1.31 Grading Response

1.31

a. The proof correctly uses Proposition 1.30/Fermat’s Little Theorem to show that if *p* and *q* are primes and that *q* divides *p* – 1 that *b* either equals 1 or *b* has order *q.* At the beginning of the proof is stated as equaling 1 (mod p) then, the proof shows that *n* divides *p – 1* when *b* = 1. The proof also shows by using Fermat’s Little Theorem that if *b* ≠ 1 then it has order *q*. Thus, the proof is sufficient.

b. The proof for calculating the ratio of success is correct. The proof correctly uses Theorem 1.31/Primitive Root Theorem to extrapolate the ratio of “bad” a’s to solve the ratio of “good” a’s by taking 1 – the ratio of “bad” a’s.