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

Student Name/ID:. . . . .

1. (2 pts)
Let a be any integer > 1. Prove that a and $a+1$ are relatively prime.
Assuming that a and $a+1$ are not relatively prime. For some integer k, we have the following equations:
$k \times n = a$ (where n is not equal to 1)
$k \times m = a+1$ (where m is not equal to 1 or n)
Sub in first equation into second: $k \times m = (k \times n) + 1$
$(m-n)k = 1$
This statement is only true if $m = 1$ and if $m - n = 1$, $\therefore$ 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 $(a-b)^2$)
   $\Leftrightarrow 0 \leq a^2 - 2ab + b^2$
   $\Leftrightarrow 0 \leq (a-b)^2$ After simplifying this it shows that for the inequality to be true $a - b = 0$ so $a = b$, or the other possibility is that $a \geq b$.

   (b) $ab + ac + bc \leq a^2 + b^2 + c^2$
   (Hint: consider $(a-b)^2 + (b-c)^2 + (c-a)^2$)
   $\Leftrightarrow 0 \leq a^2 - ab + b^2 - bc + c^2$
   $\Leftrightarrow 0 \leq \frac{1}{2}(2a^2 - 2ab + 2b^2 - 2bc + 2c^2)$
   $\Leftrightarrow 0 \leq \frac{1}{2}((a^2 - 2ab + b^2) + (b^2 - 2bc + c^2) + (c^2 - 2ac + a^2))$
   $\Leftrightarrow 0 \leq \frac{1}{2}((a-b)^2 + (b-c)^2 + (c-a)^2))$
   $\Leftrightarrow 0 \leq (a-b)^2 + (b-c)^2 + (c-a)^2)$
   From this we get that $a = b = c$ for the inequality to be true.

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:
   $a = 5k$
   $a = 5k + 1$
   $a = 5k + 2$
   $a = 5k + 3$

$a = 5k + 4$
This is true that any integer a can be expressed with any of the following formulas. Here the formulas are in the same format as in the quotient and remainder equation. Since when you divide a number by 5 the only possible remainders are 0,1,2,3, and 4, and there are all found in the equations above. It would not make sense if there was a negative remainder since it has to be positive, and a remainder ≤ 5 could be simplified to one of the above relations since 5 can go in again with that larger remainder. $\therefore$ we can conclude that for any integer a there is an integer k such that one of the above equations is true.

(b) In any sequence of five consecutive integers, exactly one of them is a multiple of 5

For this we only need to look at the first equation; $a = 5k$, this equation will always result in 5 times a number, so it would be a multiple of 5 in every sequence. If $k = 0$ it is also true since 0 is a multiple of every number. $\therefore$ we can conclude that in any sequence of consecutive integers there will always be 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, then $n = ab$ where $a > 1$ and $b > 1$. We suppose that $b \geq a$. Let d be the prime divisor of a. From the we get $d \leq a \leq b$. We can change $d \leq \sqrt{n}$ to $d^2 \leq n$.
So $d^2 \leq a^2 \leq ab = n$
$\therefore$ since $d|a$ and $a|n$ then $d|n$

(b) If $n > 1$ is not divisible by any prime p where $p \leq \sqrt{n}$, then n is a prime number
Proving this by contradiction (assuming n is composite:
$n = p \times q$ (p and q are two prime numbers)
$\sqrt{n} = m \rightarrow n = m^2$ (an integer m)
$\rightarrow p|n, q|n$
if $p < m$: p=prime and p=divisor of n
if $p > m$: $n = p \times q = m^2$, so $q < m \rightarrow q$ is a prime number.
$q =$ divisor of n such that $q < m$
Since we have proven the contradiction, n is not a composite number, and we have proven that it is a prime number.

5. (4 pts)
Let a, b and m be positive integers.

(a) (a) Prove $gcd(m \cdot a, m \cdot b) = m \cdot gcd(a, b)$
Let $d = \gcd(a, b)$
$xa + yb = d$ (x and y are integers)
$mxa + myb = md$
x(ma) + y(mb) = md
$\therefore \gcd(ma, mb) = m \gcd(a, b)$

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

$d_1 = \gcd(b, m)$ and $d_2 = \gcd(ab, m)$

From this we have $ax_1 + my_1 = d_1$, $abx_2 + my_2 = d_2$, and $ax + my = 1$
Multiply $ax + my = 1$ by d_1 and rearrange to show $d_2|d_1$
$d_1(ax + my = 1)$
$ax(bx_1 + my_1) + md_1y = d_1$
$ab(xx_1) + m(axy_1 + d_1y) = d_1$
Since $d_2 = \gcd(ab, m)$ divides any integer combination of ab and m, then $d_1|d_2$

Multiply $ax + my = 1$ by d_2 and rearrange for $d_1|d_2$
$d_2(ax + my = 1)$
$ax(abx_2 + my_2) + md_2y = d_2$
$b(a^2xx_2) + m(axy_2 + d_2y) = d_2$
Since $d_1 = \gcd(b, m)$ divides any integer linear combination of b and m, then $d_1|d_2$

$\therefore$ since we have $d_1|d_2$ and $d_1|d_2$, and d_1 and d_2 are none-negative, we conclude that $d_1 = d_2$.$\therefore$ $\gcd(ab, m) = \gcd(b, m)$

6. (2 pts)
Prove the following:
Let a be a positive integer. Then $gcd(a, a + 2) = 1$ or 2
Let $\gcd(a, a + 2) = d$. Then d divides a and $a + 2$. So d divides $a + a + 2 = 2(a + 1)$, and d divides $(a + 2) - a = 2$. We now see that d is the common divisor of $2(a + 1)$ and 2.
$\gcd(2(a + 1), 2) = 2\gcd(a + 1, 1) = 2 \times 1 = 2$
$\therefore$ d divides 2. $d = 1$ or $d = 2$.

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.)
Let $a_1 = 1$, $a_2 = 2$, $a_3 = 4$
$\gcd(1, 2) = 1$
$\gcd(1, 4) = 1$
$\gcd(4, 2) = 2$
$\therefore$ we have disproved this example since only two of the gcd's equal to 1, and the other doesn't equal to 1. So we see that all the gcd's do not equal to each other and 1 proving this statement wrong.

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 $a_1|n,\ a_2|n,\ \dots\ a_k|n$ then $m|n$
Proving using contradiction:
Divide n by m using division theorem:
$n = mq + r$
Where $r \leq 0$. Then $r = n - mq$. Since every integer a_i divides n and m, it also divides r. So we see that r is a common multiple of $a_1, a_2, ..., a_k$. r is a positive integer such that $r < m$. This contradicts the definition of lcm since we should have $m \geq r!$, so this is not possible.
$\therefore$ by proving the contradiction, we have proven that if n is a positive integer such that $a_1|n, a_2|n, ..., a_k|n$ then $m|n$

9. (4 pts)

   (a) Find the greatest common divisor of 1064 and 856.
   $1064 = 856 - 208$
   $856 = 208 \times 4 + 24$
   $208 = 24 \times 8 + 16$
   $24 = 16 + 8$
   $16 = 2 \times 8$
   $\therefore$ gdc$(1064, 856) = 8$ since last none-zero remainder was 8.

   (b) Find integers x and y so that $1064x + 856y = \gcd(1064, 856)$.
   $8 = 24 - 16$
   $8 = 24 - (208 - 24 \times 8)$
   $8 = -208 + 4 \times 9$
   $8 = -208 + (856 - 208 \times 4) \times 9$
   $8 = 856 \times 9 - (1064 - 856) \times 37$
   $8 = -37 \times 1064 + 46 \times 856$
   $\therefore x = -37$ and $y = 46$

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 $a \equiv c \pmod{n}$
    $a - b = nk$ (k is an integer)
    $b - c = nk'$
    Adding these equivalences:
    a-c = n(k + k')
    $\therefore a \equiv c(\mod n)$

    (b) that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$
    $a - b + c - d = sn + tn \rightarrow a - b + c - d = n(s + t)$
    adding $b + d$ on both sides
    $a + c \equiv b + d + n(s + t)$
    $\therefore a + c \equiv b + d(\mod n)$