Test 2, Math 3330. Answer Key

You have **80** minutes to complete the test. Each problem is worth **20** points. You cannot use any books or notes.

1. Label each of the following statements as either true of false.
   a. Let $a$ and $b$ be integers, not both zero, such that $d = (a,b)$. Then there exist unique integers $x$ and $y$ such that $d = ax + by$. F
   b. Let $a$ and $b$ be integers, not both zero. If a common divisor $e$ of $a$ and of $b$ is of the form $e = xa + yb$ for integers $x$ and $y$ then $e$ must be the greatest common divisor of $a$ and $b$. T
   c. Let $a$ be an integer. Then $(a,0) = a$. T
   d. If $a|c$ and $b|d$ then $ab|cd$. T
   e. Assume $(a,b) = 1$. Then if $a|c$ and $b|c$ one has that $ab|c$. T
   f. The identity element in a group is its own inverse. T
   g. Let $G$ be a non-abelian group. Then $xy \neq yx$ for all $x$ and $y$ in $G$. F
   h. The empty set is a subgroup of any group. F
   i. For every $n$, the group $\mathbb{Z}_n$ of addition modulo $n$ is a subgroup of the group $\mathbb{Z}$ under addition. F
   j. The set $k\mathbb{Z}$ of multiples of $k$ is a group under addition. T
   k.
2. Prove that the product of the greatest common divisor $(a,b)$ and of the lowest common multiple $[a,b]$ is equal to the product $ab$ of $a$ and $b$.
   Proof: $a = p_1^{e_1(a)}p_2^{e_2(a)}\cdots p_k^{e_k(a)}, b = p_1^{e_1(b)}p_2^{e_2(a)}\cdots p_k^{e_k(b)}$,
   $ab = p_1^{e_1(a)+e_1(b)}p_2^{e_2(a)+e_2(b)}\cdots p_k^{e_k(a)+e_k(b)}$,
   $(a,b) = p_1^{\min(e_1(a),e_1(b))}p_2^{\min(e_2(a),e_2(b))}\cdots p_k^{\min(e_k(a),e_k(b))}, [a,b] = p_1^{\max(e_1(a),e_1(b))}p_2^{\max(e_2(a),e_2(b))}\cdots p_k^{\max(e_k(a),e_k(b))}$
   and clearly for every $i$ one has that
   $$\min(e_i(a),e_i(b)) + \max(e_i(a),e_i(b)) = e_i(a) + e_i(b)$$
   which proves the claim.

3. Prove that if $(a,b) = 1$ then $(a^2,b^2) = 1$.
   Proof. $(a,b) = 1$ means that $a$ and $b$ don't have any common prime divisor. the same then hold for $a^2$ and $b$.

4. Let $G$ be a group and assume that for all elements $a$ and $b$ one has that $(ab)^2 = a^2b^2$. Prove that $G$ must be abelian.
   Proof. $(ab)^2 = a^2b^2$ means $abab = aabb$. But then $a^{-1}(abab)b^{-1} = a^{-1}(aabb)b^{-1}$. By associativity we get $(a^{-1}a)(ba)(bb^{-1}) = (a^{-1}a)(ab)(bb^{-1})$ and therefore $ba = ab$.

5. a. Find the multiplicative inverse of $6 \bmod 5$, that is $[6]_{35}^{-1}$.
   6 and 35 are relatively prime. Indeed, $1 = 6 \cdot 6 - 1 \cdot 35$ which yields $[1]_{35} = [6]_{35} \cdot [6]_{35}$ or $[6]_{35}^{-1} = [6]$
   b. Solve $6x + 3 = 0 \bmod 5$
   $6x + 3 = 0$ is the same as $6x = -3$ or $6x = 2$ (all $\bmod 5$). This is $[6]_5[6]_5x = [6]_5[2]_5$ or

$x = [12]_5 = [2]_5$. Indeed $6 \cdot 2 + 3 = 15 = 0 \bmod 5$

6. a. Prove that for every number $n > 0$, $n - 1$ has a multiplicative inverse $\bmod n$.

b. Prove $n - 1$ is its own multiplicative inverse $\bmod n$

Proof. $(n, n-1) = 1$, there are no common divisors of $n$ and $n - 1$. Also $1 = 1 \cdot n + (-1) \cdot (n-1)$. Thus $[-1]_n = [n-1]_n^{-1}$ and $[-1] = [n-1]$ Also $(n-1)(n-1)\_ = n^2 - 2n + 1 = 1 \bmod n$ shows the same thing.