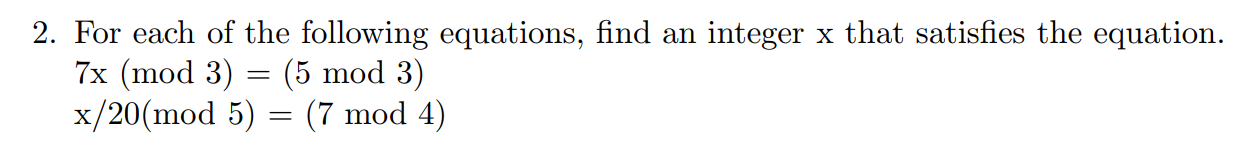
  
  
(A1) Closure  
Yes: Arithmetic Rule

(A2) Associative law  
Yes:

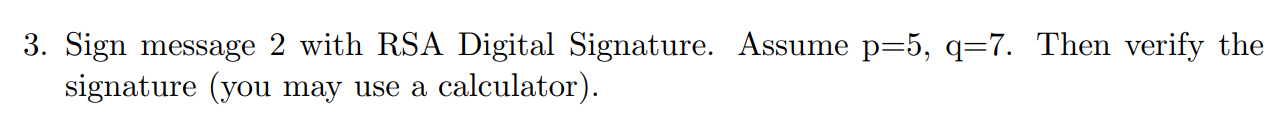
(A3) Identity Element  
Yes: a

(A4) Additive Inverse  
Yes: itself  
  
(A5) Commutative Law  
Yes  
  
(M1) Closure  
Yes

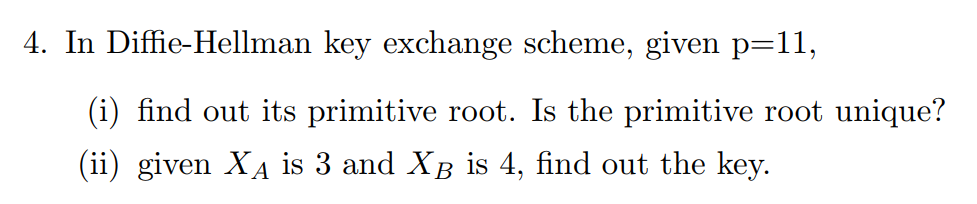
(M2) Associative Law  
Yes:  
  
(M3) Distributive Law  
Yes:  
  
(M4) Commutative Law  
Yes:  
  
(M5) Identity Element  
Yes: b  
  
(M6) Non-zero Divisor  
  
(M7) Multiplicative Inverse  
no multiplicative inverse



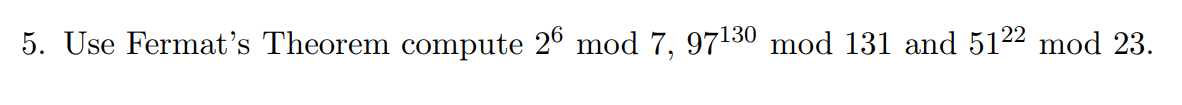
7x2 mod 3 = 5 mod 3 = 2  
60/20 mod 5 = 7 mod 4 = 3

  
  
n = 5x7 = 35  
phi(n) = 4x6 = 24  
e = 7  
  
24 = 7(3) + 3  
7 = 3(2) + 1  
---------------------------

24 – 7(3) = 3  
7 – 3(2) = 1  
  
7 – 2(24 – 7(3)) = 1  
7 – (2)24 + (6)7 = 1  
7(7) – (2)24 = 1  
---------------------------  
  
Public key = (7,35)  
Private key = (7,35)  
  
Sign it with private key:  
  
2^7 mod 35 = 23  
23^7 mod 35 = 2

  
  
(i) Multiple answers 2, 6, 7, 8  
(ii) (2^3 mod 11)^4 mod 11  
  
Text, letter

Description automatically generated  
  
  
  
  
  
  
  
  
  
  
Key = 4;

  
Fermats Theorem: if p is prime and a is an integer not divisible by p then, (x^n-1) mod n = 1  
  
2^6 mod 7 = 1  
97^130 mod 131 = 1  
51^22 mod 23 = 1