Unless stated otherwise, variables are integers.

1. Assume that x and y are each k-bit unsigned integers, with $k \geq 2$.

   (i) What is the min value of x? max value?

   (ii) What is the exact formula (as a function of x) for k?

   (iii) What is the maximum number of bits in $x * y$?

2. The code below is called with x, y, and n each having $k \geq 2$ bits.

   (i) What is the maximum number of multiplications performed by `modexp(x,y,n)`?

   (ii) What is the maximum number of bits in the final answer?

```
def modexp(x,y,n): #integers, y >= 0, n >= 2
  if y==0: return 1
  z = modexp(x,y/2,n)
  z = z*z%n
  if 1==y%2: z = x*z%n
  return z
```

3. (i) Using Euclid's algorithm, find the gcd of 313 and 61.

   (ii) Using the extended Euclid algorithm, express the gcd of 313 and 61 as a linear combination of 313 and 61.

   (iii) Using your answer to (ii), prove that your answer to (i) is correct.

   (iv) Using your answer to (ii), find $61^{-1} (\text{mod } 313)$? Your answer must be either "does not exist" or an integer in the set $\{0, 1, \ldots, 312\}$.

   (v) By factoring, find the gcd of 313 and 61. In general, would you prefer to use (i) or (v) to find the gcd of two numbers?

4. Give the output of the following program.

```
def test(n):
  c = 0
  for j in range(1,n):
    if gcd(j,n)==1: c += 1
  return c

for j in range(2,20):
  print j, test(j)
```

5. Let x be 271809. (i) Using python, find 5 to the power $x - 1$ mod x.

   (ii) What does (i) imply about the primality of x? (prime? probably prime? composite? probably composite?)

   Repeat the above for $x = 1729$, and then for $x = 12611$.