Sage can do ___!

Seewoo Lee

October 9, 2024. Math254A at UC Berkeley

Introduction

What is Sage?

What is Sage?

- **S**ystem for **A**lgebra and **G**eometry **E**xperimentation

What is Sage?

- **S**ystem for **A**lgebra and **G**eometry **E**xperimentation
- Originator: William Stein

What is Sage?

- **S**ystem for **A**lgebra and **G**eometry **E**xperimentation
- Originator: William Stein
- CAS (Computer Algebra System) based on Python

What is Sage?

- **S**ystem for **A**lgebra and **G**eometry **E**xperimentation
- Originator: William Stein
- CAS (Computer Algebra System) based on Python
- Free and open-source software

What is Sage?

- If you know how to write Python code, you can use Sage easily

What is Sage?

- If you know how to write Python code, you can use Sage easily
  - Syntax is *almost* the same, but not exactly
  - There are some Sage-specific syntax, e.g. ^ has different meaning for pure Python and Sage
  - Do *exact* calculations with integers and rational numbers

What is Sage?

- If you know how to write Python code, you can use Sage easily
  - Syntax is *almost* the same, but not exactly
  - There are some Sage-specific syntax, e.g. ^ has different meaning for pure Python and Sage
  - Do *exact* calculations with integers and rational numbers
- Sage $\neq$ fancy Python

What is Sage?

- If you know how to write Python code, you can use Sage easily
  - Syntax is *almost* the same, but not exactly
  - There are some Sage-specific syntax, e.g. ^ has different meaning for pure Python and Sage
  - Do *exact* calculations with integers and rational numbers
- Sage $\neq$ fancy Python
  - Sage = fancy (Python + GAP + PARI/GP + Singular + NTL + ...)
  - For better performance, Sage uses optimized libraries for specific tasks

How to use

- You can install it from `https://www.sagemath.org/`
- or you can visit `https://sagecell.sagemath.org/` and use online
- Companion codes (jupyter notebooks) are available at

  `https://gist.github.com/seewoo5/400dbb69b8a4a7831ea6f035d35ad08d`

Basic usage

Pre-undergraduate

- Add/multiply numbers
- Add/multiply many numbers
- Factorize a number
- Solve polynomial equations
- Pre-calculus

Pre-undergraduate

- Add/multiply numbers
- Add/multiply many numbers
- Factorize a number
- Solve polynomial equations
- Pre-calculus

Exercise. How many square-free numbers are there between 1 and 1M? (Hint: try `list(factor(60))`)

Undergraduate

- Linear algebra
- Group theory

Undergraduate

- Linear algebra
- Group theory

Exercise. How many 2 by 2 integer matrices with determinant 1 and absolute value of each entry at most $N = 100$ are there?

Undergraduate

- Linear algebra
- Group theory

Exercise. How many 2 by 2 integer matrices with determinant 1 and absolute value of each entry at most $N = 100$ are there?

- Can you make it faster? Try for $N = 1000$. (This question is for internship preparation)
- Can you find an asymptote as $N \to \infty$? (This is a hard math question)

Basic number theory

Undergraduate number theory

- Modular arithmetic
- Quadratic reciprocity
- Fermat's little theorem
- Primitive roots

Undergraduate number theory

- Modular arithmetic
- Quadratic reciprocity
- Fermat's little theorem
- Primitive roots

Exercise. We have public keys for RSA cryptosystem:

$$n = 6700238097692010877, \qquad e = 47519361519423038 11$$

and a ciphertext $c = 615476012187346704 8$. Find the message m.

p-adic numbers

- Basic arithmetic
- Polynomial over $\mathbb{Q}_p$
- Extensions of $\mathbb{Q}_p$
- Miscelleneous functions on $\mathbb{Q}_p$

p-adic numbers

- Basic arithmetic
- Polynomial over $\mathbb{Q}_p$
- Extensions of $\mathbb{Q}_p$
- Miscelleneous functions on $\mathbb{Q}_p$

Exercise. How many quadratic extensions of $\mathbb{Q}_p$ are there? Construct them with Sage.

Number fields

- Basic arithmetic
- Splitting of prime ideals
- Galois group
- Class group

Number fields

- Basic arithmetic
- Splitting of prime ideals
- Galois group
- Class group

Exercise. Choose an exercise from Marcus's book "Number Fields" and solve it with Sage.

Advanced topics

- Elliptic curves
- Modular forms
- L-functions

Homeworks (if you enjoyed)

Newton's method

Implement Newton's method for quadratic polynomials over $\mathbb{Q}_p$.

- Check that $\sqrt{2} \in \mathbb{Q}_p$ for

$$p = 479001599 = 12! - 1.$$

- If we expand it as $\sqrt{2} = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots$, then what are the two possible values of $a_{100} \in \{0, 1, \ldots, p-1\}$?

Extensions of $\mathbb{Q}_p$

Choose your favorite prime p and integer $n \geq 2$. How many extensions of $\mathbb{Q}_p$ of degree n are there? Can you construct some/all of them?

Kronecker–Weber theorem

Let $K/\mathbb{Q}$ be a number field which is the splitting field of

$$f(x) = x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1.$$

K is known to be Galois over $\mathbb{Q}$.

- Find as many as primes p that split completely in K.
- Could you find any patterns in your list? What can you conclude? (Hint: observe the primes modulo some integer.)
- Find closed form of zeros of $f(x) = 0$.

Two elliptic curves

Consider the following two elliptic curves over $\mathbb{Q}$:

$$E_1 : y^2 = x^3 - 13392x - 1080432,$$
$$E_2 : y^2 = x^3 - 432x + 8208.$$

For many primes $p \neq 11$, compare the number of $\mathbb{F}_p$-points on E_1 and E_2 (don't forget the point at infinity). What did you observe? Can you prove it?

Modularity theorem

Consider the elliptic curve

$$E : y^2 + y = x^3 - 7.$$

Again, compute the number of $\mathbb{F}_p$-points on E for many primes $p \neq 3$.

- Observe the numbers modulo 3. What did you observe?
- Now, consider the discriminant form

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n.$$

  For each prime $p \neq 3$, oberve $\tau(p) \pmod 3$. What did you find?
- How can you relate these two observations?

Some possible projects

- Choose your favorite theorem with a constructive/algorithmic proof, and implement it in Sage.
- Choose your favorite conjecture and give evidences of it. You can also try to make your own conjecture.
- Arithmetic statistics
- Cryptography (RSA, Elliptic curve, Lattice, ...).
- Sage + ML, discover anything interesting.

Happy Sage!