Math 127 Homework

Mary Radcliffe

Due 25 April 2019

Complete the following problems. Fully justify each response. You need only turn in those problems marked with a (*).

1. Prove Propositions 1 and 2 from Division notes.
2. Prove Proposition 3 from Division notes.
3. (*) Suppose $p_1, p_2, \ldots, p_r \in \mathbb{Z}$ are distinct primes. Let $a = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, and let $b = p_1^{j_1} p_2^{j_2} \ldots p_r^{j_r}$, where $k_1, k_2, \ldots, k_r, j_1, j_2, \ldots, j_r$ are nonnegative integers. Prove that $\gcd(a, b) = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, where $m_i = \min\{k_i, j_i\}$ for all $1 \leq i \leq r$.
4. For each of the following equations: determine if the equation has solutions. If so, write an expression for all possible solutions to the equation. If not, explain how you know there are no solutions.
   (a) $12a + 9b = 15$.
   (b) $12a + 9b = 1$.
   (c) $2a + 3b = 1$.
   (d) $50000a + 18412b = 1$.
5. (*) Let $a, b, c \in \mathbb{Z}$. Prove that if $a \perp b$ and $a|(bc)$, then $a|c$.
6. Given $a, b \in \mathbb{Z}$, define the *least common multiple* of a, b to be the unique nonnegative integer m such that
   - $a|m \wedge b|m$.
   - $(a|q \wedge b|q) \Rightarrow m|q$.

   We write $m = \operatorname{lcm}(a, b)$.
   (a) Prove that this definition of lcm is well-defined.
   (b) Prove that if $a, b \in \mathbb{Z}$, $m = \operatorname{lcm}(a, b)$ and $d = \gcd(a, b)$, then $md = |ab|$.
7. Define a relation $\sim$ on $\mathbb{N}$ by $x \sim y$ if $\gcd(x, y) = 1$. Is this an equivalence relation? If so, prove it. If not, explain why not.
8. Let X, Y be sets, and let $f : X \to Y$ be a function. Define a relation $\sim$ on X by $x_1 \sim x_2$ if $f(x_1) = f(x_2)$. Is this an equivalence relation? If so, prove it. If not, explain why not.
9. (*) Let X be a set, and let $\sim_1$ and $\sim_2$ be two equivalence relations on X. Define a relation on X by $x \sim y \equiv (x \sim_1 y) \wedge (x \sim_2 y)$. Prove that $\sim$ is an equivalence relation. Describe the classes of $\sim$ in terms of the classes of $\sim_1$ and $\sim_2$.
10. (*) Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, and $k, \ell \in \mathbb{N}$, such that $k \equiv \ell \pmod{n}$ and $a \equiv b \pmod{n}$.
    (a) Is it true that $a^k \equiv b^k \pmod{n}$? If so, prove it. If not, find a counterexample.
    (b) Is it true that $a^k \equiv a^\ell \pmod{n}$? If so, prove it. If not, find a counterexample.

11. Let $a \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose that $a \perp n$. Show that u, u' are both multiplicative inverses for $a \pmod{n}$ if and only if u is a multiplicative inverse for $a \pmod{n}$ and $u \equiv u' \pmod{n}$.

12. (*) Let p be a positive prime, and $k \in \mathbb{N}$. Prove that $\varphi(p^k) = p^k - p^{k-1}$.