Introduction to MAGMA

Christophe Ritzenthaler

June 6, 2018

1 For those who have never used it before...

The most important thing is the help. There exist two sorts : the html files are the most convenient. They contain, besides the description of each command, examples and even mathematical background. You can access commands by topic (finite groups, commutative algebra, algebraic geometry) or through the index.
The second help is online : when you want information about a command, let's say `RandomPrime`, you type `RandomPrime;`.

A last tip before we start : there is a automatic completion with 'tab'. This is useful when you do not remember exactly the name : MAGMA follows very closely the exact definition.

We will start with some examples that look really similar to `Maple`. To Evaluate an expression you need to end it with `;`. To define an object you write `f:=...`. As you may see it does not display the result. To see it you have to write `f;`.

1. Compute $\frac{123}{10} + \frac{33}{127}$.
2. Compute $2 + \sqrt{3}$.
3. Compute 200! and factorize this number.
4. Is $2^{1233} + 321$ prime (`IsPrime`) ?

Some examples how to handle sets, sequences, lists :

5. Define the sets $I = \{1, 4, 10\}$, $J = \{2, 4, 8\}$. Do the following operations : $I \cup J$ and $I \cap J$.

6. Create a random list of 10 integers. Extract the 8th.

Unlike `Maple`, MAGMA require to define properly where you are working. You cannot open a MAGMA section and write : $f = x^3 + 3$;. MAGMA does not know yet what is x. It is sometimes a bit tedious when you want to work with polynomials in a lot of variables but the counterpart is that it allows much more objects than the two others softwares : polynomials over extensions of finite fields or p-adic fields, matrices with coefficients in function fields .... And it is much more accurate, mathematically speaking !

Very important fields for us are the field of rationals and finite fields :

7. Create the field of rationals.
8. Create the field $F = \mathbb{F}_{23}$ (`GF`).
9. Add 20 and 5 in this field. This leads to the notion of coercion (for instance `F!20`).
10. Create the field $K = \mathbb{F}_{23^4}$. What is a defining polynomial for this field ? Compute the square root of 10 in this field.

One would like also to create extensions by choosing a defining polynomial.

11. Create the polynomial ring R with variable x over $\mathbb{F}_5$.
12. Create the polynomial $f = x^6 + 3x + 3$. Evaluate f at 2. Is f irreducible ? What is its splitting field ? Call it $F < w >$.
13. Create an extension of F of degree 3 by a polynomial of your choice.

Once we have the basic fields, we can construct polynomial rings in several variables on them

14. Construct the polynomial ring $P = \mathbb{Q}[x, y, z]$.
15. Consider $f = x^4 + y^4 + z^4 \in P$.
16. Prove that f is irreducible.
17. Compute the resultant R in x of f and $\partial f / \partial x$.
18. Create the ring $P_2 = \mathbb{Q}[u, v]$ and the morphism $(x, y, z) \mapsto (1, u, v)$ with `hom< P-> P2 | 1,u,v>`.

19. Map R into P_2 with this morphism.

We can now define varieties, in particular curves. There are multiple ways to define them, depending if they are general curves, elliptic curves, hyperelliptic curves,.... Depending on the type of curves and fields, you have also access to a larger panel of functionalities and of efficiency. Let us consider here only some basics ones.

20. Define the projective space $S = \mathbb{P}^2_{\mathbb{Q}}$ (`ProjectiveSpace(P)`).

21. Define the curve $C : f = 0$ in S.

22. Is it singular? What is its genus?

23. Consider the curve C over $F = \mathbb{F}_{73}$ (`ChangeRing`). Let's call it D. Is D smooth?

24. Compute its number of points and then its Weil polynomial.

25. Find the flexes of D.

26. Compute the dimensions $\ell(nP)$ of the Riemann-Roch spaces for $1 \leq n \leq 4$, when P is a flex point and when P is not. See the definition of a Weierstrass point.

Another example in space:

27. Define the polynomial ring R with variables x, y, z, u, v over the rationals.

28. Define the 3 homogeneous polynomials f_1, f_2, f_3 :

$$\begin{cases} f1 = x^2 + y^2 + z^2 - uv \\ f2 = xu - yv \\ f3 = 2x^2 + 3y^2 - zy + u^2 + v^2 \end{cases}$$

29. Define the projective space associated to R

30. Define the Scheme $C : f_1 = f_2 = f_3 = 0$.

31. What is its dimension ?

32. Is it singular ?

We will need only basic programming properties, like loops (`for...do`, `while...do`) and branchement (`if...then...else`) which you end with (`end for, end while, end if`).

33. Create a loop that runs through the primes less than 100 (`NextPrime`).

34. For each prime $11 \leq p \leq 100$, reduce the curve C from (21) over $\mathbb{F}_p$ and stop when its number of rational points reaches the maximal value $1 + p + 3 \cdot \lfloor 2\sqrt{p} \rfloor$.

Automorphisms.
Let G, H, M be the following matrices

$$G = \begin{pmatrix} \zeta^4 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix}, \; H = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \; M = \frac{-1}{\sqrt{-7}} \begin{pmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{pmatrix},$$

where ζ is a 7th root of unity.
Show that the automorphisms of $\mathbb{P}^2$ given by these matrices are automorphisms of the Klein's quartic $x^3y + y^3z + z^3x = 0$. What is the order of the group generated by these matrices ?

Remark 1.1. In characteristic 0, One can show (using Hurwitz bound) that automorphism group of the curve is generated by these elements. This is not true in characteristic 3 (this is the only case).

2 More advanced problems: maximal curves

2.1 Maximal curves: $g = 1$

For $5 \leq p \leq 100$ a prime, we want to compute what the maximal number of points of an elliptic curve over $\mathbb{F}_p$ is. To do so, using MAGMA , you have two solutions:

- Use the form $y^2 = x^3 + Ax + B$ at the beginning of Exercise **??**;
- See a bit further down in the exercise and run over the $\bar{\mathbb{F}}_p$-isomorphism classes using `E:=EllipticCurveFromjInvariant(j)` and then compute the twists using `Twists(E)`.

Use a graphical software (like SAGEMATH) to plot this maximum in term of p. Try to find the law satisfied by this function.

2.2 Maximal curves: $g = 2$

You can then try to run over all genus 2 curves defined over $\mathbb{F}_p$ with $2 < p \leq 30$. In order to do so, you will imitate the second item of the strategy for elliptic curves, replacing the j-invariant by three invariants $J = [j_1, j_2, j_3] \in \mathbb{F}_p^3$. The function to run over such the $\bar{\mathbb{F}}_p$-isomorphism classes is now `HyperellipticCurveFromG2Invariants(J)`. Can you see what is the law satisfied by this function? Is it as well behaved than the genus 1 case?

Another experiment is to look whether there is an influence of the number of points of the curve over $\mathbb{F}_p$ on the points over extensions.

- Run over genus 1 curves over $\mathbb{F}_{23}$ and check that two curves which have the same number of points over $\mathbb{F}_{23}$ have the same number of points over $\mathbb{F}_{23^2}$ and $\mathbb{F}_{23^3}$.
- Do the same experiment for genus 2 curves over $\mathbb{F}_{11}$. Does it hold? What do you observe?

One last experiment is to see how optimal the constant $2g$ in Hasse-Weil bound is, for a genus g curve $C/\mathbb{F}_q$ when we consider $\#C(\mathbb{F}_{q^n})$. Can you prove this result?

2.3 Maximal curves: $g = 3$

Check $N_q(3)$ for $q = 2, 4, 8, 3, 9$ by comparing with manypoints.

2.4 Higher genus

The genus 4 case is the first case for which there are open entries in manypoints. The smallest case is: is there a curve over $\mathbb{F}_{19}$ with 49 or 50 points?

Similarly is there a genus 5 curve over $\mathbb{F}_7$ with 27 or 28 points? Note that you can "easily find" a genus 5 curve over $\mathbb{F}_3$ with 13 rational points(hint $\#\mathbb{P}^2(\mathbb{F}_3) = 7$).

3 More advanced problems: geometry of curves

3.1 Edwards model

Find an explicit isomorphism between the model in $\mathbb{P}^3$ of Edwards curve and a Weierstrass model. When can be an elliptic curve be put in Edwards form?

3.2 Bitangents of plane quartics

Let $C : F = 0$ be the canonical embedding of a non hyperelliptic curve of genus 3 as a smooth plane quartic. A line L can cut the quartic with various multiplicities

1. $(1,1,1,1)$: it is the generic case;
2. $(2,1,1)$: L is tangent at C;
3. $(3,1)$: the first point of intersection is called a *flex point*;
4. $(2,2)$: L is called a *bitangent*
5. (4) : this point is called a *hyperflex*. A generic quartic has none of them.

We are going to compute some extrinsic geometry of C. We have already computed the flexes in a previous exercise and seen that they have also an intrinsic definition as *Weierstrass points*.

We then focus on the bitangents of the following quartic

$$\begin{aligned} C/\mathbb{Q} \qquad & : x^4 - 2x^3y - 4x^3z - x^2y^2 + 11x^2yz + 3x^2z^2 \\ & +2xy^3 + 5xy^2z - 7xyz^2 + y^4 - 6y^3z + 11y^2z^2 - 6yz^3 + z^4 = 0. \end{aligned}$$

In order to compute them, one can express that if $y = \alpha x + \beta$ is the affine equation of such a line then replacing y in the equation of C by this expression yields a perfect square in x. Now if g is a degree 4 polynomial in x

$$g(x) = ax^4 + bx^3 + cx^2 + dx + e = a(x^2 + b/(2a)x + (4ac - b^2)/(8a^2))^2 + * \cdot x + *$$

which gives two conditions on the lower terms. One can then get all solutions in α, β using resultant, Gröbner, etc.

Can you imagine a similar operation to compute multi-tangents to the following genus 4 curve over $\mathbb{F}_{1009}$ by $x_1^2 - x_0x_2 = 0$ and

$$\begin{aligned} x_0^3 + 966x_0^2x_1 + 336x_0^2x_2 + 475x_0x_1x_2 + 927x_0x_2^2 + 366x_1x_2^2 + \\ 364x_2^3 + 953x_0^2x_3 + 509x_0x_1x_3 + 918x_0x_2x_3 + 436x_1x_2x_3 + \\ 706x_2^2x_3 + 609x_0x_3^2 + 257x_1x_3^2 + 915x_2x_3^2 + 543x_3^3 = 0 \end{aligned}$$

3.3 Addition on the Jacobian of a plane quartic

Let C/k be a plane smooth quartic and $D^\infty = P_1^\infty + P_2^\infty + P_3^\infty$ an effective k-rational divisor of degree 3. Let D be a rational degree 0 divisor of C. Then there exists a rational effective divisor D^+ of degree 3 such that $D^+ - D^\infty \sim D$. We have seen that generically the divisor D^+ is unique.

By abuse of language we say that a curve C' *goes through* nP if $i(C, C'; P) = n$, where $i(C, C'; P)$ denotes the intersection multiplicity of C and C' at P. Let $D_1, D_2 \in \mathrm{Jac}(C)(k)$. Then $D_1 + D_2$ is equivalent to a divisor $D = D^+ - D^\infty$, where the points in the support of D^+ are given by the following algorithm:

1. Take a cubic E defined over k which goes (with multiplicity) through the support of D_1^+, D_2^+ and $P_1^\infty, P_2^\infty, P_4^\infty$. This cubic also crosses C in the residual effective divisor D_3.

2. Take a conic Q defined over k which goes through the support of D_3 and P_1^∞, P_2^∞. This conic also crosses C in the residual effective divisor D^+.

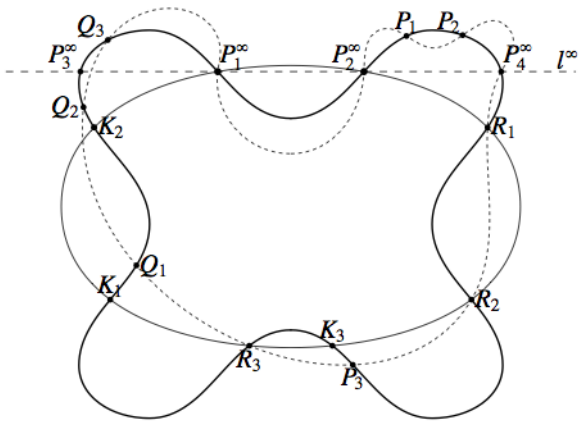

Figure 1: Description of the algorithm

Using the description of the group law for quartics, implement a Diffie-Hellman protocol for genus 3 non hyperelliptic curve. How fast can you make it? Note that there is not much hope[1] that this may be useful for

[1] or is it? Maybe for cryptographic multilinear maps

cryptography, the need of fast arithmetic on higher genus curves over finite fields exists in arithmetic statistics (see Sutherland's webpage for pictures).