An invitation to computational and symbolic algebra

Daniele Taufer

CISPA
Helmholtz Center for Information Security

19 May 2022

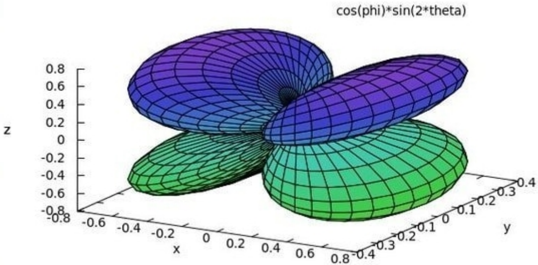
Computational algebra: should you care?

"Mathematics is the cheapest science.
Unlike physics or chemistry, it does not require any expensive equipment.
All one needs for mathematics is a pencil and paper."

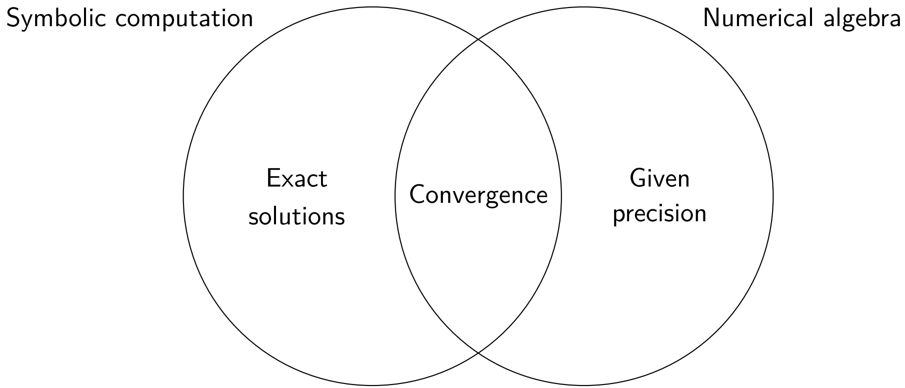
- George Polya

Computational algebra: should you care?

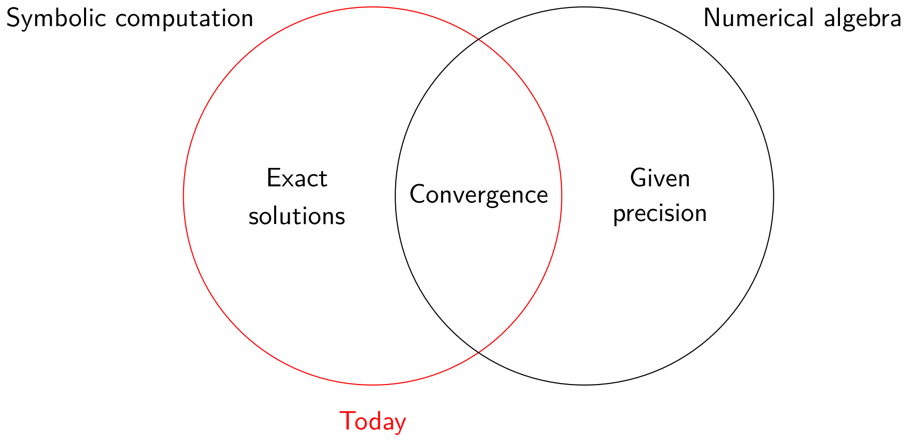
- Produce tons of examples to play with.
- Get new visual/symbolic ideas.
- Let the computer do the dirty work.
- Save yours and others time.
- Compound human knowledge
- Exhaustive searches.
- Formal proofs.
- Applications.
- Education.
- Fun!



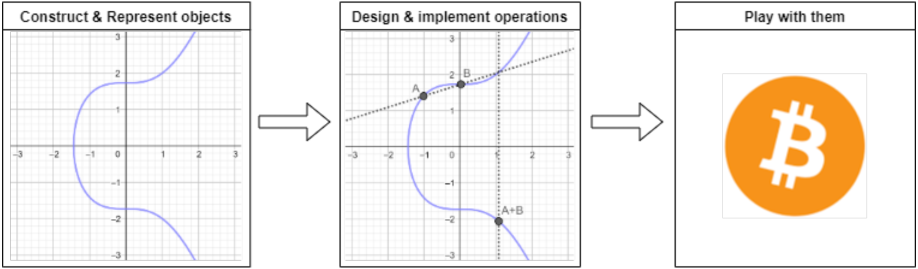
Computational algebra: what are we talking about?



Computational algebra: what are we talking about?



Computational algebra: challenges



Systems and ideals

Problems reduce to solving polynomial systems more often than one might expect!

Example

Finding the rational roots of the following system

$$\begin{cases} x^3 - y + 1 = 0, \\ x^2 + z^2 - y = 0, \\ y^2 - 3x + z = 0. \end{cases}$$

It is equivalent to finding the zeros of the ideal

$$I = \langle x^3 - y + 1,\ x^2 + z^2 - y,\ y^2 - 3x + z \rangle_{\mathbb{Q}}.$$

Systems and ideals

Hilbert's Nullstellensatz

It rules the existence of solutions over the algebraic closure:

$$\mathcal{I}\big(\mathcal{V}(I)\big) = \sqrt{I}.$$

Since $1 \notin I$, we know that it has solutions in the algebraic numbers.

Gröbner bases

A Gröbner basis for I:

$$
\begin{aligned}
&x - y - \frac{512}{8889}z^{10} - \frac{344}{8889}z^9 + \frac{8}{2963}z^8 - \frac{2095}{8889}z^7 - \frac{8353}{8889}z^6 \\
&- \frac{1424}{8889}z^5 + \frac{3262}{8889}z^4 - \frac{4622}{2963}z^3 - \frac{26674}{8889}z^2 + \frac{2490}{2963}z + \frac{30883}{8889}, \\
&y^2 - 3y - \frac{512}{2963}z^{10} - \frac{344}{2963}z^9 + \frac{24}{2963}z^8 - \frac{2095}{2963}z^7 - \frac{8353}{2963}z^6 \\
&- \frac{1424}{2963}z^5 + \frac{3262}{2963}z^4 - \frac{13866}{2963}z^3 - \frac{26674}{2963}z^2 + \frac{10433}{2963}z + \frac{30883}{2963}, \\
&yz + y + \frac{1368}{2963}z^{10} - \frac{192}{2963}z^9 + \frac{1047}{2963}z^8 + \frac{3792}{2963}z^7 + \frac{20420}{2963}z^6 \\
&- \frac{2862}{2963}z^5 - \frac{660}{2963}z^4 + \frac{28437}{2963}z^3 + \frac{77103}{2963}z^2 - \frac{12644}{2963}z - \frac{82747}{2963}, \\
&z^{11} - z^{10} + z^9 + 2z^8 + 13z^7 - 15z^6 + 2z^5 + 22z^4 + 41z^3 - 61z^2 \\
&- 56z + 55.
\end{aligned}
$$

Elimination theory

$$\begin{cases} Y = x^3 + 1, \\ X^2 + Z^2 - (x^3 + 1) = 0, \\ (x^3 + 1)^2 - 3x + z = 0. \end{cases} \to \begin{cases} y = x^3 + 1, \\ x^2 + (3x - (x^3 + 1)^2)^2 - (x^3 + 1) = 0, \\ z = 3x - (x^3 + 1)^2. \end{cases}$$

therefore it is sufficient to find the roots of

$$x^{12} + 4x^9 - 6x^7 + 6x^6 - 12x^4 + 3x^3 + 10x^2 - 6x = 0,$$

which over $\mathbb{Q}$ are $\{0, 1\}$. Hence

$$\mathcal{V}_{\mathbb{Q}}(I) = \{(0, 1, -1), (1, 2, -1)\}.$$

Resultant

Let $f = f_d x^d + f_{d-1}x^{d-1} + \dots + f_0$, $g = g_e x^e + g_{e-1}x^{e-1} + \dots + g_0 \in R[x]$, and

$$\begin{aligned}\varphi_{f,g} : \mathcal{S}_{<e} \times \mathcal{S}_{<d} &\to \mathcal{S}_{<d+e}\\ (p,q) &\mapsto fp + gq.\end{aligned}$$

Its matrix w.r.t. the standard monomial bases is

$$\begin{pmatrix} f_0 & 0 & \dots & 0 & g_0 & 0 & \dots & 0 \\ f_1 & f_0 & \dots & 0 & g_1 & g_0 & \dots & 0 \\ \vdots & \vdots & & f_0 & \vdots & \vdots & & g_0 \\ f_d & f_{d-1} & \dots & \vdots & g_e & g_{e-1} & \dots & \vdots \\ 0 & f_e & \dots & \vdots & 0 & g_e & \dots & \vdots \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & f_d & 0 & 0 & \dots & g_e \end{pmatrix}.$$

Resultant

Definition

Let $f = f_d x^d + f_{d-1}x^{d-1} + \cdots + f_0$, $g = g_e x^e + g_{e-1}x^{e-1} + \cdots + g_0 \in R[x]$.
Their resultant is

$$R_x(f,g) = \det \begin{pmatrix} f_0 & 0 & \dots & 0 & g_0 & 0 & \dots & 0 \\ f_1 & f_0 & \dots & 0 & g_1 & g_0 & \dots & 0 \\ \vdots & \vdots & & f_0 & \vdots & \vdots & & g_0 \\ f_d & f_{d-1} & \dots & \vdots & g_e & g_{e-1} & \dots & \vdots \\ 0 & f_e & \dots & \vdots & 0 & g_e & \dots & \vdots \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & f_d & 0 & 0 & \dots & g_e \end{pmatrix} \in R.$$

Resultant

Main properties

- We have
$$R_x(f,g) \in \langle f, g\rangle.$$
- If R is an integral domain, and
$$g = f_d^e \prod_{i=1}^{d}(x-\lambda_i), \quad g = g_e^d \prod_{j=1}^{e}(x-\mu_j) \in \overline{\mathrm{Frac} R}[x],$$
then
$$R_x(f,g) = f_d^e g_e^d \prod_{i,j}(\lambda_i - \mu_j)$$

Resultant

Quiz

Compute $R_x(f, g)$, where

1. $f = 3, \; g = x^2$.
2. $f = x - a, \; g = x - b$.
3. $f = x^2 - 1, \; g = x^5 - 1$.
4. $f = x^2 - 1, \; g = x^2 + 1$.
5. $f = x, \; g = xy$.

Applications of resultant

Elimination theory

$$\mathcal{V}(\langle R_x(f,g)\rangle) = \mathcal{V}(\langle f,g\rangle)$$

In our example

$$\begin{cases} x^3 - y + 1 = 0, \\ x^2 + z^2 - y = 0, \\ y^2 - 3x + z = 0. \end{cases}$$

$$\begin{cases} 0 = R_z(x^3 - y + 1, x^2 + z^2 - y) = x^6 - 2x^3y + 2x^3 + y^2 - 2y + 1, \\ 0 = R_z(x^3 - y + 1, x^2 + z^2 - y) = 10x^2 - 6xy^2 + y^4 - y. \end{cases}$$

$$\begin{aligned} 0 &= R_y(x^6 - 2x^3y + 2x^3 + y^2 - 2y + 1, 10x^2 - 6xy^2 + y^4 - y) \\ &= (x^{12} + 4x^9 - 6x^7 + 6x^6 - 12x^4 + 3x^3 + 10x^2 - 6x)^2. \end{aligned}$$

Applications of resultant

Number theory - The discriminant

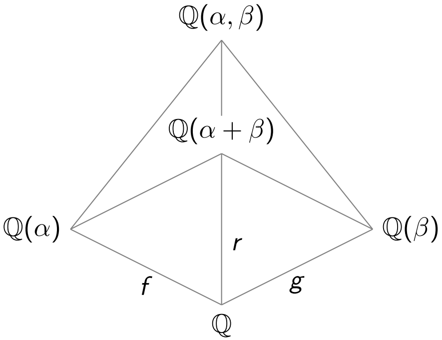
$$\Delta_f = \frac{(-1)^{\frac{d(d-1)}{2}}}{f_n} R_x(f, f')$$

An old high-school friend:

$$\begin{aligned}\Delta_{Ax^2+Bx+C} &= -\frac{1}{A} R_x(Ax^2 + Bx + C, 2Ax + B) \\ &= -\frac{1}{A} \det \begin{pmatrix} C & B & 0 \\ B & 2A & B \\ A & 0 & 2A \end{pmatrix} = -\frac{4A^2C + AB^2 - 2AB^2}{A} = B^2 - 4AC.\end{aligned}$$

Applications of resultant

Number theory - Composite extensions



$$r \mid R_y\big(f(y), g(y-x)\big).$$

Applications of resultant

Algebraic geometry

If a curve $C = C(t)$ is parametrized by

$$x = \frac{N_1(t)}{D(t)}, \quad y = \frac{N_2(t)}{D(t)},$$

then the curve equation is

$$R_t\big(xD(t) - N_1(t), xD(t) - N_2(t)\big) = 0.$$

Elliptic curves

Elliptic curves

An *elliptic curve* E defined over a *suitable* ring R is a projective smooth curve defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Projective

We look for points

$$(X : Y : Z) \in \mathbb{P}^2(R) = \{\text{Primitive triples}\}/R^*.$$

(Usual) Example

If R is a field, we want non-zero triples up to non-zero scalar multiplication, i.e.

$$\forall u \neq 0 \quad (X : Y : Z) = (uX : uY : uZ) \in \mathbb{P}^2(R).$$

Elliptic curves

Elliptic curves

An *elliptic curve* E defined over a *suitable* ring R is a projective smooth curve defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Quiz

Which of the following triples are primitive?

1. $(\sqrt{2}, \sqrt{3}, 1)$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.
2. $(x+1 : x : x^2)$, $x \in R$.
3. $(12, 9, 27)$ over $\mathbb{Q}$.
4. $(12, 9, 27)$ over $\mathbb{Z}$.
5. $(12, 9, 27)$ over $\mathbb{Z}/4\mathbb{Z}$.

Elliptic curves

Quiz+

Is $(1+\sqrt{5}, 2\sqrt{5}, 1-\sqrt{5})$ primitive in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$?

http://magma.maths.usyd.edu.au/calc/

```
R<x> := PolynomialRing(Integers());
f := x^2-5;
F<a> := NumberField(f);
O := RingOfIntegers(F);
I := ideal<O|[a+1,2*a,a-1]>;
O!1 in I;
```

Elliptic curves

Elliptic curves

An *elliptic curve* E defined over a *suitable* ring R is a projective smooth curve defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Smoothness

A certain polynomial relation Δ_E in the curve coefficients needs to be invertible.

(Usual) Example

If R is a field of characteristic $\neq 2, 3$, and the curve E is defined by

$$Y^2Z = X^3 + AXZ^2 + BZ^3,$$

then E is elliptic if and only if

$$\Delta_E = \Delta_{X^3+AX+B} = -16(4A^3 + 27B^2) \neq 0.$$

Elliptic curves

Elliptic curves

An *elliptic curve* E defined over a *suitable* ring R is a projective smooth curve defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Smoothness

A certain polynomial relation Δ_E in the curve coefficients needs to be invertible.

```
R<x,y,z,A,B> := PolynomialRing(Rationals(),5);
F := - y^2*z + x^3 + A*x*z^2 + B*z^3;
r1 := Resultant(Derivative(F,y), Derivative(F,z), y);
r2 := Resultant(Derivative(F,x), r1, x);
r2 eq z^8*16*(4*A^3+27*B^2);
```

Elliptic curves

Elliptic curves

An *elliptic curve* E defined over a *suitable* ring R is a projective smooth curve defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Suitable rings

Let R be a commutative ring with unity. For every matrix M over R, if the elements of M are primitive and every (2×2)-minor of M vanishes, then there exists an R-linear combination of the columns that is primitive.

Examples

$$\begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} \in M_2(\mathbb{Z}/6\mathbb{Z}), \quad \checkmark \qquad \begin{pmatrix} 2 & 1-\sqrt{-5} \\ 1+\sqrt{-5} & 3 \end{pmatrix} \in M_2(\mathbb{Z}[\sqrt{-5}]). \quad \times$$

Elliptic curves

Elliptic curves

An *elliptic curve* E defined over a *suitable* ring R is a projective smooth curve defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Quiz

Which of the following equations defines an elliptic curve?

1. $Y^4 = X^3 + XYZ$ over $\mathbb{Z}$.
2. $Y^2Z = X^3$ over $\mathbb{Q}$.
3. $Y^2Z = X^3 + Z^3$ over $\mathbb{Z}/3\mathbb{Z}$.
4. $Y^2Z = X^3 + Z^3$ over $\mathbb{R}$.
5. $Y^2Z = X^3 + Z^3$ over $M_{2\times 2}(\mathbb{R})$.

How elliptic curves look like

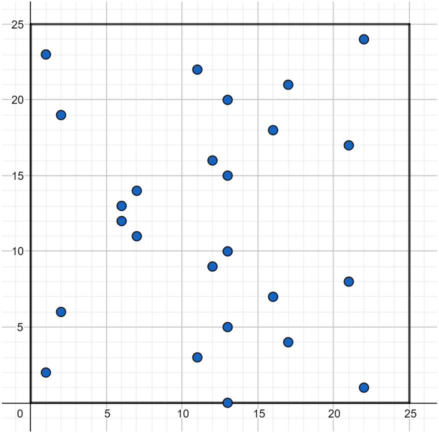


Figure: Affine points of the elliptic curve defined by $Y^2Z = X^3 + 3Z^3$ over $\mathbb{Z}/25\mathbb{Z}$.

How elliptic curves look like

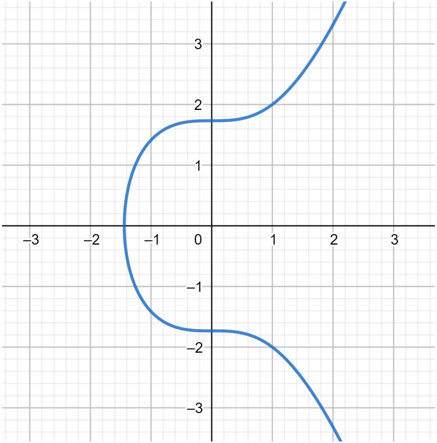


Figure: Affine points of the elliptic curve defined by $Y^2Z = X^3 + 3Z^3$ over $\mathbb{R}$.

Addition law

Over these objects, an addition law may be defined by any primitive relation among some polynomial expression of the addenda.

Let us check it!

`https://github.com/DTaufer/Computational-Algebra/blob/main/Verifying%20EC%20group`

Addition law

It restricts to the tangent-secant law

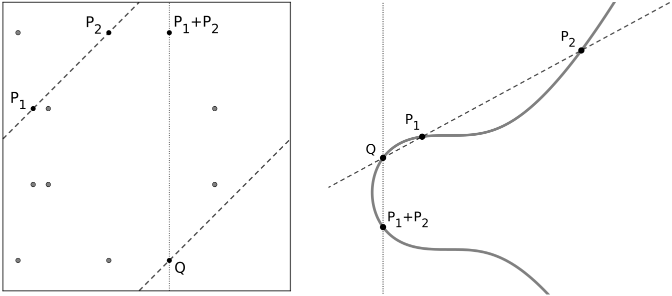


Figure: Addition law for the curve $Y^2Z = X^3 + 3Z^3$, defined over different fields.

Addition law

Over fields is easier!

```
R := GF(7);
E := EllipticCurve([R!1,2,3,4,6]);
P := Random(E); Q := Random(E);
P+Q in E;
#E eq 6;
T3:= {P3 :  P3 in E | 3*P3 eq E!0};
#T3 eq 3;
```

The problem

Let E be an elliptic curve. For a given pairs $P, Q \in E$ with $Q \in \langle P \rangle$, determining $n \in \mathbb{Z}$ such that

$$Q = nP.$$

MAGMA is super-powerful!

```
R := GF(NextPrime(10^9));
E := EllipticCurve([R!0,-5,0,1,2]);
P := Random(E); Q := Random(E);
IsPrime(#E);
time n := Log(P,Q);
n*P eq Q;
```

The problem

Let E be an elliptic curve. For a given pairs $P, Q \in E$ with $Q \in \langle P \rangle$, determining $n \in \mathbb{Z}$ such that

$$Q = nP.$$

But also MAGMA has limits...

```
p := 730750818665451459112596905638433048232067471723;
A := 425706413842211054102700238164133538302169176474;
B := 203362936548826936673264444982866339953265530166;
E := EllipticCurve([GF(p)!A,B]);
P := Random(E); Q := Random(E);
IsPrime(#E);
// time n := Log(P,Q);
```

Working around... or above?

S.E.S.

$$0 \to \pi^{-1}\big((0:1:0)\big) \to E(\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\pi} E(\mathbb{Z}/p\mathbb{Z}) \to 0.$$

Facts

- $\pi^{-1}\big((0:1:0)\big) = (\alpha p : 1 : 0)$.
- $(\alpha p : 1 : 0) + (\beta p : 1 : 0) = \big((\alpha+\beta)p : 1 : 0\big)$.
- If E is anomalous $\big($i.e. $E(\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}\big)$, we almost always have

$$E(\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{Z}/p^2\mathbb{Z}.$$

Quiz

How to exploit the above facts for efficiently solving the discrete logarithm over anomalous curves?

Working around... or above?

S.E.S.

$$0 \to \pi^{-1}\big((0:1:0)\big) \to E(\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\pi} E(\mathbb{Z}/p\mathbb{Z}) \to 0.$$

Facts

- $\pi^{-1}\big((0:1:0)\big) = (\alpha p : 1 : 0)$.
- $(\alpha p : 1 : 0) + (\beta p : 1 : 0) = \big((\alpha+\beta)p : 1 : 0\big)$.
- If E is anomalous $\big($i.e. $E(\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}\big)$, we almost always have

$$E(\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{Z}/p^2\mathbb{Z}.$$

Solution

GitHub!

Bibliography

- W. Bosma, H. W. Lenstra, *Complete Systems of Two Addition Laws for Elliptic Curves*, J. Number Theory 53 (1995), pp. 229–240.
- H. W. Lenstra, *Elliptic curves and number-theoretic algorithms*, Proc. International Congress of Mathematicians (1986), pp. 99–120.
- R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, 1996.
- M. Sala, D. Taufer, *The group structure of elliptic curves over* $\mathbb{Z}/N\mathbb{Z}$, `https://arxiv.org/abs/2010.15543v1` (2020).
- J. H. Silverman, *The Arithmetic of Elliptic Curves* (2nd Edition), Springer-Verlag (2009).