Des opérations inhabituelles

Arithmétique modulaire, nombres complexes, courbes elliptiques

Emmanuel Royer, CNRS

24 = 0 ?

Arithmétique modulaire

La mathématique du chat de Philippe Geluck. Daniel Justens. Éd. Casterman.

Une énigme

Comprenez-vous ce tableau ?

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Une énigme

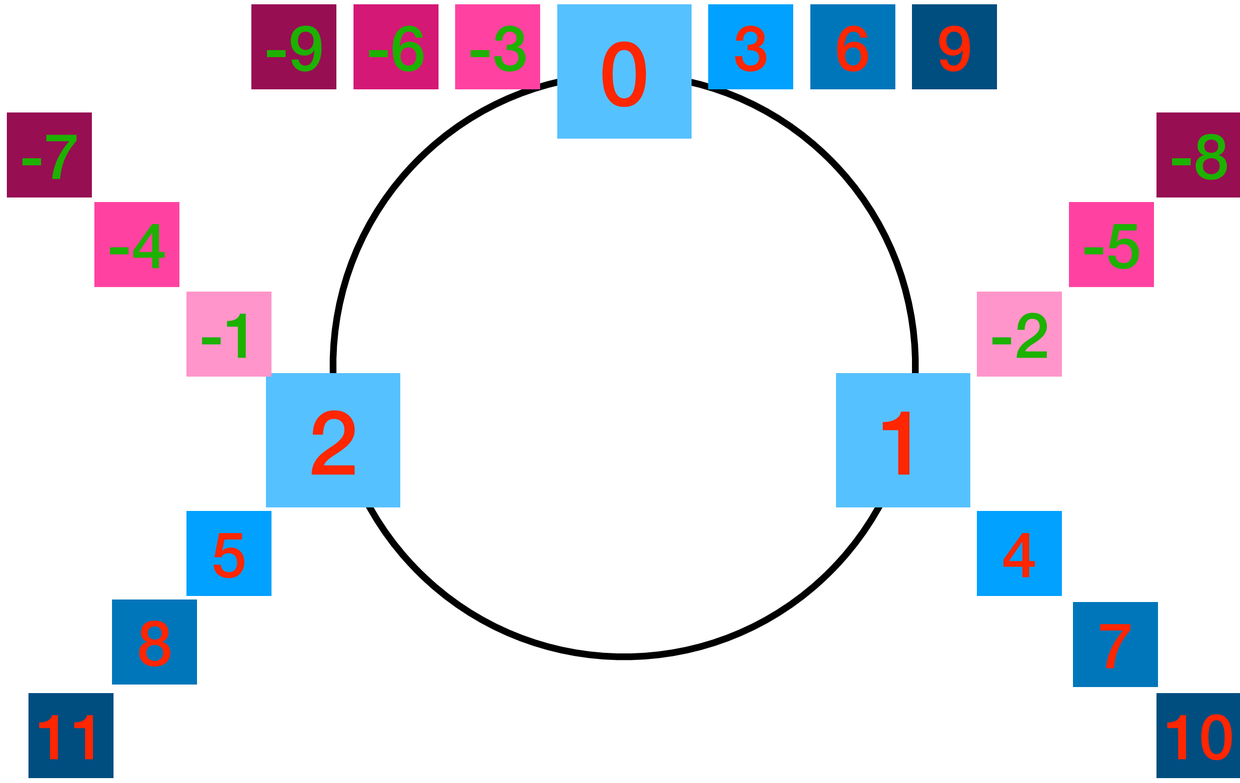
Et ce tableau ?

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Calcul modulo

Calculs modulo 3

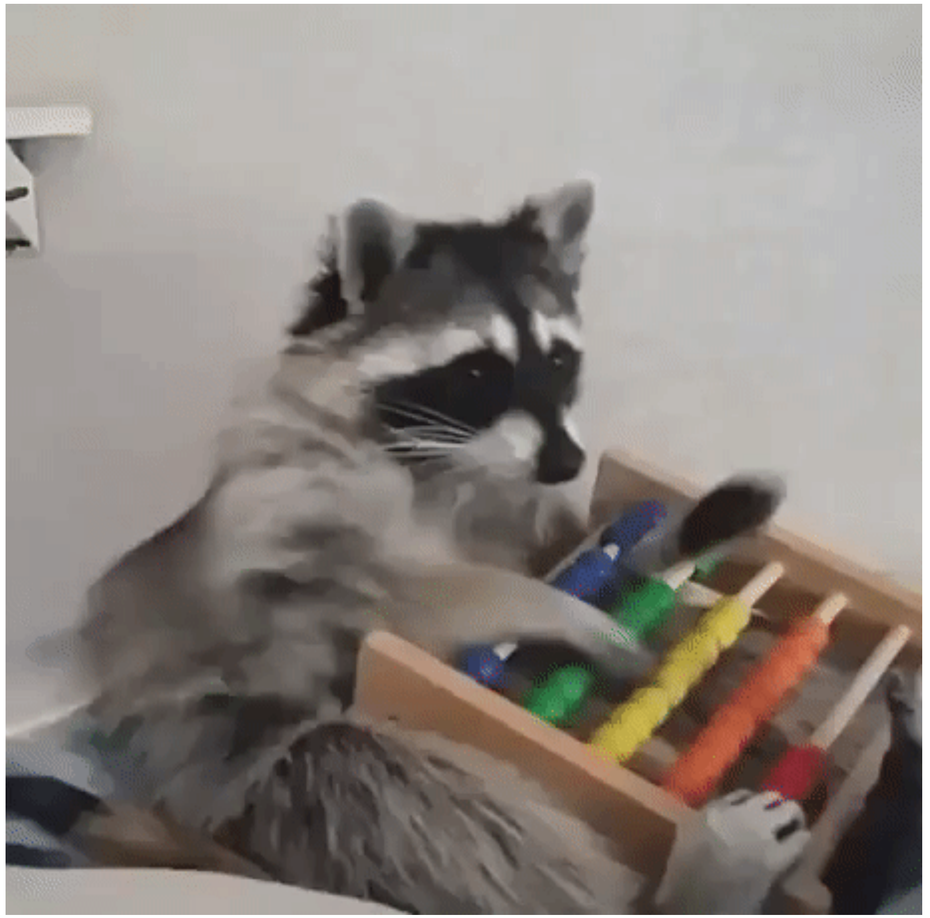
- Modulo 3, trois est la même chose que 0
- Les additions et multiplications sont « comme d'habitude » mais l'égalité change
- Si $3 \equiv 0$, alors
  - $4 = 3 + 1 \equiv 0 + 1 \equiv 1$
  - $5 = 3 + 2 \equiv 0 + 2 \equiv 2$
  - $6 = 5 + 1 \equiv 2 + 1 \equiv 3 \equiv 0$
  - $6 = 2 \times 3 \equiv 2 \times 0 \equiv 0$



Calcul modulo

Calculs modulo 7

À VOUS !



Calcul modulo

La solution !

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Calcul modulo

Puissance modulo 3

- Prendre une puissance, c'est réitérer une multiplication
- $2^7 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
- On fait le calcul modulo 3
  - $2^7 \equiv 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
  - $2^7 \equiv 4 \times 2 \times 2 \times 2 \times 2 \times 2 \equiv 1 \times 2 \times 2 \times 2 \times 2 \times 2 \equiv 2 \times 2 \times 2 \times 2 \times 2$
  - $2^7 \equiv 4 \times 2 \times 2 \times 2 \equiv 1 \times 2 \times 2 \times 2 \equiv 2 \times 2 \times 2$
  - $2^7 \equiv 2 \times 2 \times 2 \equiv 4 \times 2 \equiv 1 \times 2 \equiv 2.$

Calcul modulo

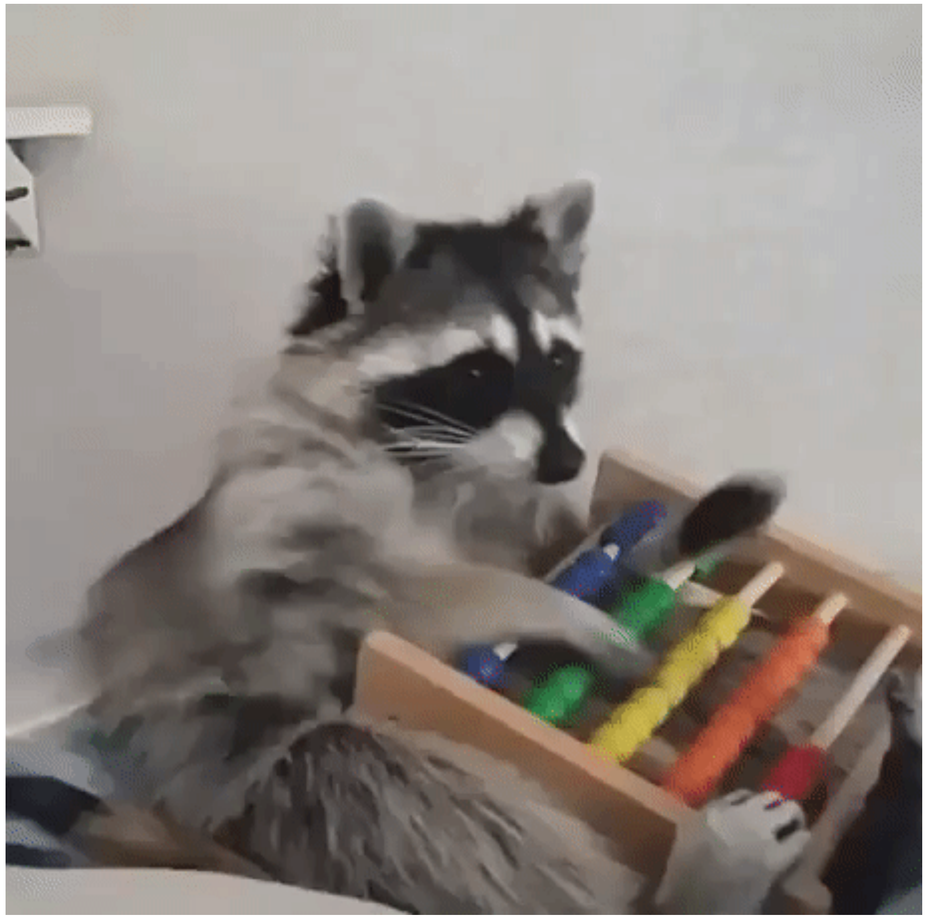
Puissance modulo 3

- $2^2 \equiv 1$
- $7 = 2 \times 3 + 1$
- donc $2^7 = (2^2)^3 \times 2 \equiv 1^3 \times 2 \equiv 2.$

Calcul modulo

Puissance modulo 17

À VOUS !



Calcul modulo

La solution !

$$3^{16} \equiv 1$$

$$3^3 = 27 \equiv 10$$

donc $3^6 = (3^3)^2 \equiv 10^2 \equiv (-7)^2 \equiv 49 \equiv 15 \equiv -2$

puis $3^{12} = (3^6)^2 \equiv (-2)^2 \equiv 4.$

Enfin $3^4 = 3 \times 3^3 \equiv 3 \times 10 \equiv 30 \equiv 13 \equiv -4.$

Ainsi $3^{16} = 3^{12} \times 3^4 \equiv 4 \times (-4) \equiv -16 \equiv 1.$

Calcul modulo

La solution !

$$3^{81} \equiv 3$$

$$81 = 5 \times 16 + 1$$

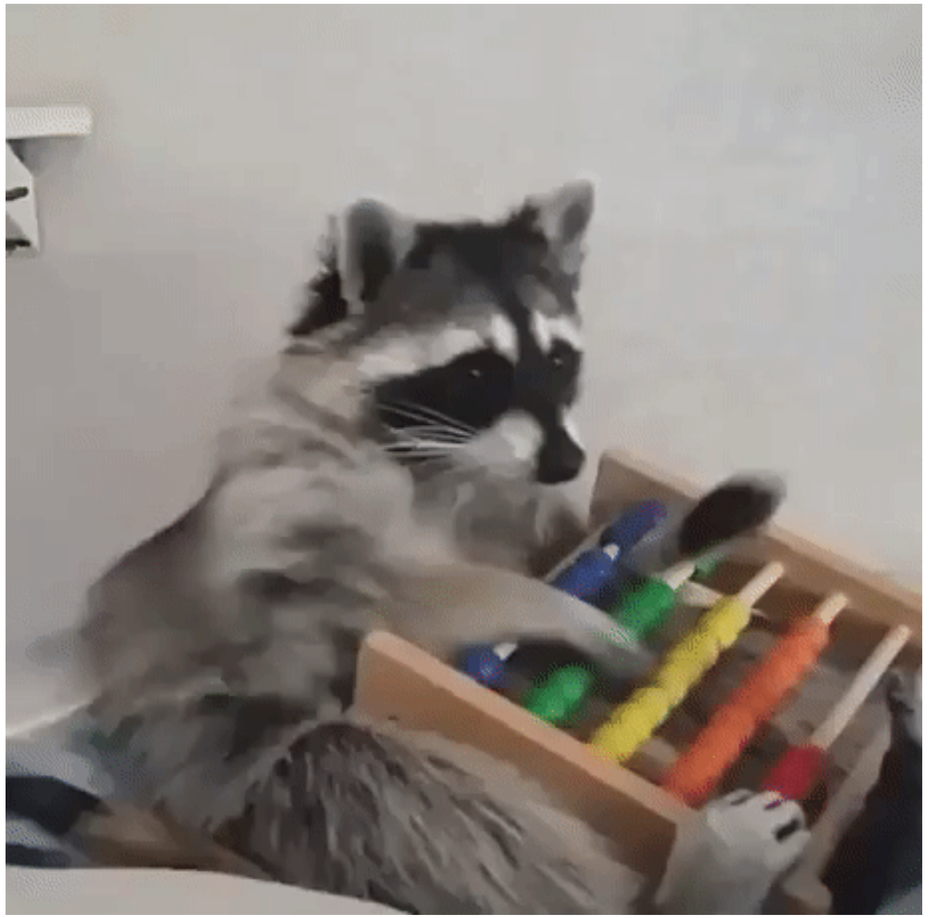
donc

$$3^{81} = (3^{16})^5 \times 3 \equiv 1 \times 3 \equiv 3.$$

Calcul modulo

Tous les éléments à partir des puissances d’un seul

À VOUS !



Calcul modulo

La solution : n tel que $g \equiv 3^n \pmod{17}$

3^n	1	2	3	4	5	6	7	8
n	0	14	1	12	5	15	11	10

3^n	9	10	11	12	13	14	15	16
n	2	3	7	13	4	9	6	8

Calcul modulo

La solution : x tel que $3x \equiv 1 \pmod{17}$

Parce qu'on connaît la table de 6

$3 \times 6 = 18$

et $18 = 1 + 17$

donc $3 \times 6 \equiv 1.$

Méthode systématique

$3^{16} \equiv 1$

donc $3 \times 3^{15} \equiv 1$

et $3^{15} \equiv 6$

donc $3 \times 6 \equiv 1.$

Des puissances égales à un

Le « petit » théorème de Fermat

Pierre de Fermat est un homme de loi du 17ème siècle, conseiller au parlement de Toulouse.

Les mathématiques ont été un loisir pour lui, à propos desquelles il écrit des lettres, énonçant des résultats sans réelles démonstrations.

Pierre de Fermat - 1601-1665

Des puissances égales à un

Le « petit » théorème de Fermat

Jeudi 18 octobre 1640, Pierre de Fermat écrit une lettre à Bernard Frénicle de Bessy.

« Monsieur,

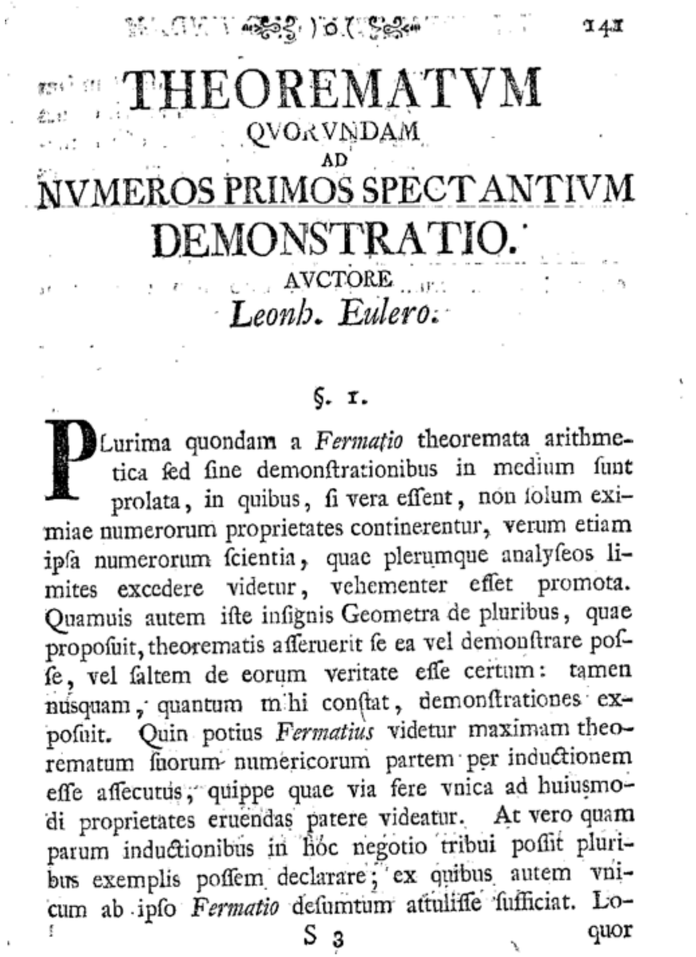
Les vacations, qui m'ont éloigné de Toulouse, m'ont en même temps éloigné de mon devoir et empêché de vous écrire plus tôt depuis la dernière de vos lettres en date du 21 septembre. (…) [J]e n'ai point vu encore aucune proposition de votre part que je n'eûsse plus tôt trouvée et considérée »


VARIA OPERA
MATHEMATICA
D. PETRI DE FERMAT,
SENATORIS TOLOSANI.
Acceſſerunt ſelectæ quædam ejuſdem Epiſtolæ, vel ad ipſum à pleriſque doctiſsimis viris Gallicè, Latinè, vel Italicè, de rebus ad Mathematicas diſciplinas, aut Phyſicam pertinentibus ſcriptæ.
OBLOQVITVR NVMERIS SEPTEM DISCRIMINA VOCVM
TOLOSÆ,
Apud JOANNEM PECH, Comitiorum Fuxenſium Typographum, juxta Collegium PP. Societatis JESU.
M. DC. LXXIX.

Vacation : « Certain temps que l'on emploie à travailler à quelque affaire ». Dictionnaire de l'Académie française. 1re édition. 1694.

Des puissances égales à un

Le « petit » théorème de Fermat



141

THEOREMATVM
QVORVNDAM
AD
NVMEROS PRIMOS SPECTANTIVM
DEMONSTRATIO.
AVCTORE
Leonh. Eulero.

§. 1.

Plurima quondam a *Fermatio* theoremata arithmetica sed sine demonstrationibus in medium sunt prolata, in quibus, si vera essent, non solum eximiae numerorum proprietates continerentur, verum etiam ipsa numerorum scientia, quae plerumque analyseos limites excedere videtur, vehementer effet promota. Quamuis autem iste insignis Geometra de pluribus, quae proposuit, theorematis asseruerit se ea vel demonstrare posse, vel saltem de eorum veritate esse certum: tamen nusquam, quantum mihi constat, demonstrationes exposuit. Quin potius *Fermatius* videtur maximam theorematum suorum numericorum partem per inductionem esse assecutus, quippe quae via fere vnica ad huiusmodi proprietates eruendas patere videatur. At vero quam parum inductionibus in hoc negotio tribui possit pluribus exemplis possem declarare; ex quibus autem vnicum ab ipso *Fermatio* desumtum attuliisse sufficiat. Lo-

S 3 quor

1741 - Première preuve par Euler

On lit dans cette lettre :

Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné -1 (…). De quoi je vous envoierais la démonstration, si je n'appréhendions d'être trop long.

Aujourd'hui, on écrit :

Si un nombre premier p ne divise pas l'entier a alors, modulo p on a $a^{p-1} \equiv 1$.

Exemple : $p = 17$ et $a = 3$ conduisent à $3^{16} \equiv 1 \pmod{17}$.

Des puissances égales à un

L'ingrédient principal : groupes finis

L'ensemble des entiers modulo un entier donné est un groupe. C'est un ensemble avec une opération $\circ$ et un élément e tels pour tous éléments a, b et c de l'ensemble alors, $a \circ b$ est dans l'ensemble et et

- $a \circ e = e \circ a = a$
- $a \circ (b \circ c) = (a \circ b) \circ c$
- Il existe d tel que $a \circ d = a \circ d = e$.

be noticed also, that if $\theta = \phi$, then, whatever the symbols α, β may be, $\alpha\theta\beta = \alpha\phi\beta$, and conversely.

A set of symbols,

$$1, \alpha, \beta \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself belongs to the set, is said to be a *group**. It follows that if the entire group is multiplied by any one of the symbols, either as further or nearer factor, the effect is simply to reproduce the group; or what is the same thing, that if the symbols of the group are multiplied together so as to form a table, thus :—

Further factors.

Nearer factors.	1	α	β	..
1	1	α	β	..
α	α	α^2	$\beta\alpha$	
β	β	$\alpha\beta$	β^2	
:				

that as well each line as each column of the square will contain all the symbols $1, \alpha, \beta \ldots$ It also follows that the product of any number of the symbols, with or without repetitions, and in any order whatever, is a symbol of the group. Suppose that the group

$$1, \alpha, \beta \ldots$$

contains n symbols, it may be shown that each of these symbols satisfies the equation

$$\theta^n = 1;$$

so that a group may be considered as representing a system of roots of this symbolic binomial equation. It is, moreover, easy to show that if any symbol α of the group satisfies the equation $\theta^r = 1$, where r is less than n, then that r must be a submultiple of n; it follows that when n is a prime number, the group is of necessity of the form

$$1, \alpha, \alpha^2 \ldots \alpha^{n-1}, \quad (\alpha^n = 1).$$

And the same may be, but is not necessarily the case, when n is a composite number. But whether n be prime or composite, the group, *assumed to be of the form in question*, is in

* The idea of a group as applied to permutations or substitutions is due to Galois, and the introduction of it may be considered as marking an epoch in the progress of the theory of algebraical equations.

1854 - Cayley définit la notion de groupe fini

Des puissances égales à un

L'ingrédient principal : groupes finis

Si a est un élément d'un groupe fini, il existe un entier n tel que

$$a^n = \underbrace{a \circ a \circ \ldots \circ a}_{n \text{ fois}} = e.$$

be noticed also, that if $\theta=\phi$, then, whatever the symbols α, β may be, $\alpha\theta\beta=\alpha\phi\beta$, and conversely.

A set of symbols,

$$1,\ \alpha,\ \beta \ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself belongs to the set, is said to be a *group**. It follows that if the entire group is multiplied by any one of the symbols, either as further or nearer factor, the effect is simply to reproduce the group; or what is the same thing, that if the symbols of the group are multiplied together so as to form a table, thus :—

Further factors.

Nearer factors.	1	α	β	..
1	1	α	β	..
α	α	α^2	$\beta\alpha$	
β	β	$\alpha\beta$	β^2	
:				

that as well each line as each column of the square will contain all the symbols $1, \alpha, \beta \ldots$ It also follows that the product of any number of the symbols, with or without repetitions, and in any order whatever, is a symbol of the group. Suppose that the group

$$1,\ \alpha,\ \beta \ldots$$

contains n symbols, it may be shown that each of these symbols satisfies the equation

$$\theta^n=1;$$

so that a group may be considered as representing a system of roots of this symbolic binomial equation. It is, moreover, easy to show that if any symbol α of the group satisfies the equation $\theta^r=1$, where r is less than n, then that r must be a submultiple of n; it follows that when n is a prime number, the group is of necessity of the form

$$1,\ \alpha,\ \alpha^2 \ldots \alpha^{n-1}, \quad (\alpha^n=1).$$

And the same may be, but is not necessarily the case, when n is a composite number. But whether n be prime or composite, the group, *assumed to be of the form in question*, is in

* The idea of a group as applied to permutations or substitutions is due to Galois, and the introduction of it may be considered as marking an epoch in the progress of the theory of algebraical equations.

1854 - Cayley définit la notion de groupe fini

Le début d’une histoire

Un tournant majeur en algèbre

C’est le début d’une histoire : l’algèbre abstraite où l’on s’intéresse plus aux relations entre les objets qu’aux objets eux-même (les opérations plutôt que les nombres).

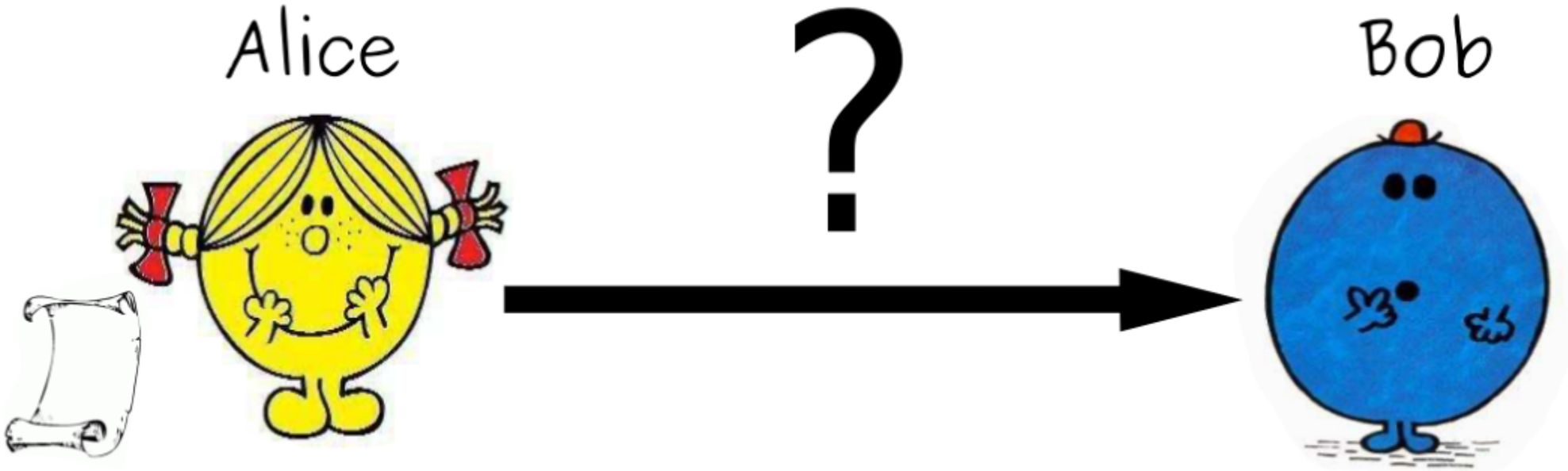
Une grande figure de cette histoire est Emmy Noether dont l’impact au aussi été majeur en physique.

En mathématique, elle développe par exemple la notion d’idéal qui permet de généraliser la décomposition en facteurs premiers à des ensembles plus vastes.

Emmy Noether (1882 - 1935)

Utilisation en cryptographie

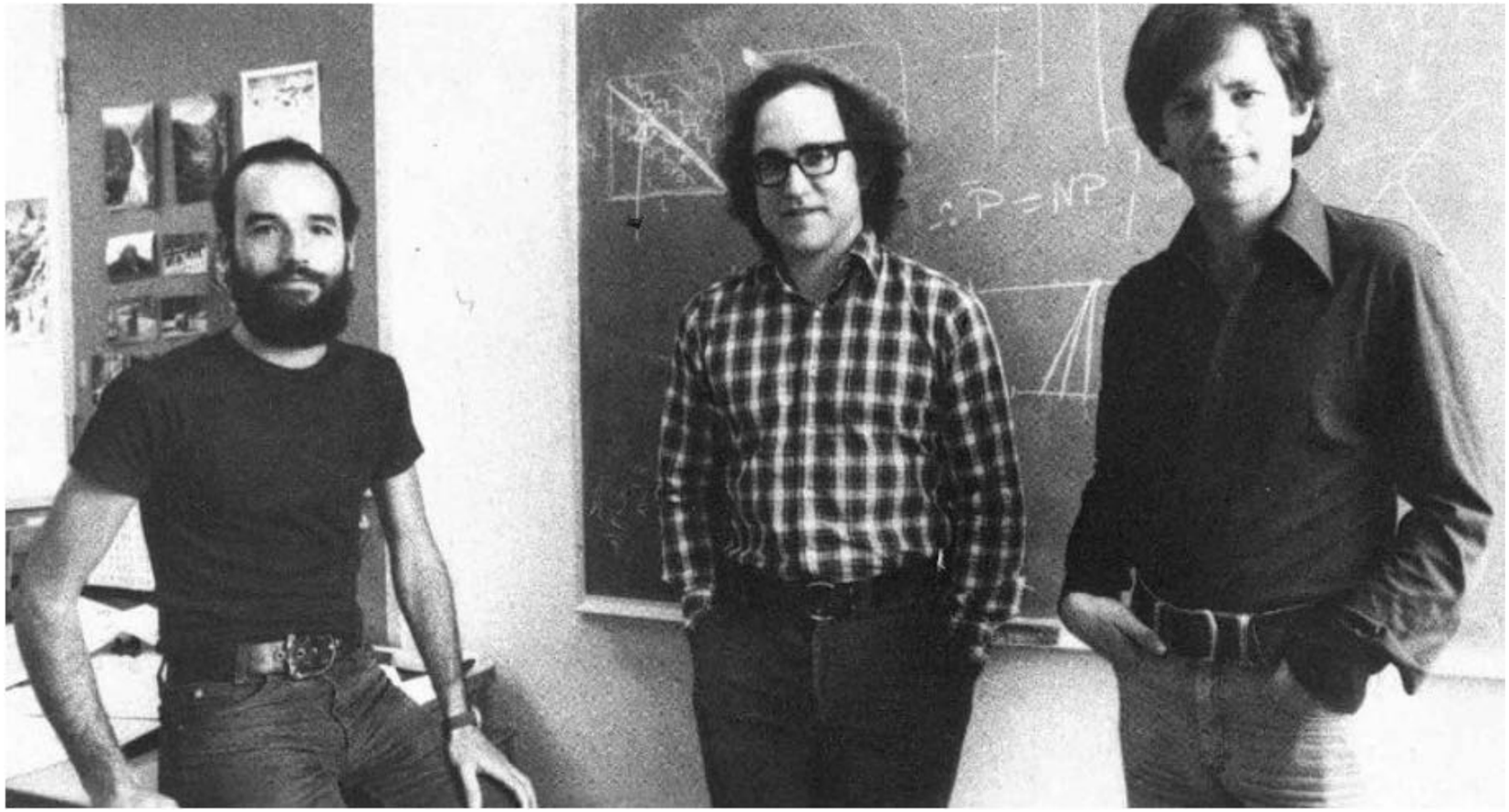
Communiquer en secret avec un inconnu…



Alice veut écrire à Bob qu'elle ne connaît pas et seul Bob doit pouvoir lire le message. Par exemple en remplaçant chaque lettre par sa place dans l'alphabet, le message est un nombre.

Utilisation en cryptographie

Communiquer en secret avec un inconnu…



En 1977, Rivest, Shamir & Adleman ont inventé une méthode qui porte leur nom, la méthode RSA.

Utilisation en cryptographie

Multiplier est facile, factoriser est dur

En secret Bob

- Construit deux nombres premiers p et q
- Calcule le produit $n = pq$
- Calcule $\varphi = (p-1)(q-1)$
- Construit $e < \varphi$ premier avec φ
- Trouve d tel que $de \equiv 1 \pmod{\varphi}$
- Publie n et e dans un annuaire

Pour envoyer le message M. Alice calcule $M^e \pmod{n}$.

Pour comprendre le message, Bob calcule $(M^e)^d \pmod{n}$. Il retrouve le message car $M^{de} = M \times M^{k\varphi}$ et $M^{\varphi} \equiv 1 \pmod{n}$.

Une autre personne que Bob ne connait pas d. Pour le calculer, elle doit connaître φ. Pour cela elle doit connaître p et q, donc factoriser n.

En pratique, il faut couper le message pour que $M < n$.

Calculer sur une courbe.

Courbes elliptiques

D.1.2 Curves over Prime Fields

For each prime p, a pseudo-random curve

$$E: y^2 \equiv x^3 - 3x + b \pmod{p}$$

of prime order n is listed[4]. (Thus, for these curves, the cofactor is always $h = 1$.) The following parameters are given:

- The prime modulus p
- The order n
- The 160-bit input seed *SEED* to the SHA-1 based algorithm (i.e., the domain parameter seed)
- The output c of the SHA-1 based algorithm

D.1.2.1 Curve P-192

p = 6277101735386680763835789423207666416083908700390324961279).

n = 6277101735386680763835789423176059013767194773182842284081

SEED = 3045ae6f c8422f64 ed579528 d38120ea e12196d5

c = 3099d2bb bfcb2538 542dcd5f b078b6ef 5f3d6fe2 c745de65

b = 64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1

G_x = 188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012

G_y = 07192b95 ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811

FIPS PUB 186-4

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Digital Signature Standard (DSS)

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900
http://dx.doi.org/10.6028/NIST.FIPS.186-4
Issued July 2013

U.S. Department of Commerce
Cameron F. Kerry, Acting Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Courbes elliptiques

Définition

Une courbe elliptique est une courbe d'équation

$$y^2 = x^3 + ax + b$$

Où a et b sont des nombres tels que $\Delta = 4a^3 + 27b^2 \neq 0$.

Exemple :

$$y^2 = x^3 - x + 1$$

$a = -1, b = 1$ et $\Delta = 23$.

$$\Delta = 4a^3 + 27b^2$$

Courbes elliptiques

Graphe

En terminale, vous apprendrez à tracer le graphe de fonctions ($y = f(x)$). Si $y^2 = x^3 + ax + b$ alors

$$y = \sqrt{x^3 + ax + b}$$

ou

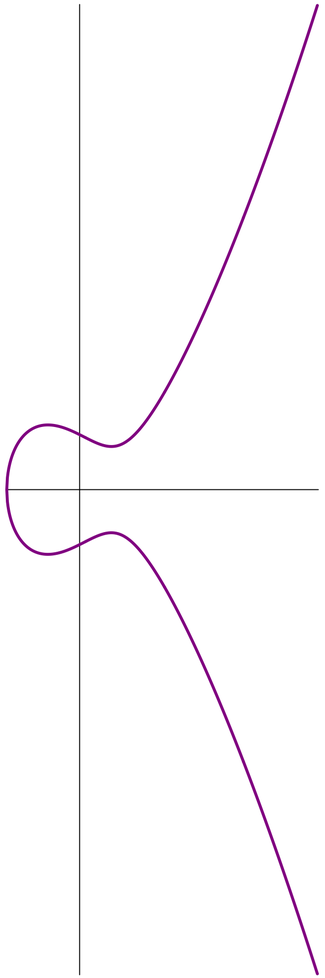
$$y = -\sqrt{x^3 + ax + b}.$$

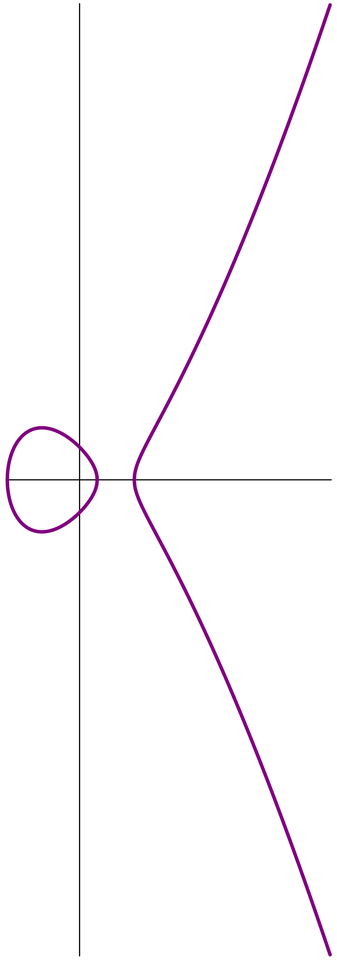
On a donc une courbe avec $y > 0$ et son symétrique par rapport à l'axe des abscisses.

Courbes elliptiques

Deux types de graphes

$\Delta > 0$





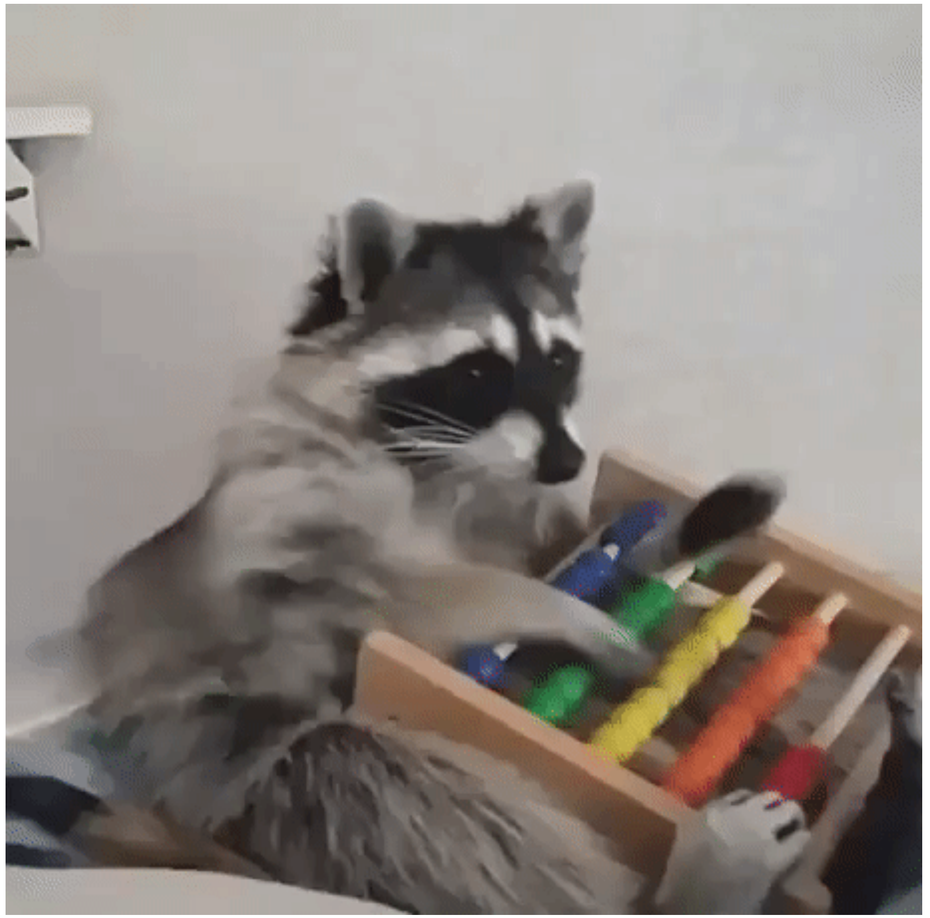
$\Delta < 0$

$$\Delta = 4a^3 + 27b^2$$

Courbes elliptiques

Deux types de graphes

À VOUS !



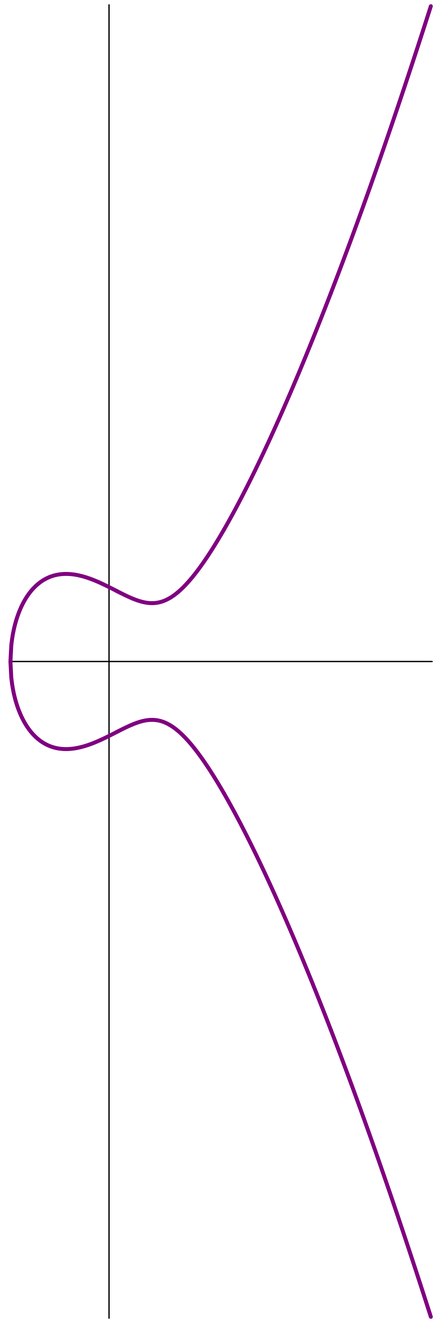
Courbes elliptiques

Deux types de graphes

$$y^2 = x^3 - x + 1$$

$a = -1 \qquad b = 1$

$$\Delta > 0$$



$$\Delta = 4 \times (-1)^3 + 27 \times 1^2 = -4 + 27 = 23$$

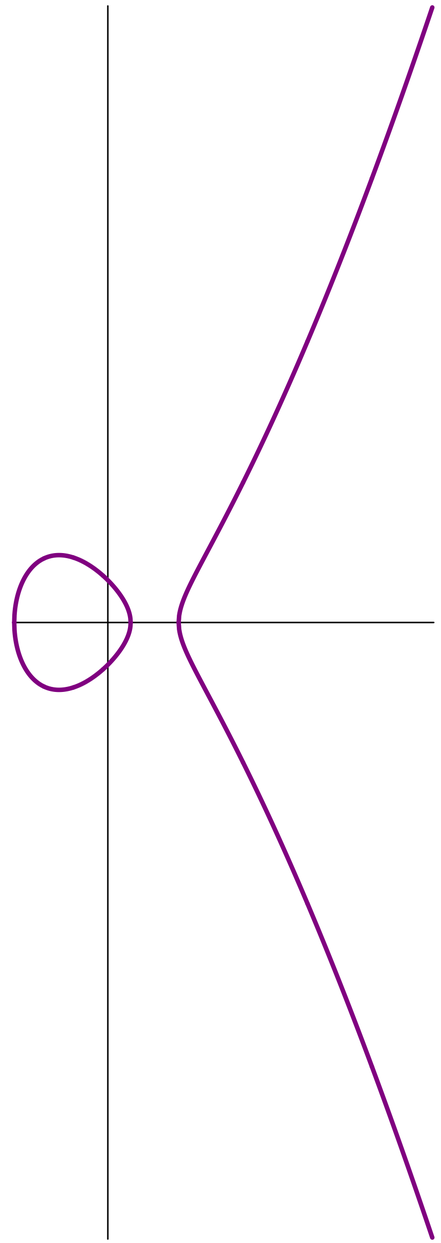
Courbes elliptiques

Deux types de graphes

$$y^2 = x^3 - x + \frac{1}{4}$$

$$a = -1 \qquad b = \frac{1}{4}$$

$$\Delta < 0$$



$$\Delta = 4 \times (-1)^3 + 27 \times \left(\frac{1}{4}\right)^2 = -4 + 27 \times \frac{1}{16}$$

$$= \frac{-4 \times 16 + 27}{16} < 0$$

Courbes elliptiques

Additionner des points distincts

Pour additionner le point P et le point Q

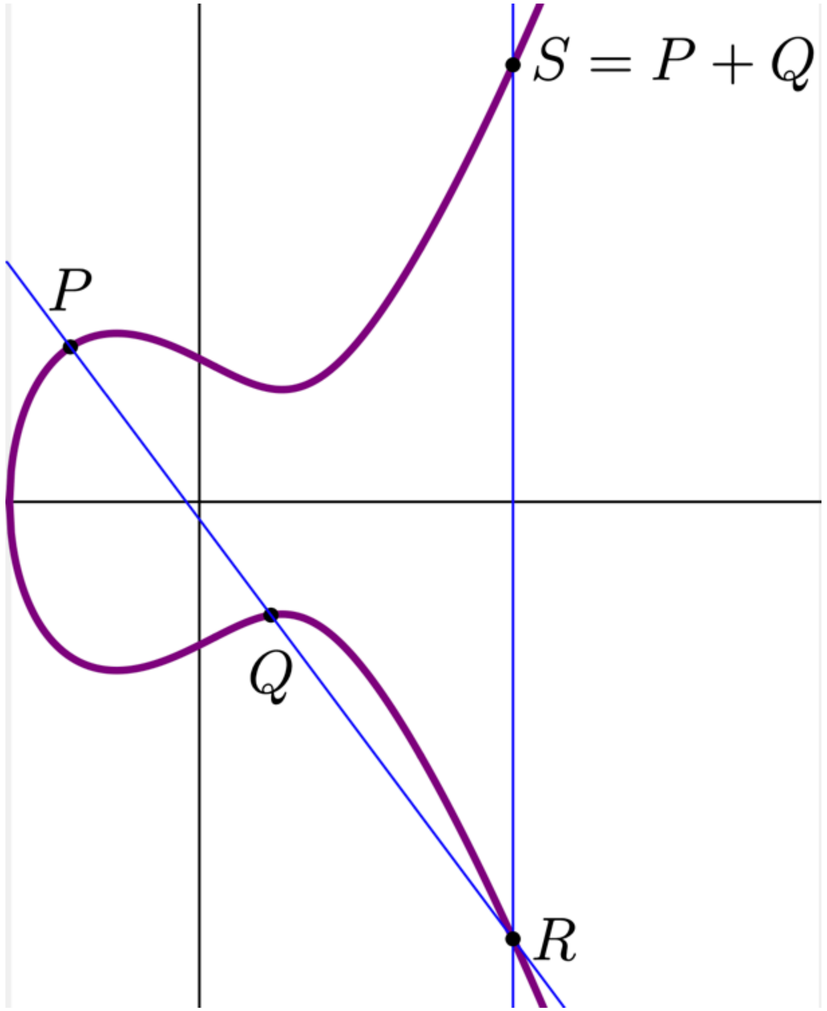
1. Tracer la droite (PQ)
2. Tracer le point R intersection de (PQ) avec la courbe
3. Tracer le point S symétrique de R par rapport à l'axe des abscisses.

Courbes elliptiques

Additionner des points distincts

Pour additionner le point P et le point Q

1. Tracer la droite (PQ)
2. Tracer le point R intersection de (PQ) avec la courbe
3. Tracer le point S symétrique de R par rapport à l'axe des abscisses.

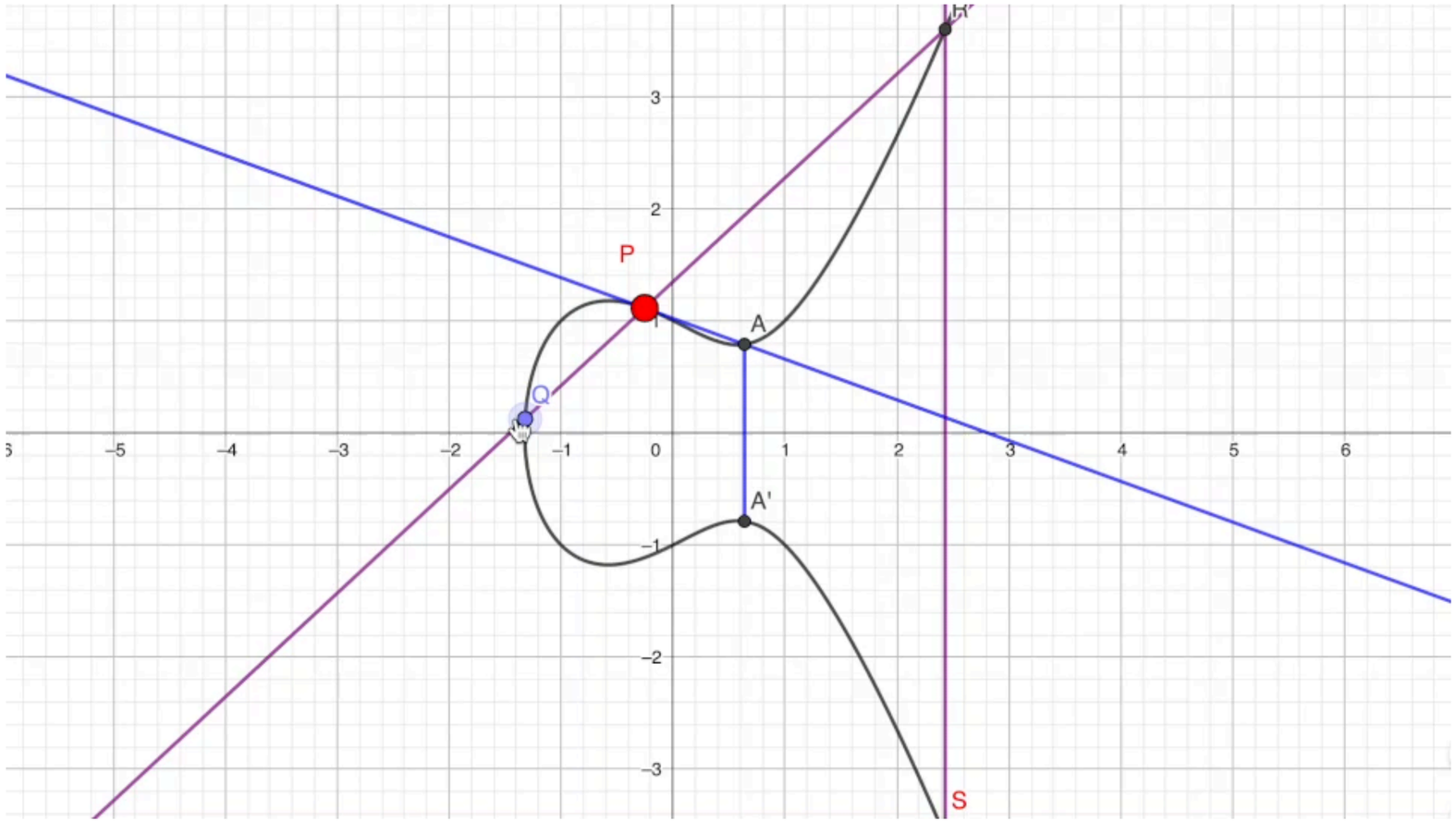


L'opposé d'un point est son symétrique par rapport à l'axe des abscisses.
Par exemple $R = -S$.

Courbes elliptiques

Additionner un point avec lui même

Pour additionner le point P avec lui même, et donc obtenir $2P$,
on additionne P et Q pour Q de plus en plus proche de P.



La somme de P et Q est S. Lorsque Q se rapproche de P, S se rapproche de A'. $2P = A'$.

Courbes elliptiques

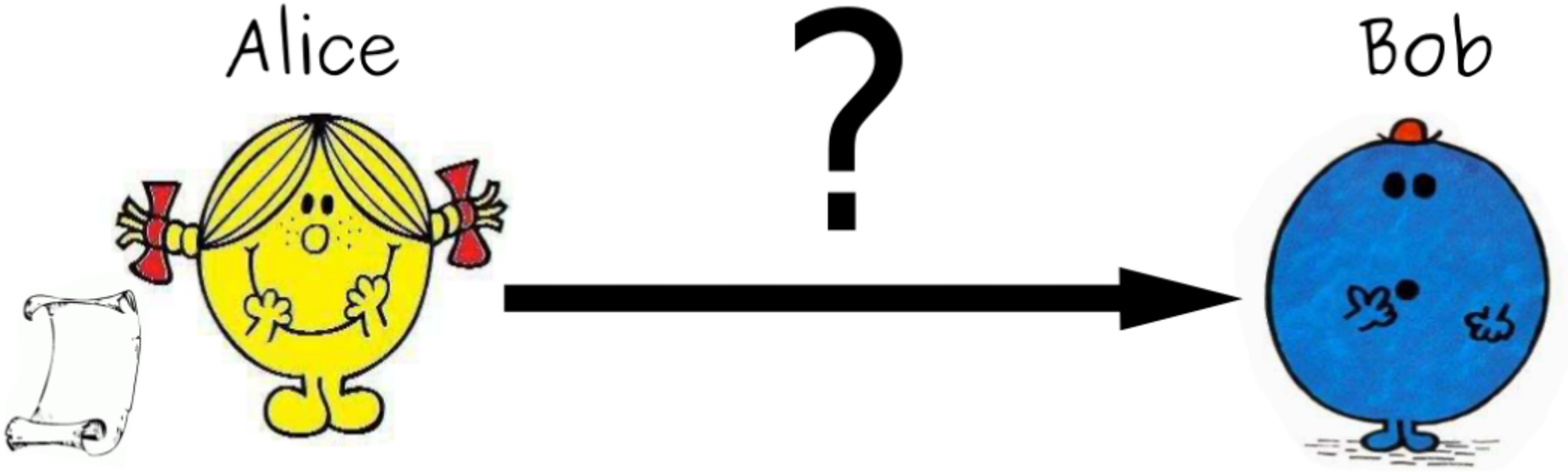
Additionner un point avec lui même

On peut alors calculer

$$
\begin{aligned}
3P &= 2P + P & -2P &= -(2P) \\
4P &= 3P + P & -3P &= -(3P) \\
5P &= 4P + P & -4P &= -(4P) \\
&\vdots & -5P &= -(5P) \\
nP &= (n-1)P + P & &\vdots \\
& & -nP &= -(nP)
\end{aligned}
$$

Courbes elliptiques

Cryptographie



Alice veut écrire à Bob qu'elle ne connaît pas et seul Bob doit pouvoir lire le message.
On suppose qu'il existe une façon de transformer un message en un point d'une courbe… (si, si, croyez moi !)

Courbes elliptiques

Cryptographie

En secret Bob

- Choisit une courbe elliptique E
- Choisit un point P sur la courbe
- Choisit un entier n
- Calcule le point $Q = nP$
- Publie E, P et Q dans un annuaire

Alice transforme son message en un point M de la courbe de Bob

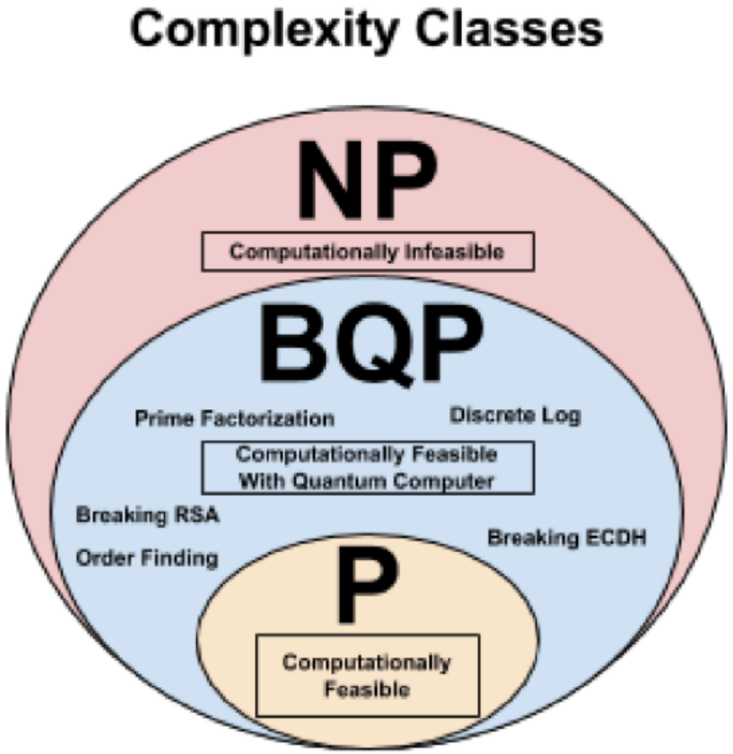
Alice choisit un entier k, calcule kP et $M + kQ$. Elle envoie kP et $M + kQ$ à Bob mais garde k secret.

Bob calcule $n(kP) = kQ$
puis $M + kQ - kQ = M$.

Une autre personne que Bob ne connait pas n. Retrouver n si on ne connait que nP est un problème très compliqué, qu'on ne sait pas faire rapidement.

Et après ?

Cryptographie post-quantique



Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers

Tanja Lange, professeure à l'université de Eindhoven