1.

a:

Elements:

- Gcd(1,21) = 1
- Gcd(2,21) = 1
- Gcd(3,21) = 3
- Gcd(4,21) = 1
- Gcd(5,21) = 1
- Gcd(6,21) = 3
- Gcd(7,21) = 7
- Gcd(8,21) = 1
- Gcd(9,21) = 9
- Gcd(10,21) = 1
- Gcd(11,21) = 1
- Gcd(12,21) = 3
- Gcd(13,21) = 1
- Gcd(14,21) = 7
- Gcd(15,21) = 3
- Gcd(16,21) = 1
- Gcd(17,21) = 1
- Gcd(18,21) = 3
- Gcd(19,21) = 1
- Gcd(20,21) = 1

Φ(21) = 12

b:

127 is een priemgetal, er zijn dus geen getallen behalve 1 die 127 delen, hierdoor is 127 copriem met alle getallen onder 127.

Φ(127) = 126

c:

De priemfactorisatie van 125 =

5^3

Alle getallen onder 125 die deelbaar zijn door 5 zitten niet in de set Z^*_{125}. De rest van de getallen wel, de getallen:

5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100, 105, 110, 115, 120 zitten niet in de set.

Dit zijn 24 getallen dus:

Φ(125) = 124 – 24 = 100

d:

De priemfactorisatie van 1651:

$13^1 * 127^1$

Alle getallen deelbaar door 13 of 127 zitten niet in Z^*_{1651}.

$\Phi(13) = 13 – 1 = 12$.

$\Phi(127) = 127 – 1 = 126$.

$\Phi(1651) = \phi(13 * 127) = \phi(13) * \phi(127) = 12 * 126 = 1512$

2.

a:

7^{1202} mod 41	= (7^{601} mod 41 * 7^{601} mod 41) mod 41	= 8
7^{601} mod 41	= (7^{300} mod 41 * 7^{300} mod 41 * 7) mod 41	= 7
7^{300} mod 41	= (7^{150} mod 41 * 7^{150} mod 41) mod 41	= 40
7^{150} mod 41	= (7^{75} mod 41 * 7^{71} mod 41) mod 41	= 32
7^{75} mod 41	= (7^{37} mod 41 * 7^{37} mod 41 * 7) mod 41	= 27
7^{37} mod 41	= (7^{18} mod 41 * 7^{18} mod 41 * 7) mod 41	= 11
7^{18} mod 41	= (7^{9} mod 41 * 7^{9} mod 41) mod 41	= 5
7^{9} mod 41	= (7^{4} mod 41 * 7^{4} mod 41 * 7) mod 41	= 13
7^{4} mod 41	= (7^{2} mod 41 * 7^{2} mod 41) mod 41	= 23
7^{2} mod 41	= (7 mod 41 * 7 mod 41) mod 41	= 8

b:

9^{1202} mod 23

$X \equiv Y \bmod \varphi(23)$

$X = 1202$

$\Phi(23) = 23 – 1 = 22$

$1202 = Y \bmod 22$

$Y = 14$

Dus $9^{1202} = 9^{14}$ mod 23

9^{14} mod 23	= (9^{7} mod 23 * 9^{7} mod 23) mod 23	= 16
9^{7} mod 23	= (9^{6} mod 23 * 9) mod 23	= 4
9^{6} mod 23	= (9^{3} mod 23 * 9^{3} mod 23) mod 23	= 3
9^{3} mod 23	= (9^{2} mod 23 * 9) mod 23	= 16
9^{2} mod 23	= (9 mod 23 * 9 mod 23) mod 23	= 12

c:

Inverse van 2 mod 13:

2^{-1} mod 13

We hebben een X nodig zodat:

2 * X mod 13 = 1

1 =   13 + 2 * - 6

Dus:

13 * 1 + 2 * -6 = 1 mod 13

2 * -6 = 1 mod 13

-6 mod 13 is de inverse van 2 mod 13

3.

a:

n = p * q

p = 19

q = 13

n = 19 * 13 = 247

ϕ(247) = ϕ(19 * 13) = ϕ(19) * ϕ(13) = (19 – 1) * (13 – 1) = 216

b:

e * d + k * (p – 1)(q – 1) = 1

e * d + k * (18)(12) = 1

7 * d + k * 216 = 1

6 = 216 – 30 * 7

1 = 7 – 1 * 6

1 = 7 – (216 – 30 * 7)

1 = 7 – 216 + 30 * 7

1 = -1 * 216 + 31 * 7

d = 31

c:

m = 20

c = m^e mod n = 20^7 mod 247 = 58

d:

m = c^d mod n = 58^{31} mod 247 = 20 e:

?

f:

$m = 2$

$s = m^d \bmod n = 2^{31} \bmod 247 = 193$