More rational points on curves

When we studied equations like $X^2+Y^2=5Z^2$, we took the approach of looking for rational solutions to $\left(\frac{X}{Z}\right)^2+\left(\frac{Y}{Z}\right)^2=5$. Our geometric method for solving this was to start with one rational solution (a,b) to ~~$X^2+Y^2=5Z^2$~~ $x^2+y^2=5$. Any other rational solution (α,β) will define, with (a,b), a line with rational slope through (a,b) $y=r(x-a)+b$. Plugging in,

$$x^2+(r(x-a)+b)^2=5$$ has one solution $x=a$; because the equation has degree 2, it then also has another, real solution, which must then be rational!

All of this can be generalized to equations of higher degree

Let $f(x,y)=0$ be a polynomial with (total) degree d

e.g. $f(x,y)=x^3y+3x^2-y^2-7$ has degree $\underline{\underline{4}}$.

We denote $C_f(\mathbb{R})=\{(x,y)\in\mathbb{R}^2 : f(x,y)=0\}$; typically a curve in $\mathbb{R}^2$.

A generic line L in $\mathbb{R}^2$ has the form $ax+by+c=0$ (a or $b\neq 0$); which we usually write $y=mx+r$ (if not vertical ($x=r$))

A point lying both on L and $C_f(\mathbb{R})$ must satisfy $f(x,y)=0$ and $y=mx+r$ (or $x=r$); plugging in, x satisfies

$p(x) = f(x,mx+r)=0$. This is a polynomial of degree d, so the Fund. Thm. of Algebra implies that p has at most

FIX ME?

d (complex) roots, unless $p(x) \equiv 0$.

If $p(x) \equiv 0$ then $y = mx + r \Rightarrow f(x,y) = 0$ ie. every point on L lies in $C_f(\mathbb{R})$. Even more is true: if $p(x) \equiv 0$, then $f(x,y) = (y-(mx+r))\, q(x,y)$. To see this, set $u = y-(mx+r)$ and write $f(x,y) = f(x, u+(mx+r))$; then write as a polynomial in u with coefficients being polynomials in x.

$$f(x, u+(mx+r)) = f_0(x) + f_1(x)u + \cdots + f_n(x)u^n.$$

Setting $u=0$, $\underset{\overset{|||}{0}}{f(x, 0+(mx+r))} = f_0(x) + 0 + \cdots + 0$

So $f_0(x) = 0$, so $f(x, u+(mx+r)) = u\big(f_1(x) + f_2(x)u + \cdots + f_n(x)u^{n-1}\big)$

But $u = y-(mx+r)$, so $f(x,y) = (y-(mx+r))(\text{ blah })$

note: the coeffs of blah come from the coeffs of f, m, and r

This gives:

Thm: If $f(x,y)$ has degree d, and if the line L defined by $y = mx+r$ meets $f(x,y)=0$ in more than d points then $f(x, mx+r) \equiv 0$, and so $f(x,y) = (y-(mx+r))\,k(x,y)$ for some polynomial k. If the coeffs of f, m, and r are all rational (resp integers), then the coeffs of k are rational (resp, integers).

Fri

This can be refined by introducing the notion of the multiplicity of a root of $f(x,y)=0$. This is analogous to the one variable case:

$x=1$ is a multiple root of $f(x) = x^3 - 2x^2 + x = 0$, because $f(1) = 0$ and $f'(1) = 3x^2 - 4x + 1\big|_{x=1} = 0$ as well.

(horizontal tangent). The analogue for $f(x,y)=0$ is

$f(a,b)=0$, $\frac{\partial}{\partial x} f(a,b)=0$ and $\frac{\partial}{\partial y} f(a,b)=0$ (horizontal tangent')

~~B~~ More generally, the multiplicity of a solution to $f(x,y)=0$ is the largest M so that $f(a,b)=0$ and $\left(\frac{\partial}{\partial x}\right)^i\left(\frac{\partial}{\partial y}\right)^j f(a,b)=0$ for all $i+j\leq M$.

Then the count of the # of roots of $f(x,y)=0$ lying on L includes multiplicity, and the result is ~~true~~ still true.

A curve $C_f(\mathbb{R})$ with no points of multiplicity >1 on it is called smooth. A point of mult 2 is called a double point, etc.

Now, our approach to ~~the~~ solving $x^2+y^2=5$ with $x,y\in\mathbb{Q}$ - Start with $(x_0,y_0)\in\mathbb{Q}^2$ a solution and plug in $y=r(x-x_0)+y_0$, $r\in\mathbb{Q}$ can be applied to cubic curves as well.

The idea now is that if $(x_0,y_0),(x_1,y_1)\in C_f(\mathbb{R})$ are rational solutions with f having rational coeffs then taking the line L through them, $y=mx+r$, the equation $f(x,mx+r)=0$ has roots x_1,x_2 allowing use to factor $x-x_1$, $x-x_2$ out of the cubic polynomial $f(x,mx+r)$ giving a third linear factor and a third root, x_2.

If f has rational coeffs ~~and~~ and $(x_0,y_0),(x_1,y_1)\in\mathbb{Q}^2$, then $(x_2,mx_2+r)\in\mathbb{Q}^2$ is a new rational solution.

If the cubic curve has a double point P with rational coordinates, then it acts like a double root of $f(x, mx+r)$ for any line with rational slope through P, so the other point of intersection (there will be only one) is also a rational point.

Ex: To detect double points, try to find simultaneous solutions to $f(x,y)=0$, $\frac{\partial f}{\partial x}(x,y)=0$, $\frac{\partial f}{\partial y}(x,y)=0$

Ex: $y^2 = x^3 - 2x^2$, i.e. $y^2 - x^3 + 2x^2 = 0$

$\frac{\partial f}{\partial x} = -3x^2 + 4x = 0$ for $x = 0$

$\frac{\partial f}{\partial y} = 2y = 0$ for $y = 0$ and $(0,0) \in C_f(\mathbb{R})$, so $(0,0)$ is a double point

Then $y = mx$ will intersect

$y^2 = x^3 - 3xy$ $\qquad y^2 - x^3 + 3xy = 0$

$f_x = -3x^2 + 3y = 0 \quad y = \frac{3}{2}x^2 \qquad \frac{3}{2}x^2 + \frac{3}{2}x = 0 \qquad x = 0$

$f_y = 2y + 3x = 0 \quad y = -\frac{3}{2}x \qquad x = -3/2$

Ex $y^2 = x^3 - 2xy - 5x + 3 \qquad y^2 - x^3 + 2xy + 5x - 3 = 0$

$f_x = -3x^2 + 2y + 5 = 0 \quad \rightarrow \quad -3x^2 - 2x + 5 = 0$

$f_y = 2y + 2x = 0 \rightarrow y = -x \qquad -(3x+5)(x-1) = 0$

$x = 5/3, y = -5/3$ nope $\qquad x = 1, y = -1$

$1 = 1 + 2 - 5 + 3$ ✓

$(1,-1)$ is a double point.

Multiple Roots

$$p(x) = (x-a)\,q(x) \iff p(a)=0$$

$$p'(x) = (x-a)\,r(x) \iff p'(a)=0.$$

$$p'(x) = (x-a)\,q'(x) + q(x) = (x-a)\,r(x)$$

$$\Longrightarrow q(x) = (x-a)\big(r(x) - q'(x)\big)$$

$$\Longrightarrow p(x) = (x-a)^2\,(\quad)$$

$$L(x) = (x,\ y_0 + r(x-x_0))$$

$$L(t) = A + vt = (x(t), y(t))$$

$$0 = f(x_0, y_0) = f(x_0, L(x_0))$$

$$f(L(t)) = f(x(t), y(t))$$

$$\frac{d}{dx} f(x, L(x)) = f_x(x, L(x)) + f_y(x, L(x)) \cdot L'(x)$$

$$f_y(x_0, L(x_0)) \cdot L'(x_0)$$

$$f'(x_0, L(x_0)) = f_x(x_0, L(x_0)) + $$

$$= (f_x, f_y) \cdot (1, L'(x_0))$$

$$\cdot \left(1, \frac{\Delta y}{\Delta x}\right)$$

$$= \frac{1}{\Delta x}(f_x, f_y)\cdot(\Delta x, \Delta y) = 0.$$

Tangents

$$a, b \in \mathbb{Q} \qquad f(a,b) = 0$$

$f(x,y) =$ cubic poly with rational coeffs.

Then $\nabla f(a,b) = (\alpha, \beta) \in \mathbb{Q}^2$.

$$L: \quad (\alpha, \beta) \cdot (x-a, y-b) = 0 \qquad \overset{L(x)}{\cancel{y}} = mx + d$$

Then $\left.\frac{d}{dx}\left(f(x, y(x)) \right)\right|_{x=a} = \underline{\underline{0}}$

$$\left[f(x, y(x)) \right]' = \frac{\partial f}{\partial x}(x, y(x)) + \frac{\partial f}{\partial y}(x, y(x)) \cdot y'(x)$$

$$\Big|_{x=a} = \alpha + \beta\left(-\frac{\alpha}{\beta} \right) = \underline{\underline{0}}.$$

$\Longrightarrow$ $x = a$ is a double root of $f(x, L(x))$!

$$1 = 1 - 3 + 3$$

$$y^2 = x^3 - 3x^2 + 3$$

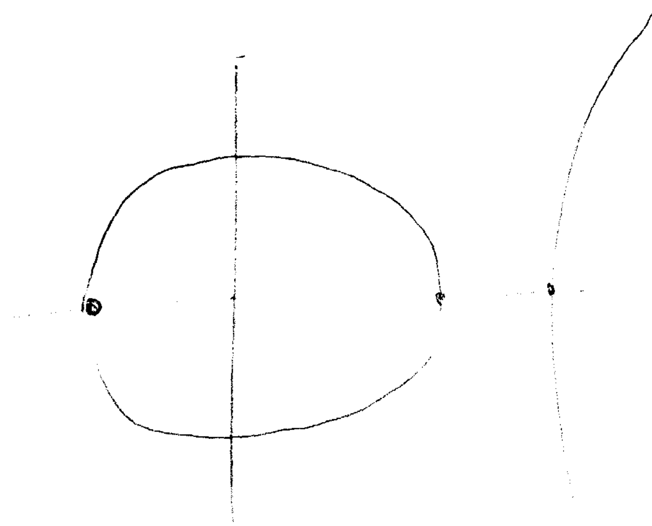
$(1,1)$ $\qquad y^2 - x^3 + 3x^2 - 3 = 0$

$$\nabla f = (-3x^2 + 6x, 2y)$$

$(3,2)$

$$3(x-1) + 2(y-1) = 0$$

$\cancel{y = \frac{2}{2}}$ $\qquad 2y = -3x + 5$



$$(2y)^2 = 4x^3 - 12x^2 + 12$$

$$(-3x+5)^2 = 4x^3 - 12x^2 + 12$$

$$4x^3 - 21x^2 + 30x - 13 = 0$$

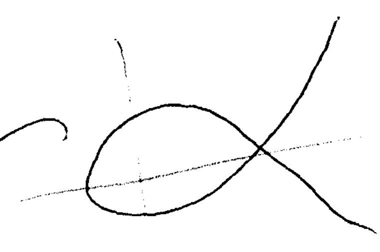
$$(x-1)(4x^2 - 17x + 13) = 0$$

$$(x-1)(x-1)(4x-13) = 0$$

$$\boxed{x = \frac{13}{4},\ y = \frac{-19}{8}}$$

<u>Repeat!</u>

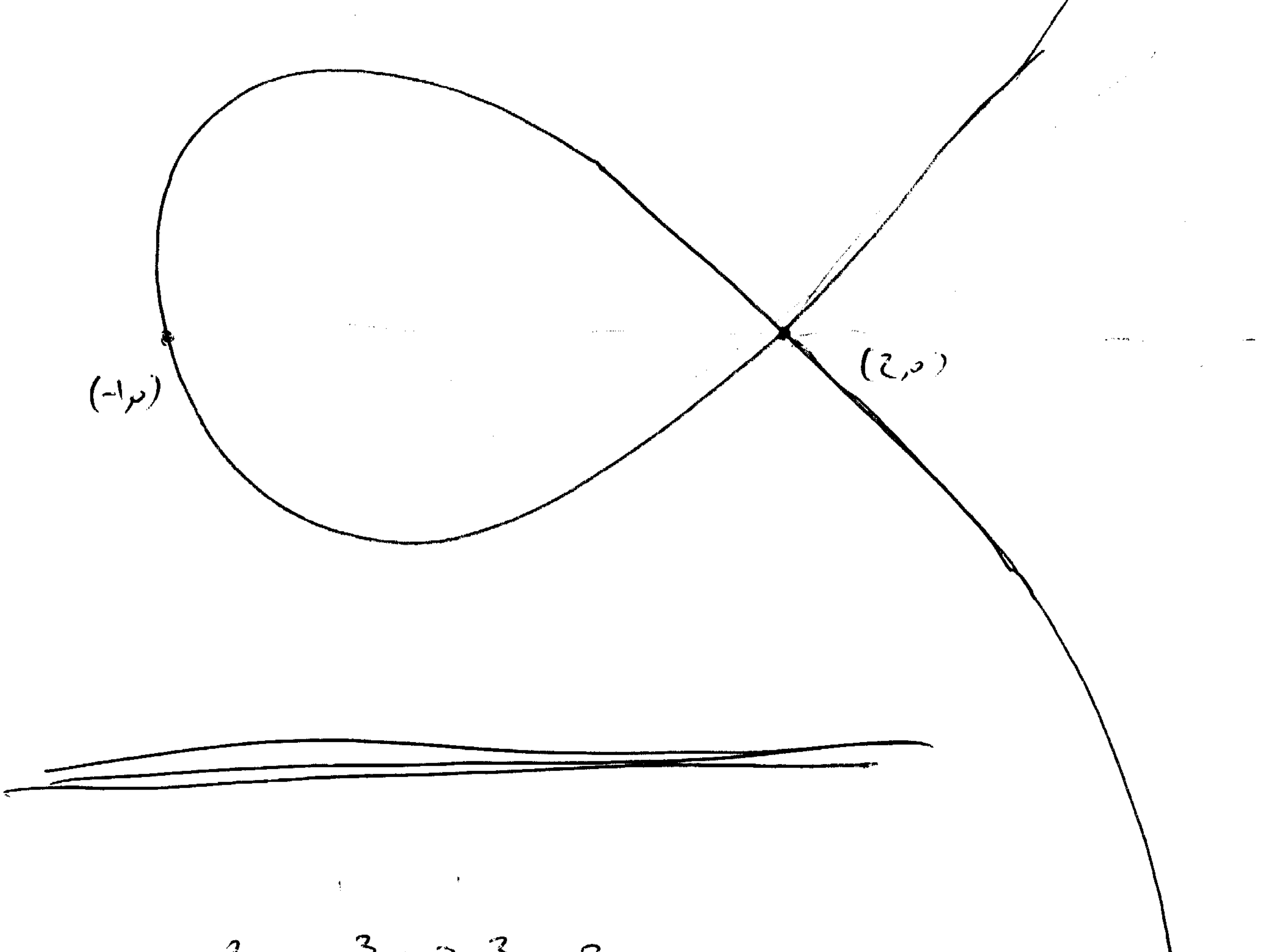
$$\frac{17809}{5776},\ \frac{-834783}{438976}$$



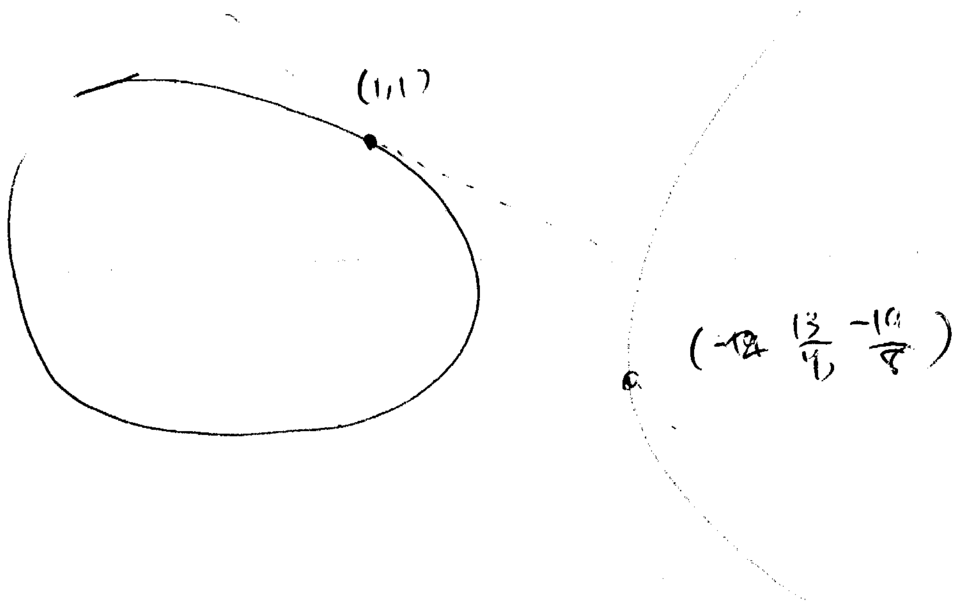
$$y^2 = (x+1)(x-2)^2$$

$$y^2 = (x+1)(x^2 - 4x + 4) = x^3 - 3x^2 + 4$$

$y^2 = x^3 - 3x^2 + 4 = (x+1)(x-2)^2$



$y^2 = x^3 - 3x^2 + 3$



$P = (a,b) \qquad a^3+b^3=9$

$f(x,y) = x^3+y^3$

$f_x = 3x^2 \quad f_y = 3y^2$

Tangent line: $(3a^2, 3b^2)\cdot(x-a, y-b) = 0$

$a^2(x-a) + b^2(y-b) = 0$

$b^2y = -a^2(x-a) + b^3$

$b^6x^3 + (b^3 - a^2(x-a))^3 = 9b^6$

$b^6x^3 + b^9 - 3b^6a^2(x-a) + 3b^3a^4(x-a)^2 - a^6(x-a)^3 - 9b^6 = 0$

$(x-a)^2(-a^6(x-a) + 3b^3a^4 + b^6(x+2a)) \neq 0$

$b^6(b^3-9)$

$b^6x^3 + (b^9 - 9b^6) - 3b^6a^2(x-a)$

$= b^6x^3 - b^6a^3 - 3b^6a^2(x-a)$

$x^3 - a^3 - 3a^2(x-a)$

$(x-a)(x^2+ax+a^2-3a^2)$

$(x-a)(x^2+ax-3a^2)$

$(x-a)(x-a)(x+2a)$

$y = a, a$ or

$x(b^6 - a^6) + (a^7 + 3b^3a^4 + 2ab^6) = 0$

$x(b^3+a^3)(b^3-a^3) + a(a^6 + 3a^3b^3 + 2b^6)$

$x(9(b^3-a^3)) + a(a^3+b^3)(a^3+2b^3)$

$x(9(b^3-a^3) + 9a(9+b^3) = 0$

$$x = \frac{-9a(9+b^3)}{9(b^3-a^3)} = \frac{a(9+b^3)}{b^3-a^3}$$

$$y = \frac{1}{b^2}\left(-a^2\left(\frac{a(9+b^3)}{b^3-a^3} \cancel{8} - a\right) + b^3\right)$$

$$= \frac{1}{b^2}\left(-a^3\left(\frac{9+a^3}{b^3-a^3}\right) + b^3\right)$$

$$= \frac{1}{b^3}\left(\frac{-9a^3 + a^6 + b^6 - b^3a^3}{\cancel{9}}\right) \ldots\ldots$$

(ωxαt , $m > 0$)

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

$\Rightarrow x+y=A \quad x^2-xy+y^2=B \qquad AB=m$

$\Rightarrow m \geq |B| = |x^2-xy+y^2| = \frac{3}{4}x^2+(y-\frac{1}{2}x)^2 \geq \frac{3}{4}x^2$

$\Rightarrow |x| \leq (\frac{4}{3}m)^{1/2}$

$\Rightarrow$

$x^3+y^3 \qquad (\frac{x}{z})^3+(\frac{y}{z})^3=m$

$x^3+y^3=mz^3$

$(\frac{y}{z})^3$

$\frac{1}{8}$

For $1 \leq m \leq 1728$: at most one solution

1^3+

$$\boxed{u^3+v^3=\alpha}$$

Set $x=\frac{12\alpha}{u+v} \qquad y=36\alpha\frac{u-v}{u+v}$

$u=\frac{36\alpha+y}{6x} \qquad v=\frac{36\alpha-y}{6x}$

$u=x+y$
$v=x-y$

$(36\alpha+y)^3+(36\alpha-y)^3=(6x)^3\alpha$

$2(36)^3\alpha^3+2\cdot3\cdot36\alpha y^2=6\cdot36x^3\alpha$

$1, 8, 27, 64, \overset{125}{\cancel{81}}, 216, 343$ $\quad \sqrt{\frac{4}{3} 43} = \sqrt{\frac{172}{3}} < \sqrt{58} < 8$

$x^3 + y^3 = m$

Need $\frac{a^3}{8} \equiv 7$

$\left(\frac{1}{2}\right)^3 + \left(\frac{a}{2}\right)^3 = \frac{a^3+1}{8}$

$\left(\frac{1}{2}\right)^3 + \left(\frac{7}{2}\right)^3 = \frac{344}{8} = \underline{\underline{43}}$

$\frac{344}{8}$

$\left(\frac{1}{3}\right)^3 + \left(\frac{a}{3}\right)^3 = \frac{a^3+1}{27}$

x	x^2	x^3
0	0	0
1	1	1
2	4	8
3	1	3
4	0	0
5	1	5
6	4	0
7	1	$\underline{\underline{7}}$

x

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14