Math 502
Written Assignment No. 4

due Thursday, April 17, 2008

1 Arithmetic on Cubic Curves

When a cubic curve is given by an equation in Weierstrass form

$$f(x,y) \;=\; y^2 + a_1xy + a_3y - a_0x^3 - a_2x^2 - a_4x - a_6 \;=\; 0$$

with $a_0 \neq 0$ one may imagine this affine curve as part of the plane $z = 1$ in 3-dimensional space. The homogeneous cubic equation

$$F(x,y,z) \;=\; z^3 f(\frac{x}{z}, \frac{y}{z}) \;=\; y^2z + a_1xyz + a_3yz^2 - a_0x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \;=\; 0$$

is the equation of a conical surface in space that contains all lines drawn from the points of the affine curve to the origin. Moreover, every non-horizontal line (i.e., line not parallel to the plane $z = 1$) lying in the cone meets the affine curve in a single point. Beyond that every non-horizontal line meets the plane $z = 1$ in a single point. One says that the set of all lines in space through the origin are the "points" of the *projective plane*. Each "point" of the projective plane represented by a non-horizontal line corresponds to the unique point it contains in the affine plane $z = 1$. The non-affine "points" of the projective plane are the horizontal lines in space passing through the origin.

The line with affine equation

$$ax + by + c \;=\; 0 \quad \text{where} \quad (a,b) \neq (0,0)$$

in the plane $z = 1$ corresponds to the set of lines through the origin of space lying in the plane with equation $ax + by + cz = 0$, which may now be viewed as the homogeneous equation of a "line" in the projective plane. In general, a "line" in the projective plane corresponds to a plane through the origin of space. The only "line" in the projective plane that is not affine is the "line" $z = 0$ whose "points" are the horizontal lines through the origin of space. One uses the notation $[x : y : z]$ to denote the "point" of the projective plane corresponding to the line in space through the origin and the point (x, y, z) when $(x, y, z) \neq (0, 0, 0)$. Note that for any $t \neq 0$ one has $[tx : ty : tz] = [x : y : z]$.

For a cubic in Weierstrass form there is exactly one horizontal line lying in the cone, which is the line in space of points $(0, y, 0)$, i.e., the "point" $[0 : 1 : 0]$. One has "addition" for the points of a cubic curve in Weierstrass form by making two stipulations:

1. $[0 : 1 : 0]$ is "zero".
2. $P + Q + R = 0$ in the addition of points on the curve if and only if P, Q, R all lie on the curve and also all lie on the same line.

As a consequence, the "negative" of a point is the third point of the cubic on the line through the given point and "zero", and the sum of two given points is the "negative" of the third point of the cubic on the line through both. In these considerations multiplicities are relevant: for example, $P+P$ is the "negative" of the third point of the cubic on the line tangent to the cubic at P.

Example. For the cubic $y^2 = x^3 + 1$ the negative of the point $(2, 3)$ is the point $(2, -3)$ since the line through $(2, 3)$ and "zero" must contain both $(2, 3) = [2 : 3 : 1]$ and $[0 : 1 : 0]$, i.e., must be the line with homogeneous equation $x - 2z = 0$ and affine equation $x = 2$. The sum of $(2, 3)$ with itself is found by computing the tangent line to the cubic at $(2, 3)$, which is the line $y = 2x - 1$, and finding where else it intersects the cubic. The third point is $(0, -1)$. The negative of the third point is $(0, 1)$, which is therefore the "double" of $(2, 3)$.

2 Tasks

Directions: Use *Maple* for assistance in responding to the following problems. Please typeset your solutions. Explain what you have done. *Maple* session details are not necessary unless you think it important to include them. Accuracy is important.

Although you may refer to books and notes, you may not seek help from others on this written assignment.

1. Relative to arithmetic on the cubic curve $y^2 + y = x^3 - x$ find the negative of the point $(2, 2)$.

2. After verifying that the points $P = (-2, 48)$ and $Q = (-16, 120)$ lie on the curve $y^2 = x^3 - 1156x$, compute $P + Q$ and $P - Q$ in the arithmetic on the curve.

3. On the cubic curve $y^2 + y = x^3 + x^2$ let P be the point $(0, 0)$ and Q the point $(1, 1)$. Compute the expressions
$$3P + 7Q \quad \text{and} \quad 7P + 3Q$$
relative to the arithmetic of points of the curve.

4. Consider the arithmetic for points with coordinates in the finite field $\mathbf{Z}/3\mathbf{Z}$ on the cubic curve $y^2 = x^3 + 2x + 1$.
   (a) List all affine points in the finite field $\mathbf{Z}/3\mathbf{Z}$ on the curve.
   (b) For the particular point $P = (0, 1)$ compute its multiples mP (in the arithmetic of points on the curve over $\mathbf{Z}/3\mathbf{Z}$) for $-5 \leq m \leq 5$.

5. Consider the arithmetic for points with coordinates in the field $\mathbf{Z}/11\mathbf{Z}$ on the cubic curve $y^2 = x^3 + 2x + 1$.
   (a) How many points are in the affine plane over $\mathbf{Z}/11\mathbf{Z}$?
   (b) How many points are in the projective plane over $\mathbf{Z}/11\mathbf{Z}$?
   (c) How many of the points in the affine plane over $\mathbf{Z}/11\mathbf{Z}$ lie on the given cubic curve?
   (d) How many of the points in the projective plane over $\mathbf{Z}/11\mathbf{Z}$ lie on the given cubic curve?