ENEE/CMSC/MATH 456: Cryptography
Euclidean Algorithm Class Exercise 4/13/19

1. Use the Extended Euclidean Algorithm to find integers X, Y such that $24X + 17Y = 1$:

We first run the non-extended EA and keep track of our answers:

24 = 17 + 7
17 = 2*7 + 3
7 = 2*3 + 1

We now set up a table:

	X	Y
24	1	0
17	0	1
7	1	-1
3	-2	3
1	5	-7

Indeed, 24*5 -17*7 = 1

Multiplicative inverse of 17 mod 24 is -7 = 17.

2. Use the Extended Euclidean Algorithm to find integers X, Y such that $27X + 16Y = 1$:

We first run the non-extended EA and keep track of our answers:

27 = 16 + 11
16 = 11 + 5
11 = 2*5 + 1

We now set up a table:

	X	Y
27	1	0
16	0	1
11	1	-1
5	-1	2
1	3	-5

Indeed, 27*3 -16*5 = 1

Multiplicative inverse of 16 mod 27 is -5 = 22.