Le fabuleux destin de la moyenne arithmético-géométrique

Antoine Chambert-Loir

Institut de recherche mathématique de Rennes, Université de Rennes 1

Fondation Jacques Hadamard, 18 mai 2011

Moyenne arithmético-géométrique

Découverte par Legendre, avant 1785.

$$a_0, b_0 > 0,$$

$$a_{n+1} = \frac{1}{2}(a_n + b_n), \quad b_{n+1} = \sqrt{a_n b_n}.$$

Les deux suites (a_n) et (b_n) sont adjacentes et ont une limite commune appelée **moyenne arithmético-géométrique**.

$$M(a_0, b_0) = \lim_{n \to +\infty} a_n = \lim_{n \to +\infty} b_n.$$

Moyenne arithmético-géométrique : Expérience numérique

La convergence est **très** rapide.

On part de 1 et $\sqrt{2}$, avec 20 décimales :

$$1.0 \qquad\qquad 1.41421356237309504888$$

Moyenne arithmético-géométrique : Expérience numérique

La convergence est **très** rapide.

On part de 1 et $\sqrt{2}$, avec 20 décimales :

1.0	1.41421356237309504888
1.20710678118654752444	1.18920711500272106677

Moyenne arithmético-géométrique : Expérience numérique

La convergence est **très** rapide.

On part de 1 et $\sqrt{2}$, avec 20 décimales :

1.0	1.41421356237309504888
1.20710678118654752444	1.18920711500272106677
1.19815694809463429560	1.19815694809463429560

Moyenne arithmético-géométrique : Expérience numérique

La convergence est **très** rapide.

On part de 1 et $\sqrt{2}$, avec 20 décimales :

1.0	1.41421356237309504888
1.20710678118654752444	1.18920711500272106677
1.19815694809463429560	1.19815235212012261226
1.19814023479387720911	1.19814023467730720588

Moyenne arithmético-géométrique : Expérience numérique

La convergence est **très** rapide.

On part de 1 et $\sqrt{2}$, avec 20 décimales :

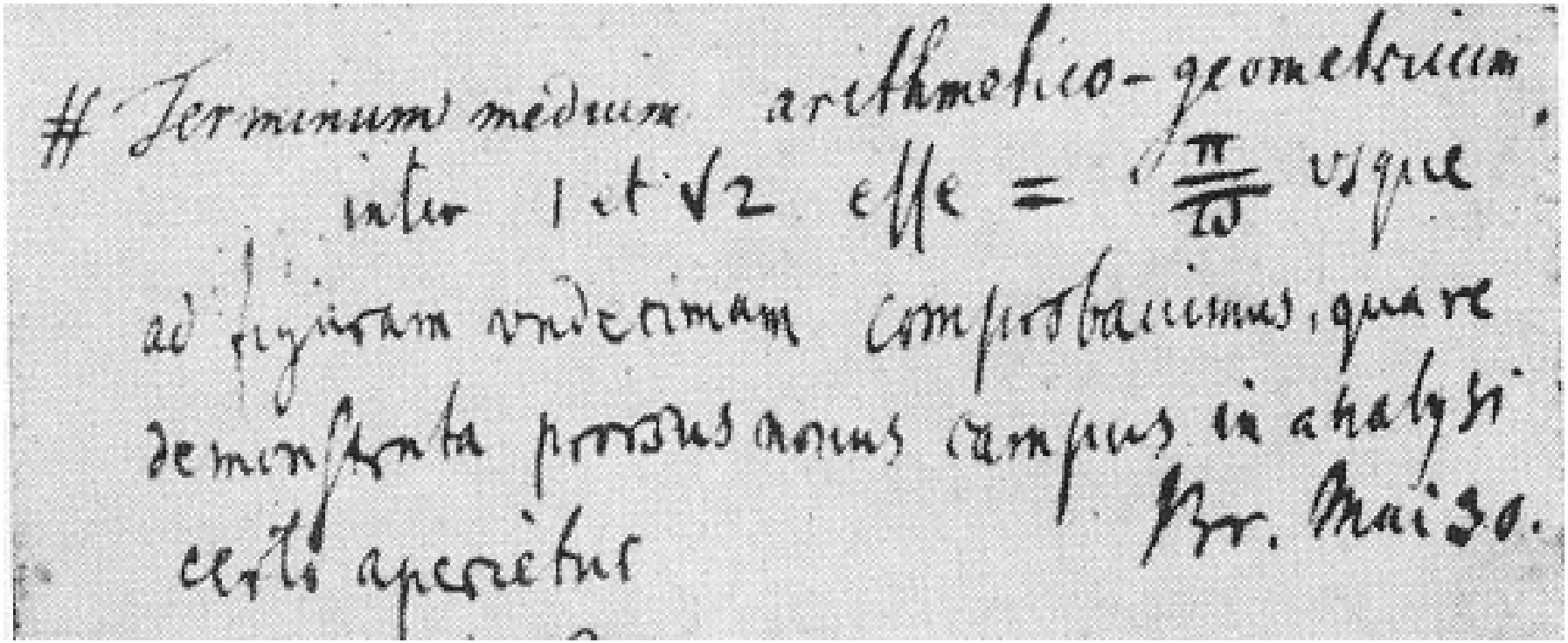
1.0	1.41421356237309504888
1.20710678118654752444	1.18920711500272106677
1.19815694809463429560	1.19811235212012206
1.19814023479387720911	1.19814023467730720588
1.19814023473559220744	1.19814023473559220755

Carl Friedrich Gauss (1777–1855)

- Écrit les **Disquisitiones Arithmeticae** à l'âge de 21 ans
- Calculateur prodigieux
- Astronome : prédit, par des calculs, la position de l'astéroïde Ceres
- Physicien : avec Weber, découvre le magnétisme

La découverte de Gauss

Entre 1796 et 1814, Gauss tint un **agenda mathématique** :

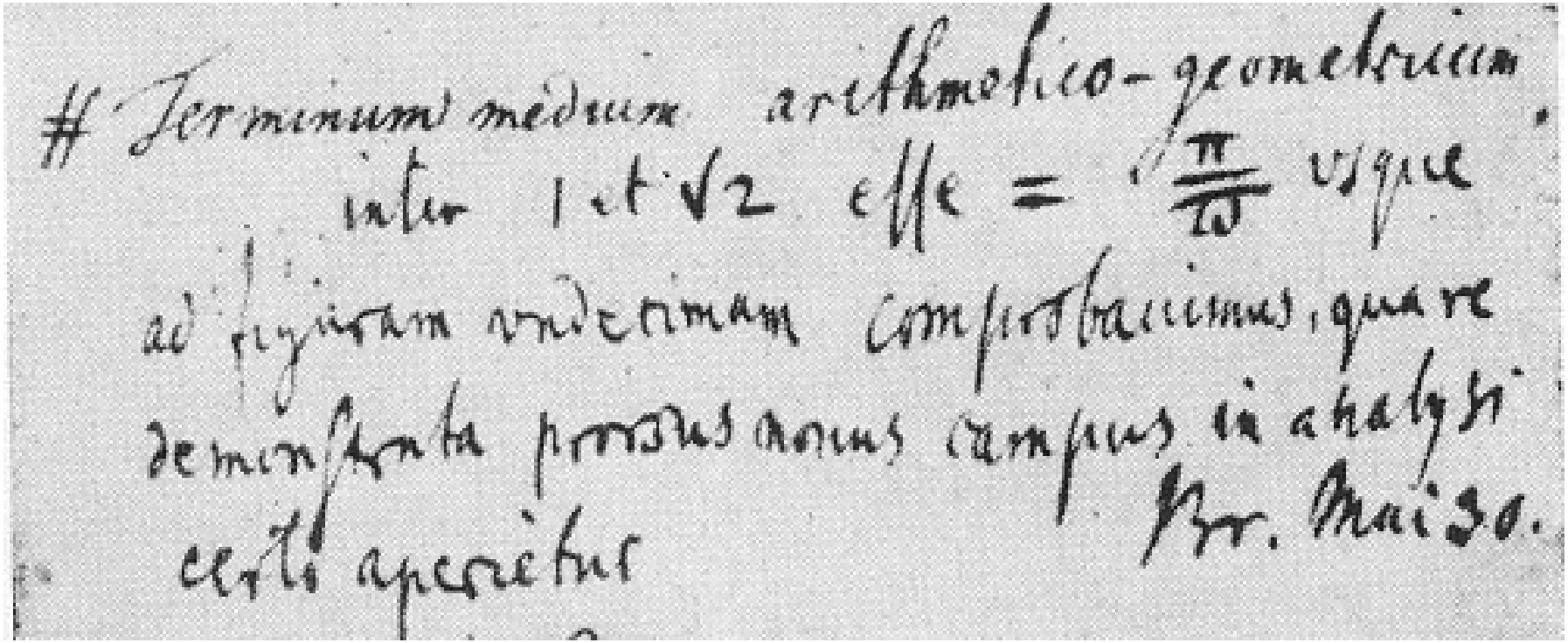


Terminum medium arithmetico-geometricum inter 1 et $\sqrt{2}$
esse $= \frac{\pi}{\omega}$ *usque ad figuram undecimam comprobavimus, qua re demonstrata prorsus novus campus in analysi certo aperietur.*

Br[unsvigae, 1799] Mai. 30.

La découverte de Gauss

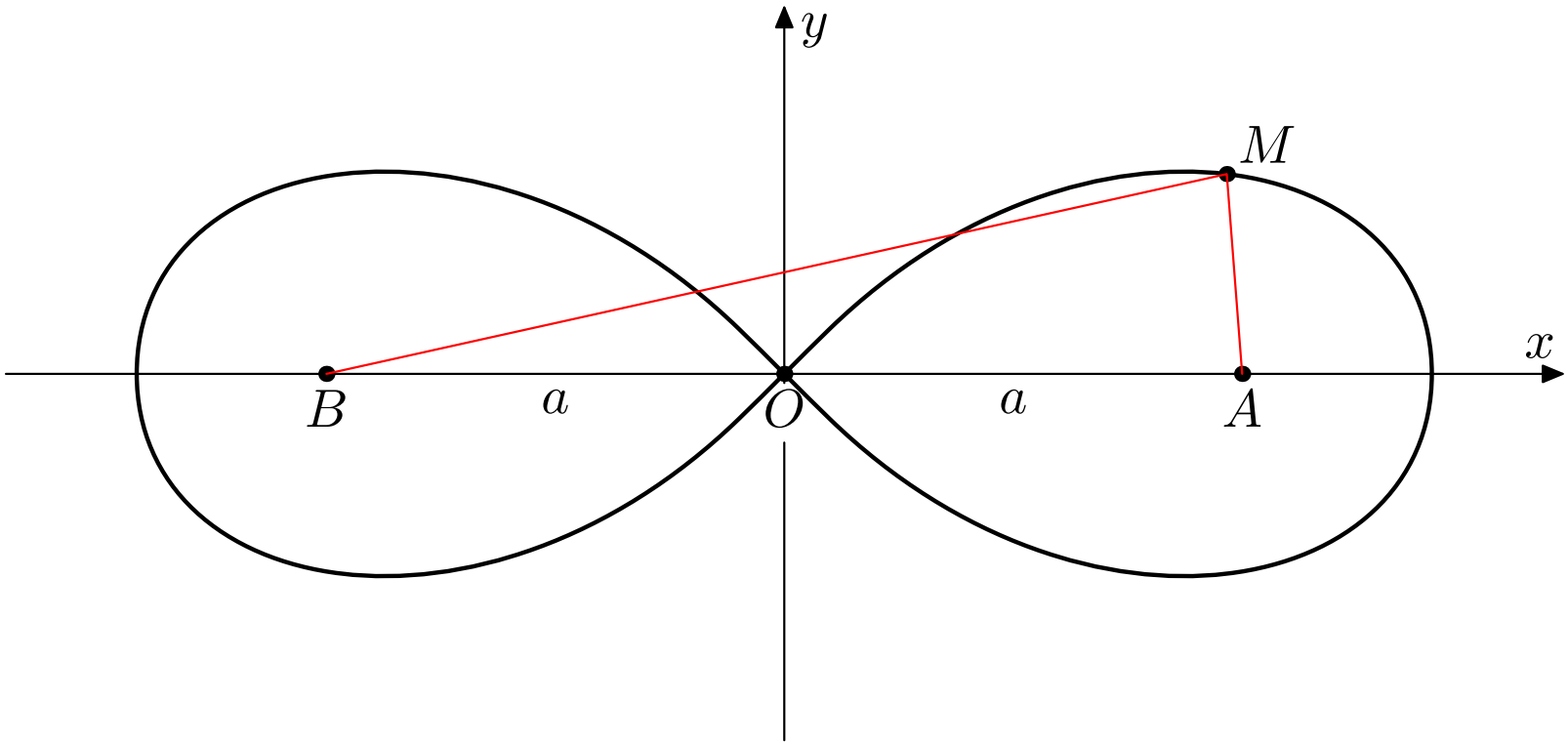
Entre 1796 et 1814, Gauss tint un **agenda mathématique** :



J'ai vérifié jusqu'à la onzième décimale que la moyenne arithmético-géométrique de 1 *et* $\sqrt{2}$ *vaut* $\frac{\pi}{\omega}$ *; une démonstration de ce fait ouvrira certainement un nouveau champ de l'analyse.*

Br[unswick,] 30 mai [1799].

Lemniscate



Si $OA = OB = a$, c'est l'ensemble des points M du plan qui vérifient $MA \cdot MB = a^2$.

Équation cartésienne :

$$(x^2 + y^2)^2 = 2a^2(x^2 - y^2).$$

Si $OA = OB = a$, c'est l'ensemble des points M du plan qui vérifient $MA \cdot MB = a^2$. Sa longueur est :

$$4(a\sqrt{2}) \int_0^1 \frac{\mathrm{d}r}{\sqrt{1-r^4}} = 2a\sqrt{2}\omega,$$

avec

$$\omega = 2 \int_0^1 \frac{\mathrm{d}r}{\sqrt{1-r^4}} \sim 2.622\,057\,554\,292\,119\,810\,4.$$

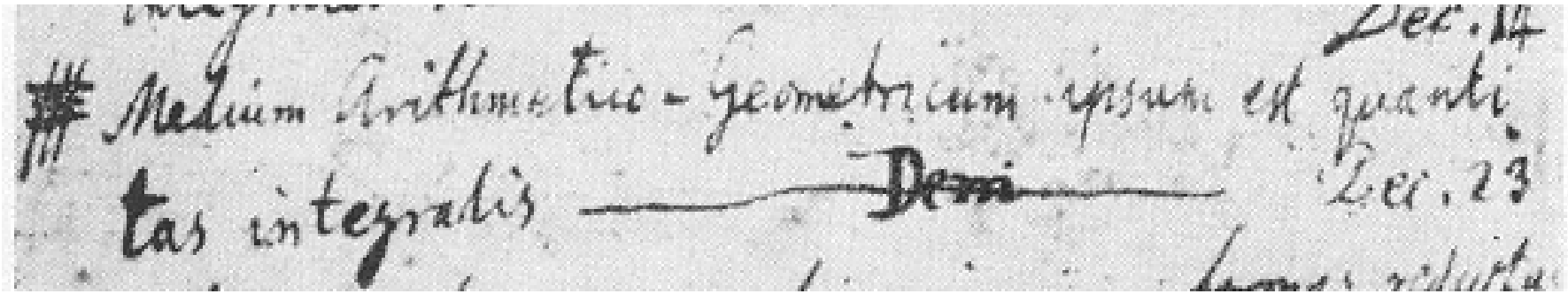
200 ans après Gauss, il est facile de constater que

$$\frac{\pi}{\omega} \sim 1.198\,140\,234\,735\,592\,207\,5.$$

La découverte de Gauss : ... Sept mois plus tard

La moyenne arithmético-géométrique est elle-même une quantité intégrale. Dém[ontré]. *23 déc. [1799].*

Medium Arithmetico-Geometricum ipsum est quantitas integralis. Dem[onstrantum]. [1799] Dec. 23.



Théorème

$$\frac{\pi}{M(a,b)} = \int_{-\infty}^{\infty} \frac{dt}{\sqrt{(a^2+t^2)(b^2+t^2)}}$$

THÉORÈME

$$I(a,b)=\int_{-\infty}^{\infty}\frac{dt}{\sqrt{(a^2+t^2)(b^2+t^2)}}=\frac{\pi}{M(a,b)}.$$

Démonstration moderne : effectuer le changement de variables $u=\frac{1}{2}(t-ab/t)$ et montrer que

$$I(a,b)=I\Big(\frac{a+b}{2},\sqrt{ab}\Big).$$

Si (a_n,b_n) est la suite qui définit la moyenne arithmético-géométrique, on obtient donc

$$I(a,b)=I(a_0,b_0)=I(\frac{a_0+b_0}{2},\sqrt{a_0b_0})=I(a_1,b_1)=\cdots=I(a_n,b_n)=\ldots$$

En passant à la limite, on a donc

$$I(a,b)=I(M(a,b),M(a,b))=\int_{-\infty}^{\infty}\frac{dt}{M(a,b)^2+t^2}=\frac{\pi}{M(a,b)}.$$

THÉORÈME

$$I(a,b)=\int_{-\infty}^{\infty}\frac{dt}{\sqrt{(a^2+t^2)(b^2+t^2)}}=\frac{\pi}{M(a,b)}.$$

La *démonstration de Gauss* est infiniment plus compliquée : partant de la relation

$$M(1+x,1-x)=(1+x)M\Big(1,\frac{1-x}{1+x}\Big)=(1+x)M\Big(1+\frac{2\sqrt{x}}{1+x},1-\frac{2\sqrt{x}}{1+x}\Big),$$

il a identifié les coefficients du développement en série de $1/M(1+x,1-x)$. Il obtient le développement de

$$\frac{2}{\pi}\int_0^{\pi/2}\frac{d\varphi}{\sqrt{1-(1-x^2)\sin^2\varphi}}.$$

Elles apparaissent progressivement au 19^{e} siècle.
La motivation vient d'abord de l'étude de certaines intégrales définies, telle

$$K(k) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}},$$

qui s'interprète en fait comme la demi-**longueur** de la courbe plane d'équation

$$y^2 = (1-x^2)(1-k^2x^2), \quad 0 \leqslant x \leqslant 1.$$

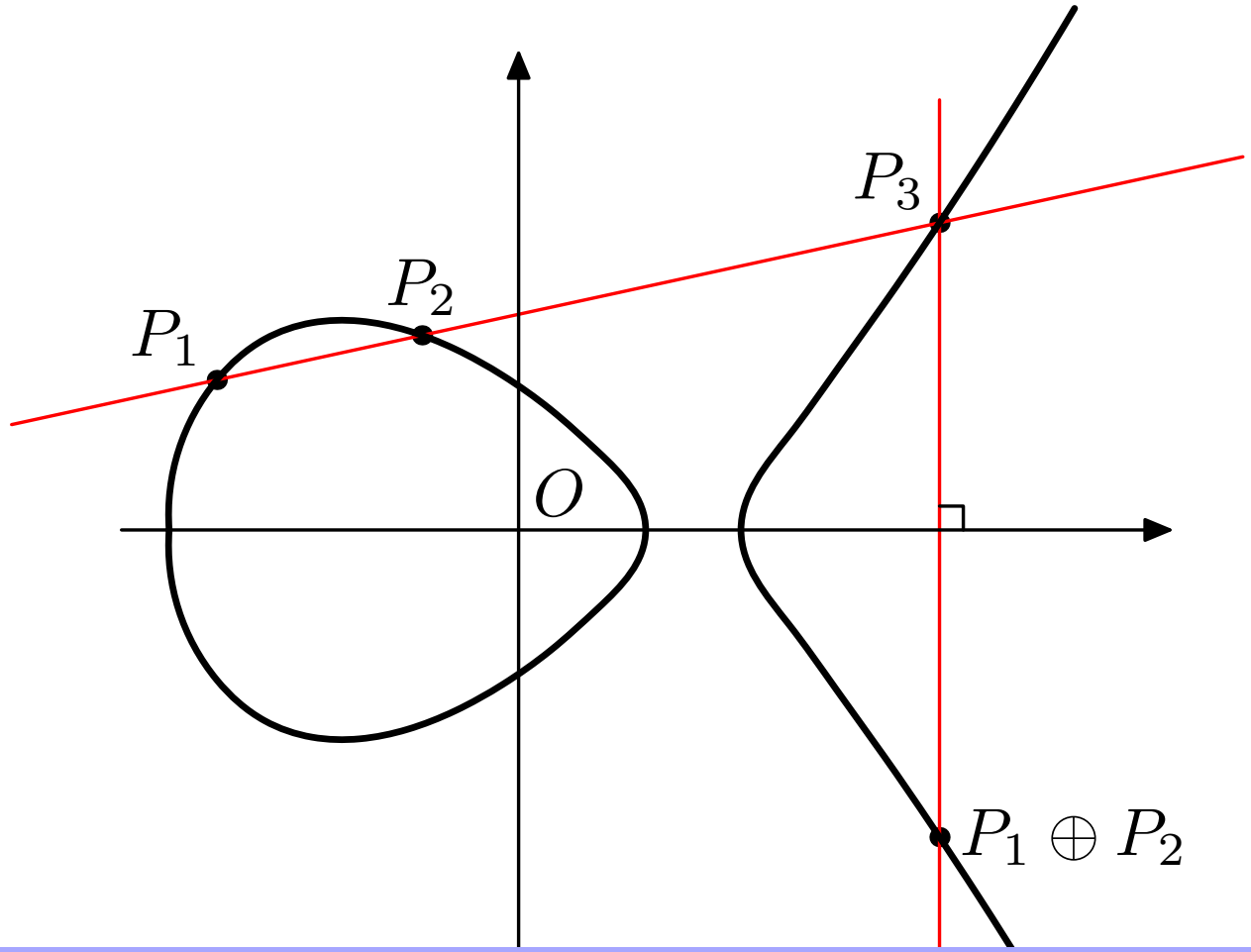
Aujourd'hui, on préfère les écrire sous la forme

$$y^2 = x^3 + ax + b, \qquad \Delta = 4a^3 + 27b^2 \neq 0.$$

Paramétrisation par des fonctions méromorphes $\mathbf{C} \to \mathbf{C}$ doublement périodiques.

Courbes elliptiques : Loi de groupe (Abel)

Elles donnent lieu à une loi de groupe sur les points de la courbe auxquels on adjoint un point « à l'infini » qui est l'**origine** du groupe. La relation $P_1 \oplus P_2 \oplus P_3 = 0$ signifie que les points P_1, P_2 et P_3 sont **alignés.**



COURBES ELLIPTIQUES : UN CHAMP D'ÉTUDE IN(DÉ)FINI...

- genèse de la géométrie algébrique (Abel, Jacobi,...) ;
- application à certains systèmes intégrables (toupies) ;
- propriétés arithmétiques superbes (Hasse, Mordell, Weil,...) ;
- cryptographie, tests de primalité ;
- solution de l'équation KdV (équation des ondes dans un canal, « solitons ») ;

sans oublier que ce sont les courbes elliptiques qui ont fourni la clef du **théorème de Fermat** (Hellegouarch, Frey, Ribet, Wiles) !

Cryptographie à clef publique

1976 : Diffie et Hellman inventent la **cryptographie à clef publique**

Cryptographie traditionnelle : celui qui sait coder un message sait le décoder.
Cryptographie à clef publique : avec la **clef publique**, tout le monde peut coder un message à votre intention, mais vous seul possédez la **clef privée** qui permet de les décoder.

Au cœur du développement du commerce via Internet, des cartes de paiement,...

Leur méthode repose sur l'arithmétique modulo un nombre premier p et sur le petit théorème de Fermat :

$$\text{si } p \text{ ne divise pas un entier } N, \text{ alors } N^{p-1} \equiv 1 \pmod{p}.$$

Cela donne un intérêt **pratique** à la question fondamentale de savoir décider si un entier donné p est, ou non, un nombre premier.

Tests de primalité

- Algorithme naïf : impraticable (il faudrait de l'ordre de 10^{250} années pour un nombre de 500 chiffres)
- Rabin-Miller, Pollard, Shanks,... : améliorations mais toujours impraticable pour de très grands nombres.
- 1980. Adleman, Pomerance, Rumely : sommes de Gauss/Jacobi. Rendu **praticable** par Cohen, Lenstra (1983).
- 1993. Algorithme d'Atkin–Morain. Repose sur des **courbes elliptiques.** Il a permis de prouver la primalité de nombres de plus de 25 000 chiffres !
- 2002. Algorithme d'Agrawal–Kayal–Saxena (n'utilise pas les courbes elliptiques).

TESTS DE PRIMALITÉ

- Algorithme naïf : impraticable (il faudrait de l'ordre de 10^{250} années pour un nombre de 500 chiffres)
- Rabin-Miller, Pollard, Shanks,... : améliorations mais toujours impraticable pour de très grands nombres.
- 1980. Adleman, Pomerance, Rumely : sommes de Gauss/Jacobi. Rendu **praticable** par Cohen, Lenstra (1983).
- 1993. Algorithme d'Atkin–Morain. Repose sur des **courbes elliptiques.** Il a permis de prouver la primalité de nombres de plus de 25 000 chiffres !
- 2002. Algorithme d'Agrawal–Kayal–Saxena (n'utilise pas les courbes elliptiques).

Tests de primalité

- Algorithme naïf : impraticable (il faudrait de l'ordre de 10^{250} années pour un nombre de 500 chiffres)
- Rabin-Miller, Pollard, Shanks,... : améliorations mais toujours impraticable pour de très grands nombres.
- 1980. Adleman, Pomerance, Rumely : sommes de Gauss/Jacobi. Rendu **praticable** par Cohen, Lenstra (1983).
- 1993. Algorithme d'Atkin–Morain. Repose sur des **courbes elliptiques.** Il a permis de prouver la primalité de nombres de plus de 25 000 chiffres !
- 2002. Algorithme d'Agrawal–Kayal–Saxena (n'utilise pas les courbes elliptiques).

TESTS DE PRIMALITÉ

- Algorithme naïf : impraticable (il faudrait de l'ordre de 10^{250} années pour un nombre de 500 chiffres)
- Rabin-Miller, Pollard, Shanks,... : améliorations mais toujours impraticable pour de très grands nombres.
- 1980. Adleman, Pomerance, Rumely : sommes de Gauss/Jacobi. Rendu **praticable** par Cohen, Lenstra (1983).
- 1993. Algorithme d'Atkin–Morain. Repose sur des **courbes elliptiques.** Il a permis de prouver la primalité de nombres de plus de 25 000 chiffres !
- 2002. Algorithme d'Agrawal–Kayal–Saxena (n'utilise pas les courbes elliptiques).

TESTS DE PRIMALITÉ

- Algorithme naïf : impraticable (il faudrait de l'ordre de 10^{250} années pour un nombre de 500 chiffres)
- Rabin-Miller, Pollard, Shanks,... : améliorations mais toujours impraticable pour de très grands nombres.
- 1980. Adleman, Pomerance, Rumely : sommes de Gauss/Jacobi. Rendu **praticable** par Cohen, Lenstra (1983).
- 1993. Algorithme d'Atkin–Morain. Repose sur des **courbes elliptiques.** Il a permis de prouver la primalité de nombres de plus de 25 000 chiffres !
- 2002. Algorithme d'Agrawal–Kayal–Saxena (n'utilise pas les courbes elliptiques).

Cryptographie, courbes elliptiques

En cryptographie à clef publique, on peut utiliser, plutôt que le groupe des entiers inversibles modulo p, où p est un nombre premier, celui des points d'une courbe elliptique dans le **corps fini** $\mathbf{Z}/p\mathbf{Z}$. Il est très important que le cardinal de ce groupe,

$$N = 1 + \#\{(x,y) \in (\mathbf{Z}/p\mathbf{Z})^2 \, ; \, y^2 = x^3 + ax + b\},$$

soit lui-même un nombre premier. Pour cela, il faut calculer N.

- 1985 : Algorithme de Schoof, très rapide. Repose sur le théorème de Lagrange et sur le fait que l'on sait (Hasse, 1933) que

  $$\left|p + 1 - N\right| \leqslant 2\sqrt{p}.$$

  (Améliorations : Elkies, Atkin.)
- 1999 : Satoh, puis Fouquet, Gaudry, Harley
- 2000 : Mestre (implémenté par Harley) utilise la **moyenne arithmético-géométrique** dans le contexte des « nombres p-adiques » pour calculer très rapidement le nombre de points.
- De nombreuses améliorations et extensions depuis 10 ans...

Cryptographie, courbes elliptiques

En cryptographie à clef publique, on peut utiliser, plutôt que le groupe des entiers inversibles modulo p, où p est un nombre premier, celui des points d'une courbe elliptique dans le **corps fini** $\mathbf{Z}/p\mathbf{Z}$. Il est très important que le cardinal de ce groupe,

$$N = 1 + \#\{(x,y) \in (\mathbf{Z}/p\mathbf{Z})^2 \, ; \, y^2 = x^3 + ax + b\},$$

soit lui-même un nombre premier. Pour cela, il faut calculer N.

- 1985 : Algorithme de Schoof, très rapide. Repose sur le théorème de Lagrange et sur le fait que l'on sait (Hasse, 1933) que

  $$\left|p + 1 - N\right| \leqslant 2\sqrt{p}.$$

  (Améliorations : Elkies, Atkin.)
- 1999 : Satoh, puis Fouquet, Gaudry, Harley
- 2000 : Mestre (implémenté par Harley) utilise la **moyenne arithmético-géométrique** dans le contexte des « nombres p-adiques » pour calculer très rapidement le nombre de points.
- De nombreuses améliorations et extensions depuis 10 ans...

En cryptographie à clef publique, on peut utiliser, plutôt que le groupe des entiers inversibles modulo p, où p est un nombre premier, celui des points d'une courbe elliptique dans le **corps fini** $\mathbf{Z}/p\mathbf{Z}$. Il est très important que le cardinal de ce groupe,

$$N = 1 + \#\{(x,y) \in (\mathbf{Z}/p\mathbf{Z})^2 \,;\, y^2 = x^3 + ax + b\},$$

soit lui-même un nombre premier. Pour cela, il faut calculer N.

- 1985 : Algorithme de Schoof, très rapide. Repose sur le théorème de Lagrange et sur le fait que l'on sait (Hasse, 1933) que

  $$\left|p + 1 - N\right| \leqslant 2\sqrt{p}.$$

  (Améliorations : Elkies, Atkin.)
- 1999 : Satoh, puis Fouquet, Gaudry, Harley
- 2000 : Mestre (implémenté par Harley) utilise la **moyenne arithmético-géométrique** dans le contexte des « nombres p-adiques » pour calculer très rapidement le nombre de points.
- De nombreuses améliorations et extensions depuis 10 ans...

En cryptographie à clef publique, on peut utiliser, plutôt que le groupe des entiers inversibles modulo p, où p est un nombre premier, celui des points d'une courbe elliptique dans le **corps fini** $\mathbf{Z}/p\mathbf{Z}$. Il est très important que le cardinal de ce groupe,

$$N = 1 + \#\{(x,y) \in (\mathbf{Z}/p\mathbf{Z})^2 \, ; \, y^2 = x^3 + ax + b\},$$

soit lui-même un nombre premier. Pour cela, il faut calculer N.

- 1985 : Algorithme de Schoof, très rapide. Repose sur le théorème de Lagrange et sur le fait que l'on sait (Hasse, 1933) que

  $$\left|p + 1 - N\right| \leqslant 2\sqrt{p}.$$

  (Améliorations : Elkies, Atkin.)
- 1999 : Satoh, puis Fouquet, Gaudry, Harley
- 2000 : Mestre (implémenté par Harley) utilise la **moyenne arithmético-géométrique** dans le contexte des « nombres p-adiques » pour calculer très rapidement le nombre de points.
- De nombreuses améliorations et extensions depuis 10 ans...