SOAR Math Course **Homework Twelve Solutions** Spring, 2003

These solutions are written at the request of students. Please let me know if you don't understand these solutions; I'm happy to expand on them if necessary.

3. One thing we didn't cover in class is that the various elliptic curve expressions, from

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

to

$$y^2 = x^3 + Ax^2 + Bx + C \tag{2}$$

and finally

$$y^2 = x^3 + ax + b, \tag{3}$$

may be obtained by changing variables. This question is essentially algebra, walking through these changes.

(a) Show that if we change y to $y - \frac{a_1}{2}x - \frac{a_3}{2}$, the expression (1) changes to equation (2). (Here we leave x unchanged.)

Solution: We re-write the left-hand side of expression (1) as

$$y^2 + a_1xy + a_3y = y(y + a_1x + a_3)$$

Now we replace y with $y - \frac{a_1}{2}x - \frac{a_3}{2}$, as required. This left-hand side becomes

$$y(y + a_1x + a_3) = \left(y - \frac{a_1}{2}x - \frac{a_3}{2}\right)\left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right).$$

This is of the form $(y - k)(y + k) = y^2 - k^2$, where $k = \frac{a_1}{2}x + \frac{a_3}{2}$. We square this to get

$$\begin{aligned} y(y + a_1x + a_3) &= y^2 - \left(\frac{a_1}{2}x + \frac{a_3}{2}\right)^2 \\ &= y^2 - \left(\frac{a_1^2}{4}x^2 + \frac{a_1a_3}{2}x + \frac{a_3^2}{4}\right). \end{aligned}$$

This means that equation (1) becomes

$$y^2 - \left(\frac{a_1^2}{4}x^2 + \frac{a_1a_3}{2}x + \frac{a_3^2}{4}\right) = x^3 + a_2x^2 + a_4x + a_6,$$

or

$$y^2 = x^3 + \left(a_2 + a_1^2/4\right)x^2 + \left(a_4 + a_1a_3/2\right)x + \left(a_6 + a_3^2/4\right).$$

This is the same form as expression (2), with $A = a_2 + a_1^2/4$, $B = a_4 + a_1a_3/2$, and $C = a_6 + a_3^2/4$.

(b) Show that if we change x to $(x - 3A)/9$ and y to $y/27$, the expression (2) changes to equation (3).

Solution: Now we start with

$$y^2 = x^3 + Ax^2 + Bx + C \tag{2}$$

and replace x with $(x - 3A)/9$ and y with $y/27$. From expression (2), we get

$$\left(\frac{y}{27}\right)^2 = \left(\frac{x-3A}{9}\right)^3 + A\left(\frac{x-3A}{9}\right)^2 + B\left(\frac{x-3A}{9}\right) + C. \tag{2}$$

We expand these expressions to find that

$$\frac{y^2}{729} = \left(\frac{x^3 - 9Ax^2 + 27A^2x - 27A^3}{729}\right) + A\left(\frac{x^2 - 6Ax + 9A^2}{81}\right) + B\left(\frac{x-3A}{9}\right) + C.$$

We multiply through by 729 to clear the denominators. We get

$$y^2 = \left(x^3 - 9Ax^2 + 27A^2x - 27A^3\right) + 9A\left(x^2 - 6Ax + 9A^2\right) + 81B\,(x - 3A) + 729C,$$

or

$$\begin{aligned} y^2 &= x^3 + (-9A + 9A)\,x^2 + \left(27A^2 - 54A^2 + 81B\right)x \\ &\quad + \left(-27A^3 + 81A^2 - 243AB + 729C\right) \\ &= x^3 + 27\left(-2A^2 + 3B\right)x + 27\left(-A^3 + 3A^2 - 9AB + 27C\right) \end{aligned}$$

This is the required expression (3), with coefficients $a = 27\,(-2A^2 + 3B)$ and $b = 27\,(-A^3 + 3A^2 - 9AB + 27C)$.

This means that, in a sense, the two expressions (1) and (3) represent the same object. (Compare this notion with the discussion in problem 3 of homework 6. We've just transformed one expression into the other.)