SOAR Math Course Homework Six Spring, 2003

These homework problems are meant to expand your understanding of what goes on during class. Any you turn in will be graded and returned to you. Answers may or may not be posted on the web, depending on demand.

1. Do the problems on the RSA handout from class today. Note that this will probably involve either writing a computer program or using an existing computer package (like Maple or Mathematica).

2. [Postponed From Last Week] On Friday at 3:00 PM, I will publish on the web page a public key and an encrypted message. I will encrypt the message using $A = 01$, $B = 02$, up through $Z = 26$ and space as 27 and concatenate a fixed number of characters at a time. I will not use lower-case letters or punctuation.

   (a) Decrypt the message using my public key.

   (b) [Challenge Part One] Factor my product of two primes and send me a message encrypted using my key.

   (c) Make up your own public and private key and email me a message with these keys. I will post the message and the public key on the web page. (I may restrict the size of the primes permitted.) *Your key and message are due by the start of class next week.*

   (d) [Challenge Part Two] Next week, decrypt everyone else's messages.

   (e) [Challenge Part Three] If possible, "break" other people's code and email me a message using their private key. (Also send me a factorization of their product of two primes.)

   This is something of a race. Prizes may or may not be awarded.

3. This problem will give you some idea of where the term $bc - ad$ comes in to the Farey series. In class we discussed parallelograms with corners $(0, 0)$, (b, a), (d, c), and $(b+d, a+c)$, and somehow this term $bc-ad$ or $ad-bc$ showed up. Where does it come from?

   Consider the *lattice* in the plane constructed of points (m, n) where both m and n are integers. It should look something like Figure 1. (This is called the *fundamental lattice*.) We're going to change from (x, y) to (x', y') via the transformation:

$$\begin{aligned} x' &= bx + dy \\ y' &= ax + cy. \end{aligned} \tag{$*$}$$

   (This transformation, with $x' = x - 2y$ and $y' = -x + y$, is illustrated in Figures 2 and 3. In Figure 2, the grid lines are the lines $x =$ a constant or $y =$ a constant. After the transformation, in Figure 3, the lines are $x' =$ a constant and $y' =$ a constant. Notice that the dots of the lattice are at intersection points for both grids!)

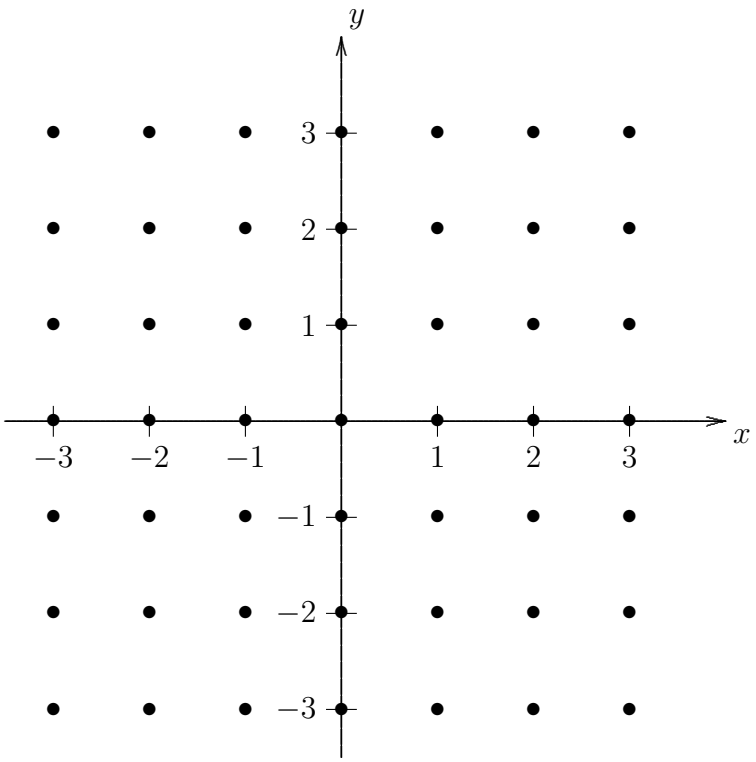

Figure 1: The Fundamental Lattice

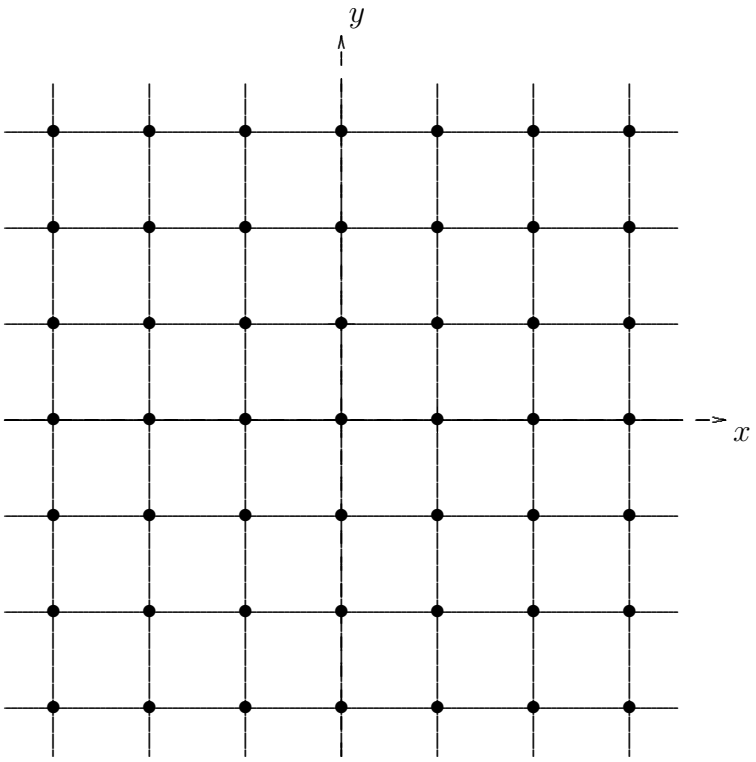

Figure 2: The Lattice With Grid

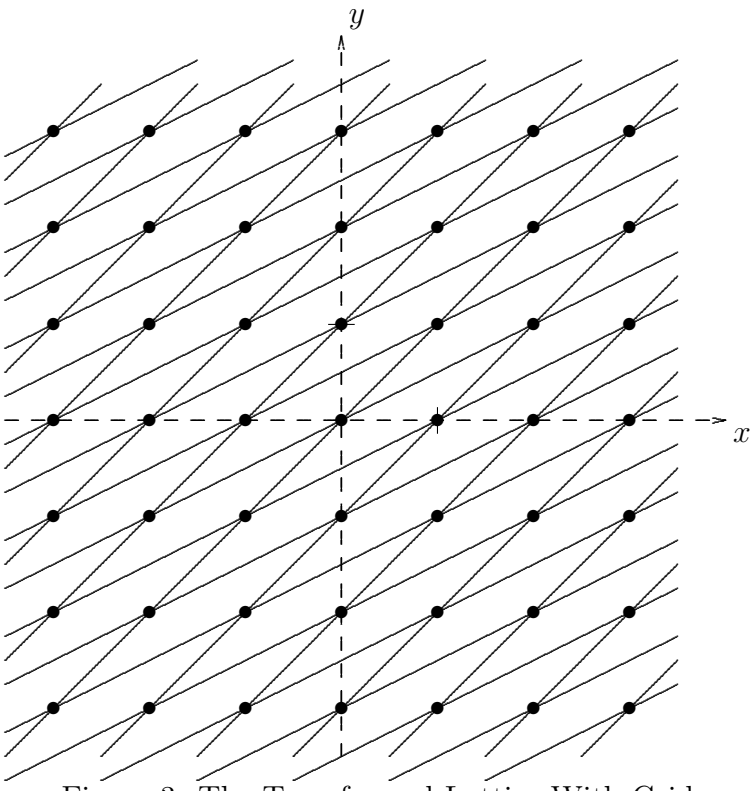

Figure 3: The Transformed Lattice With Grid

(a) Show that if $(x, y) = (1, 0)$, then $(x', y') = (b, a)$. Similarly, show that if $(x, y) = (0, 1)$, then $(x', y') = (d, c)$.

(b) Show that (x, y) may be written in terms of (x', y') as

$$x = \frac{cx' - dy'}{bc - ad}$$
$$y = -\frac{ax' - by'}{bc - ad}.$$

(c) Assume that $\Delta = bc - ad = \pm 1$. Show that if (x', y') are both integers, then (x, y) are integers as well. (This means that if $\Delta = \pm 1$, then the transformation $(*)$ takes points on the lattice to points on the lattice.)

(d) Assume that whenever (x, y) are integers, then (x', y') are also integers. Show that this implies that Δ divides a, b, c, and d. (Hint: choose (x, y) carefully to show this. For example, what happens when $(x, y) = (1, 0)$?)

(e) Show that the previous part implies that $\Delta^2 | ad - bc = \Delta$, so $\Delta = \pm 1$. (This means that if the transformation $(*)$ takes points on the lattice to points on the lattice, then $\Delta = \pm 1$.)

Transformations of the type $(*)$ with $\Delta = \pm 1$ are called *unimodular transformations.*