Problem 1.32

(e) Write a computer program to check for primitive roots and use it to find all primitive roots modulo 229. Verify that there are exactly φ229 of them.

Program is on GitHub, “Crypt\_hw2\_E.java”

6, 7, 10, 23, 24, 28, 29, 31, 35, 38, 39, 40, 41, 47, 50, 59, 63, 65, 66, 67, 69, 72, 73, 74, 77, 79, 87, 90, 92, 96, 98, 102, 105, 110, 112, 113, 116, 117, 119, 124, 127, 131, 133, 137, 139, 142, 150, 152, 155, 156, 157, 160, 162, 163, 164, 166, 170, 179, 182, 188, 189, 190, 191, 194, 198, 200, 201, 205, 206, 219, 222, 223

φ229 = 72, program returned 72 primitive roots

(f) Use your program from (e) to find all primes less than 100 for which 2 is a primitive root.

3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83

(g) Repeat the previous exercise to find all primes less than 100 for which 3 is a primitive root. Ditto to find the primes for which 4 is a primitive root.

Primes with 3 as a primitive root:

5, 7, 17, 19, 29, 31, 43, 53, 79, 89

Primes with 4 as a primitive root:

There are no primes less than 100 for which 4 is a primitive root