PROBLEM 1. a) False. Counterexample: $a = 1, b = -1$

b) False. Counterexample: $a = 7$

c) True. Since $a \equiv b(\bmod m)$ we have $a.c \equiv b.c(\bmod m)$. Similarly, since $c \equiv d(\bmod m)$, $bc \equiv bd(\bmod m)$. The first congruency implies that $ac - bc$ is divisible by m and the second one implies that $bc - bd$ is divisible by m. Therefore the summation of them is also divisible by m. So, $(ac - bc) + (bc - bd) = ac - bd$ is divisible by m. Hence $ac \equiv bd(\bmod m)$

d) False. Counterexample: $a = 4, n = 1$.

e) False. If $m = 41$ then $m^2 + m + 41 = 41^2 + 41 + 41 = 41(41 + 1 + 1)$ and therefore it is not a prime number.

PROBLEM 2. Notice that $\gcd(a, b) = \gcd(a, b - a)$. Therefore if $\gcd(a, 2009) = 1$ then $\gcd(2009 - a, 2009) = 1$. This means that all the positive integer numbers smaller than 2009 which are co-prime with respect to 2009 can be paired up in the form

$$(1, 2008), (2, 2007), (3, 2006), \ldots.$$

Since the summation of the numbers of each pair is equal to 2009, therefore the summation of all the positive integer numbers that are co-prime with respect to 2009 is also divisible by 2009. In fact, using this argument we can find the exact value for this summation. Since the number of positive integers that are co-prime with respect to 2009 is equal to $\phi(2009)$, therefore the number of the pairs is equal to $\frac{\phi(2009)}{2}$. Hence the summation of all these numbers is equal to $\frac{\phi(2009)}{2} \times 2009$.

PROBLEM 3. a) First notice that "e" is the 5-th letter, so it is encoded to 14. Now, to encrypt it, we must find 14^3 (mod 71).

$$14^2 = 196 \equiv 54(\bmod 71) 14^3 = 14 \times 14^2 \equiv 14 \times 54 \equiv 46(\bmod 71).$$

Similarly we can encrypt the other letters. Finally, the ciphertext is 46-5-38-31

b) We know that in RSA cryptosystem we we have $k.K \equiv 1(\bmod \phi(m))$. So, in our case we must have $3k \equiv 1$ (mod 71). Using Euclid's algorithm we can find the inverse of 3 (mod 70) which equals to 47.

c) Using the private key, we can decrypy the ciphertext simply by raising the ciphertext to the power k and then taking the residual of it modulo 71. First we decrypt 16. We have:

$$\begin{aligned}
16^{35} &= (4^2)^{35} = 4^{70} \equiv 1(\bmod 71) \\
16^2 &= 256 \equiv 43 \equiv 3(\bmod 71) \\
16^4 &= (16^2)^2 \equiv 43^2 \equiv 3(\bmod 71) \\
16^{12} &= (16^4)^3 \equiv 3^3 \equiv 27(\bmod 71) \\
16^{47} &= 16^{35} \times 16^{12} \equiv 16^{12} \equiv 27(\bmod 71)
\end{aligned}$$

Now we decrypt 13.

$$\begin{aligned}
13^2 &= 169 \equiv 27(\bmod 71)\\
13^4 &= (13^2)^2 \equiv 27^2 \equiv 19(\bmod 71)\\
13^8 &= (13^4)^2 \equiv 19^2 \equiv 6(\bmod 71)\\
13^{32} &= (13^8)^4 \equiv 6^4 \equiv 18(\bmod 71)\\
13^{34} &= 13^{32} \times 13^2 \equiv 18 \times 27 \equiv 60(\bmod 71)\\
13^{35} &= 13 \times 13^{34} \equiv 13 \times 60 \equiv 70 \equiv -1(\bmod 71)\\
13^{12} &= (13^4)^3 \equiv 19^3 \equiv 43(\bmod 71)\\
13^{47} &= 13^{12} \times 13^{35} \equiv 43 \times (-1) \equiv 28(\bmod 71)
\end{aligned}$$

And to decrypt 6:

$$\begin{aligned}
6^4 &\equiv 18(\bmod 71)\\
6^{12} &= (6^4)^3 \equiv 18^3 \equiv 10(\bmod 71)\\
6^8 &= (6^4)^2 \equiv 18^2 \equiv 40(\bmod 71)\\
6^{16} &= (6^8)^2 \equiv 40^2 \equiv 38(\bmod 71)\\
6^{32} &= (6^{16})^2 \equiv 38^2 \equiv 24(\bmod 71)\\
6^{34} &= 36 \times 6^{32} \equiv 36 \times 24 \equiv 12(\bmod 71)\\
6^{35} &= 6 \times 6^{34} \equiv 6 \times 12 \equiv 1(\bmod 71)\\
6^{47} &= 6^{12} \times 6^{35} \equiv 10(\bmod 71)
\end{aligned}$$

So, 16-13-6 is decrypted to 27-28-10 and after subtracting 9 from them, the plaintext becomes "rsa"

Problem 4. We can formulate the problem as the following:

$$n \equiv 0(\bmod 11) n \equiv -1(\bmod 10) n \equiv -2(\bmod 9)$$

since the numbers $9, 10, 11$ are pairwise relatively co-prime, we can use Chinese remainder theorem to solve this system of congruency equations. One solution is $n = 979$.

Problem 5. .

a) If n is an odd number then $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots + b^{n-1})$ therefore $a^n + b^n$ is divisible by $a + b$.

b) If $n = 4k + 2$ then $n/2 = 2k + 1$ is an odd number. Now, using the previous part we know that $(a^2)^{2k+1} + (b^2)^{2k+1}$ is divisible by $a^2 + b^2$.

c) Suppose that $a^2 + b^2$ is divisible by p but a, b are not divisible by p so $\gcd(a, p) = \gcd(b, p) = 1$. Since p is a prime number, $\phi(p) = p - 1$ and therefore we have $a^{p-1} \equiv 1(\bmod p)$ and $b^{p-1} \equiv 1(\bmod p)$. Therefore $a^{p-1} + b^{p-1} \equiv 2(\bmod p)$. On the other hand, since $p = 4k + 3$, we have $p - 1 = 4k + 2$ and using the previous part, $a^{p-1} + b^{p-1}$ is divisible by $a^2 + b^2$. Notice that $a^2 + b^2$ is divisible by p. Hence $a^{p-1} + b^{p-1}$ is also divisible by p. But we already showed that $a^{p-1} + b^{p-1} \equiv 2(\bmod p)$. This means that $0 \equiv 2(\bmod p)$. This is a contradiction.