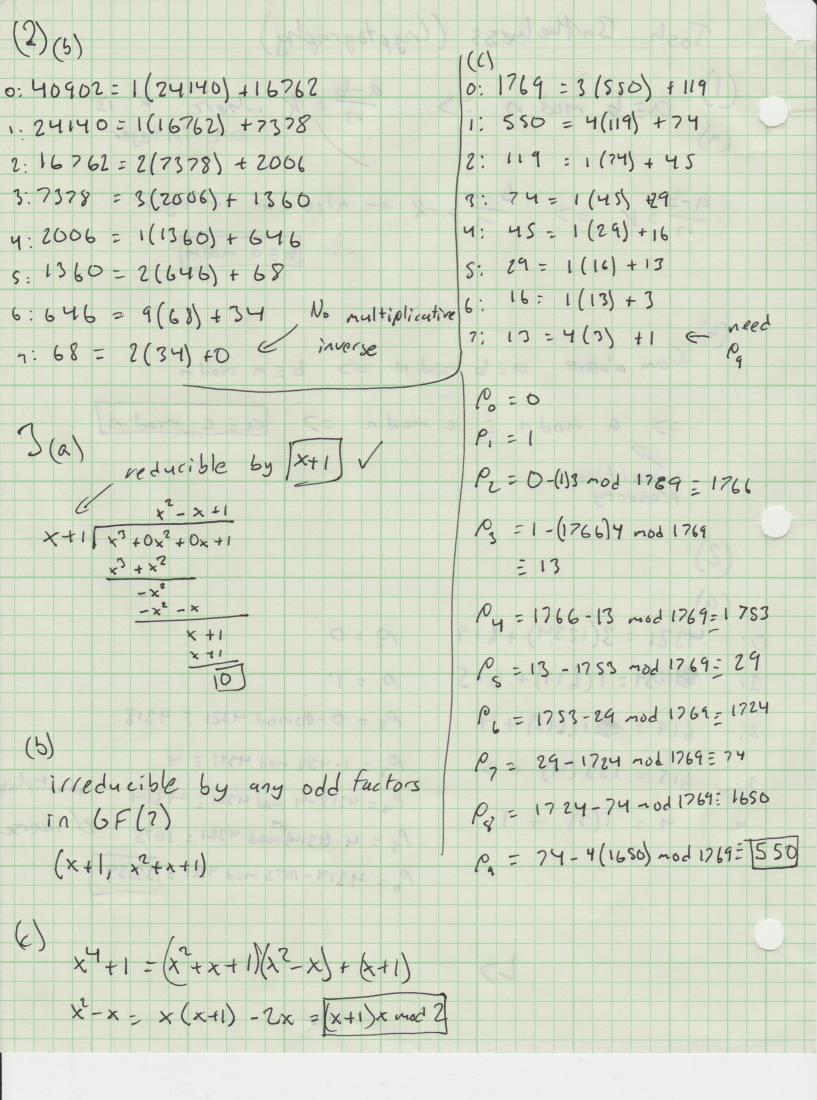
Josh Bathelmess (Cryptography) (1) $a = b \mod n = > \frac{a-b}{n} = k \text{ where } k = is$ (a) an integer $\frac{a-b}{n} = K = \sum_{n=1}^{b-a} \frac{b-a}{n} = -K = also an integer$ b = a mod n a=bmodn => b=a modn aic mod n) => a modn = transitive property 4321 = 3(1234) + 619 PO = 0 0: 1: 對1234:1(619)+615 P = 1 Pz = 0-115 nod 4321 = 4318 619 = 151(615) + 4 615 = 153 (4) + 3 Pg = 1-4318 mod 4321 = 4 Py = 4318-4 mod 4321 = 4314 4 = 1(3) + 1 d'inverse Ps = 4-4314) mod 4321 = 1075 05 51 2 1 2 1 4 (18 20) mod 12 13 2 2 2 Pb = 4314-1075 mod 4321 = 13239

L> (1+8+(x-5)) + x+1)=1+1x-1

S Som X (+X)= XS- (1+X) x = X-1X



H(KIC) = 3-1.75=[1.25]