Group 7 – Grading done by Group 2

1.26

The provide two good examples that contradict the assumption that there are a finite number of primes by showing that there will always be a new prime created by using the equation they have use. Very good job!

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 a^n 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.

1.32

A) CORRECT

2 is NOT a primitive root modulo 7

2 is a primitive root modulo 13

2 is a primitive root modulo 19

2 is NOT a primitive root modulo 23

B) CORRECT

3 is a primitive root modulo 5

3 is a primitive root modulo 7

3 is NOT a primitive root modulo 11

3 is a primitive root modulo 17

C) CORRECT

23 has 10 primitive roots, 10 were provided

29 has 12 primitive roots, 12 were provided

41 has 16 primitive roots, 16 were provided

43 has 12 primitive roots, 12 were provided

D) CORRECT

11 has 4 primitive roots, 4 were provided

E) CORRECT

229 has 72 primitive roots, 72 were provided

F) CORRECT

All primes listed have 2 as a primitive root

G) CORRECT

All primes listed have 3 as a primitive root

There are no primes less than 100 with 4 as a primitive root, none were provided

1.33

The problem is to prove that g is a primitive value. They do this proof by contradiction. The proof is well written and easy to follow. They clearly showed that g is a primitive root.

1.34

a) Their proof to show that X2 ≡ b (mod p) has either two solutions or no solutuions

does the job in proving it.

b)

i)

Correct

The solutions were found to be x = 3, 4

ii)

Correct

The solutions were found to be x = 4, 7

iii)

Correct

There were no solutions

iv)

Correct

Solutions were found

c)

Correct

Another solution was found which did not contradict.

d)

Correct

It was proven that k has a square root if and only if k is even.

Problem 1.36	
correct	2 ^ (3-1)/2 (mod 3) = 2.0
correct	2 ^ (5-1)/2 (mod 5) = 4.0
correct	2 ^ (7-1)/2 (mod 7) = 1.0
correct	2 ^ (11-1)/2 (mod 11) = 10.0
correct	2 ^ (13-1)/2 (mod 13) = 12.0
correct	2 ^ (17-1)/2 (mod 17) = 1.0
correct	2 ^ (19-1)/2 (mod 19) = 18.0

Overall, Group 7 did a very good job on this assignment and I would say that they should receive an A.