M2 AAG
Algorithms in number theory

Kevin Destagnol, Chimène & Stéphane Fischler

LMO, Université Paris-Saclay

January 26 2026

Course information

- lecture :
  - 2h every Wednesday
  - 10am-12pm, room 1A12
  - theoretical part
  - Heads up: first lecture on February 4 !
- practical session :
  - 2h every other Thursday
  - 4:15pm-6:15pm, room 0E4
  - first session on January 26
  - coding in Sagemath (based on Python)
  - No prerequisite in coding nor in Sagemath
- Lectures notes will be provided

Grading

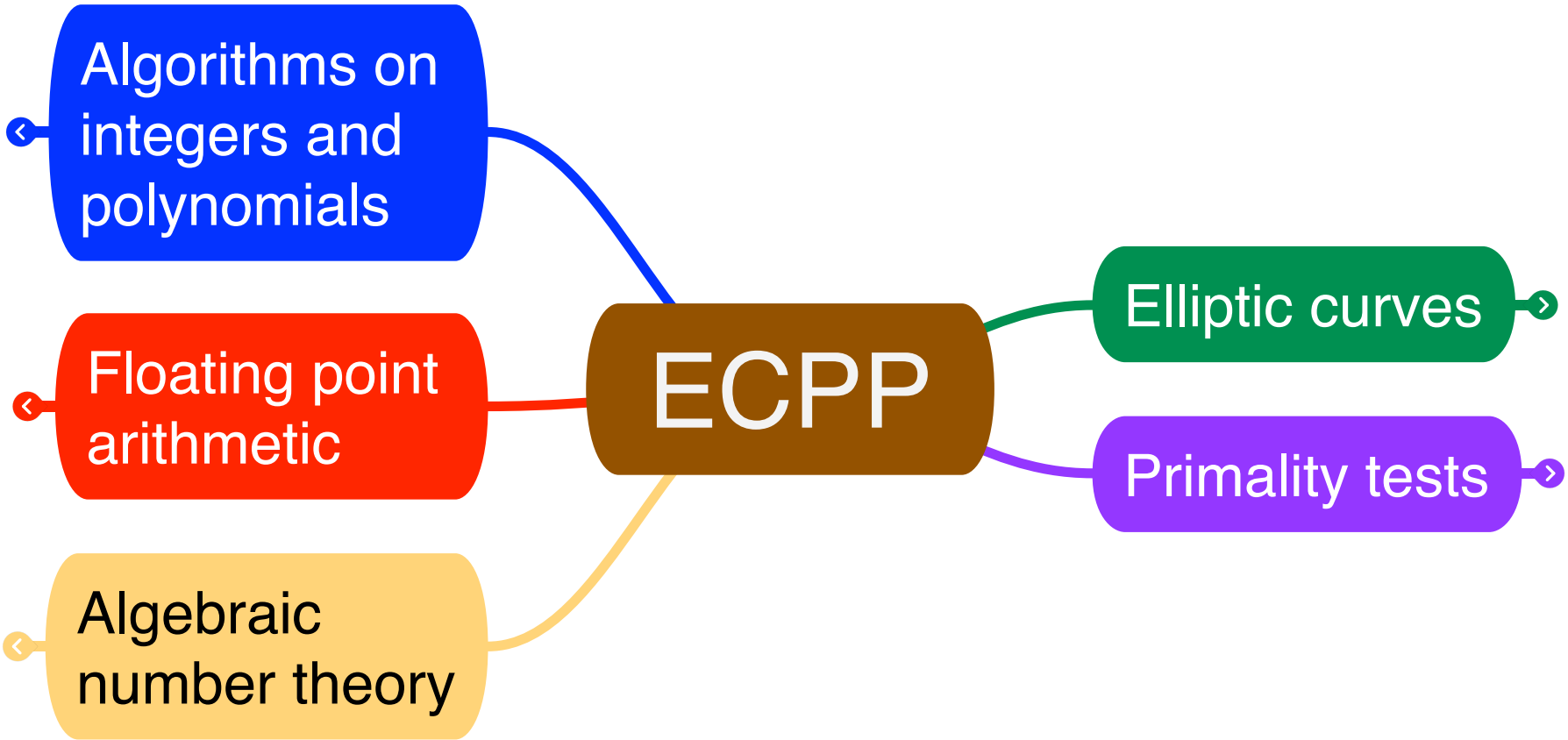
- Coding test:
  - 20% of the total grade
  - Implementing easy algorithms in Sagemath
  - No internet access
  - Sagemath online help and lecture notes available
- Lecture :
  - 80% of the total grade
  - Presentation during a "special seminar" with all students
  - About a specific algorithm
  - Written notes of your work (including coding part)

Content

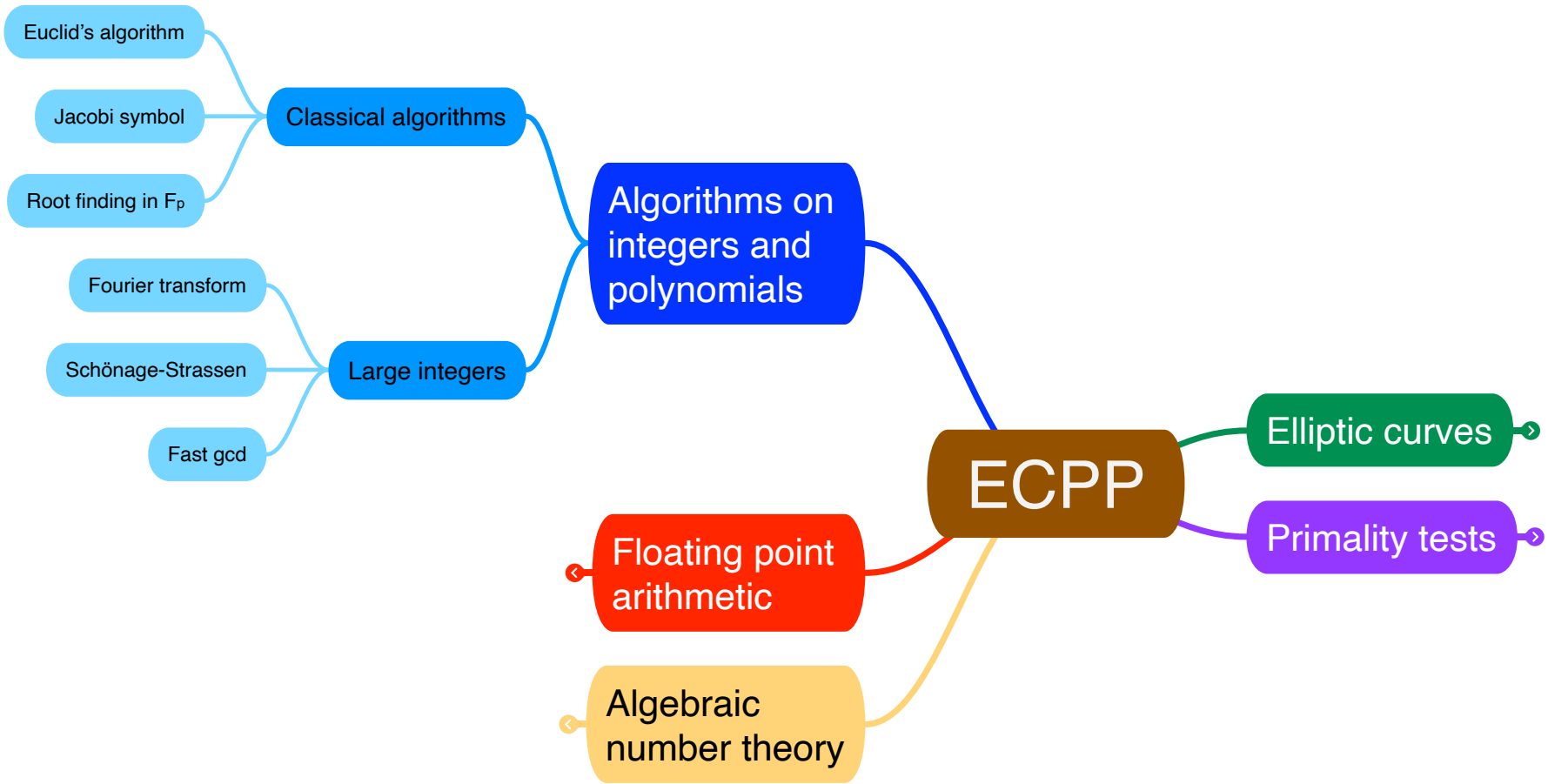
- Tools:
  - Algorithms on integer and polynomials
  - Floating point arithmetic
  - Elliptic curves (including complex multiplication and Hilbert class polynomial)
- Primality tests
- Factorization
- Discrete logarithm

Elliptic Curves Primality Proving: tools involved

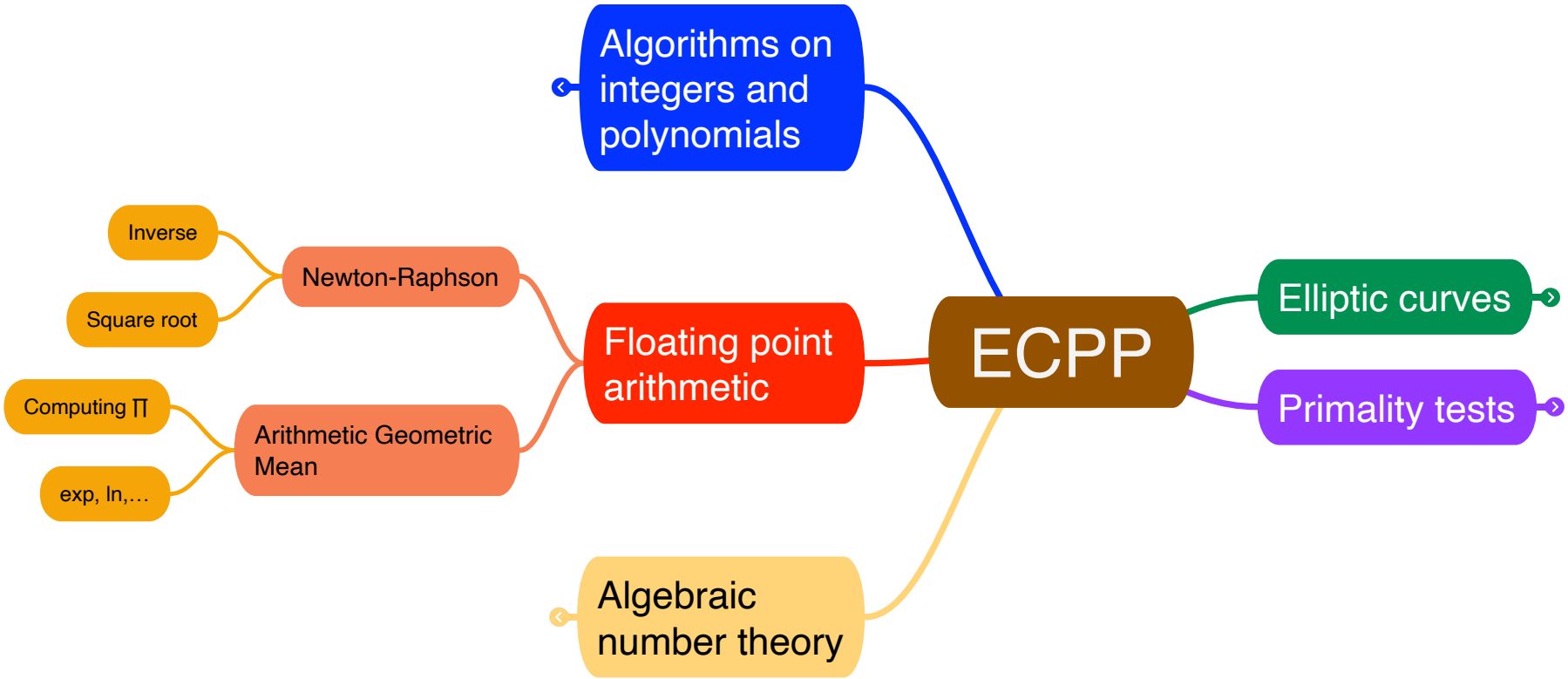
Elliptic Curves Primality Proving: tools involved



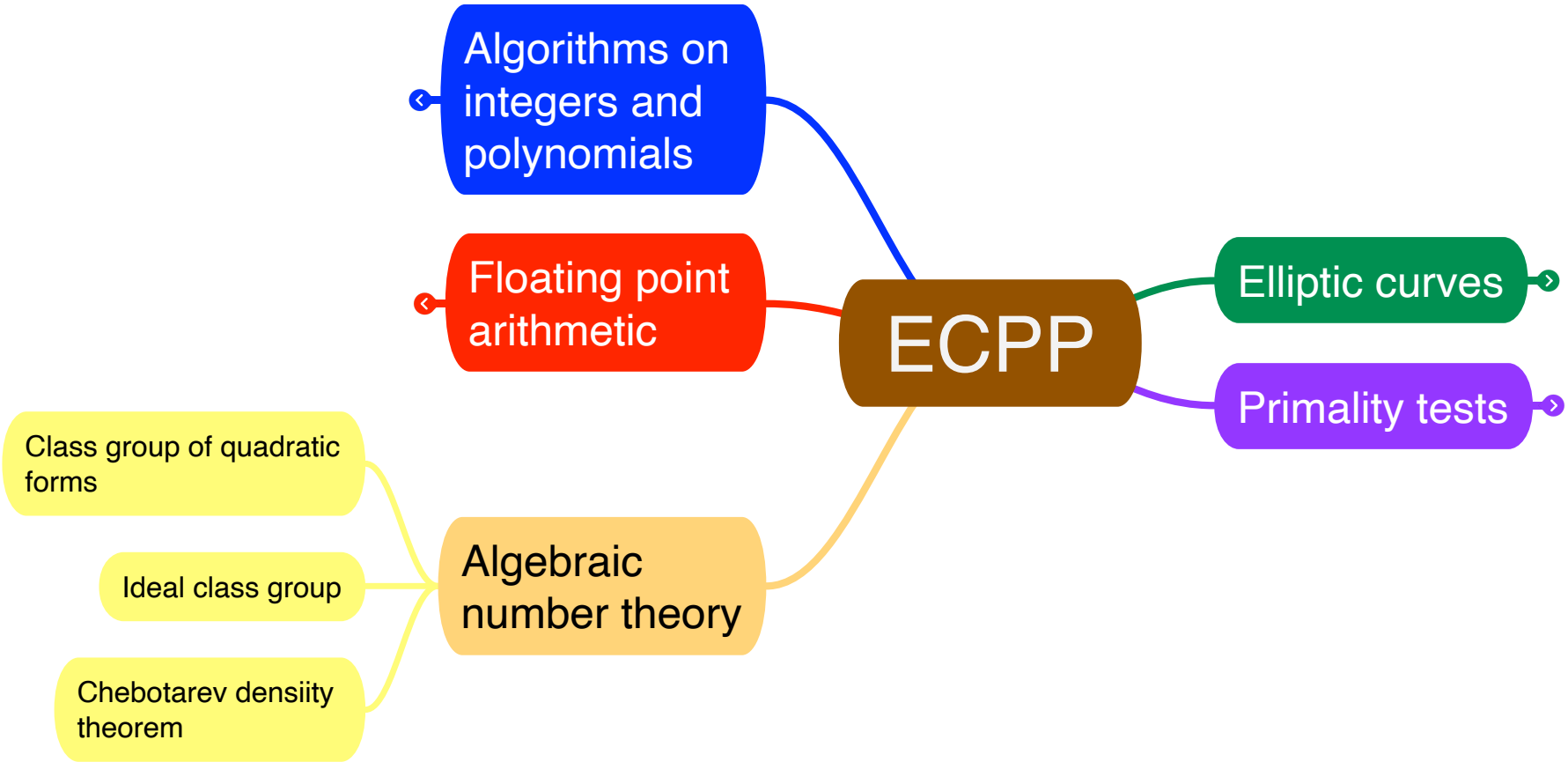
Elliptic Curves Primality Proving: tools involved



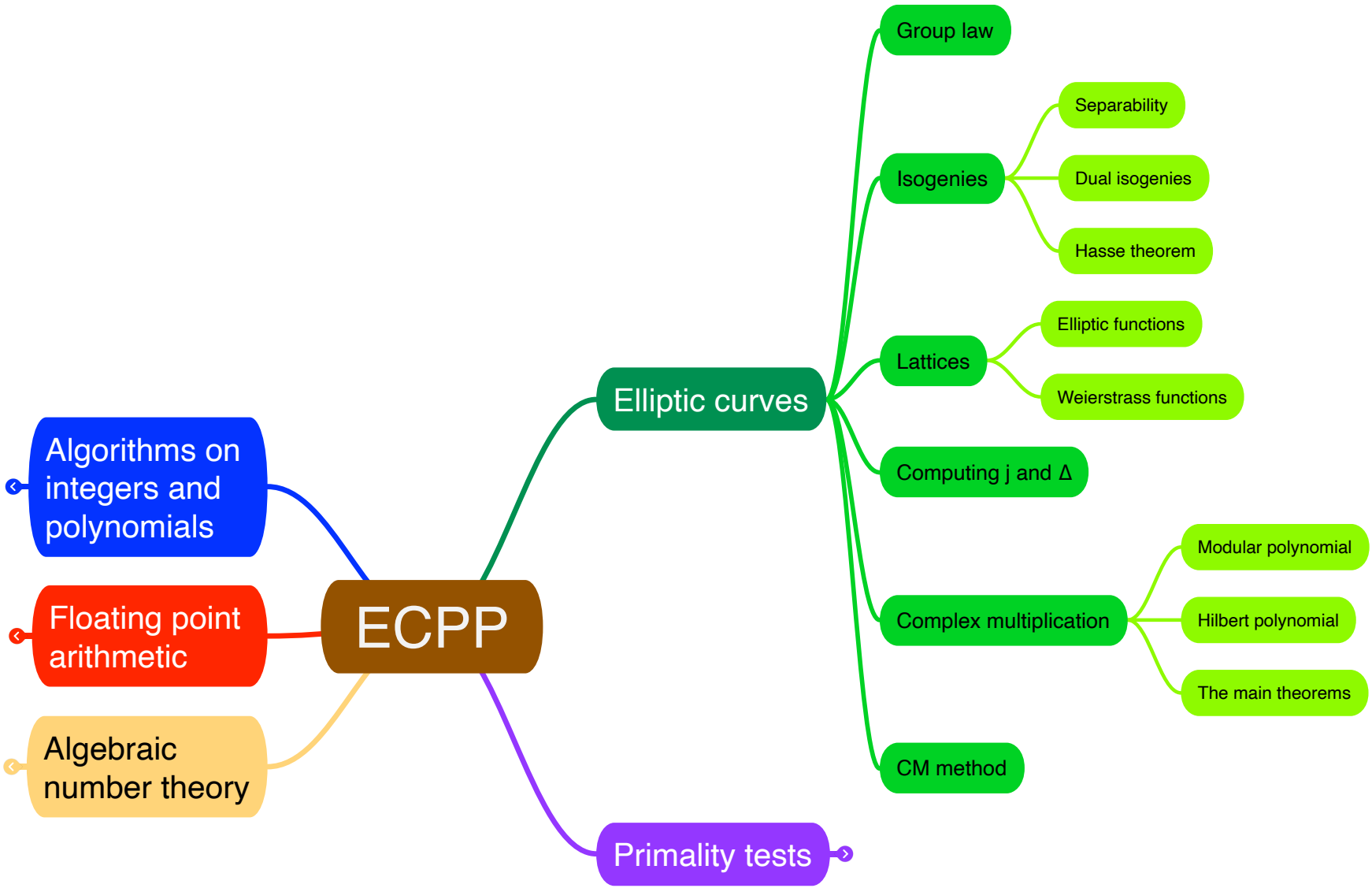
Elliptic Curves Primality Proving: tools involved



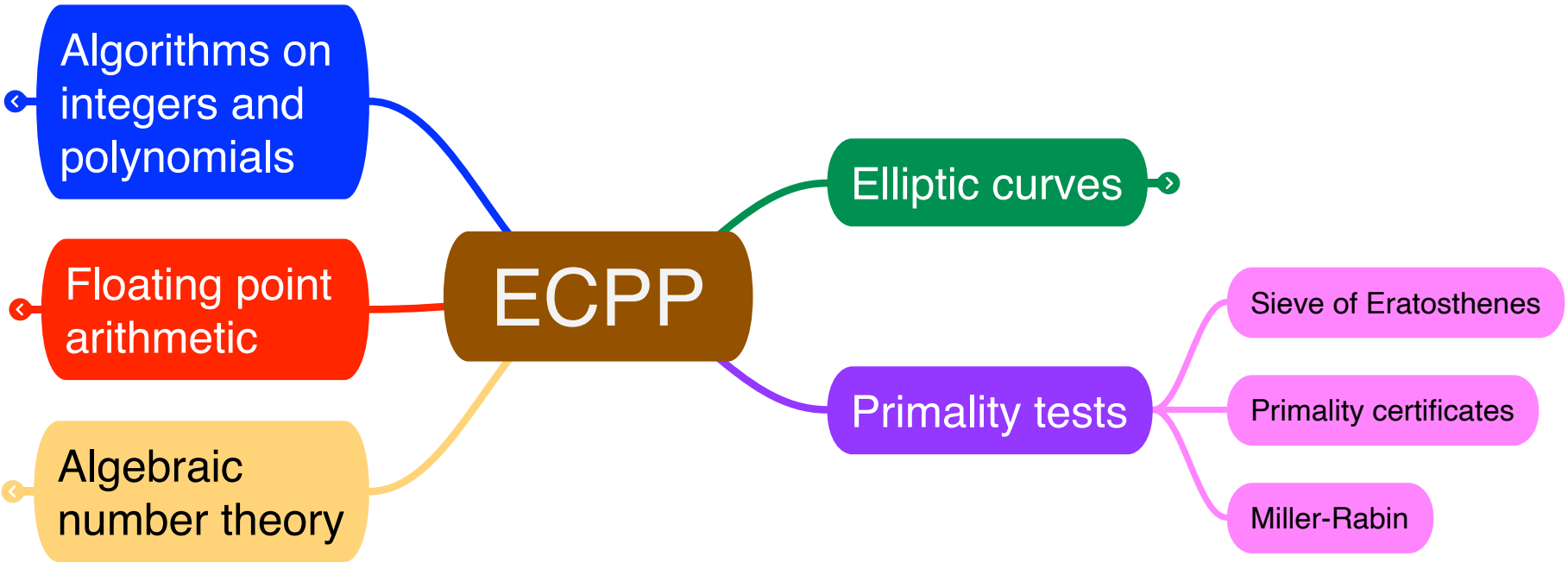
Elliptic Curves Primality Proving: tools involved



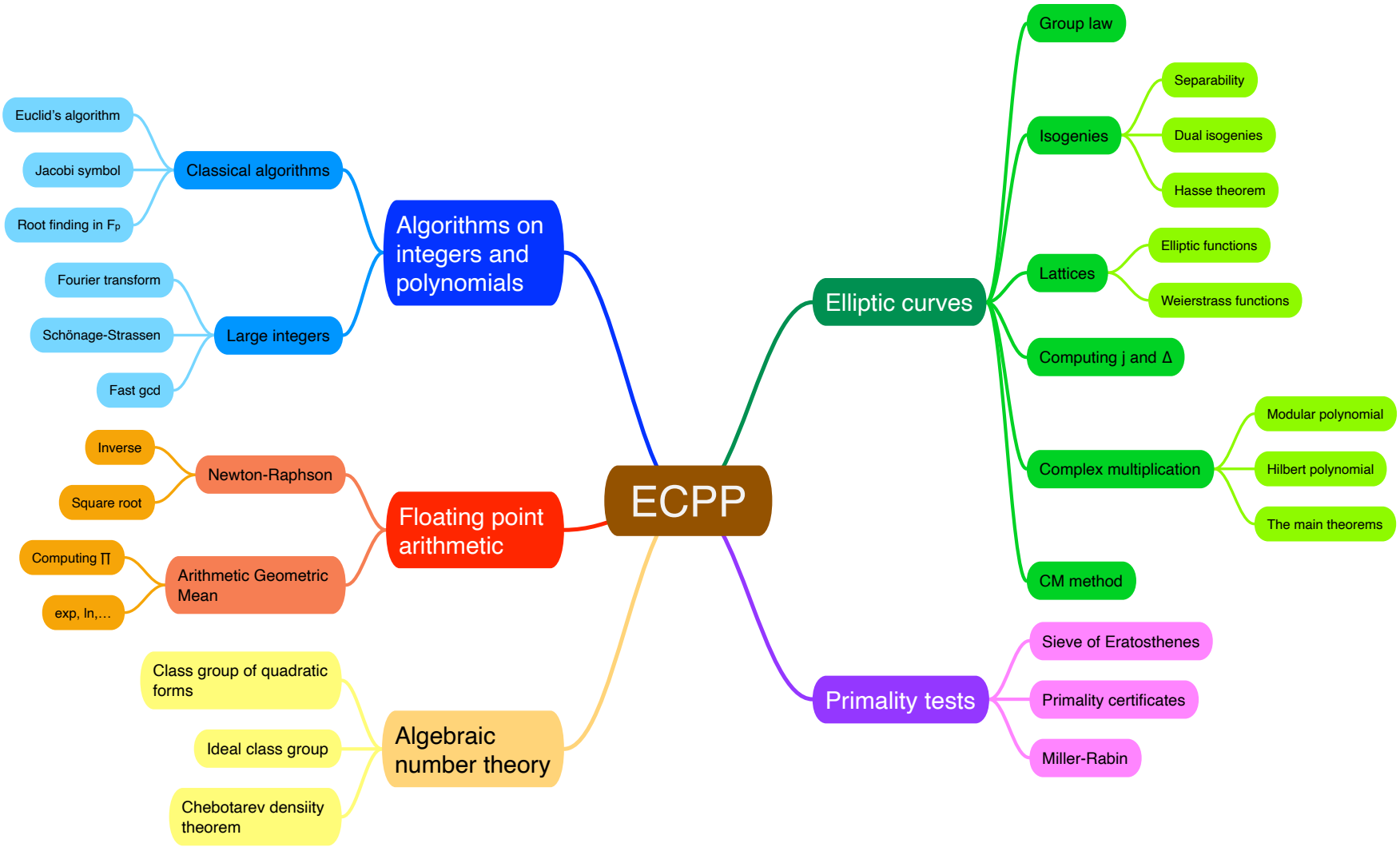
Elliptic Curves Primality Proving: tools involved



Elliptic Curves Primality Proving: tools involved



Elliptic Curves Primality Proving: tools involved



An example of fast ECPP

We want to test:
$N = 2027$

An example of fast ECPP

We take 2 prime numbers:

$q_1^* = (-1)^{\frac{7-1}{2}} \cdot 7 = -7, \quad q_2^* = (-1)^{\frac{13-1}{2}} \cdot 13 = 13$

such that they are squares: $\left(\frac{-7}{2027}\right) = \left(\frac{13}{2027}\right) = 1$

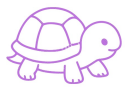
Let $D = q_1^* \cdot q_2^* = -7 \cdot 13 = -91 < 0$

An example of fast ECPP

Using Cornacchia's algorithm, we find:
$U = 88, V = 2$ such that
$4 \cdot N = 4 \cdot 2027 = U^2 - D \cdot V^2 = 88^2 + 91 \cdot 2^2$
Let $m = 2027 + 1 - U = 1940$
Then its smooth part is $c = 20 > 1$
and let $N' = 97 > \sqrt{2027}$ such that $m = c \cdot N'$

An example of fast ECPP

$N' = 97$ is pseudo-prime by Miller-Rabin primality test

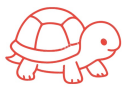


An example of fast ECPP

We compute the class group of quadratic forms of discriminant $D = -91$

An example of fast ECPP

We compute the Hilbert polynomial:
$H_{-91}(X) = X^2 + 10359073013760X - 3845689020776448$



An example of fast ECPP

In $\mathbb{F}_{2027}[X]$, we have:

$H = H_{-91}(X) = X^2 + 1440X + 1795$

We find a root of H: $j = 477$

An example of fast ECPP

Following the CM-method, we have:

$a = 3 \cdot j \cdot (1728 - j) = 340$

$b = 2 \cdot j \cdot (1728 - j)^2 = 1807$

As $\left(\frac{2}{2027}\right) = -1$, $s = 2$ is not a square

so $a' = s^2 \cdot a = 1360$, $b' = s^3 \cdot b = 267$

An example of fast ECPP

We take randomly: $x = 25$
so $y_2 = x^3 + ax + b = 1608$ and $\left(\frac{y_2}{2027}\right) = 1$
we take the square root of y_2: $y = 836$
$M = [25 : 836 : 1] \in E$ where $(E) : y^2 = x^3 + ax + b$
$M' = [20]M = [377 : 1497 : 1] \neq O$ and
$[N']M' = [97]M' = [1959 : 396 : 1] \neq O$
Failure !

An example of fast ECPP

We try again with the quadratic twist:
$x' = 25$ so $y_2' = x'^3 + a'x' + b' = 1244$ and $\left(\frac{y_2'}{2027}\right) = 1$
we take the square root of y_2': $y' = 381$
$M = [25 : 381 : 1] \in E'$ where $(E') : y^2 = x^3 + a'x + b'$
$M' = [20]M = [1297 : 1437 : 1] \neq O$ and $[N']M' = [97]M' = O$

An example of fast ECPP

Thus $N = 2027$ is prime if $N' = 97$ is prime !

An example of fast ECPP

We start again from scratch with $N = 97$!

An example of fast ECPP

We start again from scratch with $N = 97$!

Website

https://www.imo.universite-paris-saclay.fr/~stephane.fischler/ens/M2.html