RSA Weaknesses - Questions

Question 1: The RSA cryptosystem can be very weak if you do not choose your primes carefully. Alice has chosen to use the public modulus $N = 400640231$. You hear (from a friend) that she has used primes that are very close to each other. Find the prime factorisation of N.

(Hint: N is too big to start your factor search from the prime 3, you must use the fact that the primes are very close to each other to find a better number to start searching from.)

Extension: Use maple to try and factor the more realistic public modulus:
$N = 120714580105450732527687012439049966078721636560924592611272025960112778327142529977981$
$9184412315551064812103346303$, given that the two primes used have a difference of less than 5000.

(Hint: You may wish to write a program to do the search for you.)

Question 2: (i) Alice uses RSA encryption with $e = 3$ and receives the ciphertext $c = 442450728$ from Bob. Show that this particular ciphertext can easily be decrypted without even knowing Alice's value of N.

(ii) Can you explain this behaviour in general? Show that given any public key (N, e) we may easily decrypt any ciphertext c arising from a plaintext p with $p < N^{\frac{1}{e}}$ (without even having to use the value of N). Is this a major weakness of "low public exponent RSA"?

(Hint: Can we really just drop the mod N here?)

Question 3: Alice and Bob have public keys of the form (N, e_1) and (N, e_2) respectively, so that they use the same public modulus. Suppose that e_1 and e_2 are coprime. Show that we can easily decrypt any message that is sent to both Alice and Bob (if the two corresponding ciphertexts are intercepted).

Question 4 In this question we investigate a weak form of Hastad's attack on RSA. Specifically, we show that if you send the same message to e or more people with the same RSA encryption exponent e, then the plaintext can always be obtained easily from the intercepted ciphertexts.

For simplicity, consider the case $e = 3$, so that we can find three people with public keys of the form $(N_1, 3), (N_2, 3)$ and $(N_3, 3)$. You may assume that the moduli N_1, N_2 and N_3 are distinct.

(i) We can use Euclid's algorithm to find $\gcd(N_1, N_2)$, $\gcd(N_1, N_3)$ and $\gcd(N_2, N_3)$. If one or more of these values is greater than 1, how would this be a big help?

(ii) We may assume now that N_1, N_2 and N_3 are pairwise coprime. Suppose the plaintext message sent to these three people is p and that the three corresponding ciphertexts c_1, c_2, c_3 are intercepted. Using the definition of RSA encryption, what congruences do p, c_1, c_2 and c_3 satisfy?

(iii) Show that this information is enough to be able to find the plaintext p. (Hint: CRT)

Extension: Generalise this argument to the case of arbitrary e, so that you have the existence of e people with public keys $(N_1, e), (N_2, e), \ldots, (N_e, e)$, an unknown plaintext p that is sent to each of these people and the corresponding intercepted ciphertexts $c_1, c_2, \ldots, c_e$.