd(a, b)$

Given that $a, b, m \geq 0$.

$n = gcd(a, b)$

n must divide both a and b.

$n|a$

$n|b$

Therefore exsits:

$a = nc$

$b = nd$

And multiply by m so

$ma = mnc$

$mb = mnd$ and since c and d are positive we can divide both ma and mb by mk

$mn|ma$

$mn|mb$

$\therefore mn|gcd(ma, mb)$

Let $k|gcd(ma.mb)$

$ma = kg$

$ma = kh$

If k divides m, then n also divides k also divides mn. If k divides and both a and b then $k|gcd(a, b)$ and therefore $k|n$ and $k|mn$ because $n = gcd(a, b)$

However if not, then k = pq, so p divides m and q divides a and b.

$p|m$

$q|a$

$q|b$

This means that $q|gcd(a, b) = n$ and $k = pq|mn$

Therefore every divisor of $gcd(ma, mb)$ is also a divisor fo mn and mn is the greatest common divisor of ma and mb.

$\therefore gcd(ma, mb) = mn = mgcd(a, b)$

(b) Prove that if $gcd(a, m) = d$ and $gcd(b, m) = 1$, then $gcd(a \cdot b, m) = d$

$gcd(a, m) = d$

$d|a$

$d|m$

Therefore there exists a positive integer k and g such that:

$a = dk$

$m = dg$

Then multiply each side:

$ab = dkb$

$m = dg$

Since d, g, and kb are integers then we can do this:

$d|ab$

$d|m$

If d divides both ab and m then:

$d|gcd(ab, m)$ Let $n|gcd(ab, m)$
$n|ab$
$n|m$
There exists a positive integers p and q such that
$ab = np$
$m = nq$
If n divides a, then n divides both a and m. Therefore $n|gcd(a, m)$. However, this also means that $n|dasd = gcd(a, m)$.
If n divides b, then n divides both b and m. Therefore $n|gcd(b, m)$. However, this also means that $n|1 = gcd(b, m)andn = 1$ and n is a positive integer.
If n does not divide a or b then $n = pq$ such that p divides a and q divides b:
$p|a$
$q|b$
However this means that $q|b$ and $q|m$ which implies that $q|1as1 = gcd(b, m)$. This also implies that $n = p$ divides a and therefore it it not possible for n to divide a nor b.
Therefore evert divisor of $gcd(ab, m)$ is also a divisor of d and therefore d is the greatest common divisor. $\therefore gcd(ab, m) = d$

6. (2 pts)
Prove the following:
Let a be a positive integer. Then $gcd(a, a + 2) = 1$ or 2
Ler $gcd(a, a + 2) = d$. Then we divide d with a and a+2.
$d|a + (a + 2) = 2(a + 2)$
$d|(a + 2) - a = 2$
Therefore d is the largest common divisor of 2(a+1) and 2.
However:
$gcd(2(a + 2), 2)$
$= 2gcd(a + 1, 1)$
$= 2 * 1$
$= 2$
$\therefore$ d divides 2, and $d = 1or2$

7. (2 pts)
We can extend the definition of gcd to any finite set of integers:
For any set of integers $\{a_2, a_2, \ldots, a_k\}$, define $gcd(a_1, \ldots, a_k)$ to be the largest integer g such that $g \mid a_i \quad \forall i \in \{1, 2, \ldots, k\}$
Prove or disprove:
$gcd(a_1, a_2, a_3) = 1$ if and only if $gcd(a_1, a_2) = gcd(a_1, a_3) = gcd(a_2, a_3) = 1$
(Remember, to disprove a proposition we only need to show a single example where it is not true.)
To disprove this, we nee only one example where this is not true. We can immediately

see that this is not true, as $gcd(a_1, a_3)$ will not always equal the same as (a_1, a_2) for example:
$gcd(a_1, a_2) = gcd(a_1, a_3) = gcd(a_2, a_3) = 1$ for 2,3,4:
$gcd(2, 3) = gcd(2, 4) = gcd(3, 4) = 1$
$1 = 2 = 1 = 1$ is not true.
Therefore this is disproved.

8. (2 pts)
We can define the least common multiple for a set of k integers as follows:
$lcm(a_1, \ldots, a_k)$ is the smallest positive integer that is a multiple of each of the a_i values.
Let $\{a_1, a_2, \ldots, a_k\}$ be a set of positive integers and let $m = lcm(a_1, \ldots, a_k)$
Prove that if n is any positive integer such that $a_1|n,\ a_2|n,\ \ldots\ a_k|n$ then $m|n$
Using division we can see:
$n = mq + r$
Where $r \geq 0, r \leq m$. If $r = 0, n = mq, som|n$ and therefore we are done.
So if $r \geq 0$, then $r = n - mq$.
since every $a|n$ and every $a|m$ then every $a|r$
Therefore r is a common multiple of every a.
r is also a positive integer such that $r \leq m$
However this is contradiction of lcm, so this is not possible.

9. (4 pts)

(a) Find the greatest common divisor of 1064 and 856.
Using the Euclidean algorithm we can see:
$1064 = 856 * 1 + 208$
$865 = 208 * 4 + 24$
$208 = 24 * 8 + 16$
$24 = 16 * 1 + 8$
$16 = 8 * 2 + 0$
Therefore the greatest common divisor is 8.

(b) Find integers x and y so that $1064x + 856y = \text{gcd}(1064, 856)$.
Here we can substitute gcd(1064,856) with 8:
$8 = 24 - 16$
$= 24 - (208 - 24 * 8)$
$= -208 + 24 * 9$
$= -208 + (856 - 208 * 4) * 9$
$= 856 * 9 - 208 * 37$
$= 856 * 9 - (1064 - 856) * 37$
$= -37 * 1064 + 46 * 856$
Therefore we can take $x = -37, andy = 46$ as one solution.

10. (2 pts)
Prove, using only the definition of **congruence modulo n** ,

(a) that if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$
By definition:
$a - b = nk$ and
$b - c = nq$
Add:
$(a-b) + (b-c) = nk + np$
$a - c = n(k+p)$
Then we can divide by n:
$\therefore a \equiv c \pmod{n}$

(b) that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$
By definition a divides b if there exists an integer c such that $b = ac$
and a is congruent to b modulo n if n divides $a - b$
By definition of the congruence:
n divides $a - b$
n divides $c - d$
Then by definition we can make the following equations:
$a - b = nk$
$c - d = np$
Add :
$(a-b) + (c-d) = nk + ng$
$a - b + c - d = n(k+g)$
$(a+c) - (b-d) = n(k+q)$
Then we can distribute the negative and divide by n:
$\therefore a + c \equiv b + d \pmod{n}$.