Acknowledgement: The idea of using Bezout's theorem to prove the contraverse of problem 1 came from Jonathan Bianchini

Name: Jaime Arana-Rochel
Section: 1

Homework #3

Q1

A) Proof by showing that $P \to Q$ and $Q \to P$ implies $P \leftrightarrow Q$

Let's assume that the system of congruences has a solution. For the system of congruences,

$$x \equiv a_1(mod\ m_1) \quad x \equiv a_2(mod\ m_2)$$

we have the following due to congruence definitions

$$m_1|x - a_1 \quad and \quad m_2|x - a_2$$

Let $gcd(m_1, m_2) = d$. By definition $d|m_1$ and $d|m_2$ which also obviously means that $d|x-a_1$ and $d|x - a_2$. Using the division definition on the above,

$$x - a_1 = k_1 d \quad and \quad x - a_2 = k_2 d$$

Substituting the value of x (x $= k_1 d + a_1$) from the first equation into the second equation, we get

$$k_1 d + a_1 - a_2 = k_2 d$$

$$a_1 - a_2 = (k_2 - k_1)d$$

Using the division definition again on the equation above, we have that $d = gcd(m_1, m_2)\ |a_1 - a_2$. This proves the conditional $P \to Q$. Now we proceed to proving the converse.

Assume that $gcd(m_1, m_2)\ |a_1 - a_2$. Using Bezout's theorem we can write

$$gcd(m_1, m_2) = sm_1 + tm_2$$

Therefore $sm_1 + tm_2 \,|\, a_1 - a_2$. By the division definition and some shifting of terms, we can write the following equations,

$$a_1 - a_2 = k(sm_1 + tm_2)$$

$$a_1 - a_2 = ksm_1 + ktm_2$$

$$a_1 - ksm_1 = a_2 + ktm_2$$

In the equation above, s t and k are just integers so let,

$$k_1 = -ks$$

$$k_2 = kt$$

Substituting k_1 and k_2 back into the equation we get

$$a_1 + k_1 m_1 = a_2 + k_2 m_2$$

We set the variable x equal to the above equality such that

$$x = a_1 + k_1 m_1 \implies x - a_1 = k_1 m_1$$

$$and$$

$$x = a_2 + k_2 m_2 \implies x - a_2 = k_2 m_2$$

By the division definition,

$$m_1 \,|\, x - a_1 \quad and \quad m_2 \,|\, x - a_2$$

Using the modulo congruence definitions we can then write

$$x \equiv a_1 (mod\, m_1) \quad and \quad x \equiv a_2 (mod\, m_2)$$

We've constructed the congruences from our value of x, thus proving the converse $Q \to P$. By proving both conditionals we can say that $P \leftrightarrow Q$, satisfying the problem.

Q2

Problem: Prove if $f(x)$ and $g(x)$ are polynomials with leading terms ax^n and bx^m respectively, then $f(x)/g(x) \sim (a/b)x^{n-m}$

We notice that as the input to $f(x)$ and $g(x)$ get sufficiently large, then the smaller terms in the polynomials disappear leaving only the leading terms since the leading terms grow the fastest.

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = \frac{ax^n}{bx^m} = \frac{ax^{n-m}}{b} = (a/b)x^{n-m}$$

We now take the following limit,

$$\lim_{x \to \infty} \frac{f(x)/g(x)}{(a/b)x^{n-m}} = \frac{(a/b)x^{n-m}}{(a/b)x^{n-m}} = 1$$

Since our limit yielded a 1, then we know that $f(x)/g(x) \sim (a/b)x^{n-m}$ by definition.

Q3

Problem: Give a complete proof that for $f(n) = n^2$ and $g(n) = n^2 log\, n$ we have that $f = O(g)$ and $f = o(g)$

First we prove that $f = O(g)$. By definition of $Big\ O$

$$f = O(g) \implies |n^2| \leq C\,|n^2 log\, n| \qquad \forall\, x \leq x_0$$

$$= |n^2| \leq \ |n^2|\ C|log\, n|$$

$$1 \leq C|log\, n|$$

This inequality is obviously true, which shows that $f = O(g)$. Now we prove that $f = o(g)$. We take the limit of $f(n)$ over $g(n)$

$$\lim_{x\to\infty} \frac{f(n)}{g(n)} = \frac{n^2}{n^2 log\, n} = \frac{1}{log\, n} = 0$$

Based on this limit, by definition $f = o(g)$.

Q4

Problem: Rank the functions by order of growth.

$$2^{2^{n+1}}, 2^{2^n+1}, n!\,, 2^{n^2}, 2^n, n^{log\, n}, (log\, n)^{log\, n}, n^3, n^2,$$

$$\{log(n!), nlog\, n\}, 2^{(log\, n)^2}, 2^{\sqrt{log\, n}}, (log\, n)^2, log\, n, log(log\, n)$$

The pair in the list grouped with braces is an equivalence class.