Math 445 H.W. #9 Solutions

38. $f(x,y)$ polynomial with degree $\le d$. Set

$$p(t) = (1+t^2)^d f\left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right).$$ Each monomial in f is of the form $ax^m y^n$ with $m+n \le d$. Then

$$(1+t^2)^d a\left(\frac{2t}{1+t^2}\right)^m\left(\frac{1-t^2}{1+t^2}\right)^n = a(2t)^m(1-t^2)^n(1+t^2)^{d-(m+n)}$$

has degree $m+2n+2(d-(m+n)) = 2d-m \le 2d$.

So $p(t)$ is a sum of polynomials of degree $\le 2d$, so is itself a polynomial of degree $\le 2d$.

Since $$\left(\frac{2t}{1+t^2}\right)^2+\left(\frac{1-t^2}{1+t^2}\right)^2 = \frac{4t^2+1+t^4-2t^2}{(1+t^2)^2} = \frac{1+2t^2+t^4}{(1+t^2)^2} = \frac{(1+t^2)^2}{(1+t^2)^2} = 1,$$

the points $\left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$ lie on the unit circle $x^2+y^2=1$.

Also, since $(1+t^2)^d \ge 1^d = 1$ for all t,

$$p(t)=0 \iff f\left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)=0.$$ So if $C_f(\mathbb{R})$ meets the unit circle in more than $2d$ points, then there are more than $2d$ values of t for which $p(t)=0$ [Note that there is one point of the unit circle, $(0,-1)$, which does not correspond to any t ($1-t^2=-(1+t^2) \Rightarrow 1=-1$.), but if $(0,-1)\in C_f(\mathbb{R})$, then $p(t)/(1+t^2)^d \to 0$ as $t\to\infty$, so the degree of $p(t)$ is $\le 2d-1$.]

$$\overset{\displaystyle f\left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)}{\shortparallel}$$

Note: all other points on the unit circle is equal to $\left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$, for some (unique) value of t.

So if $(0,-1) \notin G_f(\mathbb{R})$ then $p(t)$ has degree $\le 2d$ and is zero for $> 2d$ values of t. If $(0,-1) \in G_f(\mathbb{R})$ then $p(t)$ has degree $\le 2d-1$ and is zero for $> 2d-1$ values of t. In either case $p(t)$ has more roots than its degree, so $p(t)=0$ for every value of t, so $f(x,y)=0$ for every (x,y) on the unit circle (other than $(0,-1)$ }, which must also take the value 0, by continuity of f ...).

So the unit circle is contained in $G_f(\mathbb{R})$.

39. If $y^2 = ax^3+bx^2+cx+d = p(x)$ has a double point A, then $A=(r,0)$, where $r=$ a double root of $p(x)$.

$f(x,y) = y^2 - p(x)$ has a double point at $(x_0,y_0) \Longleftrightarrow$

$f(x_0,y_0)=0$ and $\nabla f(x_0,y_0) = (-p'(x_0), 2y_0) = (0,0)$.

But $2y_0=0 \Rightarrow y_0=0$, so $f(x_0,y_0)=0=0-p(x_0)$, so $p(x_0)=0$. And $-p'(x_0)=0 \Rightarrow p'(x_0)=0$. So x_0 is a double root of $p(x)$, and $y_0=0$. So $(x_0,y_0)=(x_0,0)$, with x_0 a double root of $p(x)$. ///

40. $y^2 = x^3 - 4x^2 - 3x + 18$ has a double ~~root~~ point.

By problem #39, such a point comes from a double root of $p(x) = x^3 - 4x^2 - 3x + 18$. But $p(-2) = -8 - 16 + 6 + 18 = 0$ so $(x+2) | p(x)$; $p(x) = (x+2)(x^2 - 6x + 9) = (x+2)(x-3)^2$.

So $(3,0)$ is a double point of the curve. It is also a rational point; so every line with rational slope through $(3,0)$ will hit the curve $G_f(\mathbb{R})$, $f(x,y) = y^2 - (x^3 - 4x^2 - 3x + 18)$ in another rational point (and conversely; rational points lie on lines with rational slope through $(3,0)$). So we compute: if $y = m(x-3)$, then

$$0 = f(x,y) = (m(x-3))^2 - (x^3 - 4x^2 - 3x + 18)$$

$$= m^2(x-3)^2 - (x+2)(x-3)^2 = (x-3)^2(m^2 - (x+2))$$

$\Longleftrightarrow$ $x = 3$ or $m^2 - (x+2) = 0$, i.e. $x = m^2 - 2$.

Then $y = m(x-3) = m((m^2-2)-3) = m^3 - 5m$.

So the rational points of $G_f(\mathbb{R})$ consists of the points (m^2-2, m^3-5m) for $m \in \mathbb{Q}$, and $(3,0)$ (which does not correspond to a rational value of m).

HW9D

41. If $A \neq B$ lie on the elliptic curve $C_f(\mathbb{R})$, and the line through A & B is tangent to $C_f(\mathbb{R})$ at B, then $A+2B = \underline{O}\underline{O}$.

Since the line L through A & B is tangent at B, A lies on the tangent line at B, so $BB = A$, & $AB = B$.

Then $A+2B = A+B+B = A+(B+B) = A+(\underline{O}(BB)) = A+(\underline{O}A)$
$= \underline{O}(A(\underline{O}A))$.

But $A(\underline{O}A) = \underline{O}$, since $A(\underline{O}) = A\underline{O} = \underline{O}A$ (ie., the points A, $\underline{O}$ and $\underline{O}A$ all lie on a line).

So $A+2B = \underline{O}(A(\underline{O}A)) = \underline{O}(\underline{O}) = \underline{O}\underline{O}$. //

42. The cubic curve $axy = (x+1)(y+1)(x+y+b)$ has 3 points at infinity.

To find points at infinity, we projectivize the equation ~~aXYZ = (X~~

$$Z^3\left(a\left(\frac{X}{Z}\right)\left(\frac{Y}{Z}\right)\right) = Z^3\left(\frac{X}{Z}+1\right)\left(\frac{Y}{Z}+1\right)\left(\frac{X}{Z}+\frac{Y}{Z}+b\right), \text{ ie.}$$

$aXYZ = (X+Z)(Y+Z)(X+Y+bZ)$. To find points at infinity, we set $Z=0$ and solve.

H9E

$$0 = (X+0)(Y+0)(X+Y+0) = XY(X+Y)$$, i.e.

$X=0$ ($\longleftrightarrow$ $0:1:0$) or $Y=0$ ($\longleftrightarrow$ $1:0:0$) or

$X+Y=0$ ($\longleftrightarrow$ $1:-1:0$)

So the points at infinity on $G_f(\mathbb{R})$, ~~f(x,y)=axy-(~~

$f(x,y) = axy - (x+1)(y+1)(x+y+b)$ are

$0:1:0$ ($\longleftrightarrow$ vertical lines $x=$ constant),
$1:0:0$ ($\longleftrightarrow$ horizontal lines $y=$ constant), and
$1:-1:0$ ($\longleftrightarrow$ lines $x+y=$ constant). ///