Name: _____

Read and take notes on Sections 19.1, Gaussian Elimination and 19.3, Dixon's Algorithm.

Reading Questions

1. Section 19.1 is a review of one of the basic algorithms in linear algebra: using row reduction to find a dependency relation among m vectors in an n-dimensional vectorspace, where $m > n$. Make sure you know the relevant terms: linear dependency relation, linear combination of vectors, etc.

2. From Section 19.3, make sure you understand what a factor base is and what it means for a number to be smooth with respect to a factor base.

3. In the very simplest cases, if we are lucky, Dixon's Algorithm can be significantly abbreviated, as follows:

   > We aim to factor a number n. We choose a factor base $S = \{p_1, \ldots, p_t\}$. We choose a number a and let $b = a^2 \,\%\, n$. Suppose we are *lucky* and b is both smooth with respect to S and a square in $\mathbb{Z}$. In this case let $x = a$ and $y = \sqrt{b}$ (the square root of b in $\mathbb{Z}$.) Then $x^2 = y^2 \bmod n$, and, if we are again lucky, $x \neq \pm y$, in which case $\gcd(x \pm y, n)$ are proper factors of n.

   Use this simple version of Dixon's Algorithm with factor base $\{2, 3\}$ to factor n, for

   (a) $n = 323$, with lucky choice $a = 18$.

   (b) $n = 1147$, with lucky choice $a = 34$.

4. What struck you in this reading? What is still unclear? What remaining questions do you have?