# Primality Proving with Elliptic Curves

Laurent Théry
Marelle Project

# Prime Number

Inductive $\mathbb{N}$ := `O`: $\mathbb{N}$ | `S` $(n : \mathbb{N}) : \mathbb{N}$

Definition $m + n$ := if $m$ is `S` $m'$ then `S` $(m' + n)$ else $n$

Definition $m * n$ := if $m$ is `S` $m'$ then $n + (m' * n)$ else `O`

Definition $m \mid n$ := $\exists q,\ n = q * m$

Definition prime $p$ := $\forall m,\ m \mid p \Rightarrow m = 1 \lor m = p$

$\land \quad p \neq 1$

INRIA

# Prime Number

```
Theorem ex₁:   prime 1234567891.
Proof.
```

```
Qed.
```

# Fermat little theorem

| | | | | | | |
|---|---|---|---|---|---|---|
| $b_{k-1}$ | $b_{k-1}a$ | $b_{k-1}a^2$ | $\dots$ | $b_{k-1}a^i$ | $\dots$ | $b_{k-1}a^{m-1}$ |
| $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ |
| $b_i$ | $b_ia$ | $b_ia^2$ | $\dots$ | $b_ia^i$ | $\dots$ | $b_ia^{m-1}$ |
| $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ | $\dots$ |
| $b_1$ | $b_1a$ | $b_1a^2$ | $\dots$ | $b_1a^i$ | $\dots$ | $b_1a^{m-1}$ |
| $1$ | $a$ | $a^2$ | $\dots$ | $a^i$ | $\dots$ | $a^{m-1}$ |

$$a^m = 1 \bmod n$$

$$a^{n-1} = a^{mk} = (a^m)^k = 1 \bmod n$$

# Pocklington Certificate

$m$ is the order of $a$:

$$a^m = 1 \;\texttt{mod}\; n \wedge \forall k, k \,|\, m \Rightarrow a^{m/k} \neq 1 \;\texttt{mod}\; n$$

Projection from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ $\quad (p \,|\, n)$:

$$gcd(u, n) = 1 \wedge u \neq 0 \;\texttt{mod}\; n \Rightarrow u \neq 0 \;\texttt{mod}\; p$$

# Pocklington Certificate

Let $N$ be an integer. Assume that there exists $a$ coprime to $n$ and $m$ such that

$$a^m = 1 \bmod n$$

$$\forall p,\ \texttt{prime}\, p \ \wedge \ p \,|\, m \ \Rightarrow \ gcd(a^{m/p} - 1, n) = 1$$

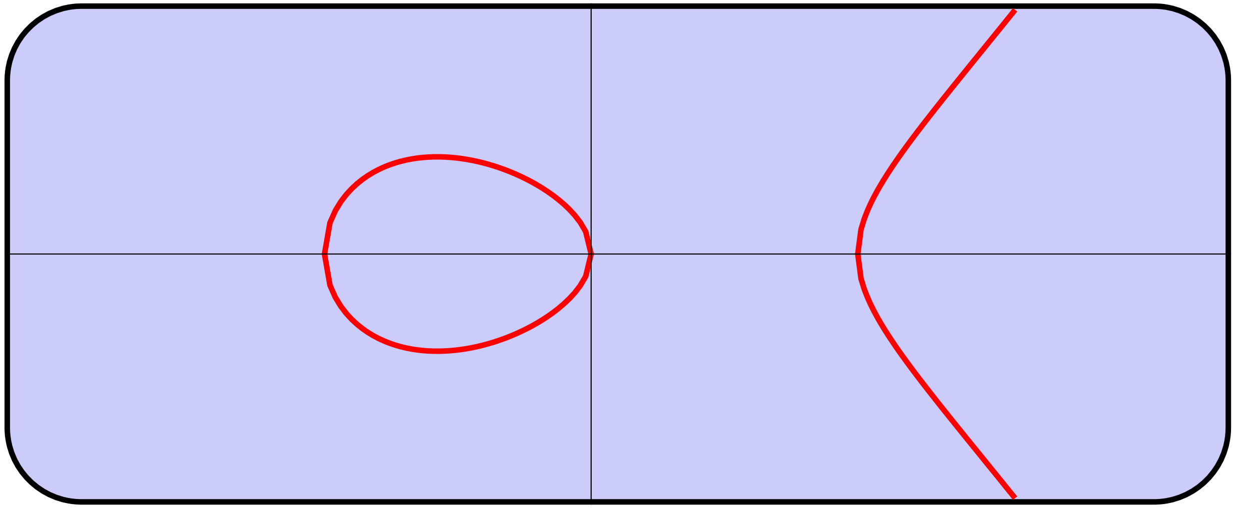
Then, if $m \geq \sqrt{n}$, $n$ is prime.

# Elliptic Curve

Cubic curve:

$y^2 = x^3 + Ax + B \qquad (4A^3 + 27B^2 \neq 0)$

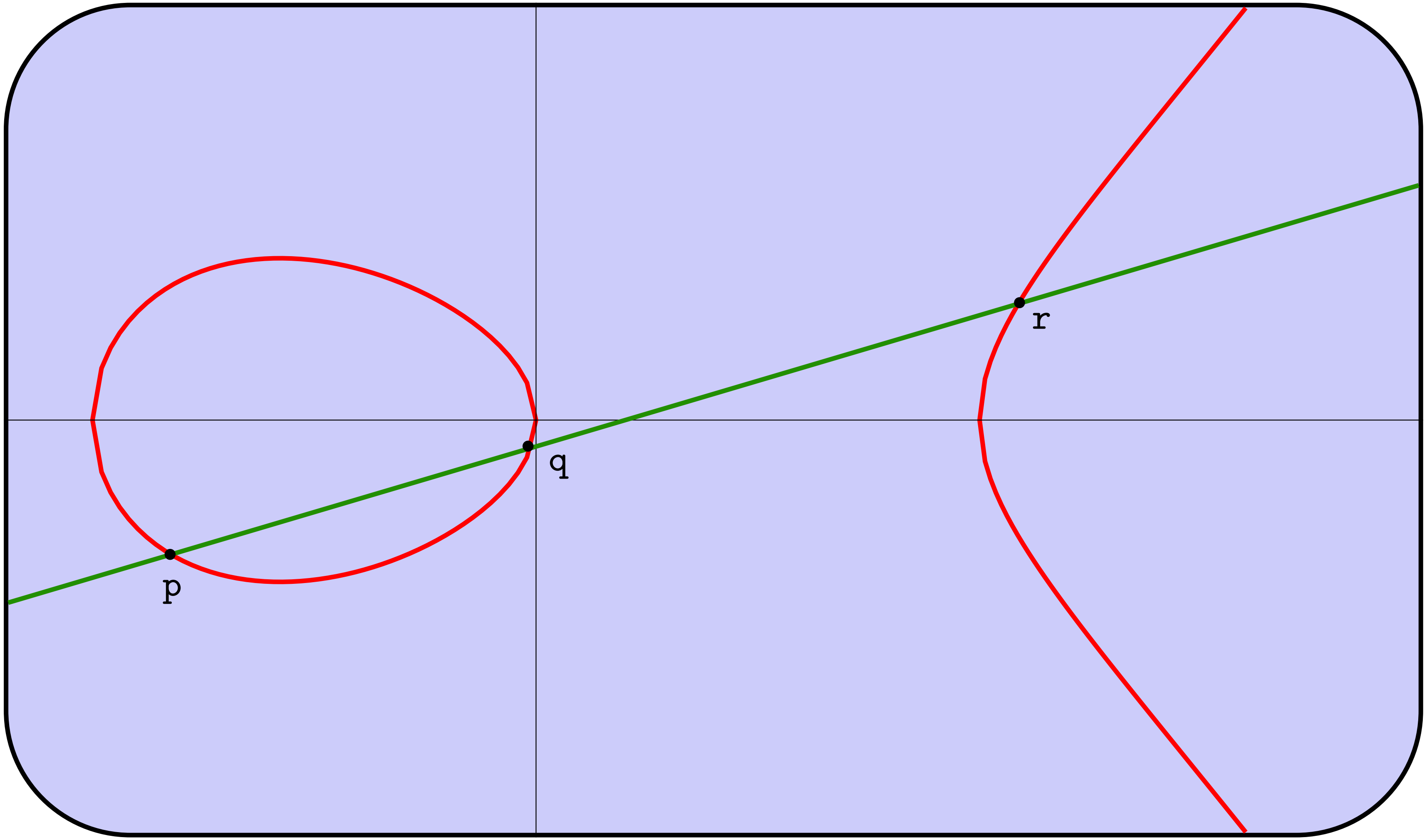
Example: $y^2 = x^3 - x$



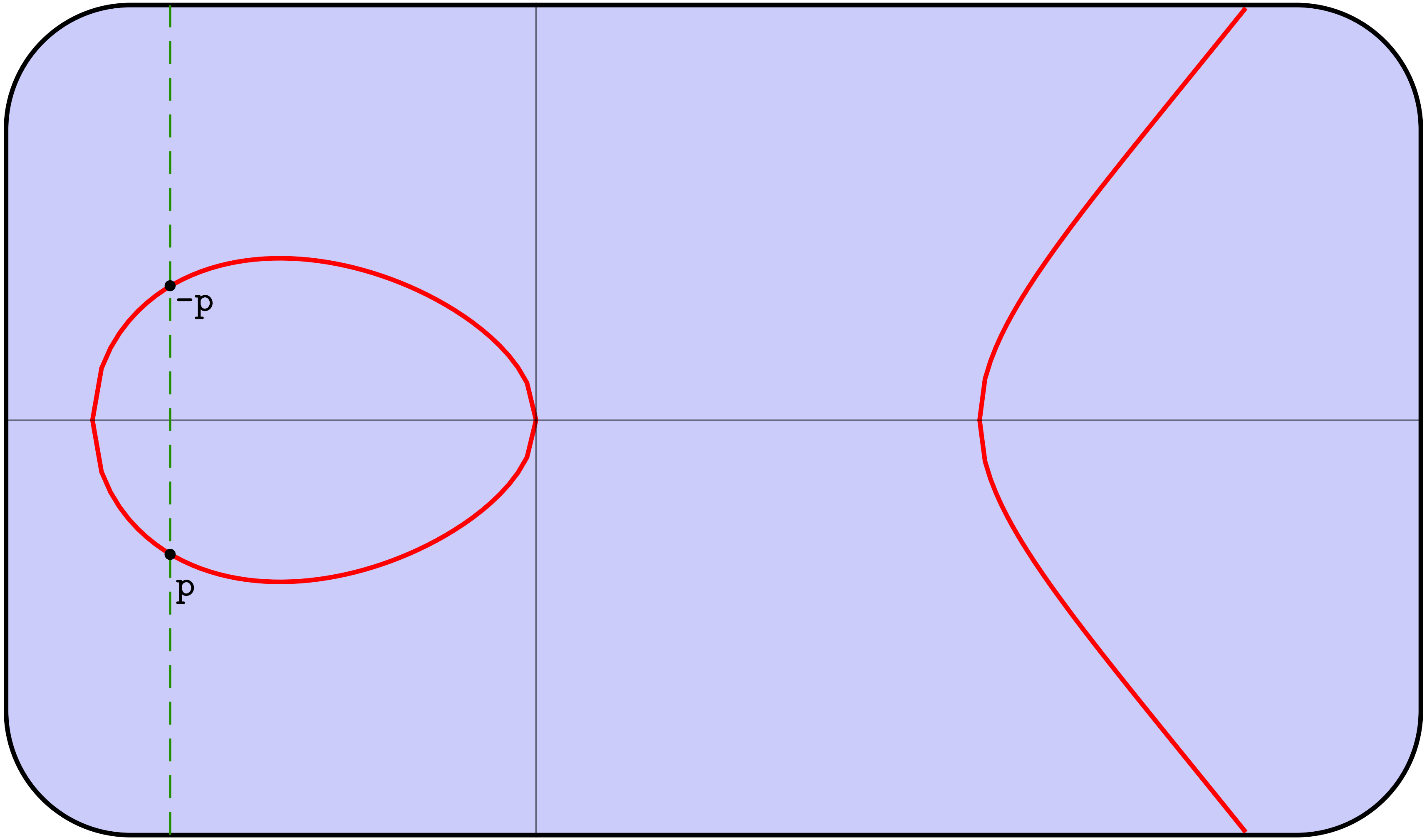
# Formalisation

```
Inductive elt: Set :=
| inf_elt: elt
| curve_elt (x: K) (y: K) (H: y^2 = x^3 + A * x + B): elt.
```

# Elliptic Curve



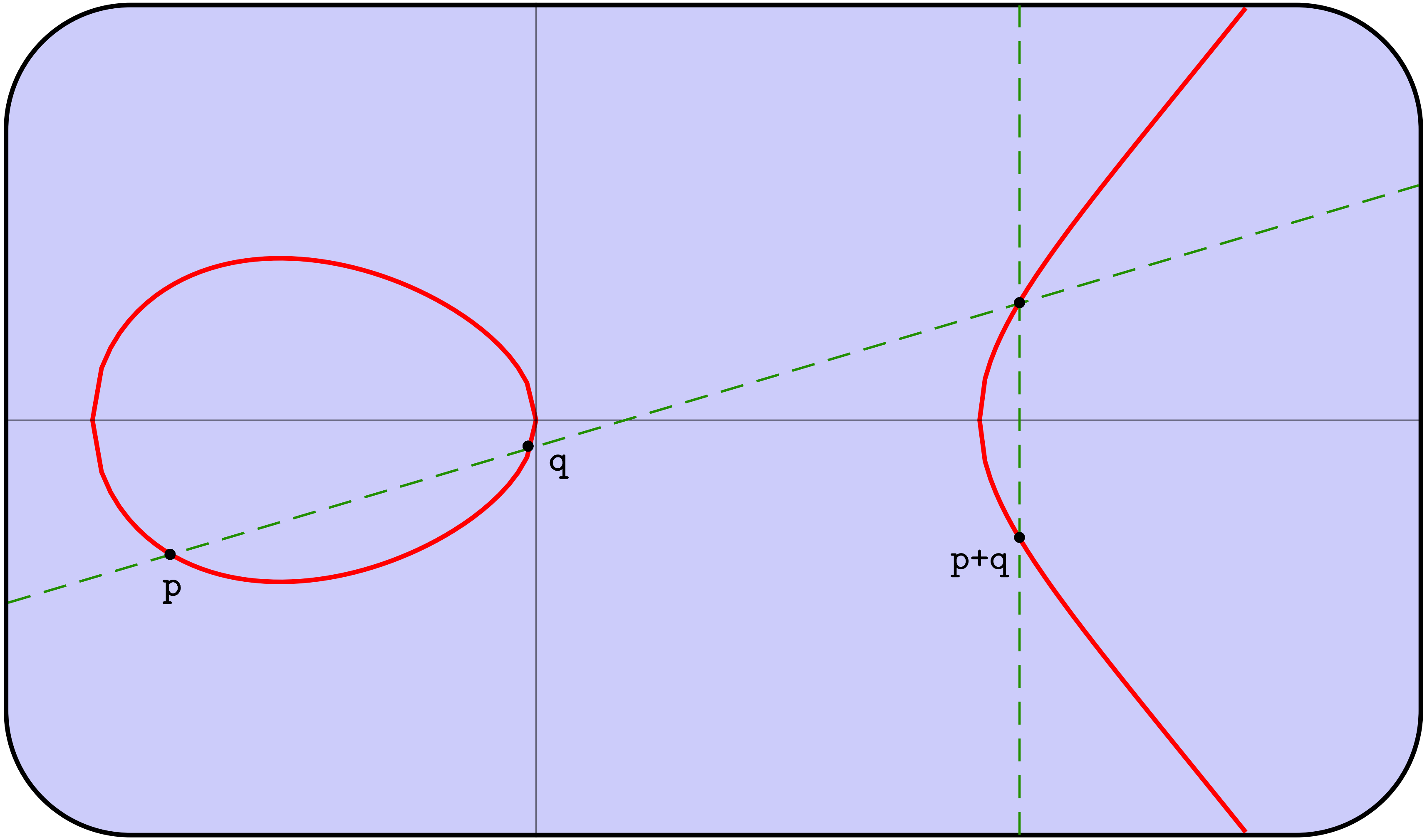
# Elliptic Curve



# Formalisation

```
Definition -p :=
  match p with
  | inf_elt ⇒ inf_elt
  | curve_elt x y H ⇒ curve_elt x (-y) opp_lem
  end.
```

# Elliptic Curve



# Formalisation

```
Definition p₁ + p₂ :=
  match p1, p2 with
  | inf_elt, _ ⇒ p₂
  | _, inf_elt ⇒ p₁
  | curve_elt x₁ y₁ H₁, curve_elt x₂ y₂ H₂ ⇒
    if x₁ == x₂ then
      if (y₁ == -y₂) then inf_elt else
      let l = (3 * x₁² + A)/(2 * y1) in
      let x₃ = l² - 2 * x₁ in
      curve_elt x₃ (-y₁ - l * (x₃ - x₁)) add_lem₁          ⊕t
    else
      let l = (y₂ - y₁)/(x₂ - x₁) in
      let x₃ = l² - x₁ - x₂ in
      curve_elt x₃ (-y₁ - l * (x₃ - x₁)) add_lem₂          ⊕g
```

# Formalisation

(`elt`, +) is a commutative group

The difficult part: $p_1 + (p_2 + p_3) = (p_1 + p_2) + p_3$

Reduce to $p_1 \oplus (p_2 \oplus p_3) = (p_1 \oplus p_2) \oplus p_3$

Further reduce to

1. $p_1 \oplus_g (p_2 \oplus_g p_3) = (p_1 \oplus_g p_2) \oplus_g p_3$.
2. $p_1 \oplus_g (p_2 \oplus_t p_2) = (p_1 \oplus_g p_2) \oplus_g p_2$.
3. $p_1 \oplus_g (p_1 \oplus_g (p_1 \oplus_t p_1)) = (p_1 \oplus_t p_1) \oplus_t (p_1 \oplus_t p_1)$
4. $p_1 \oplus_g (p_2 \oplus_g (p_1 \oplus_g p_2)) = (p_1 \oplus_g p_2) \oplus_t (p_1 \oplus_g p_2)$

# Explicit computation

$$
\begin{aligned}
& y^2 = x^3 + Ax + B && \wedge \\
& l = (3x^2 + A)/2y && \wedge \\
& x_1 = l^2 - 2x && \wedge \\
& y_1 = -y - l(x_1 - x) && \wedge \\
\Rightarrow\quad & y_1^2 = x_1^3 + Ax_1 + B &&
\end{aligned}
$$

Common denominator:

$$2^{10}y^8 - 2^{10}y^6x^3 - 2^{10}Ay^6x - 2^{10}By^6 = 0$$

# Explicit computation

Common denominator:

$$2^{10}y^8 - 2^{10}y^6x^3 - 2^{10}Ay^6x - 2^{10}By^6 = 0$$

Rewriting:

$$2^{10}(x^3 + Ax + B)^4 - 2^{10}(x^3 + Ax + B)^3x^3$$
$$-2^{10}A(x^3 + Ax + B)^3x - 2^{10}B(x^3 + Ax + B)^3 = 0$$

Ring Equality: Qed

# First equation

$$
\begin{array}{lll}
 & \mathtt{x}_1 - \mathtt{x}_2 \neq 0 & \wedge \\
 & \mathtt{x}_4 - \mathtt{x}_3 \neq 0 & \wedge \\
 & \mathtt{x}_2 - \mathtt{x}_3 \neq 0 & \wedge \\
 & \mathtt{x}_5 - \mathtt{x}_1 \neq 0 & \wedge \\
 & \mathtt{y}_1^2 = \mathtt{x}_1^3 + \mathtt{A} * \mathtt{x}_1 + \mathtt{B} & \wedge \\
 & \mathtt{y}_2^2 = \mathtt{x}_2^3 + \mathtt{A} * \mathtt{x}_2 + \mathtt{B} & \wedge \\
 & \mathtt{y}_3^2 = \mathtt{x}_3^3 + \mathtt{A} * \mathtt{x}_3 + \mathtt{B} & \wedge \\
 & \mathtt{x}_4 = (\mathtt{y}_1 - \mathtt{y}_2)^2/(\mathtt{x}_1 - \mathtt{x}_2)^2 - \mathtt{x}_1 - \mathtt{x}_2 & \wedge \\
 & \mathtt{y}_4 = -(\mathtt{y}_1 - \mathtt{y}_2)/(\mathtt{x}_1 - \mathtt{x}_2) * (\mathtt{x}_4 - \mathtt{x}_1) - \mathtt{y}_1 & \wedge \\
 & \mathtt{x}_6 = (\mathtt{y}_4 - \mathtt{y}_3)^2/(\mathtt{x}_4 - \mathtt{x}_3)^2 - \mathtt{x}_4 - \mathtt{x}_3 & \wedge \\
 & \mathtt{y}_6 = -(\mathtt{y}_4 - \mathtt{y}_3)/(\mathtt{x}_4 - \mathtt{x}_3) * (\mathtt{x}_6 - \mathtt{x}_3) - \mathtt{y}_3 & \wedge \\
 & \mathtt{x}_5 = (\mathtt{y}_2 - \mathtt{y}_3)^2/(\mathtt{x}_2 - \mathtt{x}_3)^2 - \mathtt{x}_2 - \mathtt{x}_3 & \wedge \\
 & \mathtt{y}_5 = -(\mathtt{y}_2 - \mathtt{y}_3)/(\mathtt{x}_2 - \mathtt{x}_3) * (\mathtt{x}_5 - \mathtt{x}_2) - \mathtt{y}_2 & \wedge \\
 & \mathtt{x}_7 = (\mathtt{y}_5 - \mathtt{y}_1)^2/(\mathtt{x}_5 - \mathtt{x}_1)^2 - \mathtt{x}_5 - \mathtt{x}_1 & \wedge \\
 & \mathtt{y}_7 = -(\mathtt{y}_5 - \mathtt{y}_1)/(\mathtt{x}_5 - \mathtt{x}_1) * (\mathtt{x}_7 - \mathtt{x}_1) - \mathtt{y}_1 & \\
\Rightarrow & \mathtt{x}_6 - \mathtt{x}_7 = 0 &
\end{array}
$$

# First equation

$- (2) * y_2^8 * x_3^7 * x_2^6 +$

$2 * (2 * (1 + 2)) * y_2^8 * x_3^7 * x_2^5 * x_1 -$

$2 * (1 + 2 * (1 + 2 * (1 + 2))) * y_2^8 * x_3^7 * x_2^4 * x_1^2 +$

$2 * (2 * (2 * (1 + 4))) * y_2^8 * x_3^7 * x_2^3 * x_1^3 -$

$2 * (1 + 2 * (1 + 2 * (1 + 2))) * y_2^8 * x_3^7 * x_2^2 * x_1^4 +$

$2 * (2 * (1 + 2)) * y_2^8 * x_3^7 * x_2 * x_1^5 -$

$2 * y_2^8 * x_3^7 * x_1^6 + 2 * (2 * (1 + 2)) * y_2^8 * x_3^6 * x_2^7 -$

$2 * (1 + 2 * (1 + 2 * (2 * 4))) * y_2^8 * x_3^6 * x_2^6 * x_1 +$

$2 * (2 * (2 * (1 + 2 * (2 * (1 + 4))))) * y_2^8 * x_3^6 * x_2^5 * x_1^2 -$

$2 * (1 + 2 * (2 * (2 * (1 + 2 * (2 * (1 + 2)))))) * y_2^8 * x_3^6 * x_2^4 * x_1^3 +$

$2 * (2 * (1 + 2 * (1 + 2 * (2 * 4)))) * y_2^8 * x_3^6 * x_2^3 * x_1^4 -$

$2 * (1 + 2 * (2 * (1 + 4))) * y_2^8 * x_3^6 * x_2^2 * x_1^5 +$

$2 * y_2^8 * x_3^6 * x_1^7 -$

..................................................

..................................................

..................................................

20000 lines!!

# Reflection

One Reification

Ring

Horner Representation: $P \rightsquigarrow P' + x^i Q'$

Rewrite $[m = R]$

Naive: $P \rightsquigarrow P = P' + mQ' \rightsquigarrow P' + RQ'$

Common denominator

$$P_1/Q_1 + P_2/Q_2 \rightsquigarrow (P_1'Q_2' + P_2'Q_1')/Q_1'Q_2'$$

Result: `field[H₁; H₂]` 80 seconds.

# Elliptic Certificate

Order of a point:

$$m.P = \underbrace{P + \cdots + P}_{m} = 0$$

Projective coordinate:

$$(3/4, 1/3) \rightsquigarrow (9 : 4 : 12)$$

# Elliptic Certificate

Let $n$ be an integer. Assume that there exist an elliptic curve $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ and $\mathtt{gcd}(4A^3 + 27B^2, n) = 1$, a point $P = (x_P : y_P : 1)$ such that $y_P^2 = x_P^3 + Ax_P + B \mathtt{\ mod\ } n$, and an integer $m$ such that

- $m.P = (0 : 1 : 0) \mathtt{\ mod\ } n$ ;
- for all prime $p|m$, $(m/p).P = (x_p : y_p : z_p) \mathtt{\ mod\ } n$ with $\mathtt{gcd}(z_p, n) = 1$.

Then, if $4n < (m-1)^2$, $n$ is prime

# Elliptic Certificate

{

329719147332060395689499,

−94080,

9834496,

0,

3136,

8209062,

[(40165264598163841, 1)]

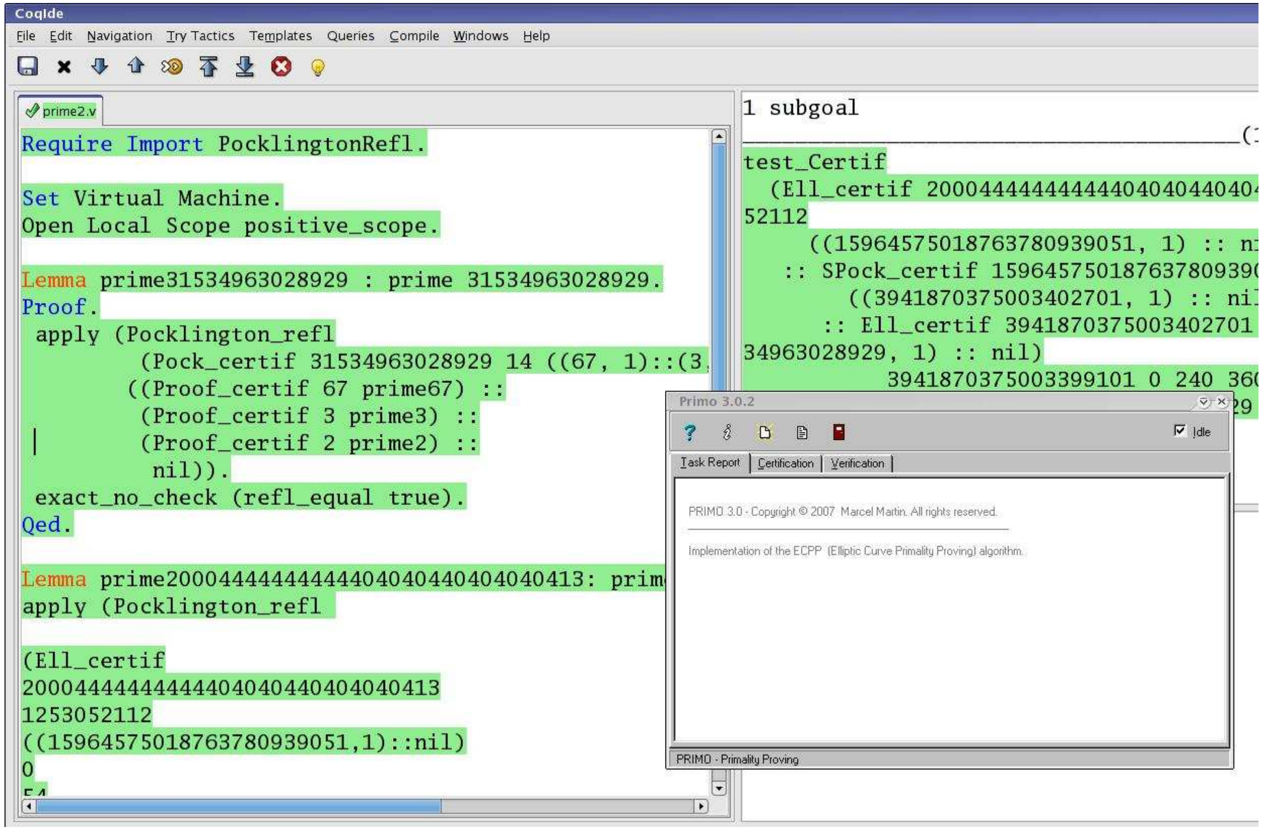
}

with the curve $y^2 = x^3 - 94080x + 9834496$ and the point $8209062.(0, 3136)$ whose order is $40165264598163841$, $329719147332060395689499$ is prime if $40165264598163841$ is prime .

# Checking certificates

```
Definition double(p₁, sc₁) =
  if p₁ = 0 then (0, sc₁) else
  let (x₁ : y₁ : z₁) = p₁ in
    if y₁ = 0 then (0, z₁sc₁) else
    let m = 3x₁² + Az₁² and l = 2y₁z₁ in
    let l₂ = l² and x₂ = m²z₁ − 2x₁l₂ in
    ((x₂l : l₂(x₁m − y₁l) − x₂m : z₁l₂l), sc₁)
```

# A Demo


CoqIde
File Edit Navigation Try Tactics Templates Queries Compile Windows Help
prime2.v
Require Import PocklingtonRefl.
Set Virtual Machine.
Open Local Scope positive_scope.
Lemma prime31534963028929 : prime 31534963028929.
Proof.
apply (Pocklington_refl
(Pock_certif 31534963028929 14 ((67, 1)::(3,
((Proof_certif 67 prime67) ::
(Proof_certif 3 prime3) ::
(Proof_certif 2 prime2) ::
nil)).
exact_no_check (refl_equal true).
Qed.
Lemma prime2000444444444444040404440404040413: prim
apply (Pocklington_refl
(Ell_certif
2000444444444444040404440404040413
1253052112
((15964575018763780939051,1)::nil)
0
1 subgoal
test_Certif
(Ell_certif 20004444444444440404044040
52112
((15964575018763780939051, 1) :: n
:: SPock_certif 15964575018763780939
((3941870375003402701, 1) :: ni
:: Ell_certif 3941870375003402701
34963028929, 1) :: nil)
3941870375003399101 0 240 36
Primo 3.0.2
Idle
Task Report Certification Verification
PRIMO 3.0 - Copyright © 2007 Marcel Martin. All rights reserved.
Implementation of the ECPP (Elliptic Curve Primality Proving) algorithm.
PRIMO - Primality Proving

# Conclusions

Proving Primality Proving

Ubiquity of computing