WORKSHEET #8 – MATH 5405
SPRING 2016

DUE TUESDAY, MARCH 8TH

Let's experiment with the quadratic sieve.

Let's try to factor $n = 3403$ using this method.

1. Compute $a = \lfloor \sqrt{3403} \rfloor$.

2. Now write down the next 6 integers after a and compute their squares mod n and then factor them.

3. If I didn't make a mistake, one of those integers is a perfect square. Use that number to factor n using the fact that if $a^2 - b^2 \equiv_n 0$ then $(a - b)$ or $(a + b)$ has a decent chance to contain a factor of n.

Now we're going to try the same thing but use the linear algebra method. We choose a new $n = 87463$ and notice that $\lfloor \sqrt{n} \rfloor = 295$

4. First verify that for each $p = 2, 3, 13, 17, 19, 29$, n is a square modulo that p. Also check that n is not a square compared to all other primes less than or equal to 30.

5. Fill in the following table.

	-1	**2**	**3**	**13**	**17**	**19**	**29**
265							
278							
296							
299							
307							
316							

6. Now find a linear combination of the rows which gives zero (mod 2).

7. Finally, use that linear combination to factor 87463.