Exercise 1 Extend the Franklin-Reiter attack to ciphertexts c_1 and c_2 (for the same public key) where c_1 is an encryption of m and c_2 is an encryption of $am + b$ for known integers a and b.

Exercise 2 Show that one can prevent the Wiener attack by adding a multiple of $\varphi(N)$ to e.

Exercise 3 Show how to perform the Wiener attack when $\varphi(N)$ is replaced by $\lambda(N)$. What is the bound on the size of d for which the attack works?

Exercise 4 Let $N = pq$, with $p < q < 2p$, and suppose you know r such that $r|(p-1)$ and $r|(q-1)$. Show that if $r > \sqrt{3}N^{1/4}$ then it is possible to factor N in polynomial time.

Hint: recall Wiener's attack.