Problem 1, Ma/CS 6a Set 1, Matt Lim

We will first prove the prime decomposition property by contradiction. Assume to the contrary that "every natural number $n \geq 2$ is either a prime or a product of primes" is not true. So, consider the set of natural numbers S that are not primes or product of primes. By the well ordering principle, there is a least number in this set. Call this number n. We have that n is not a product of primes. This means that one of its factors has to be non-prime and not be a product of primes, which means it is in S. But this is a contradiction since n is the least number in S, so it cannot have a factor that is greater than it.

We will now use induction to prove that there are infinitely many primes. To do this, we will prove that given a set of primes of size $n-1$, we can generate a set of primes of size n. Our base case will be a set of primes of size 1. We will call this set S. If we multiply all the numbers in this set together and add 1, we can see that this number is either a prime that is not in S, or is a product of a prime that is not in S. This is because of prime decomposition, and because the number is larger than all the primes in S and not a factor of any of the primes in S. Either way, we can add this new prime to S to make a set of primes of size 2. So the base case holds. Now, for the inductive assumption. Assume that given a set of primes of size $k-1$, we can generate a set of primes of size k, for all $1 \leq k \leq n$. Given this assumption, we have that there are sets of primes of size n. Now we must show that given a set of primes of size n, we can generate a set of primes of size $n+1$. So, let us consider an arbitrary set of primes S of size n. To generate a prime number not in S, multiply all elements of S together and add 1. We can see that this number is either a prime that is not in S, or is a product of a prime that is not in S. This is true because of prime decomposition, and because the number is larger than all the primes in S and not a factor of any of the primes in S. Either way, we can add this new prime to S to make a set of primes of size $n+1$. Thus, by induction, we can conclude that given a set of primes of size $n-1$, we can generate a set of primes of size n. By this inductive proof, it is clear that there are infinitely many primes. To see why, assume to the contrary that there are not, and that there exist only some finite set of primes of size n. But then, given what we proved, we can generate a set of primes of size $n+1$, which is a contradiction.

Problem 2, Ma/CS 6a Set 1, Matt Lim

Assume to the contrary that the pair q, r is not unique. Then we have that some other pair $q_2, r_2 \in \mathbb{N}$ exists such that $a = bq_2 + r_2$ and $0 \leq r_2 \leq b$. Consider the case where $q_2 > q$; that is, $q_2 = q + x$, where $x \in \mathbb{N}$ and $x \geq 1$. We also have that $r_2 = r + y$, where $r \in \mathbb{Z}$. Then we have that

$$a = bq_2 + r_2$$

$$a = b(q + x) + (r + y)$$

$$a = bq + bx + (r + y)$$

We have that $y = -bx \leq -b$, which means that $(r + y) = r_2 < 0$, since $r < b$. But this is a contradiction.

Now consider the case where $q_2 < q$; that is, $q_2 = q - x$, where $x \in \mathbb{N}$ and $x \geq 1$. We also have that $r_2 = r + y$, where $r \in \mathbb{Z}$. Then we have that

$$a = bq_2 + r_2$$

$$a = b(q - x) + (r + y)$$

$$a = bq - bx + (r + y)$$

We have that $y = bx \geq b$, which means that $(r + y) = r_2 \geq b$, since $0 \leq r$. But this is a contradiction.

So in either case we obtain a contradiction. Thus, we can conclude that the pair q, r is unique.

Problem 3, Ma/CS 6a Set 1, Matt Lim

(a) Let c_k be the greater of a_k and b_k (if they are equal, just let it be b_k); that is, $c_k = (a_k > b_k) \ ? \ a_k \ : \ b_k$. Then we have that

$$LCM(p_1^{a_1} p_2^{a_2} ... p_k^{a_k}, p_1^{b_1} p_2^{b_2} ... p_k^{b_k}) = p_1^{c_1} p_2^{c_2} ... p_k^{c_k}$$

Let d_k be the lesser of a_k and b_k (if they are equal, just let it be b_k); that is, $d_k = (a_k < b_k) \ ? \ a_k \ : \ b_k$. Then we have that

$$GCD(p_1^{a_1} p_2^{a_2} ... p_k^{a_k}, p_1^{b_1} p_2^{b_2} ... p_k^{b_k}) = p_1^{d_1} p_2^{d_2} ... p_k^{d_k}$$

(b)

Problem 4, Ma/CS 6a Set 1, Matt Lim

Problem 5, Ma/CS 6a Set 1, Matt Lim