What to Contribute to Sage

I-Sage-ny Days 123

Giacomo Pope (NCC Group) 17th Jan 2024

Whatever You Want!

Use Sage.
Break Sage.
Fix Sage.

Consider Contributing...

- When something you **need is missing**

Consider Contributing...

- When something you **need is missing**
- When you find yourself **writing the same boilerplate** code multiple times

Consider Contributing...

- When something you **need is missing**
- When you find yourself **writing the same boilerplate** code multiple times
- When you find an algorithm **surprisingly** slow

Consider Contributing...

- When something you **need is missing**
- When you find yourself **writing the same boilerplate** code multiple times
- When you find an algorithm **surprisingly** slow
- When you know how an algorithm could be **generalised**

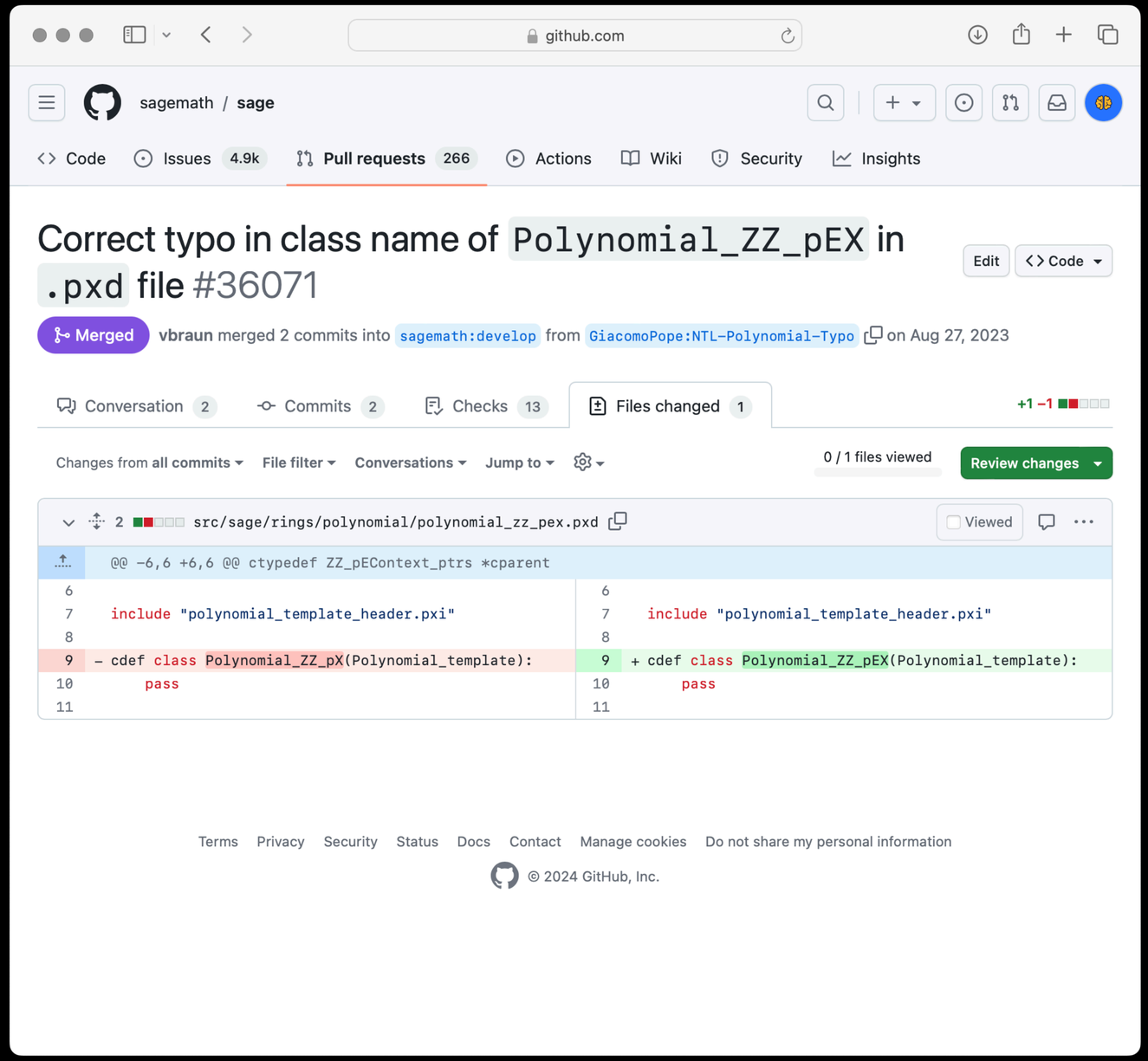
Consider Contributing...

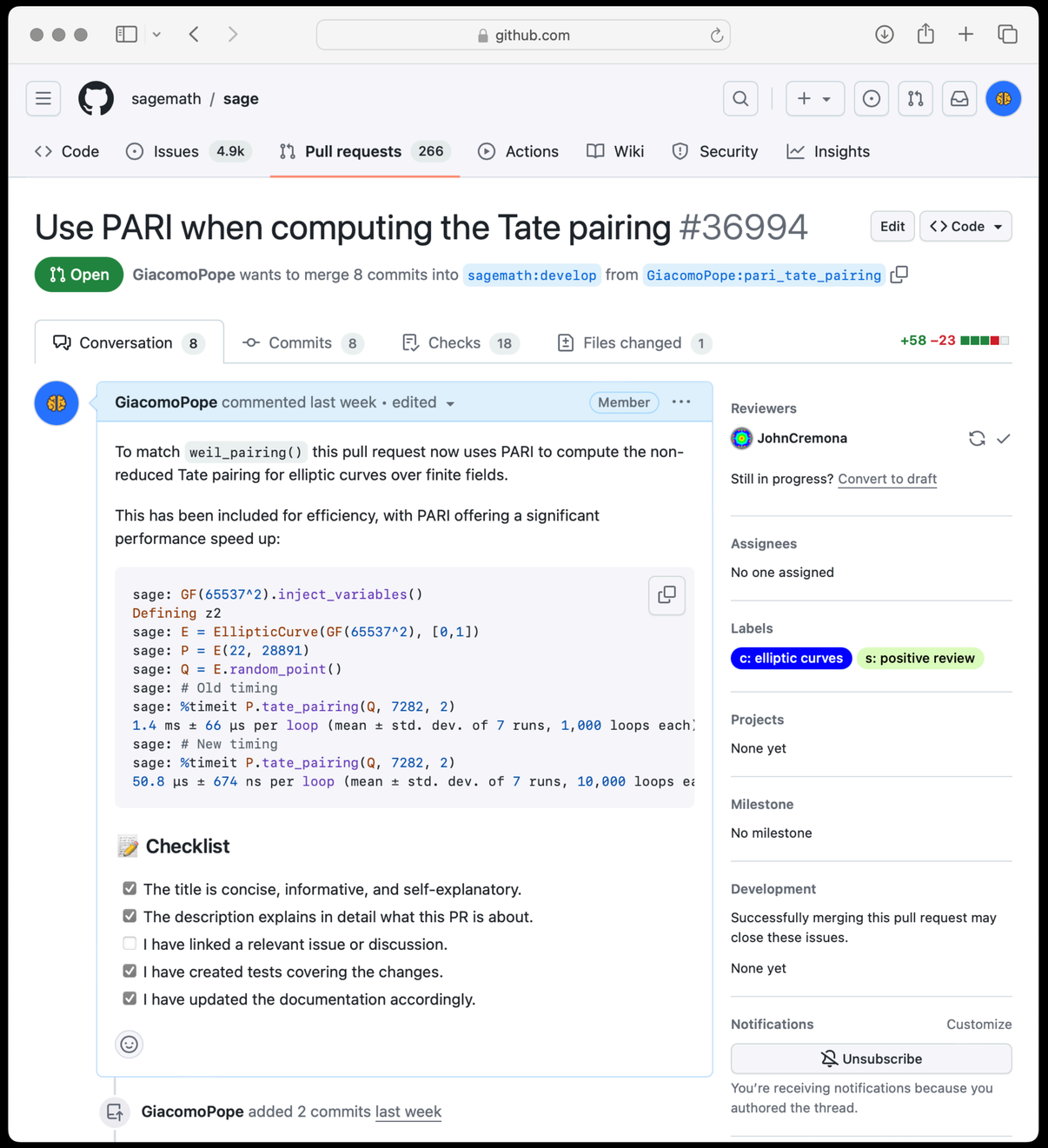
- When something you **need is missing**
- When you find yourself **writing the same boilerplate** code multiple times
- When you find an algorithm **surprisingly** slow
- When you know how an algorithm could be **generalised**
- There is a **special purpose external library** you want to integrate

Consider Contributing...

- When something you **need is missing**
- When you find yourself **writing the same boilerplate** code multiple times
- When you find an algorithm **surprisingly** slow
- When you know how an algorithm could be **generalised**
- There is a **special purpose external library** you want to integrate
- When something which **should** work simply **doesn't**

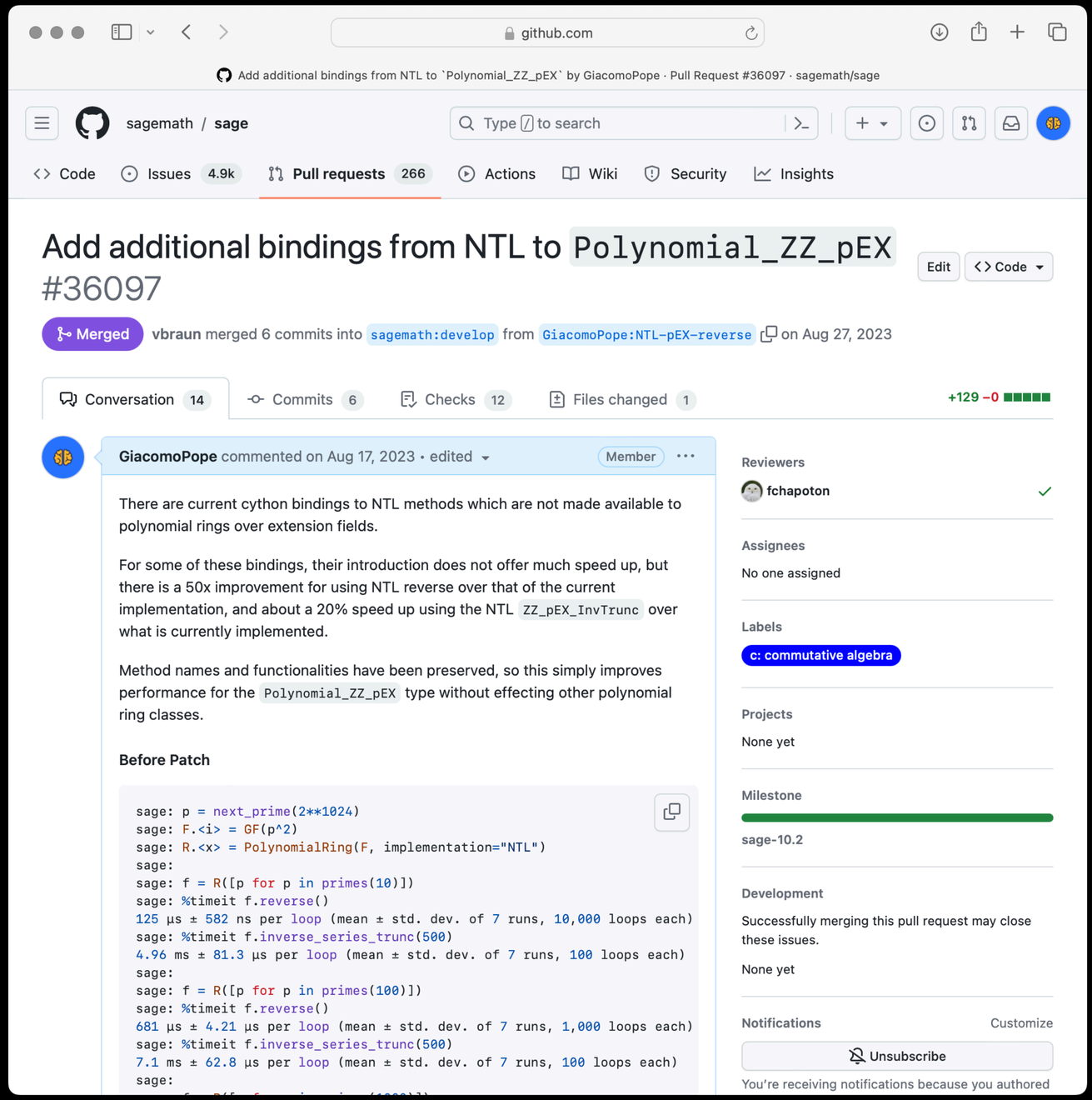
Sometimes you'll fix typos





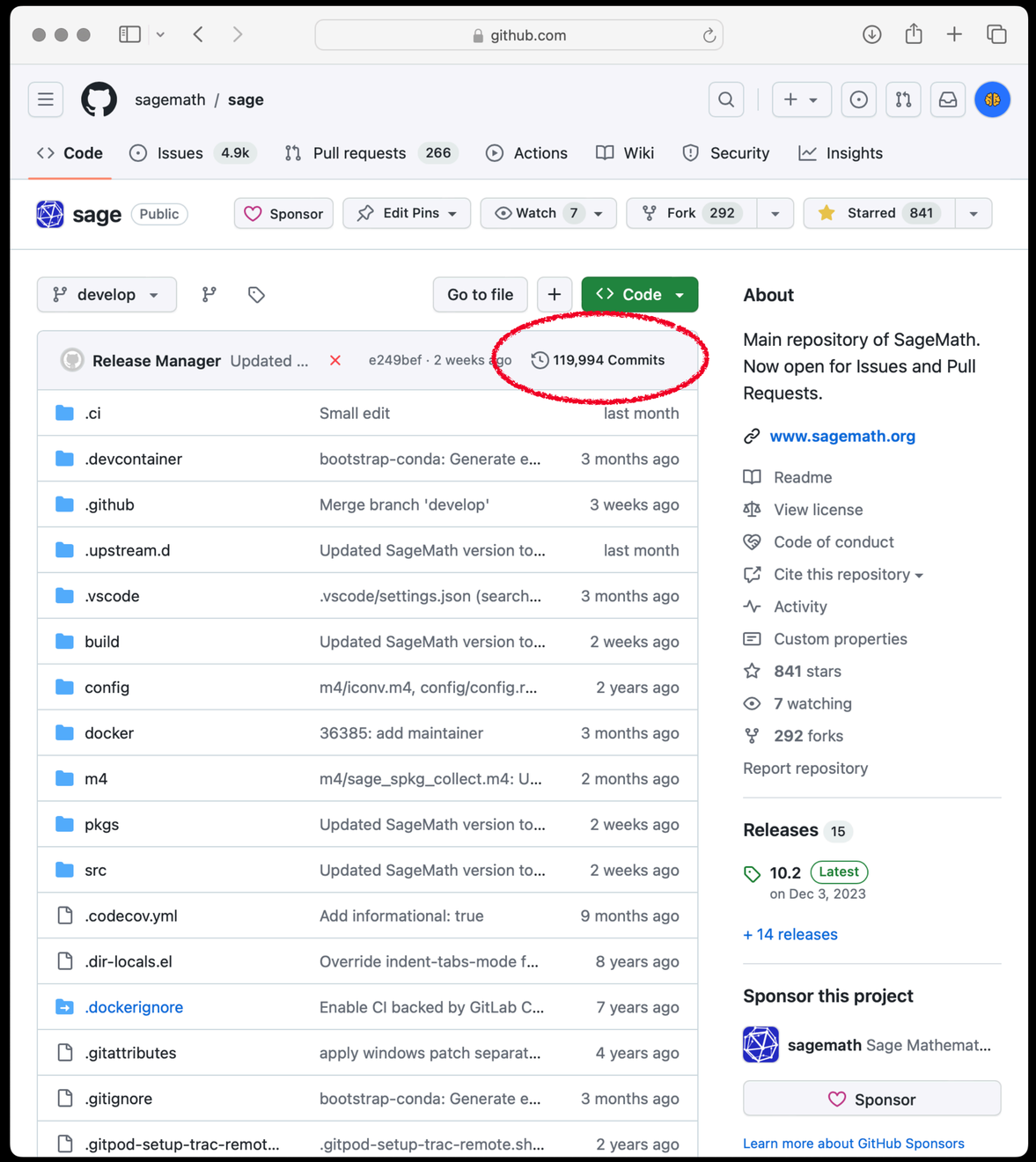
Or find that Pari can do something 25 times faster

Or finally learn Cython to use NTL to reverse polynomials 50x faster



You don’t have to make huge changes to make **good progress**

Sage is as it is after 120,000 of these small steps



The Wishlist

The Wishlist

- Improving functionality of **elliptic curves**

The Wishlist

- Improving functionality of **elliptic curves**
- Improving **isogenies** in genus one

The Wishlist

- Improving functionality of **elliptic curves**
- Improving **isogenies** in genus one
- Improving functionality of **hyperelliptic curves**

The Wishlist

- Improving functionality of **elliptic curves**
- Improving **isogenies** in genus one
- Improving functionality of **hyperelliptic curves**
- Including **isogenies** in genus two

The Wishlist

- Improving functionality of **elliptic curves**
- Improving **isogenies** in genus one
- Improving functionality of **hyperelliptic curves**
- Including **isogenies** in genus two
- Improvement of the **quaternion algebra**, orders and ideals

Improving Elliptic Curves

- A collection of **small quality of life** improvements

Improving Elliptic Curves

- A collection of **small quality of life** improvements
- Computing **endomorphism rings** of ordinary and supersingular curves

Improving Elliptic Curves

- A collection of **small quality of life** improvements
- Computing **endomorphism rings** of ordinary and supersingular curves
- Improving the computation of **torsion bases**

Improving Elliptic Curves

- A collection of **small quality of life** improvements
- Computing **endomorphism rings** of ordinary and supersingular curves
- Improving the computation of **torsion bases**
- Allow the computation of random points of a **given order**

Improving Elliptic Curves

- A collection of **small quality of life** improvements
- Computing **endomorphism rings** of ordinary and supersingular curves
- Improving the computation of **torsion bases**
- Allow the computation of random points of a **given order**
- Construction of **Kummer lines** from elliptic curves

Improving Elliptic Curves

- A collection of **small quality of life** improvements
- Computing **endomorphism rings** of ordinary and supersingular curves
- Improving the computation of **torsion bases**
- Allow the computation of random points of a **given order**
- Construction of **Kummer lines** from elliptic curves
- Simplification of **morphisms** to elliptic curves

Improving Isogenies in Genus One

- Implement **Fractional Isogenies** as a new class

Improving Isogenies in Genus One

- Implement **Fractional Isogenies** as a new class
- Implement a **meet-in-the-middle** search for isogenies of known degree

Improving Isogenies in Genus One

- Implement **Fractional Isogenies** as a new class
- Implement a **meet-in-the-middle** search for isogenies of known degree
- Fix a 15 year old bug in `multiplication_by_m()` to handle inseparable isogenies

Improving Isogenies in Genus One

- Implement **Fractional Isogenies** as a new class
- Implement a **meet-in-the-middle** search for isogenies of known degree
- Fix a 15 year old bug in `multiplication_by_m()` to handle inseparable isogenies
- Use **VeluSqrt** to compute large degree isogenies when computing factored isogenies

Improving Isogenies in Genus One

- Implement **Fractional Isogenies** as a new class
- Implement a **meet-in-the-middle** search for isogenies of known degree
- Fix a 15 year old bug in `multiplication_by_m()` to handle inseparable isogenies
- Use **VeluSqrt** to compute large degree isogenies when computing factored isogenies
- Allow the computation of isogenies from **irrational points**

Improving Isogenies in Genus One

- Implement **Fractional Isogenies** as a new class
- Implement a **meet-in-the-middle** search for isogenies of known degree
- Fix a 15 year old bug in `multiplication_by_m()` to handle inseparable isogenies
- Use **VeluSqrt** to compute large degree isogenies when computing factored isogenies
- Allow the computation of isogenies from **irrational points**
- Different methods to compute **dual isogenies**

Improving Higher Genus Curves

Generally, hyperelliptic curves are missing many expected functions and Magma is currently superior 🌋 😔

Improving Higher Genus Curves

Generally, hyperelliptic curves are missing many expected functions and Magma is currently superior 🌋 😔

- Allow the computation of **random points** on a curve

Improving Higher Genus Curves

Generally, hyperelliptic curves are missing many expected functions and Magma is currently superior 🌋 😔

- Allow the computation of **random points** on a curve
- Allow the computation of **random elements** of a Jacobian

Improving Higher Genus Curves

Generally, hyperelliptic curves are missing many expected functions and Magma is currently superior 🌋 😔

- Allow the computation of **random points** on a curve
- Allow the computation of **random elements** of a Jacobian
- Compute **pairings** of hyperelliptic curves

Improving Higher Genus Curves

Generally, hyperelliptic curves are missing many expected functions and Magma is currently superior 🌋 😔

- Allow the computation of **random points** on a curve
- Allow the computation of **random elements** of a Jacobian
- Compute **pairings** of hyperelliptic curves
- Compute **isomorphisms** between curves

Improving Higher Genus Curves

Generally, hyperelliptic curves are missing many expected functions and Magma is currently superior 🌋 😔

- Allow the computation of **random points** on a curve
- Allow the computation of **random elements** of a Jacobian
- Compute **pairings** of hyperelliptic curves
- Compute **isomorphisms** between curves
- Include **Kummer surfaces** and fast arithmetic

Improving Higher Genus Curves

Generally, hyperelliptic curves are missing many expected functions and Magma is currently superior 🌋 😔

- Allow the computation of **random points** on a curve
- Allow the computation of **random elements** of a Jacobian
- Compute **pairings** of hyperelliptic curves
- Compute **isomorphisms** between curves
- Include **Kummer surfaces** and fast arithmetic
- Include **Dixmier Ohno** invariants for (plane quartics)

Including Isogenies in Genus Two

- Currently there is **no support** for isogenies in higher genus

Including Isogenies in Genus Two

- Currently there is **no support** for isogenies in higher genus
- Generally, contributions should be inspired from genus one `EllipticCurveHom`

Including Isogenies in Genus Two

- Currently there is **no support** for isogenies in higher genus
- Generally, contributions should be inspired from genus one `EllipticCurveHom`
- Include **Richelot Isogenies** between Jacobians of hyperelliptic curves

Including Isogenies in Genus Two

- Currently there is **no support** for isogenies in higher genus
- Generally, contributions should be inspired from genus one `EllipticCurveHom`
- Include **Richelot Isogenies** between Jacobians of hyperelliptic curves
- Including **gluing and splitting** isogenies between E1 x E2 and H

Including Isogenies in Genus Two

- Currently there is **no support** for isogenies in higher genus
- Generally, contributions should be inspired from genus one `EllipticCurveHom`
- Include **Richelot Isogenies** between Jacobians of hyperelliptic curves
- Including **gluing and splitting** isogenies between E1 x E2 and H
- Include (2,2)-isogenies using the **theta model**

Including Isogenies in Genus Two

- Currently there is **no support** for isogenies in higher genus
- Generally, contributions should be inspired from genus one `EllipticCurveHom`
- Include **Richelot Isogenies** between Jacobians of hyperelliptic curves
- Including **gluing and splitting** isogenies between E1 x E2 and H
- Include (2,2)-isogenies using the **theta model**
- Evaluation of **eta and theta functions** in genus two

Improvement of Quaternions

- Generally: make **Deuring-like computations easier**

Improvement of Quaternions

- Generally: make **Deuring-like computations easier**
- Allow **sampling of small norm** elements

Improvement of Quaternions

- Generally: make **Deuring-like computations easier**
- Allow **sampling of small norm** elements
- Allow computation of **basis changes**

Improvement of Quaternions

- Generally: make **Deuring-like computations easier**
- Allow **sampling of small norm** elements
- Allow computation of **basis changes**
- Improve **multiplication of ideals**

Improvement of Quaternions

- Generally: make **Deuring-like computations easier**
- Allow **sampling of small norm** elements
- Allow computation of **basis changes**
- Improve **multiplication of ideals**
- Computations of **isomorphisms**

Improvement of Quaternions

- Generally: make **Deuring-like computations easier**
- Allow **sampling of small norm** elements
- Allow computation of **basis changes**
- Improve **multiplication of ideals**
- Computations of **isomorphisms**
- Simple methods such as `is_integral()`, `is_cyclic()`, `is_principal()`

Improvement of Quaternions

- Generally: make **Deuring-like computations easier**
- Allow **sampling of small norm** elements
- Allow computation of **basis changes**
- Improve **multiplication of ideals**
- Computations of **isomorphisms**
- Simple methods such as `is_integral()`, `is_cyclic()`, `is_principal()`
- Inclusion of the **KLPT** algorithm

There will always be more maths

Going Forward

- We will (probably?) not finish **everything** on this wishlist

Going Forward

- We will (probably?) not finish **everything** on this wishlist
- The wishlist is **not complete**

Going Forward

- We will (probably?) not finish **everything** on this wishlist
- The wishlist is **not complete**
- The main hope is that everyone here feels more **confident** to continue contributing

Going Forward

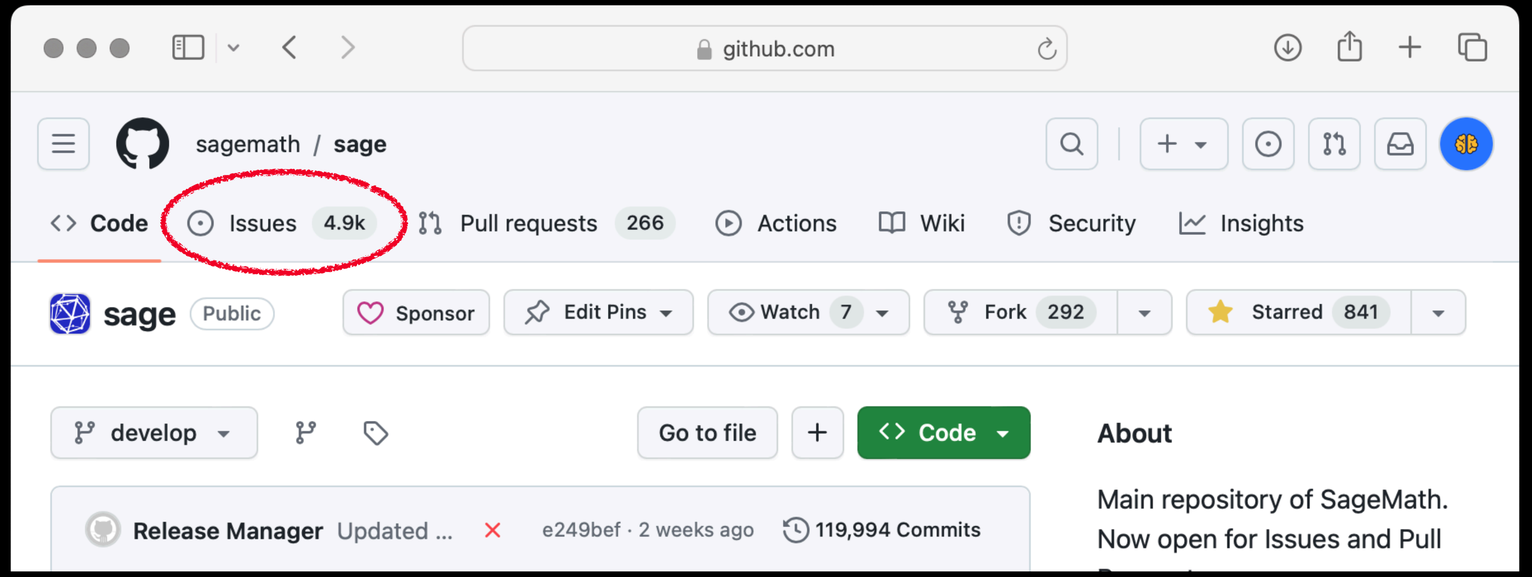
- We will (probably?) not finish **everything** on this wishlist
- The wishlist is **not complete**
- The main hope is that everyone here feels more **confident** to continue contributing
- Sage is a **tool** to aid your research

Going Forward

- We will (probably?) not finish **everything** on this wishlist
- The wishlist is **not complete**
- The main hope is that everyone here feels more **confident** to continue contributing
- Sage is a **tool** to aid your research
- The more you use it, the easier this “**What?**” question will become

Going Forward

- We will (probably?) not finish **everything** on this wishlist
- The wishlist is **not complete**
- The main hope is that everyone here feels more **confident** to continue contributing
- Sage is a **tool** to aid your research
- The more you use it, the easier this “**What?**” question will become
- Do what you can, when you can, if you want to


github.com
sagemath / sage
Code
Issues 4.9k
Pull requests 266
Actions
Wiki
Security
Insights
sage Public
Sponsor
Edit Pins
Watch 7
Fork 292
Starred 841
develop
Go to file
Code
About
Release Manager Updated ...
e249bef · 2 weeks ago
119,994 Commits
Main repository of SageMath.
Now open for Issues and Pull