Bad Choices for RSA Keys

Recall that in the RSA cryptosystem the encrypting key consists of an integer $n = pq$, p and q distinct primes, and a positive integer e with $(e, \phi(n)) = 1$, and that the security of this as a public key system lies in the fact that decryption amounts to being able to factor n. Consequently, it would be a bad idea to choose for n an integer that is easy to factor by some method.

Problem 1. Show that the choice $n = 23360947609$ is bad by showing that n can easily be factored using Fermat factorization.

Problem 2. More generally, Fermat factorization will factor $n = pq$ in relatively few steps if p and q are close to each other. Let's see why.

a. Show that if $n = pq$ then

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Show this means that Fermat factorization will end when (in the notation on page 113) $t = (p+q)/2$.

b. Fermat factorization starts with the initial value $t = [\sqrt{n}] + 1$. Use this and part (a) to show that we can factor n through Fermat factorization in at most $(p-q)/2 + 1$ steps (where we assume, of course, that $p > q$).