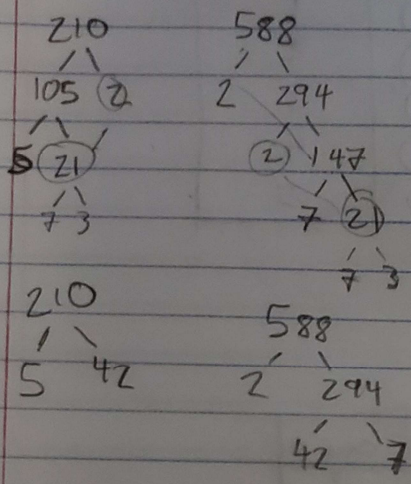
1.18, 1.20, 1.27

Taylor Whitlock
Section 002
HW #3

1.18) gcd(210, 588)



A	B
588	210
210	168
168	42
42	0

Euclid's Algorithm

1.20) 20 mod 79:

AX+BY=D

INVERSE = 4

A	B	X	Y	D	Return	Call #
79	20	1	-4	1	(-4, 1)	1
20	19	0	1	1	(1, -1)	2
19	1	1	0	1	(0, 1)	3
1	0	None	None	None	(1, 0)	4

3 mod 62

A	B	x	Y	D	Return	Call #
62	3	1	-1	1	(-1, 21)	1
3	2	0	1	1	(1, -1)	2
2	1	1	0	1	(0, 1)	3
1	0	None	None	None	(1, 0)	4

INVERSE = 21

21 mod 91

A	B	X	Y	D	Return	Call #
91	21	0	1	7	(1, -4)	1
21	7	1	0	7	(0, 1)	2
7	0	None	None	None	(1, 0)	3

INVERSE DOES NOT EXIST

1.20 CONT

5 MOD 23

A	B	X	Y	D	RETURN	CALL #
23	5	-1	2	1	(2, -9, 1)	1
5	3	1	-1	1	(-1, 2, 1)	2
3	2	0	1	1	(1, -1, 1)	3
2	1	1	0	1	(0, 1, 1)	4
1	0	NONE	NONE	NONE	(1, 0, 1)	5

INVERSE = 14

1.27

3 MOD 352

A	B	X	Y	D	RETURN	CALL #
352	3	0	1	1	(1, -117, 1)	1
3	1	1	0	1	(0, 1, 1)	2
1	0	ϕ	ϕ	ϕ	(1, 0, 1)	3

$-117 \text{ MOD } 352 \equiv 235 \text{ (MOD } 352)$ $d = 235$

$y = M^e \text{ (MOD } 391) = 68921 \% 391 = 105$

ENCRYPTION = 105