Tutorial: Arithmetic of Elliptic Curves

Submission Guidelines All problems must be submitted in class today. Submissions should be done in plain paper clearly mentioning your name and roll number.

1. Prove that the norm function defined by Eqn (4.11) is multiplicative, that is, $\mathrm{N}(G_1G_2) = \mathrm{N}(G_1)(G_2)$ for all polynomial functions $G_1, G_2 \in K[C]$.

   A: Let $G_1 = a_1(x)+yb_1(x)$ and $G_2 = a_2(x)+yb_2(x)$ be polynomial functions, and $G = G_1G_2$. Using the fact that $y^2 = v(x) - u(x)y$, we can express $G = a(x) + yb(x)$ with $a(x) = a_1(x)a_2(x) + b_1(x)b_2(x)v(x)$, and $b(x) = a_1(x)b_2(x) + a_2(x)b_1(x) - b_1(x)b_2(x)v(x)$. But then, $\hat{G} = a(x) - (u(x) + y)b(x)$. Again after simple calculations using $y^2 = v(x) - u(x)y$ show that $\hat{G} = \hat{G}_1\hat{G}_2$. It then follows that $\mathrm{N}(G) = G\hat{G} = G_1G_2\hat{G}_1\hat{G}_2 = (G_1\hat{G}_1)(G_2\hat{G}_2) = \mathrm{N}(G_1)\mathrm{N}(G_2)$.

2. Consider the real hyperbola $H : X^2 - Y^2 = 1$. Find all the zeros and poles (and their respective multiplicities) of the following rational function on H:

$$R(x, y) = \frac{2y^4 - 2y^3x - y^2 + 2yx - 1}{y^2 + yx + y + x + 1} \tag{1}$$

   Hint: Split the numerator and the dinominator of R into linear factors.

   A: Since $x^2 - y^2 = 1$ is on the curve, we have $2y^4 - 2y^3x - y^2 + 2yx - 1 = (2y^4 - 2y^2) - (2y^3x - 2yx) + (y^2 - 1) = (y^2 - 1)(2y^2 - 2yx + 1) = (y - 1)(y + 1)(y - x)^2$, and $y^2 + yx + y + x + 1 = x^2 + yx + x + y = (x + 1)(y + x)$. Therefore,

$$R(x, y) = \frac{(y - 1)(y + 1)(y - x)^2}{(x + 1)(y + x)}$$

   Zeros of $y-1$: The line $y - 1 = 0$ cuts the hyperbola at $P_1 = (\sqrt{2}, 1)$ and $P_2 = (-\sqrt{2}, 1)$. we can take $y - 1$ as a uniformizer at each of these two points, and conclude that P_1 and P_2 are simple zeros of R.

   Zeros of $y+1$: The line $y + 1 = 0$ cuts the hyperbola at $P_3 = (\sqrt{2}, -1)$ and $P_4 = (-\sqrt{2}, -1)$. we can take $y + 1$ as the uniformizer at each of these two points, and colclude that P_3 and P_4 are simple zeros of R.

   Zeros of $x+1$: The line $x+1 = 0$ touches the hyperbola at $P_5 = (-1, 0)$. At this point, the non-tangent line y can be taken as uniformizer. we have

$$R(x, y) = y^{-2}\left[\frac{(y - 1)(y + 1)(y - x)^2(x - 1)}{y + x}\right].$$

   Thus, P_5 is a pole of R with multiplicity two.

   Zeros of $(y-x)^2$: The line $y - x = 0$ does not meet the curve at any finite point. However, it touches the curve at $\mathcal{O}_1 = [1, 1, 0]$, one of its point at infinity. The vertical line $x = \infty$ (or $1/x = 0$) meets but is not tangential to the hyperbola at $\mathcal{O}_1$. Thus, $1/x$ can be taken as a uniformizer at $\mathcal{O}_1$. But

$$R(x, y) = \frac{(y - 1)(y + 1)(y^2 - x^2)^2}{(x + 1)(y + x)^3} = (1/x)^2\left[\frac{\left(\frac{y}{x} - \frac{1}{x}\right)\left(\frac{y}{x} + \frac{1}{x}\right)(-1)^2}{\left(1 + \frac{1}{x}\right)\left(\frac{y}{x} + 1\right)^3}\right]$$

   At $\mathcal{O}_1$, we have $y/x = 1$ and $1/x = 0$. It follows that $\mathcal{O}_1$ is a zero of R with multiplicity two.

Zeros of $y+x$: The only intersection of the line $y+x$ with the hyperbola is at $\mathcal{O}_2$ (the second point at infinity on the curve). We can again take $1/x$ as the uniformizer at $\mathcal{O}_2 = [1,-1,0]$. We write

$$R(x,y) = \frac{(y-1)(y+1)(y-x)^2}{(x+1)(y^2-x^2)} = (1/x)^{-4}\left[\frac{\left(\frac{y}{x}-\frac{1}{x}\right)\left(\frac{y}{x}+\frac{1}{x}\right)\left(\frac{y}{x}-1\right)^3}{\left(1+\frac{1}{x}\right)(-1)}\right]$$

But $y/x = -1$ and $1/x = 0$ at $\mathcal{O}_2$, so $\mathcal{O}_2$ is a pole of R of multiplicity four.

3. Find all the zeros and poles (and their multiplicities) of the rational function x/y on the curve $Y^2 = X^3 - X$ defined over $\mathbb{C}$.

A: For elliptic curves, we prefer to use the explicit formulas given as Eqns. (4.13), (4.14), and (4.15). The given rational function is written as $G(x,y)/H(x,y)$ with $G(x,y) = x$ and $H(x,y) = y$.

Finite zeros of $G(x,y)$: The only zero of x is the special point $P_1 = (0,0)$. We have $e = 1$ and $l = 0$, so the multiplicity of P_1 is $2e = 2$.

Finite zeros of $H(x,y)$: The zeros of y are the special points $P_1 = (0,0)$ and $P_2 = (1,0)$, and $P_3 = (-1,0)$. For each of these points, we have $e = 0$ and $l = 1$, so $\mathrm{ord}_{P_i}(y) = 1$ for $i = 1,2,3$.

Zeros and poles of $R = G/H$: P_1 is a zero of R of multiplicity $2-1 = 1$. P_2 and P_3 are poles of multiplicity one. Moreover, $\mathrm{ord}_{\mathcal{O}}(G) = -2$ and $\mathrm{ord}_{\mathcal{O}}(H) = -3$, so that $\mathrm{ord}_{\mathcal{O}}(R) = -2+3 = 1$, that is, R has a simple zero at $\mathcal{O}$.