A Formalizer, a Mathematician, and a Computer Algebra System Walk into a Bar: Bridging Formal and Computational Mathematics

Edgar Costa (MIT)

November 4, 2023, Simons Collaboration Meeting

Slides available at `edgarcosta.org`

Joint work with Alex J. Best, Mario Carneiro, and James Davenport.

What is true?

Question

Do I believe the output from a computer algebra system?

What is true?

Question

Do I believe the output from a computer algebra system?

Theorem

The number $3 \cdot 2^{189} + 1$ *is a prime number.*

Proof 🪄 🎩

```
sage: (3 * 2^189 + 1).is_prime(proof=True)
True
magma > IsPrime(3 * 2^189 + 1 : Proof:=true);
true
gp ? isprime(3 * 2^189 + 1)
%1 = 1
```

What is true?

Theorem

The number $3 \cdot 2^{189} + 1$ is a prime number.

Proof 🪄 ⚡ 🎩 💥

Take $n := 3 \cdot 2^{189} + 1$. It is sufficient to exhibit a such that

$$1 \notin \{a^{(n-1)/2} \bmod n, a^{(n-1)/3} \bmod n\}.$$

```
sage: n = 3 * 2^189 + 1
....: a = Zmod(n)(10)
....: 1 not in [a^((n-1)/2), a^((n-1)/3)]
True
```

Since n is a proth number, it is enough exhibit a such that $a^{(n-1)/2} \equiv -1 \bmod n$.

There several other possible prime certificates.

What is true?

Theorem

The class group of $K := \mathbb{Q}(\sqrt{5}, \sqrt{-231}) =$ 4.0.1334025.9 is $C_2 \times C_2 \times C_{12}$.

Proof 🪄 🎩

```
sage: K.class_group().invariants()
(12, 2, 2)
magma> Invariants(ClassGroup(K));
[ 2, 2, 12 ]
julia> class_group(K)[1]
GrpAb: (Z/2)^2 x Z/12
```

Proof 🪄 ⚡ 🎩 💥

```
magma> Degree(HilbertClassField(K));
48
☠️ segmentation fault (core dumped)
```

What is true?

$$C_1 : y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45$$

$$C_2 : y^2 + xy = -x^5 + 2573x^4 + 92187x^3 + 2161654285x^2 + 406259311249x + 93951289752862$$

Theorem

There is an isogeny of degree 31^2 between $\mathrm{Jac}(C_1)$ and $\mathrm{Jac}(C_2)$.

Proof 🪄 🎩 3h

Compute the isogeny class via Bommel–Chidambaram–Costa–Kieffer:

```
sage -python genus2isogenies.py ...
```

Proof 🪄 ⚡ 🎩 💥 6.5h

Produce a divisor in $C_1 \times C_2$ via Costa–Mascot–Sijsling–Voight:

```
magma> Correspondence(C1, C2, heuristic_isogeny);
...
```

Spectrum of options

- 📜 Generate certificates of correctness a posteriori
  - Primality proving
  - Homomorphisms between Jacobians
  - LLL lattice basis reduction

Spectrum of options

- 📜 Generate certificates of correctness a posteriori
  - Primality proving
  - Homomorphisms between Jacobians
  - LLL lattice basis reduction
- ⚙️ Formalize the algorithm
  - Smith and Hermite normal form
  - Factorisation over $\mathbb{Z}[x]$
  - LLL lattice basis reduction algorithm
  - Tate's algorithm

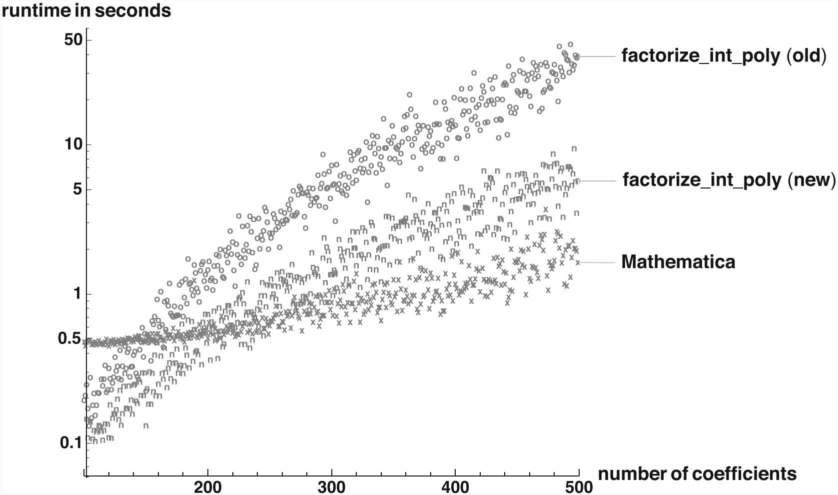
Spectrum of options

- Generate certificates of correctness a posteriori
  - Primality proving
  - Homomorphisms between Jacobians
  - LLL lattice basis reduction
- Formalize the algorithm
  - Smith and Hermite normal form
  - Factorisation over $\mathbb{Z}[x]$
  - LLL lattice basis reduction algorithm
  - Tate's algorithm
- By pure thought generate an alternative proof

Spectrum of options

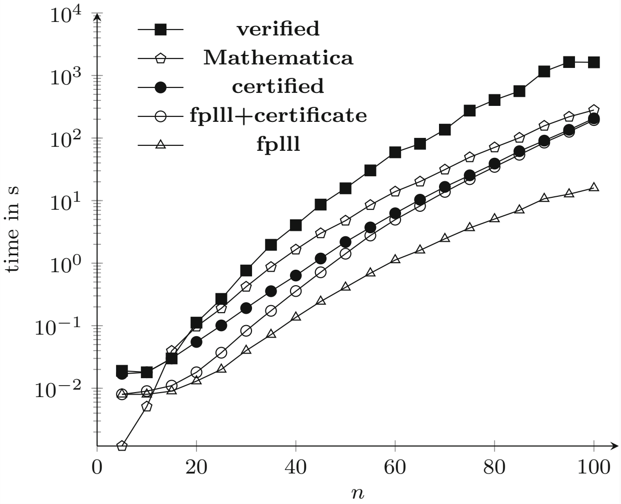
- 📜 Generate certificates of correctness a posteriori
  - Primality proving
  - Homomorphisms between Jacobians
  - LLL lattice basis reduction
- ⚙️ Formalize the algorithm
  - Smith and Hermite normal form
  - Factorisation over $\mathbb{Z}[x]$
  - LLL lattice basis reduction algorithm
  - Tate's algorithm
- 🪄 By pure thought generate an alternative proof
  - a magician never reveals their secrets

Formalization of factorization over $\mathbb{Z}[x]$



by Divasón–Joosten–Thiemann–Yamada

LLL lattice basis reduction algorithm



by Thiemann–Bottesch–Divasón–Haslbeck–Joosten–Yamada

Tate's algorithm (work in progress by Best–Dahmen–Huriot-Tattegrain)

- Some of the output is out of reach to be formalized:
    - Kodaira symbol
    - Conductor exponent
    - Tamagawa number
    - ...
- They verified that the algorithm terminates under some mild assumptions
- Works in characteristic 2 and 3
- Verified output for some explicit families, e.g., $y^2 = x^3 + p$ gives I_1 for $p > 5$
- Verified the local data on LMFDB (~ 13 million curves) in ~ 10 minutes
- Future: show that the output is invariant under change of coordinates

The sweet spot

- Generate bread crumbs for a certificate along the way
  - Primality testing via elliptic curves
  - Factorisation over $\mathbb{Z}[x]$
  - Class group computation?
- Generate certificates of correctness a posteriori
  - Primality proving
  - Homomorphisms between Jacobians
  - LLL lattice basis reduction algorithm
- Formalize the algorithm
  - Smith and Hermite normal form
  - Factorisation over $\mathbb{Z}[x]$
  - LLL lattice basis reduction algorithm
  - Tate's algorithm
- By pure thought generate an alternative proof
  - a magician never reveals their secrets

🍯 Factorisation over $\mathbb{Z}[x]$ (Best–Carneiro–Costa–Davenport)

Theorem (Mignotte)

Take $f, g \in \mathbb{Z}[X]$, and let $n = \deg f$. If g divides f, then

$$\|g\|_\infty \leq \binom{n-1}{\lceil n/2 \rceil}(\|f\|_2 + lc(f)) =: B_f$$

🍯 Factorisation over $\mathbb{Z}[x]$ (Best–Carneiro–Costa–Davenport)

Theorem (Mignotte)

Take $f, g \in \mathbb{Z}[X]$, and let $n = \deg f$. If g divides f, then

$$\|g\|_\infty \leq \binom{n-1}{\lceil n/2 \rceil}(\|f\|_2 + lc(f)) =: B_f$$

To show that f is irreducible, is enough to give a factorization of f over $\mathbb{Z}/p^e[x]$, with $p^e > 2B_f + 1$, such that no nontrivial factor lifts as a factor of f over $\mathbb{Z}[x]$.

Such factorization is free! Already part of the factorization algorithm.

🍯 Factorisation over $\mathbb{Z}[x]$ (Best–Carneiro–Costa–Davenport)

To show that f is irreducible, is enough to give a factorization of f over $\mathbb{Z}/p^e[x]$, with $p^e > 2B_f + 1$, such that no nontrivial factor lifts as a factor of f over $\mathbb{Z}[x]$.

Such factorization is free! Already part of the factorization algorithm.

Theorem

$f := x^6 - 3x^5 + 5x^4 - 5x^3 + 5x^2 - 3x + 1$ *is irreducible*

Proof 🍯

🖼️
```
sage: f.is_irreducible()
True
```

🍯 Factorisation over $\mathbb{Z}[x]$ (Best–Carneiro–Costa–Davenport)

To show that f is irreducible, is enough to give a factorization of f over $\mathbb{Z}/p^e[x]$, with $p^e > 2B_f + 1$, such that no nontrivial factor lifts as a factor of f over $\mathbb{Z}[x]$.

Such factorization is free! Already part of the factorization algorithm.

Theorem

$f := x^6 - 3x^5 + 5x^4 - 5x^3 + 5x^2 - 3x + 1$ *is irreducible*

Proof 🍯

🖼️
```
sage: f.is_irreducible()
True
```

🔎 🎁 Over $\mathbb{Z}/3^e[x]$ f factors as $g \cdot h$, with $\deg g = \deg h = 3$

⚙️ the putative lifts to $\mathbb{Z}[x]$ do not divide f

Factorisation over $\mathbb{Z}[x]$ (Best–Carneiro–Costa–Davenport)

Theorem

$f := x^6 - 3x^5 + 5x^4 - 5x^3 + 5x^2 - 3x + 1$ *is irreducible*

Proof

```
sage: f.is_irreducible()
True
```

- Over $\mathbb{Z}/3^e[x]$ f factors as $g \cdot h$, with $\deg g = \deg h = 3$
- the putative lifts to $\mathbb{Z}[x]$ do not divide f

Our goal is to build a *tactic* in lean to automatically generate such formal proofs.

🍯 Factorisation over $\mathbb{Z}[x]$ (Best–Carneiro–Costa–Davenport)

Theorem

$f := x^6 - 3x^5 + 5x^4 - 5x^3 + 5x^2 - 3x + 1$ *is irreducible*

Proof 🍯

🖼️
```
sage: f.is_irreducible()
True
```

🔎 🎁 Over $\mathbb{Z}/3^e[x]$ f factors as $g \cdot h$, with $\deg g = \deg h = 3$

⚙️ the putative lifts to $\mathbb{Z}[x]$ do not divide f

Our goal is to build a *tactic* in lean to automatically generate such formal proofs.

Can we do a similar thing for class group computations? 🧸