LAB 5
CS 135

PROBLEM 1

Prove that if n is an **odd** positive integer, then $n^2 \equiv 1 \pmod{8}$.

PROBLEM 1 ANSWER KEY

$n = 2k+1$ definition of an odd #

$n^2=(2k+1)^2=4k^2+4k+1=4k(k+1)+1$

SInce 4 divides $4k(k+1)$

And 2 divides $k(k+1)$ two consecutive #s, one is bound to be even

Then $2*4 \mid 4k(k+1)$

And $4k(k+1) + 1 \equiv 1 \pmod 8$ adding 1 to above

PROBLEM 2

Use Euclid's Algorithm to solve the following:

gcd(101, 4620)

PROBLEM 2 ANSWER KEY

gcd(4620, 101)

gcd(101, 75)	4620 = 101*45 + 75
gcd(75, 26)	101 = 75*1 + 26
gcd(26, 23)	75 = 26*2 + 23
gcd(23, 3)	26 = 23*1 + 3
gcd(3, 2)	23 = 3*7 + 2
gcd(2, 1)	3 = 2*1 + 1
gcd(1, 0)	

PROBLEM 3

Use the Pulverizer to express gcd(1529,14039) as a linear combination of 1529 and 14039.

PROBLEM 3 ANSWER KEY

gcd(14039, 1529)

gcd(1529, 278)

gcd(278, 139)

gcd(139, 0)

139

$14039 = 9*1529+278$

$1529 = 5*278+139$

$278 = 2*139$

Putting it all together:

$139 = 1529-5*278$

$= 1529 - 5(14039-9*1529)$

$= -5*14039+46*1529$ simplify