1.31

a) Using Fermat’s Little Theorem/Proposition 1.30, given

and ,

when we raise both sides of the equation by q we get,

or

.

So, the order of b divides the prime *q* and if *b* ≠ 1, then *b* has order *q* by the theorem.

b) Using the Primitive Root Theorem/Theorem 1.31, let *g* and *p* be primitive roots. Let

Then,

if and only if *p* – 1 divides *k(p – 1)/q* given by part a.

That is, if and only if *k* is a multiple of *q.*

There are *(p – 1)/q* such multiples of *q* in the interval 0 to *p – 1*. Thus, the probability of

is or . So, the probability of success is to find

such that .