1. In Aug 31's lecture (slide 5), we discussed a recursive multiplication algorithm. If the input is an m-bit number x and an n-bit number y, how long does it take to multiply x and y? Justify your answer.

Usually, it will be O(n^2) or O(m^2) for smaller int values (assuming our processor and memory can contain both). However, as n and m get sufficiently large and we can't hold both in the limited amount of registers on the processor then it will go to O(n*m).

2. Compute gcd(770, 546) in the following three different ways. Show your steps.
(a) By finding the factorization of each number;

$770 = 2 * 335 = 2 * 5 * 77 = 2 * 5 * 7 * 11$ $(all\ primes\ so\ can't\ factor\ further)$
$546 = 2 * 273 = 2 * 91 = 2 * 7 * 13$
So, we can combine common prime factors to:
$770 = 5 * 11 * 14$
$546 = 13 * 14$
so gcd(770,546)=14

(b) By using the Euclid algorithm;

$770/546 = 546 * 1 + 224$
$546/224 = 224 * 2 + 98$
$224/98 \ \ = 98 * 2 + 28$
$98\ /28 \ \ = 28 * 3 + 14$
$28/14 \ \ \ = 14 * 2 + 0$
so gcd(770,546)=14

(c) By using the extended Euclid algorithm (also finds x and y).

Building off 2b):
$224 \ = \ 1 * 770 - 1 * 546$
$98 \ \ = \ 1 * 546 - 2 * 224 \ = \ 1 * 546 - 2 * (1 * 770 - 1 * 546) \ = \ 3 * 546 - 2 * 770$
$28 \ \ = \ 1 * 224 - 2 * 98 \ \ = \ 1 * 224 - 2 * (3 * 546 - 2 * 770)$
$= \ (1 * 770 - 1 * 546) - 6 * 546 \ + \ 4 * 770 \ = \ 5 * 770 - 7 * 546$
$14 \ \ = \ 1 * 98 - 3 * 28 = 1 * (3 * 546 - 2 * 770) - 3 * (5 * 770 - 7 * 546)$
$= 24 * 546 - 17 * 770$
so 14 = – 17*770 + 24*546 (x=-17, y=24)

3. What is the result of 7^7293 (mod 342)? Show your steps.

We will use modular multiplication properties to get the result of this large power:

1) Compute the powers of 7:

$$7 \; mod \; 342 \; = \; 7$$
$$7^2 mod \; 342 = 49$$
$$7^4 mod \; 342 = 7$$
$$7^8 mod \; 342 = 49$$
$$7^{16} mod \; 342 = 7$$

Noticing the pattern of alternating values 7 and 49, we can easily extrapolate:

$$7^{32} mod \; 342 = 49$$
$$7^{64} mod \; 342 = 7$$
$$7^{128} mod \; 342 = 49$$
$$7^{256} mod \; 342 = 7$$
$$7^{512} mod \; 342 = 49$$
$$7^{1024} mod \; 342 = 7$$
$$7^{2048} mod \; 342 = 49$$
$$7^{4096} mod \; 342 = 7$$

Now given 7293, we convert it to binary so we can more easily compute our required value:

1110001111101

$$7^{4096} * 7^{2048} * 7^{1024} * 7^{64} * 7^{32} * 7^{16} * 7^{8} * 7^{4} * 7^{1} = 7^{7293}$$
$$7 * 49 * 7 * 7 * 49 * 7 * 49 * 7 * 7 = 7^6 * 7^{2^3} = 7^{12} \; mod \; 342$$

= 13841287201 mod 342 = 1

4. Results:

Testing for 1024 :
Key Generation took 0.00112414360046 seconds
Encryption took 0.000118017196655 seconds
Decryption took 3.81469726562e-06 seconds
****
Testing for 4096 :
Key Generation took 0.0105400085449 seconds
Encryption took 0.000447034835815 seconds
Decryption took 4.05311584473e-06 seconds
****
Testing for 8192 :
Key Generation took 0.0437829494476 seconds
Encryption took 0.00170278549194 seconds
Decryption took 1.50203704834e-05 seconds
****
[Finished in 0.1s]