ALGEBRAIC GEOMETRY

HOMEWORK 2

(1) Consider the equation $X^2 - DY^2 = 1$, where $D \in \mathbb{C}[T]$ is a nonconstant polynomial of degree $\deg D > 0$. Let $n(D)$ denote the number of distinct zeros of D. Show that the equation does not have any solutions $X, Y \in \mathbb{C}[T]$ except $(\pm 1, 0)$ if $2n(D) \leq \deg D$.

Let $A = X^2$, $B = -DY^2$ and $C = -1$; then $A + B + C = 0$. Moreover, $\deg \operatorname{rad} ABC \leq \deg X + \deg Y + n(D)$. By Mason's Theorem we have

$$\deg A = 2 \deg X < \deg \operatorname{rad} ABC \leq \deg X + \deg Y + n(D)$$
$$\deg B = 2 \deg Y + \deg D < \deg X + \deg Y + n(D).$$

Adding and simplifying gives $\deg D < 2n(D)$. Thus if $2n(D) \leq \deg D$, no nontrivial solutions exist.

(2) Describe all solutions $X, Y, Z \in \mathbb{F}_p[T]$ of the Fermat equation $X^p + Y^p = Z^p$.

In fields with characteristic p, we have $0 = X^p + Y^p - Z^p = (X + Y - Z)^p$, hence the solution set is given by $\{(X, Y, -X - Y) : X, Y \in \mathbb{F}_p[T]\}$.

(3) Find all points at infinity on the following curves in $\mathbb{A}^2\mathbb{C}$:
(a) $2x^2y + x + y^2 = 0$;
(b) $x^4 + y^4 = 1$.

(a) The projective curve has equation $F(X, Y, Z) = 2X^2Y + XZ^2 + Y^2Z = 0$. Putting $Z = 0$ we get $XY = 0$, so the points at infinity are $[1 : 0 : 0]$ and $[0 : 1 : 0]$.
(b) Here $F(X, Y, Z) = X^4 + Y^4 - Z^4 = 0$; putting $Z = 0$ gives $X^4 + Y^4 = 0$. The four points at infinity are $[1 : \pm\zeta : 0]$ and $[1 : \pm\zeta^3 : 0]$, where $\zeta = \exp(\frac{2\pi i}{8})$ is a primitive eighth root of unity and satisfies $\zeta^4 = -1$.

(4) Find all points on the projective closure of the curve $y^2 = x^3 + x$ over $\mathbb{F}_3$.

The "affine" points are $[0 : 0 : 1]$ and $[2 : \pm 1 : 1]$. For points at infinity, homogenize and put $Z = 0$; we find $[0 : 1 : 0]$ as the only point at infinity (this holds for any elliptic curve).

A deep theorem of Hasse says that the number N_p of points on an elliptic curve over $\mathbb{F}_p$ satisfies $|N_p - (p + 1)| \leq 2\sqrt{p}$.

(5) Parametrize the conic $\mathcal{C} : x^2 + xy + y^2 = 3$ over $\mathbb{Q}$. Extend the corresponding map $\phi : \mathbb{A}^1\mathbb{Q} \longrightarrow \mathcal{C}(\mathbb{Q})$ to a polynomial map $\phi^\# : \mathbb{P}^1\mathbb{Q} \longrightarrow \mathcal{C}^\#(\mathbb{Q})$, where $\mathcal{C}^\#(\mathbb{Q})$ denotes the rational points on $\mathcal{C}$ in the projective plane. Is ϕ injective, surjective, bijective? What about $\phi^\#$?

Using $P = (-1, -1)$ as your base point you get

$$x = \frac{-t^2 + 2t + 2}{t^2 + t + 1}, \quad y = \frac{2t^2 + 2t - 1}{t^2 + t + 1}.$$

In cases like these, pari helps you check your calculations. Just type in

```
x=(-t^2+2*t+2)/(t^2+t+1):y=(2*t^2+2*t-1)/(t^2+t+1)
x^2+x*y+y^2-3
```

and press enter after each line: pari gives the result 0.

ϕ is not surjective: from the construction we see that the second point of intersection of the line $x = -1$ with the curve is not parametrized (it would correspond to infinite slope), and this point is $Q = (-1, 2)$. It is, however, injective because different values of t give different points (just look at the picture).

Putting $t = \frac{r}{s}$ and clearing denominators we find

$$\phi^{\#} : [r : s] \longmapsto [-r^2 + 2rs + 2s^2 : 2r^2 + 2rs - s^2 : r^2 + rs + s^2].$$

This map $\phi^{\#}$ is surjective: we have $\phi^{\#}([1 : 0]) = [-1 : 2 : 1]$, the other affine points are in the image anyway, and since the projective curve does not have a point at infinity (it is an ellipse) the claim follows. For the same reason, $\phi^{\#}$ is injective: if $\phi^{\#}([r : s]) = \phi^{\#}([r' : s'])$ and the images lie in the affine plane and are different from Q, then $[r : s] = [r' : s']$; moreover, $[-1 : 2 : 1]$ is the image of $[1 : 0]$ and no other point.