Introduction to SageMath

1. Introduction

Cécile Armana

Laboratoire de Mathématiques de Besançon
Université Bourgogne Franche-Comté, France

African Mathematical School
Introduction to Number Theory, Cryptography and related courses

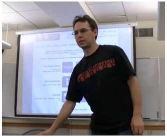
September 06-18, 2021 — AIMS-Senegal

What is SageMath?

SageMath is a free open-source mathematics software.

`https://www.sagemath.org/`

Started in 2004 by the mathematician William Stein.



Originally: **S**ystem for **A**rithmetic **G**eometry **E**xperimentation... But now, much more!

SageMath is open source

Goal: creating a viable free open source alternative to commercial softwares such as Magma, Maple, Mathematica and Matlab.

Anyone can:

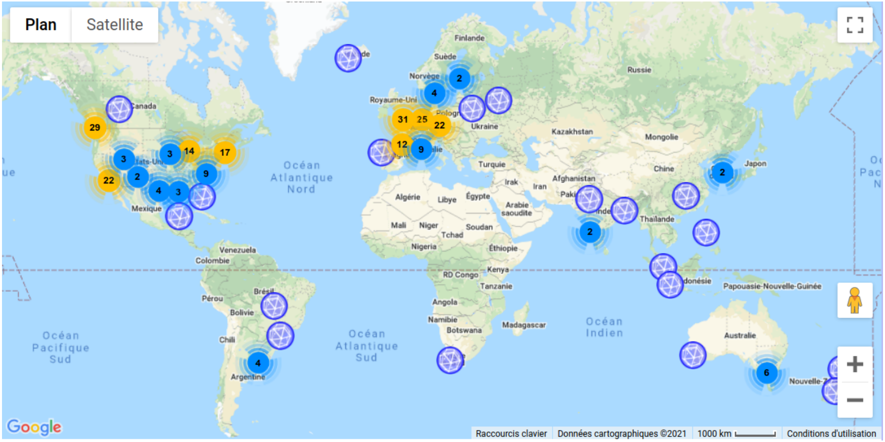
- install it and use it for free
- see the source code and modify it (fix bugs, add new features,...)
- share it, redistribute it, sell it... but no one can close the code.

The SageMath model:

- the source code is distributed under the GPL licence
- based on the programming language Python (see Prof. Nitaj's course)
- built on top of many other open source softwares or libraries: Axiom, Maxima, PARI/GP, GAP, Singular, NumPy/Scipy, R,...
- developed by its users; used by researchers, teachers, students.

SageMath community around the world

Currently 272 contributors in 190 different places.



Mailing lists, Sage days/workshops,...

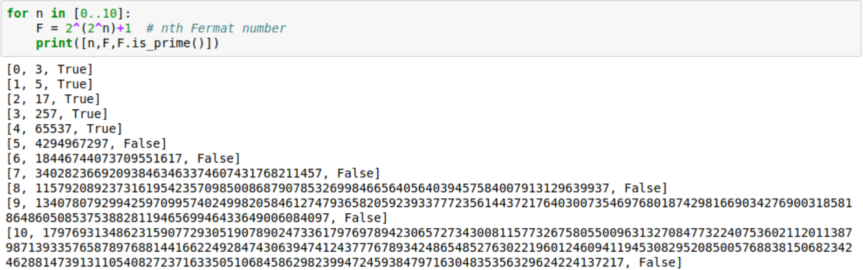
SageMath is a mathematics software

Nowadays:

- algebra and symbolic computation
- groups, fields, commutative algebra
- number theory
- algebraic geometry, arithmetic geometry
- geometry, topology
- combinatorics
- analysis
- numerical computation
- ...

Why using a mathematical software?

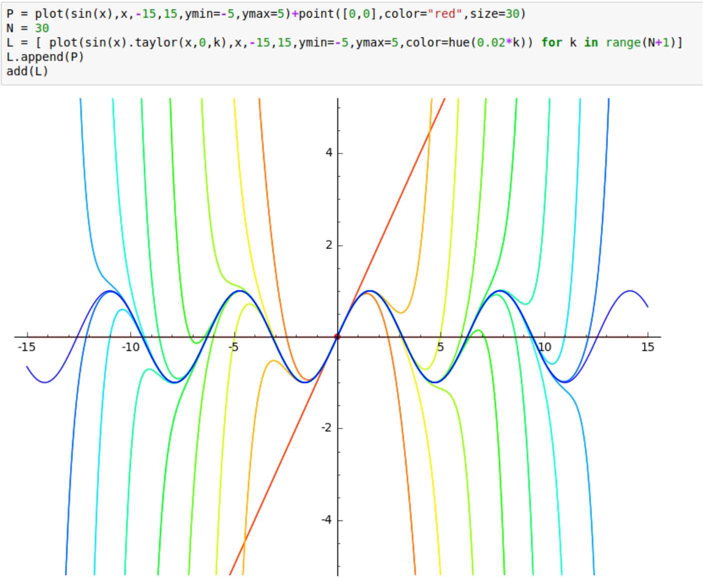
- check the result of hand calculations
- do/automate heavy calculations
- compute and plot datas
- experiment
- make or test conjectures
- develop new algorithms



```
for n in [0..10]:
    F = 2^(2^n)+1  # nth Fermat number
    print([n,F,F.is_prime()])
```

```
[0, 3, True]
[1, 5, True]
[2, 17, True]
[3, 257, True]
[4, 65537, True]
[5, 4294967297, False]
[6, 18446744073709551617, False]
[7, 340282366920938463463374607431768211457, False]
[8, 115792089237316195423570985008687907853269984665640564039457584007913129639937, False]
[9, 134078079299425970995740249982058461274793658205923933777235614437217640300735469768018742981669034276900318581
864860508537538828119465699464336490060840970, False]
[10, 179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342
462881473913110540827237163350510684586298239947245938479716304835356329624224137217, False]
```

Teaching with SageMath

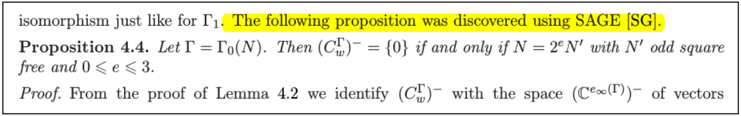


```
P = plot(sin(x),x,-15,15,ymin=-5,ymax=5)+point([0,0],color="red",size=30)
N = 30
L = [ plot(sin(x).taylor(x,0,k),x,-15,15,ymin=-5,ymax=5,color=hue(0.02*k)) for k in range(N+1)]
L.append(P)
add(L)
```

Research with SageMath

- Guessing statements by experimenting with SageMath and then prove them rigorously.

  V. Pasol, A. Popa, *Modular forms and period polynomials*, Proc. Lond. Math. Soc.(2013).



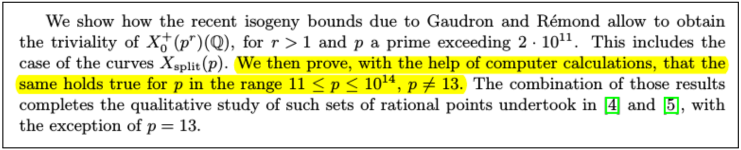
isomorphism just like for Γ_1. The following proposition was discovered using SAGE [SG].

Proposition 4.4. *Let* $\Gamma = \Gamma_0(N)$. *Then* $(C_w^\Gamma)^- = \{0\}$ *if and only if* $N = 2^e N'$ *with* N' *odd square free and* $0 \leqslant e \leqslant 3$.

Proof. From the proof of Lemma 4.2 we identify $(C_w^\Gamma)^-$ with the space $(\mathbb{C}^{e_\infty(\Gamma)})^-$ of vectors

- Reduce a difficult problem to a computation realizable on a computer and do it with SageMath.

  Yu. Bilu, P. Parent, M. Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier (2013).



We show how the recent isogeny bounds due to Gaudron and Rémond allow to obtain the triviality of $X_0^+(p^r)(\mathbb{Q})$, for $r > 1$ and p a prime exceeding $2 \cdot 10^{11}$. This includes the case of the curves $X_{\mathrm{split}}(p)$. We then prove, with the help of computer calculations, that the same holds true for p in the range $11 \leq p \leq 10^{14}$, $p \neq 13$. The combination of those results completes the qualitative study of such sets of rational points undertook in [4] and [5], with the exception of $p = 13$.

- …

How can I use SageMath?

Download and install it on your computer ($\sim$ 8 Gb of hard drive):

`https://www.sagemath.org/`

... and then use it offline. → Preferred method during the school, Sage is preinstalled on the computers at AIMS.

or

Use it online:

- on the CoCalc platform:

  `https://cocalc.com/`

  First create an account. Using the platform is free for casual use but performance can be limited.

- on SageCell interface (for testing commands and small computations):

  `https://sagecell.sagemath.org/`

And now...

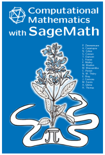
A short demo!

Then this week, my next “lectures”:

- Only practical sessions: you will learn, teach yourselves and experiment with Sage (I will be here to help you).
- Six (very long) Sage notebooks (chap. 2 to chap. 7): basics of Sage + specialized topics in relation with others courses of the school: arithmetic and applications to crypto., groups, fields and Galois theory, algebraic number theory,...
- Download these files at: `http://armana.perso.math.cnrs.fr/senegal2021/`
- Some previous knowledge of these topics is required to work on the notebooks. Go at your own pace and according to your taste or mathematical background.

References if you need help

- Explore the Sage tutorial
  `https://doc.sagemath.org/html/en/tutorial/`
- Online book Computational Mathematics with SageMath
  `http://sagebook.gforge.inria.fr/english.html`
  En français : Calcul mathématique avec Sage
  `http://sagebook.gforge.inria.fr/`



- Sage Quick reference cards: `https://wiki.sagemath.org/quickref`
- Learn the basics of Python
  `https://doc.sagemath.org/html/en/thematic_tutorials/tutorial-programming-python.html`
  `https://docs.python.org/3/tutorial/`
- Many other references
  `http://www.sagemath.org/help.html`
  `https://doc.sagemath.org/`