Factoring bivariate polynomials

$\mathbb{F}[X,Y]$, Fix $\mathbb{F} = \mathbb{F}_q$ for the remainder

Given $Q(X,Y) \in \mathbb{F}[X,Y]$, we want to factor it into irreducibles over $\mathbb{F}[X,Y]$.

Ideal runtime = $\begin{cases} \text{poly}(d, \log|\mathbb{F}|) & \text{if } \mathbb{F} \text{ finite} \\ \text{poly}(d, t) & \text{if } \mathbb{F} = \mathbb{Q}, \text{ each coeff is a } t\text{-bit integer} \end{cases}$

Idea 1

$$\mathbb{F}[X,Y] = (\mathbb{F}[X])[Y]$$

$\mathbb{F}[X]$ like $\mathbb{Z}$

$\subseteq (\mathbb{F}(X))[Y]$

$\mathbb{F}(X)$ like $\mathbb{Q}$.

$\subseteq (\mathbb{F}[[X]])[Y]$

$\mathbb{F}[[X]]$ like $\mathbb{R}/\mathbb{Q}$.

Idea 2 Find "approximate roots" of

$Q_*(Y) \in (\mathbb{F}[[X]])[Y]$

and then recover the minimal poly of the approximate root.

More concretely

For $Q(X,Y)$, try to find power series $u(X)$ s.t.

$$Q(X, u(X)) = 0.$$

Then find $H(X,Y) \in \mathbb{F}[X,Y]$ with low degree s.t.

$$H(X, u(X)) \approx 0$$

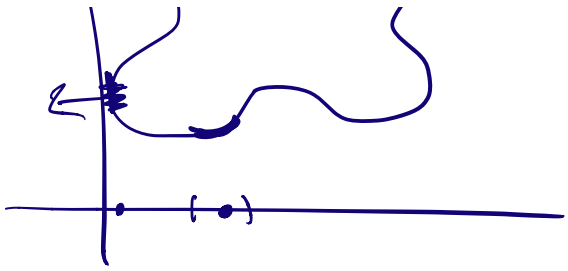
$\uparrow$

$X^{\text{high power}}$ divides

$H(X, u(X))$

Implicit Function Thm

$F(X,Y) = 0$. F is C^∞, then for any (x,y)



At any (x,y) s.t. $\frac{\partial F}{\partial y}(x,y) \neq 0$.

$\exists$ g : Nbd of x $\to$ $\mathbb{R}$ s.t.

$F(x, g(x)) = 0$.

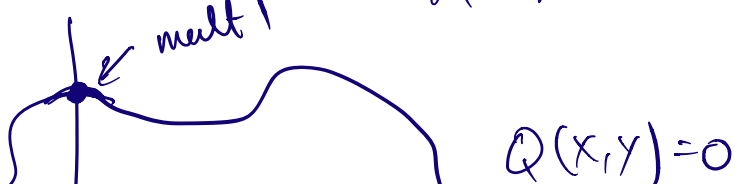
$g \in C^\infty$.

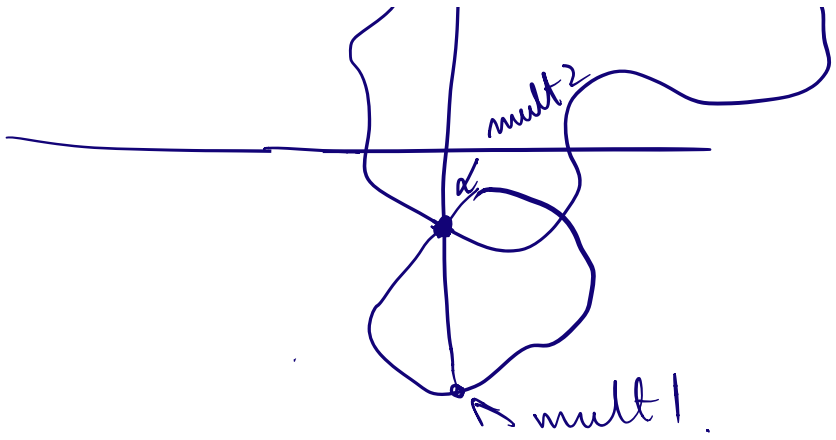
Goal Find a power series $u(X)$ s.t.

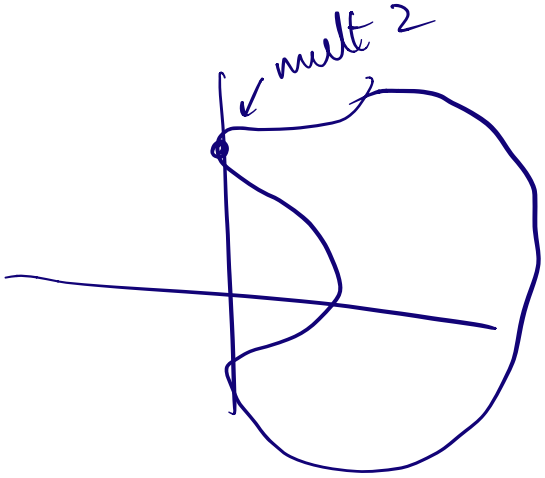
$Q(X, u(X)) = 0$.

Assumption $\begin{cases} Q(0,\alpha) = 0 & \text{for some } \alpha \in \mathbb{F} \\ \frac{\partial Q}{\partial Y}(0,\alpha) \neq 0. \end{cases}$

$\Leftrightarrow$ $Q(0,Y)$ has a multiplicity one root at $Y = \alpha$.







We know $Q(0, \alpha) = 0$.

Let us find $a_0, a_1, \ldots a_t, \ldots$ s.t.

$$Q(X, a_0 + a_1 X + \cdots + a_t X^t) = 0 \pmod{X^{t+1}}$$

$\forall t$.

$\rightsquigarrow$ For $t = 0$, can take $a_0 = \alpha$.

$$Q(X, a_0) = Q(0, \alpha) \pmod{X}$$

$= 0 \pmod{Y}$.

- For general t, suppose we have

$r(X) = a_0 + a_1 X + \cdots + a_{t-1} X^{t-1}$ s.t.

$$Q(X, r(X)) = 0 \pmod{X^t}$$

Let us find a_t s.t.

$$Q(X, r(X) + a_t X^t) = 0 \pmod{X^{t+1}}$$

$$\| $$

$$Q(X, r(X)) + \frac{\partial Q}{\partial Y}(X, r(X)) \cdot a_t X^t + m(a_t X^t)^2 + m(a_t X^t)^3 + \cdots$$

Aside on Taylor series

$Q(Y)$ is a polynomial in Y.

$Q(Y + H) =$ some poly in Y, H

$= Q^{(0)}(Y) + H \cdot Q^{(1)}(Y) + H^2 Q^{(2)}(Y) +$

$$\ldots$$

$$+ H^d Q^{(d)}(Y)$$

$Q^{(i)}(Y) \triangleq$ i^{th} Hasse derivative

$$\left(= \frac{\text{usual } i^{th} \text{ derivative}}{i!} \right.$$

when $i <$ characteristic)

$Q^{(0)}(Y) = Q(Y)$ always

$Q^{(1)}(Y) = \frac{\partial Q}{\partial Y}(Y)$ always

So want a_t s.t.

$$Q(X, n(X)) + a_t \cdot \boxed{\frac{\partial Q}{\partial Y}(X, n(X)) \cdot X^t} \equiv 0 \pmod{X^{t+1}}$$

$$\lambda X^t \pmod{X^{t+1}}$$

$$a_t \cdot \left(\text{const term of } \frac{\partial Q}{\partial Y}(X, \eta(X)) \right) \cdot X^t$$

$$\| $$

$$a_t \cdot \frac{\partial Q}{\partial Y}(0, \alpha) \cdot X^t.$$

$\frac{\partial Q}{\partial Y}(0,\alpha) \in \mathbb{F}$

Want a_t s.t.

$$\left(\lambda + a_t \cdot \frac{\partial Q}{\partial Y}(0, \alpha) \right) = 0$$

linear eqn in $\mathbb{F}$.

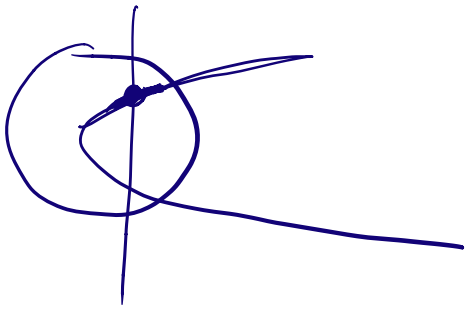
$\neq 0$

Such a_t always exists!

So $\exists$ solution $u(X) \in \mathbb{F}[[X]]$.

"Hensel lifting".

$$Q(x,y) = \left(x^2+y^2-10\right)\left(y^2-(x+1)\right)$$



$$Q(0,y) = \left(y^2-10\right)\left(y^2-1\right)$$

$$= \left(y-\sqrt{10}\right)\left(y+\sqrt{10}\right)\left(y-1\right)\left(y+1\right)$$

Take $\alpha = 1$

Lifting $(0,1)$ to get a power series

$u(x) = 1 + ax + \cdots$

s.t. $Q(x, u(x)) = 0$

we will get.

$1 + \frac{1}{2}\cdot x + \cdots\cdots$

taylor series for

$\sqrt{1+x}$.

This has nothing to do

with X^2+Y^2-10.

Final piece is recognizing smallest $H(X,Y)$ s.t. $H(X, u(X)) = 0$

where H is low degree and we only have some finite # of coeffs of $u(X)$.

Whole algorithm

1. Take $GCD\left(Q(X,Y), \frac{\partial Q}{\partial Y}(X,Y)\right)$ over $\mathbb{F}(X)$.
   (field)

   Use this to remove repeated factors that have positive Y-degree.

2. Want $Q(0,Y)$ to have a multiplicity one root.

   Claim For all but $O(d^2)$ values of $x \in \mathbb{F}$,

$Q(x,y)$ has no repeated roots.

(using the fact that $Q(X,Y)$ has no repeated factors with positive Y-degree)

A polynomial

$$B(Y) = b_0 + b_1 Y + \cdots + b_d Y^d$$

(*) ... has repeated roots or is degree $< d$ iff

$$\operatorname{disc}(B) = \begin{bmatrix} b_0 & \cdots & b_d & 0 & 0 & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_d & 0 & 0 & \cdots & 0 \\ & & \ddots & & & & & \\ 0 & \cdots & 0 & b_0 & \cdots & & b_d & \\ b_1 & 2b_2 & 3b_3 & \cdots & db_d & 0 & \cdots & 0 \end{bmatrix}$$

is singular.

$$Q(X,Y) = B(Y) = b_0(X) + b_1(X)\cdot Y + \cdots + b_d(X) Y^d$$

$\mathrm{disc}(B) =$ [matrix with $\mathbb{F}[X]$ entries.]

$\mathrm{disc}(B)(x) = 0$ iff

$Q(x, Y)$ has repeated roots

or has degree $< d$.

But $\mathrm{disc}(B)(X) \neq 0$ of degree $\leq d^2$.

$\Downarrow$

we got rid of repeated factors (applying $\circledast$ over $\mathbb{F}(X)$)

$\Rightarrow$ $Q(x, Y)$ has no repeated roots except for $O(d^2)$ values of $x \in \bar{\mathbb{F}}$.

3. Replace $Q(X, Y)$ with

$Q(X + x \cdot Y)$ for random x

4. Find a root α of $Q(0, Y)$.

5. Do Hensel lifting to find

$$\tilde{u}(X) = \alpha + a_1 X + \cdots + a_t X^t$$

s.t. $Q(X, \tilde{u}(X)) \equiv 0 \pmod{X^{t+1}}$

for $t = \text{poly}(d) \left(= \Omega(d^2)\right)$

6. Try to Find $H(X, Y)$ of degree $\leq (d, d^*)$ (in X, in Y)

For $d^* = 1, 2, \ldots d-1$,

s.t. $H(X, \tilde{u}(X)) = 0 \pmod{X^{t+1}}$.

[SYSTEM OF LINEAR EQNS over $\mathbb{F}$]

$u(X) - \tilde{u}(X) \mid H(X, u(X)) - H(X, \tilde{u}(X))$

X^{t+1} divides this $\rightarrow 0$

So X^{t+1} divides $H(X, \tilde{u}(X))$.

If we found such an $H(X, Y)$,

want to claim: $H(X,Y) \mid Q(X,Y)$

Resultant (H, Q) viewed as polynomials in Y, coeffs in $\mathbb{F}(X)$.

$\leq O(d)$ [$\mathbb{F}[X]$ entries] $O(d)$

each coeff deg $\leq d$.

So $\det(\mathrm{Res}(H,Q))$ is a poly in X of degree $O(d^2)$.

$$\mathrm{Res}(H,Q) = \prod_{\substack{\alpha \text{ root of } H \\ \beta \text{ root of } Q}} (\alpha - \beta)$$ ✓

For (β) = $u(X)$

(α) = whichever power series solution of H we get from Hensel lifting

α, must equal

$\tilde{u}(x) \equiv u(x) \mod x^{t+1}$.

$(\alpha - \beta)$ is divisible by x^{t+1}.

So if $t > O(d^2)$, the RHS is divisible by $x^{\Omega(d^2)}$

but LHS has deg $< d^2$

So LHS is 0.

$\Rightarrow \text{Res}(H, Q) = 0$

$\Rightarrow$ H, Q have a common factor.