

HW 7, Due Jan 13

1. (30 points)

(a) Find ALL solutions to

$$x^2 + 15x + 5 \equiv 0 \pmod{21}$$

(NOTE- the solutions are in $\{0, 1, 2, \dots, 20\}$).

(b) How would you do part 1 NOT using Brute force? COHERENT, CLEAR, CONCISE as usual.

2. (30 points) For this problem we are working mod 21.

(a) Find a linear function $f(x) = ax + b$ that has NO roots OR prove that there is no such linear function.

(b) Find a linear function $f(x) = ax + b$ that has EXACTLY one root OR prove that there is no such linear function.

(c) Find a linear function $f(x) = ax + b$ that has AT LEAST two roots OR prove that there is no such linear function.

3. (30 points) Let p be a prime such that $p - 1 = 2q^2r$ where q, r are primes. Write a program that will, given p, q, r, g , test if g is a generator. YOUR PROGRAM CAN USE THE POWER FUNCTION. So you can write things like *if g^{q^4} is an odd Fibonacci number then*

4. (10 points) Let p be a prime. How many affine ciphers are there mod p ?