Problem 1

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

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 $y \in \mathbb{Z}$. 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 $y \in \mathbb{Z}$. 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

(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

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

We find the LCM this way because the LCM must contain the prime factorization of both numbers (clearly this is a multiple of both numbers). Any more than that and it will not be the least common multiple, and any less and it will not be a multiple of both numbers.

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

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

We find the GCD this way because the GCD must contain the smaller part of the prime factorization of both numbers (clearly this will divide both numbers). Any more than that and it will not divide the smaller number, and any less and it will not be the greatest common divisor.

(b) Let $p_1, p_2, ..., p_k$ and $a_1, a_2, ..., a_k$ and $b_1, b_2, ..., b_k$ be defined as in part (a). Consider the prime factorization $p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ of a, and the prime factorization $p_1^{b_1}p_2^{b_2}...p_k^{b_k}$ of b. Given our definition of c_k and d_k from above, it is clear that $c_k + d_k = a_k + b_k$ for all k. Then we have the following:

$$LCM(a,b) \cdot GCD(a,b) = p_1^{c_1}p_2^{c_2}...p_k^{c_k} \cdot p_1^{d_1}p_2^{d_2}...p_k^{d_k}$$

$$LCM(a,b) \cdot GCD(a,b) = p_1^{c_1+d_1}p_2^{c_2+d_2}...p_k^{c_k+d_k}$$

$$LCM(a,b) \cdot GCD(a,b) = p_1^{a_1+b_1}p_2^{a_2+b_2}...p_k^{a_k+b_k}$$

$$LCM(a,b) \cdot GCD(a,b) = a \cdot b$$

Problem 4

(a) We can see that, for $0 \leq |a| \leq 7$, we have $a^2 \equiv r_a \bmod 8$. Our work below shows this:

$$0^2 \equiv 0 \bmod 8$$

$$1^2 \equiv 1 \bmod 8$$

$$2^2 \equiv 4 \bmod 8$$

$$3^2 \equiv 1 \bmod 8$$

$$4^2 \equiv 0 \bmod 8$$

$$5^2 \equiv 1 \bmod 8$$

$$6^2 \equiv 4 \bmod 8$$

$$7^2 \equiv 1 \bmod 8$$

For $|a| > 7$, $k^2 \equiv a^2 \bmod 8$, for some $0 \leq |k| \leq 7$. This is because $k \equiv a \bmod 8$ and the fact that if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$ (congruency and multiplication). Then, because congruency is transitive, we have that for $|a| > 7$, $a^2 \equiv r_a \bmod 8$. So we have proved that for any $a \in \mathbb{Z}$, we have $a^2 \equiv r_a \bmod 8$.

(b) We have that 1003456789 mod $8 \equiv 5$. 5 is not equivalent to 0, 1, or 4. But part (a) says that for any $a \in \mathbb{Z}$, we have $a^2 \equiv r_a \bmod 8$, where r_a is either 0, 1, or 4. Thus we can conclude that 1003456789 is not a perfect square.

(c) Assume to the contrary that a number of the form $3^n + 3^m + 1$, where $n, m \in \mathbb{N}$, is a perfect square. For this problem we will do everything under mod8. By part (a), this means we have

$$3^n + 3^m + 1 \equiv 3^n \bmod 8 + 3^m \bmod 8 + 1 \bmod 8 \equiv r_a$$

We will now show that 3^n mod 8, where $n \in \mathbb{N}$, is always equivalent to either 1 or 3. To do this we will use induction. Our base case is when $n = 0$. Then we have 1 mod $8 \equiv 1$, and our claim is satisified. Next comes our inductive assumption. We will assume that 3^n mod 8 is equivalent to either 1 or 3 for some natural number $n > 0$. Now we must show that 3^{n+1} mod 8 is equivalent to either 1 or 3. To see this is true, consider the following:

$$3^{n+1} \bmod 8 \equiv 3 \cdot 3^n \bmod 8$$

We then have that either

$$3^{n+1} \bmod 8 \equiv 9 \equiv 1$$

or

$$3^{n+1} \bmod 8 \equiv 3$$

Thus, by induction, we have that $3^n \bmod 8$, where $n \in \mathbb{N}$, is always equivalent to either 1 or 3. Using this, we have three cases:

$$3^n + 3^m + 1 \equiv 1 + 1 + 1 \equiv 3 \equiv r_a$$

$$3^n + 3^m + 1 \equiv 1 + 3 + 1 \equiv 5 \equiv r_a$$

$$3^n + 3^m + 1 \equiv 3 + 3 + 1 \equiv 7 \equiv r_a$$

All such cases, given r_a, are contradictions. Thus we can conclude that no number of the form $3^n + 3^m + 1$, where $n, m \in \mathbb{N}$, is a perfect square.

Problem 5

$$p = 2161 \text{ and } q = 3989$$

$$n = pq = 8620229$$

$$\varphi(pq) = n - p - q + 1 = 8614080$$

$$e = 6949$$

Now we will use the extended Euclidean algorithm to find $de \equiv 1 \bmod \varphi(n)$.

8614080	1	0
6949	0	1
4269	1	-1239
2680	-1	1240
1589	2	-2479
1091	-3	3719
498	5	-6198
95	-13	16115
23	70	-86773
3	-293	363207
2	2121	-2629222
1	-2414	2992429

Then we have that letting $d = 2992429$ gives us $de \equiv 1 \bmod \varphi(n)$.
Now we can encrypt $m = 2014$.

$$X = m^e \bmod n$$

$$X = 2014^{6949} \bmod 8620229$$

$$X = 7986909$$

Decrypting this X would go as follows.

$$X^d \bmod n = 7986909^{2992429} \bmod 8620229$$

$$X^d \bmod n = 2014$$