Solutions to Assignment II

Rationa Points on Curves 2006

Problem 1

Let C, D be plane projective curves given by the homogeneous equations $F(x, y, z) = 0$ and $G(x, y, z) = 0$ respectively. Let n, m be the degrees of F, G respectively.
Suppose C and D intersect in a finite number of points. Suppose in addition that each intersection point is a smooth point of both C and D and that the intersection is transversal (i.e. the tangents of C, D at the point of intersection are distinct). Then the Theorem of Bezout asserts that there are precisely mn points of intersection. Assume in addition that the line $z = 0$ intersects C in n distinct points. Prove Bezout's theorem by considering the zeros and poles of the rational function $G(x, y, z)/z^m$ on C.
Solution. Denote the rational function $G(x, y, z)/z^m$ by f. The poles of f are clearly given by $z = 0$. This line intersects C in n distinct points which we denote by $P_1, \ldots, P_n$. Suppose first that none of these points are in the intersection of C and D, i.e all intersection points of C and D are in the affine part $z \neq 0$. Then $G(x, y, z)$ does not vanish in any of the P_i and thus f has a pole of order m at each point P_i. Hence f has degree mn. The zeros of f are precisely the points of intersection between C and D because G vanishes at these points. Let Q be such an intersection point. Let $l(x, y) = 0$ be the affine equation of the tangent line of D at Q. Since the intersection is transversal the function $l(x, y)$ is a local parameter of C at Q. Hence f has vanishing order 1 at Q. The total number of zeros must be mn, hence there are mn points of intersection between C and D.
In the general case we proceed as follows. Choose a line which does not contain any point of $C \cap D$ and which intersects C in n distinct points. Introduce new projective coordinates so that this line becomes the line $z = 0$. We are now in the situation again where $z = 0$ contains no points of $C \cap D$ and proceed as above.

Problem 2

Consider the plane projective curve E given by the affine equation $y^2 = f(x)$ where $f(x)$ is a quartic polynomial with distinct zeros. From problem A.4.2 of Hindry/Silverman we know that E has genus 1. Let $P = (x_0, y_0)$ be a point on E and suppose that y_0 is non-zero. Then, according to the Riemann-Roch theorem, the space $L(3P)$ has dimension 3. We construct this space as follows.

a) Show that there exist a, b, c such that $q(x, y) = y + ax^2 + bx + c$ has a zero of order 3 at P (Hint:use $x - x_0$ as local parameter).

b) Show that there exists a fourth zero which we denote by Q.

c) Show that $L(3P)$ coincides with the space of functions $p(x,y)/q(x,y)$ where $p(x,y)$ is a polynomial of the form $a'y + b'x^2 + c'x + d'$ with the restriction that it vanishes in Q.

Solution

a) Consider the space of functions spanned by $y, 1, x, x^2$. This is a four dimensional space. By linear algebra there exist $\alpha, \beta, \gamma, \delta \in k$ not all zero, such that $\delta y + \alpha(x-x_0)^2 + \beta(x-x_0)x + \gamma$ has vanishing order at least 3 at P. Clearly $\gamma = -\delta y_0$.

Suppose $\delta = 0$. Then $\alpha(x-x_0)^2 + \beta(x-x_0)$ has vanishing order 3 or higher at P. Since $x - x_0$ is a local parameter at P this implies that $\alpha = \beta = 0$ and we have the trivial function. So we conclude that $\delta \neq 0$ and we can assume it to be 1. By expansion of $y + \alpha(x-x_0)^2 + \beta(x-x_0) + \gamma$ we find our statement.

b) To determine the zeros of $y + ax^2 + bx + c$ we substitute $y = -ax^2 - bx - c$ into $y^2 = f(x)$ to get the equation $(ax^2 + bx + c)^2 = f(x)$. We already know that x_0 is a triple solution by construction. If the equation has degree 4, denote the fourth solution by x_1. Then the point $(x_1, -ax_1^2 - bx_1 - c)$ is our point Q. If the equation $(ax^2 + bx + c)^2 = f(x)$ has degree 3, there is no extra zero Q, only the function $y + ax^2 + bx + c$ has pole order one at one of the two points at infinity (this possibility was overlooked when writing down the problem, sorry). Let us for the moment ignore the latter possibility.

c) Let $p(x,y) = a'y + b'x^2 + c'x + d'$ be a function that vanishes at Q. The space of these functions is three dimensional. Then the function $p(x,y)/q(x,y)$ has a pole of order at most 3 at the point P and no other finite poles. It remains to check that it has no poles in the points at infinity.

Problem 3

Suppose we want to determine the Q-rational points on the curve E given by $y^2 = 2x^4 + x^3 + 2x^2 + 1$. We note the rational point $P = (0,1)$. So E is an elliptic curve. Use the construction in problem (2) to give a basis of the space $L(3P)$. Find a birational map $E \to E'$ where E' is an elliptic curve in weierstrass normal form $Y^2 = g(X)$, with $g(X)$ of degree 3, such that P is mapped to the point at infinity. Determine $g(X)$.

Solution Let us expand the function y near the point P in its (Taylor) expansion around $x = 0$. We get $y = 1 + x^2 + O(x^3)$. Hence $y - 1 - x^2$ vanishes of order 3 at P. To compute the fourth zero of $y - 1 - x^2$ we substitute $y = 1 + x^2$ in $y^2 = 2x^4 + x^3 + 2x^2 + 1$ to get $0 = x^4 + x^3$ (after some simplification). So the fourth zero is -1 and the point Q is $(-1, 2)$. A basis for $L(3P)$ is now given by

$$1, \quad \frac{x+1}{y-1-x^2}, \quad \frac{x(x+1)}{y-1-x^2}.$$

Note that $(x+1)/(y-1-x^2)$ equals $(y+1+x^2)/x^3$. So our basis reads

$$1, \quad X = \frac{y+1+x^2}{x^2}, \quad Y = \frac{y+1+x^2}{x^3}.$$

Note that Y has a pole of order 3 at P and X a pole of order 2. According to our course there exists a linear relation between $Y^2, XY, Y, X^3, X^2, X, 1$ giving us the desired third degree equation.
The actual computation can be quite cunbersome (I had not realised that). That is why we present two methods.
The map $(x, y) \mapsto (X, Y)$ is a birational map. The inverse is easily seen to be $(X, Y) \mapsto (x, y) = (X/Y, X^3/Y^2 - X^2/Y^2 - 1)$. Let us now substitute the latter formulas in $y^2 = 2x^4 + x^+2x^2 + 1$. We find

$$\left(\frac{X^3 - X^2}{Y^2} - 1\right)^2 = 2\frac{X^4}{Y^4} + \frac{X^3}{Y^3} + 2\frac{X^2}{Y^2} + 1.$$

Elaboration of the left hand side,

$$\frac{(X^3 - X^2)^2}{Y^4} - 2\frac{X^3 - X^2}{Y^2} + 1 = 2\frac{X^4}{Y^4} + \frac{X^3}{Y^3} + 2\frac{X^2}{Y^2} + 1.$$

After cancellation of terms on the left and right,

$$\frac{(X-1)^2X^4}{Y^4} - 2\frac{X^3}{Y^2} = 2\frac{X^4}{Y^4} + \frac{X^3}{Y^3}.$$

We multiply by Y^4 and divide by X^3 to obtain

$$X(X-1)^2 - 2Y^2 = 2X + Y.$$

Hence $2Y^2 + Y = X^3 - 2X^2 - X$. After splitting off squares,

$$2(Y + 1/4)^2 = X^3 - 2X^2 - X + 1/8.$$

The second method is more straightforward, but one needs a computer algebra system or a lot of patience in computation. We extend our expansion of y in terms of x to order 7,

$$y = 1 + x^2 + \frac{x^3}{2} + \frac{x^4}{2} - \frac{x^5}{2} - \frac{5x^6}{8} + O\left(x^7\right).$$

From this follows

$$X = \frac{2}{x^2} + 2 + \frac{x}{2} + \frac{x^2}{2} - \frac{x^3}{2} - \frac{5x^4}{8} + O\left(x^5\right)$$

and

$$Y = \frac{2}{x^3} + \frac{2}{x} + \frac{1}{2} + \frac{x}{2} - \frac{x^2}{2} - \frac{5x^3}{8} + O\left(x^4\right).$$

$$Y^2 = \frac{4}{x^6} + \frac{8}{x^4} + \frac{2}{x^3} + \frac{6}{x^2} - \frac{1}{4} + O(x)$$

$$XY = \frac{4}{x^5} + \frac{8}{x^3} + \frac{2}{x^2} + \frac{6}{x} + O(x)$$

$$X^3 = \frac{8}{x^6} + \frac{24}{x^4} + \frac{6}{x^3} + \frac{30}{x^2} + \frac{6}{x} + 14 + O(x)$$

$$X^2 = \frac{4}{x^4} + \frac{8}{x^2} + \frac{2}{x} + 6 + O(x).$$

Some linear algebra shows that $r = 2Y^2 + Y - X^3 + 2X^2 + X$ vanishes at P. Since r has no poles outside P we conclude that r vanishes identically.

Problem 4, A.4.9 of Hindry/Silverman

Let C be the smooth projective curve defined by $aX^3 + bY^3 + cZ^3 + dXYZ = 0$. We assume that a, b, c, d lie in a field k of characteristic zero and assume that not all a, b, c, d are zero.

a) Write down the condition on a, b, c, d for C to be smooth.

b) Let $P = (x, y, z) \in C$ and let L be the tangent line to C at P. Then $L \cap C$ consists of the point P with multiplicity 2 and a second point P'. Compute the coordinates of P' in terms of the coordinates of P and a, b, c, d.

c) Assume now $k = \mathbb{Q}$ and that a, b, c, d are square-free integers with a, b, c distinct. Let $P = (x, y, z) \in C(\mathbb{Q})$ with $x, y, z \in \mathbb{Z}$ and $\gcd(ax, y, z) = 1$. Similarly write the point P' defined in (b) by $P' = (x', y', z')$ with x', y', z' relatively prime integers. Prove that $|x'y'z'| > |xyz|$. Conclude that $C(\mathbb{Q})$ is either empty or infinite, and find examples for both instances.

Solution

a) Taking partial derivatives we find the following equations for a singularity on C

$$3aX^2 + dYZ = 0, \quad 3bY^2 + dXZ = 0, \quad 3cZ^2 + dXY = 0.$$

When at least one of a, b, c is zero, we have a singular point. For example, if $a = 0$, the point $(1 : 0 : 0)$ is singular. When $d = 0$, no singular point can be found. So let us assume that $abcd \neq 0$. Suppose $X = 0$. Then the equations imply $Y = Z = 0$. Similarly when we assume $Y = 0$ or $Z = 0$. So, $XYZ \neq 0$. Since $X \neq 0$ we might as well take $X = 1$. Hence from the last two equations $Z = -3bY^2/d, Y = -3cZ^2/d$. These two equations imply $Y = -\omega d/(27cb^2)^{1/3}, Z = -\omega^2 d/(27cb^2)^{1/3}$, where ω is a cube root of unity. Substitute this in the first equation to get $3a = -d^3/(27b^3c^3)^{1/3}$ hence $27abc = -d^3$. This means that we have a singular point if $27abc + d^3 = 0$. Actually in that case C is a union of three straight lines as can be seen from

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z).$$

So the condition for smoothness is $abc(d^3 + 27abc) \neq 0$.

b) The tangent line is given by the equation

$$(3ax^2 + dyz)X + (3by^2 + dxz)Y + (3cz^2 + dxy)Z = 0.$$

To simplify matters let us take $Z = 1$ in the equations for L and C and eliminate Y from them. So we substitute $Y = -((3ax^2 + dyz)X + (3cz^2 + dxy))/(3by^2 + dxz)$ in the equation for C. We get a cubic equation in X. The coefficient of X^3 reads

$$a - b(3ax^2 + dyz)^3/(3by^2 + dxz)^3$$

and the constant coefficient is

$$c - b(3cz^2 + dxy)^3/(3by^2 + dxz)^3.$$

Hence we know that the product of the three solutions of the cubic equation is minus the quotient of these two coefficients. More particularly,

$$\left(\frac{x}{z}\right)^2 \left(\frac{x'}{z'}\right) = -\frac{c(3by^2 + dxz)^3 - b(3cz^2 + dxy)^3}{a(3by^2 + dxz)^3 - b(3ax^2 + dyz)^3}.$$

A straightforward computation (using Mathematica) gives

$$c(3by^2 + dxz)^3 - b(3cz^2 + dxy)^3 = (by^3 - cz^3)(-d^3x^3 + 27b^2cy^3 + 27bcdxyz + 27bc^2z^3).$$

The second factor on the right equals $-dx^3 + 27bc(by^3 + dxyz + cz^3)$ which is easily seen to be $-dx^3 - 27abcx^3$. Similarly we get

$$a(3by^2 + dxz)^3 - b(3ax^2 + dyz)^3 = (by^3 - ax^3)(-dz^3 - 27abcz^3).$$

Hence

$$\frac{x'}{z'} = \frac{z^2(by^3 - cz^3)(-d^3 - 27abc)x^3}{x^2(ax^3 - by^3)(-d^3 - 27abc)z^3} = \frac{x(by^3 - cz^3)}{z(ax^3 - by^3)}.$$

Let us take $x' = x(by^3 - cz^3)$, $z' = z(ax^3 - by^3)$. By symmetry we deduce that $y' = y(cz^3 - ax^3)$.

c) Let x', y', z' be as in (b). Let g be the gcd of these numbers then a gcd-free representation of P' is given by $x'/g, y'/g, z'/g$. Notice that $|x'y'z'/g^3| \geq |xyz|$ where we have equality if and only if $x' = \pm gx, y' = \pm gy, z' = \pm gz$. This happens if and only if $|by^3 - cz^3| = |ax^3 - by^3| = |cz^3 - ax^3|$. However, three integers whose sum equals zero and which all have the same absolute value are necessarily all 0. I.e. $ax^3 = by^3 = cz^3$, which is impossible since a, b, c are distinct and square free.

So given a rational point P on C we can construct a point P' with $|x'y'z'| > |xyz|$. From P' we construct a new point P'' with $|x''y''z''| > |x'y'z'|$, etc.

The curve $x^3 + 2y^3 + 3z^3 = 0$ obviously has the rational point $(1 : 1 : -1)$. The curve $x^3 + 2y^3 + 7z^3 = 0$ has no rational points. If there were a soultion then $x^3 + 2y^3$ is divisible by 7. But this is only possible if x, y are divisible by 7. Hence $7^3|7z^3$, so $7|z$ contradicting our assumption $\gcd(x, y, z) = 1$.