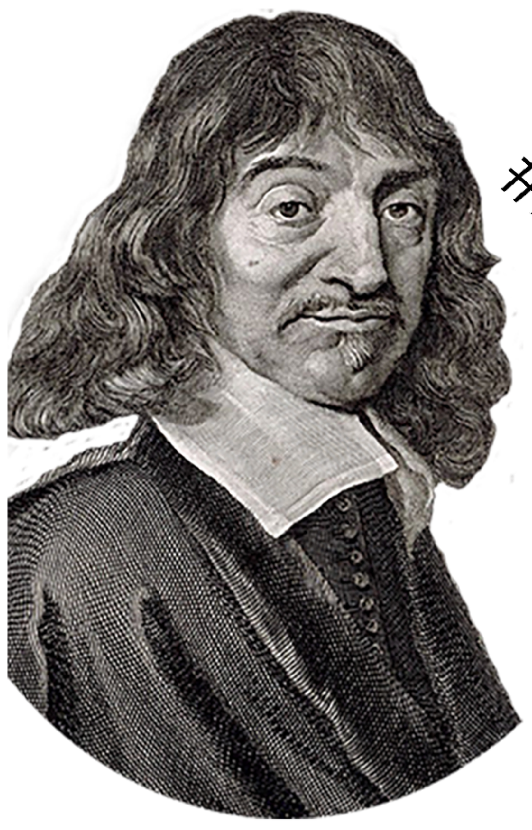
# A $p$-adic Descartes solver: the Strassmann solver


UTSA The University of Texas at San Antonio™

**Josué Tonelli-Cueto**
The University of Texas at San Antonio
josue.tonelli.cueto@bizkaia.eu

UTSA DEPARTMENT OF MATHEMATICS


## Descartes's Rule of Signs



$$\#\mathcal{Z}(f,\mathbb{R}_+)\leq \mathrm{V}(f)$$

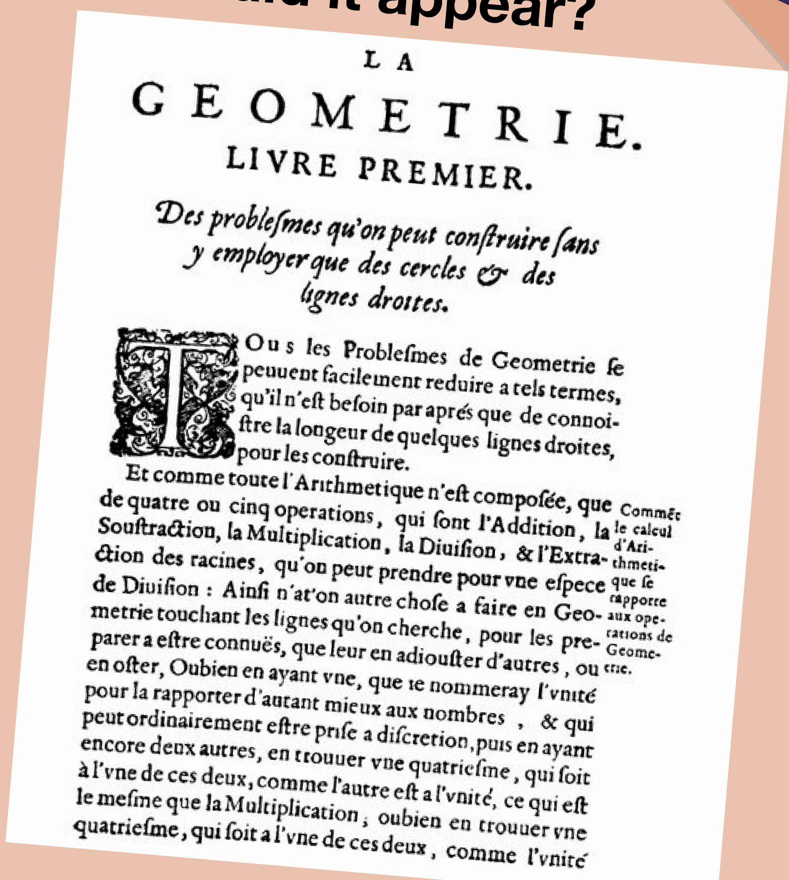
**Theorem**

Let $f=\sum_k f_k\mathrm{T}^k\in\mathbb{R}[\mathrm{T}]$ be an univariate polynomial and let $\mathrm{V}(f)$ be the number of sign changes in the sequence $f_0,f_1,f_2,\dots$ (with zeros omitted). Then

$$\#\mathcal{Z}(f,\mathbb{R}_+)\leq \mathrm{V}(f)$$

where $\mathcal{Z}(f,\mathbb{R}_+)$ is the set of positive zeros.

**Where did it appear?**



LA
GEOMETRIE.
LIVRE PREMIER.

*Des problesmes qu'on peut construire sans y employer que des cercles & des lignes droites.*

TOus les Problesmes de Geometrie se peuuent facilement reduire a tels termes, qu'il n'est besoin par aprés que de connoistre la longeur de quelques lignes droites, pour les construire.

Et comme toute l'Arithmetique n'est composée, que de quatre ou cinq operations, qui sont l'Addition, la Soustraction, la Multiplication, la Diuision, & l'Extraction des racines, qu'on peut prendre pour vne espece de Diuision : Ainsi n'a'on autre chose a faire en Geometrie touchant les lignes qu'on cherche, pour les preparer a estre connuës, que leur en adiouster d'autres, ou en oster, Oubien en ayant vne, que ie nommeray l'vnité pour la rapporter d'autant mieux aux nombres , & qui peut ordinairement estre prise a discretion, puis en ayant encore deux autres, en trouuer vne quatriesme, qui soit à l'vne de ces deux, comme l'autre est a l'vnité, ce qui est le mesme que la Multiplication ; oubien en trouuer vne quatriesme, qui soit a l'vne de ces deux , comme l'vnité

Commēt le calcul d'Arithmetique se rapporte aux operations de Geometrie.

It appear in the three-volume appendix *La Geometrie* to his famous *Discours de la méthode*.

## Descartes Solver

**Input**: $f\in\mathbb{R}[\mathrm{T}]$ & $\mathrm{I}=(a,b)$
**Output**: Isolating intervals for $\mathcal{Z}(f,(a,b))$.
*Routine*:
Subdivide $(a,b)$ into smaller intervals,
until for all obtained intervals J,

$$\mathrm{V}(f,\mathrm{J})\leq 1.$$

**Complexity**

$\mathfrak{f}=\sum_{k=0}^d\mathfrak{f}_k\mathrm{T}^k\in\mathbb{R}[\mathrm{T}]$ random polynomial of degree $d$ with i.i.d. random coefficients uniformly distributed in $[-1,1]$.

**Expected Number of Arithmetic Operations**:

$$\tilde{O}\left(d^2\right)$$

## Strassmann Solver

**Input**: $f\in\mathbb{R}[\mathrm{T}]$ & $\mathrm{B}=x+p^{-s}$
**Output**: Isolating intervals for $\mathcal{Z}(f,\mathrm{B})$.
*Routine*:
Subdivide B into smaller closed balls,
until for all obtained balls $y+p^{-t}\mathbb{Z}_p$,

$$\mathrm{St}(f;y,p^{-t})\leq 1.$$

**An important detail**

To avoid checking $p+1$ balls at each subdivision step, we use the Cantor-Zassenhaus factorization algorithm

**Complexity & Precision**

$\mathfrak{f}=\sum_{k=0}^d\mathfrak{f}_k\mathrm{T}^k\in\mathbb{Z}_p[\mathrm{T}]$ random $p$-adic polynomial of degree $d$ with i.i.d. random coefficients uniformly distributed in $\mathbb{Z}_p$.

**Expected Number of Arithmetic Operation**:

$$O(d^2\log^3 d\log p)$$

If $p\leq\tilde{O}(d)$,

$$\tilde{O}(dp)\leq\tilde{O}(d^2)$$

**Expected Needed Precision**:

$$d+\tilde{O}(1)$$

## Strassmann's Theorem

$$\#\mathcal{Z}(f,\mathbb{Z}_p)\leq \mathrm{St}(f)$$

**Theorem**

Let $f=\sum_k f_k\mathrm{T}^k\in\mathbb{Q}_p[\mathrm{T}]$ be an univariate polynomial and let

$$\mathrm{St}(f)=\max\{k\mid \text{for all } l\leq k,\ |f_l|_p\leq|f_k|_p\}$$

be the so-called *Strassmann index*. Then

$$\#\mathcal{Z}(f,\mathbb{Z}_p)\leq \mathrm{St}(f)$$

where $\mathcal{Z}(f,\mathbb{Z}_p)$ is the set of $p$-adic integer roots.

**Holocaust Victim**


As many others Germans of Jewish origin, Reinhold Strassmann was a Holocaust victim. Today, *Stolpersteins*, as the one above, lie all over Europe indicating the places where Holocaust victims—of Jewish origin or not—used to live.

## Properties

$$\mathrm{V}(f;a,b):=\mathrm{V}\left((\mathrm{T}+1)^{\mathrm{d}(f)}f\left(\frac{a+b\mathrm{T}}{\mathrm{T}+1}\right)\right)$$

**Overcounting**

$$\#\mathcal{Z}(f,(a,b))\leq\mathrm{V}(f;a,b).$$

**Exactness I**

If $\mathrm{V}(f;a,b)\leq 1$, then

$$\#\mathcal{Z}(f,(a,b))\leq\mathrm{V}(f;a,b).$$

**Exactness II (Obreshkoff)**

Let

$$\mathcal{D}_{a,b}:=\frac{a+b}{2}\left\{z\in\mathbb{C}:\left|z-\frac{1}{\tan\frac{1}{\mathrm{d}(f)+2}}\right|<\frac{1}{\sin\frac{1}{\mathrm{d}(f)+2}}\right\}.$$

Then

$$\#\mathcal{Z}\left(f,\mathcal{D}_{a,b}\cap\overline{\mathcal{D}_{a,b}}\right)\leq\mathrm{V}(f;a,b)\leq\#\mathcal{Z}\left(f,\mathcal{D}_{a,b}\cup\overline{\mathcal{D}_{a,b}}\right)$$

**Subdivision Property**

If $\bigcup_k(a_k,b_k)\subset(a,b)$ is a disjoint union, then

$$\sum_k\mathrm{V}(f;a_k,b_k)\leq\mathrm{V}(f;a,b).$$

## A $p$-adic Smale's 17th Problem?

Fix a prime $p$. Let $\mathfrak{f}\in\mathbb{Z}_p[\mathrm{X}_1,\dots,\mathrm{X}_n]^n$ be a random $p$-adic polynomial system such that

$$\mathfrak{f}_k=\sum_{|\alpha|\leq d_k}\mathfrak{f}_{k,\alpha}\mathrm{X}^\alpha$$

with the $\mathfrak{f}_{k,\alpha}$ independent random $p$-adic variable uniformly distributed in $\mathbb{Z}_p$. Is there a deterministic algorithm that decides whether or not $\mathfrak{f}$ has a zero in $\mathbb{Z}_p^n$ (resp. $\mathbb{Q}_p^n$) in average polynomial-time with respect the number of coefficients?

## Properties

$$\mathrm{St}(f;x,p^{-s}):=\mathrm{St}\left(f\left(x+p^s\mathrm{T}\right)\right)$$

**Overcounting**

$$\#\mathcal{Z}(f,x+p^{-s}\mathbb{Z}_p)\leq\mathrm{St}(f;x,p^{-s}).$$

**Exactness I**

If $\mathrm{St}(f;x,p^{-s})\leq 1$, then

$$\#\mathcal{Z}(f,x+p^{-s}\mathbb{Z}_p)\leq\mathrm{St}(f;x,p^{-s}).$$

**Exactness II**

Let

$$\mathcal{D}_{x,p^{-s}}:=x+p^{-s}\left\{z\in\mathbb{C}_p:|z|<1\right\}.$$

Then

$$\mathrm{St}(f;x,p^{-s})\leq\#\mathcal{Z}\left(f,\mathcal{D}_{x,p^{-s}}\right).$$

**Subdivision Property**

If $\bigcup_k\left(x_k+p^{-s_k}\mathbb{Z}_p\right)\subset x+p^{-s}\mathbb{Z}_p$ is a disjoint union, then

$$\sum_k\mathrm{V}(f;x_k,p^{-s_k})\leq\mathrm{St}(f;x,p^{-s}).$$

Poster supported by NSF grant DMS 2232812