CRM-CNRS
International Research Lab

Mathématiques des secrets

Arithmétique modulaire, groupes, courbes elliptiques

Emmanuel Royer, CNRS, Université Clermont-Auvergne

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

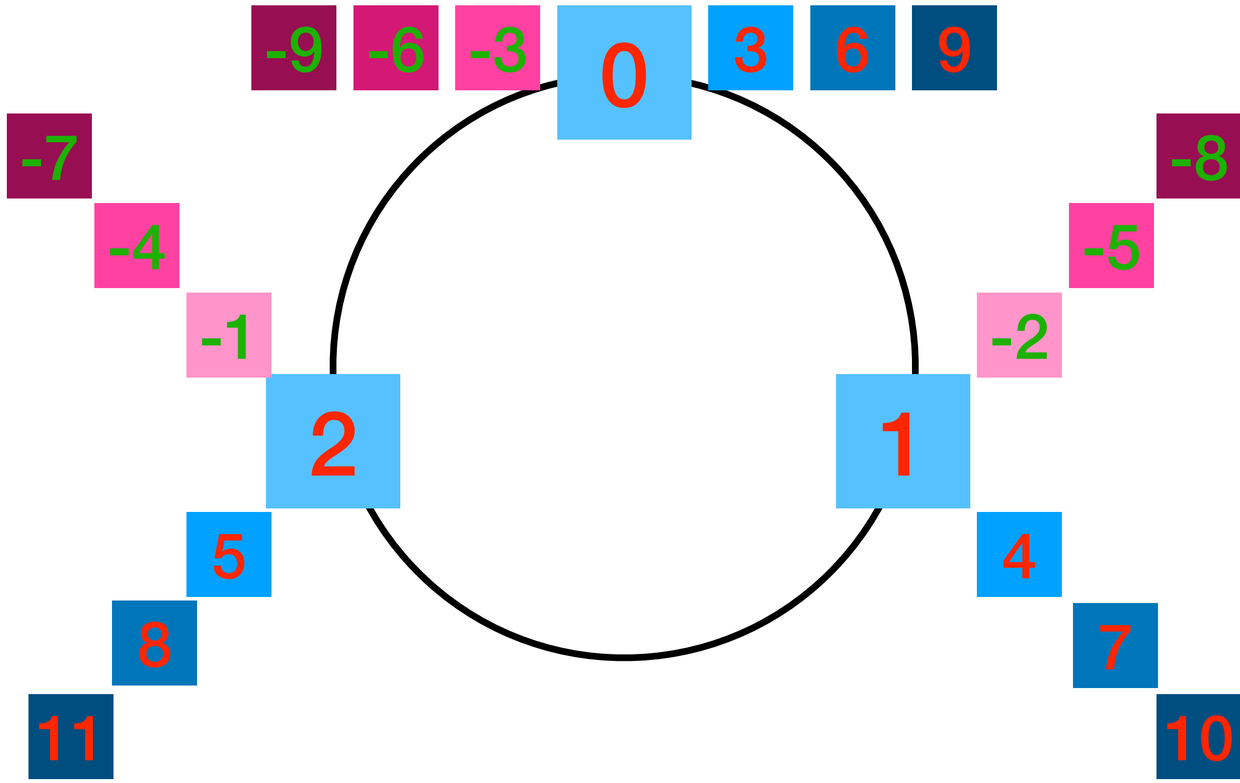
Et ce tableau ?

	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

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 : plus efficace

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

Calcul modulo

Puissance modulo 17

À VOUS !

Que vaut

$3^{16} \pmod{17}$?

Calcul modulo

$$3^{16} \equiv 1 \pmod{17}$$

La solution : première méthode !

$$3^2 \equiv 9$$
$$3^3 \equiv 27 \equiv 10$$
$$3^4 \equiv 30 \equiv 13$$
$$3^5 \equiv 39 \equiv 5$$
$$3^6 \equiv 15$$
$$3^7 \equiv 45 \equiv 11$$
$$3^8 \equiv 33 \equiv 16$$
$$3^9 \equiv 48 \equiv 14$$
$$3^{10} \equiv 42 \equiv 8$$
$$3^{11} \equiv 24 \equiv 7$$
$$3^{12} \equiv 21 \equiv 4$$
$$3^{13} \equiv 12$$
$$3^{14} \equiv 36 \equiv 2$$
$$3^{15} \equiv 6$$
$$3^{16} \equiv 18 \equiv 1$$

Calcul modulo

$$3^{16} \equiv 1 \pmod{17}$$

La solution : première méthode !

$3^2 \equiv 9$

$3^3 \equiv 27 \equiv 10$

$3^4 \equiv 30 \equiv 13$

$3^5 \equiv 39 \equiv 5$

$3^6 \equiv 15$

$3^7 \equiv 45 \equiv 11$

$3^8 \equiv 33 \equiv 16$

$3^9 \equiv 48 \equiv 14$

$3^{10} \equiv 42 \equiv 8$

$3^{11} \equiv 24 \equiv 7$

$3^{12} \equiv 21 \equiv 4$

$3^{13} \equiv 12$

$3^{14} \equiv 36 \equiv 2$

$3^{15} \equiv 6$

$3^{16} \equiv 18 \equiv 1$

Un peu long…

Calcul modulo

$$3^{16} \equiv 1 \pmod{17}$$

La solution : deuxième méthode !

$16 = 2^4$ donc

$$3^{16} \equiv \left(\left((3^2)^2\right)^2\right)^2 \equiv \left((9^2)^2\right)^2$$

$$\equiv \left(\left((-8)^2\right)^2\right)^2 \equiv \left((64)^2\right)^2$$

$$\equiv \left(13^2\right)^2 \equiv 16^2$$

$$\equiv (-1)^2 \equiv 1$$

Moins de calcul…

Exponentiation binaire

Comment aller vite ? Et si on avait deux doigts au lieu de dix ?

$$n = \underbrace{a_0}_{0 \text{ ou } 1} + \underbrace{a_1}_{0 \text{ ou } 1} 2 + \underbrace{a_2}_{0 \text{ ou } 1} 2^2 + \ldots + \underbrace{a_k}_{0 \text{ ou } 1} 2^k$$

donc

$$x^n = x^{a_0}(x^2)^{a_1}\left(x^{2^2}\right)^{a_2} \ldots \left(x^{2^k}\right)^{a_k}$$

Exponentiation binaire

Comment aller vite ? Et si on avait deux doigts au lieu de dix ?

$$n = \underbrace{a_0}_{0 \text{ ou } 1} + \underbrace{a_1}_{0 \text{ ou } 1} 2 + \underbrace{a_2}_{0 \text{ ou } 1} 2^2 + \ldots + \underbrace{a_k}_{0 \text{ ou } 1} 2^k$$

donc

Pour passer de l'un à l'autre, on élève au carré

$$x^n = x^{a_0} (x^2)^{a_1} \left(x^{2^2}\right)^{a_2} \ldots \left(x^{2^k}\right)^{a_k}$$

$(\ldots)^{a_j}$ **vaut soit 1 soit** $(\ldots)$

Calcul modulo

Puissance modulo 17

À VOUS !

Que vaut

$3^{81} \pmod{17}$?

Calcul modulo

La solution !

$$3^{81} \equiv 3 \pmod{17}$$

On se souvient que $3^{16} \equiv 1$.

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

donc

$$3^{81} = (3^{16})^5 \times 3 \equiv 1 \times 3 \equiv 3 \pmod{17}.$$

Calcul modulo

Il n'y a pas que 81 dans la vie…

$3^n \pmod{17}$?

$$n = 16q + r \quad (0 \leq r < 16)$$

donc

$$3^n = (3^{16})^q \cdot 3^r \equiv 3^r \pmod{17}.$$

Calcul modulo

Il n'y a pas que 81 dans la vie…

$3^n \pmod{17}$?

$$n = 16q + r \quad (0 \leq$$

donc

16 valeurs possibles.

$$3^n = (3^{16})^q \cdot 3^r \equiv 3^r \pmod{17}.$$

Calcul modulo

À VOUS !

Calculez $3^n \pmod{17}$ pour toutes les valeurs de n .

Calcul modulo

Valeurs de $3^n \pmod{17}$.

n	0	1	2	3	4	5	6	7
3^n	1	3	9	10	13	5	15	11

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

Calcul modulo

Valeurs de $3^n \pmod{17}$.

Que remarquez-vous ?

n	0	1	2	3	4	5	6	7
3^n	1	3	9	10	13	5	15	11

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

Calcul modulo

Tous les entiers non nuls modulo 17 sont des puissances de 3.

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

À VOUS !

Trouvez un entier x tel que

$$3x = 1 \pmod{17}\,.$$

Calcul modulo

Solution : x **tel que** $3x \equiv 1 \pmod{17}$

$$3^{16} \equiv 1 \pmod{17}$$

donc

$$3 \times 3^{15} \equiv 1 \pmod{17}$$

et $3^{15} \equiv 6 \pmod{17}$

donc

$$3 \times 6 \equiv 1 \pmod{17}.$$

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

Tout ce que tu me dis, je le savais déjà !

« 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 derniere 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

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.

Des puissances égales à un

Le « petit » théorème de Fermat

On lit dans cette lettre :

p

divise

il existe k

a^k

$a^k - 1$

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.

a

Pout tout a, vraiment ?

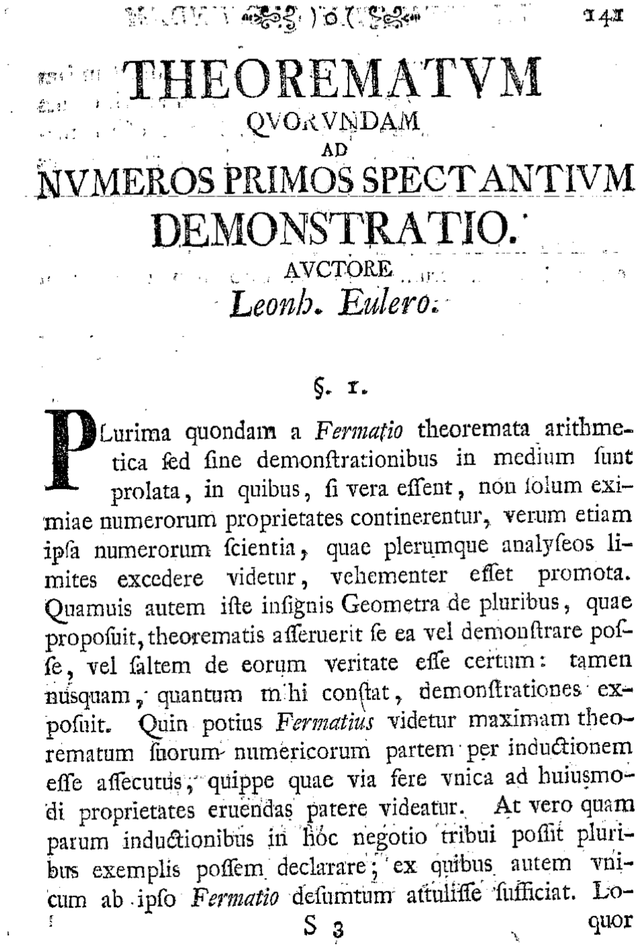
l'entier k est multiple de $p - 1$

Des puissances égales à un

Le « petit » théorème de Fermat

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.



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 eſſet 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 attuliſſe ſufficiat. Lo-

S 3 quor

1741 - Première preuve par Euler

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

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

- $a \circ e = e \circ a = a$ — Élément neutre
- $a \circ (b \circ c) = (a \circ b) \circ c$ — Associativité
- Il existe d tel que $a \circ d = d \circ a = e$. — Inverse

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

Exemple de groupe

Entiers non nuls modulo 17

L'ensemble des entiers $\{1,...,16\} \pmod{17}$ est un groupe à 16 éléments pour le produit : si n, a, b, c sont des éléments de cet ensemble,

- $n \times 1 = 1 \times n = n$
- $a \times (b \times c) = (a \times b) \times c$
- Il existe d tel que $n \times d \equiv d \times n \equiv 1 \pmod{17}$.

1 est l'élément neutre

Associativité

d est l'inverse de n.

On a vu $n \equiv 3^k \pmod{17}$ et $3^{16} \equiv 1 \pmod{17}$ donc on prend $d = 3^{16-k}$.

Exemple de groupe

Attention

L'ensemble des entiers $\{1,...,5\} \pmod 6$ n'est PAS un groupe pour le produit.

En effet, 2 n'a pas d'inverse.

Exemple de groupe

Attention

L'ensemble des entiers $\{1,...,5\} \pmod 6$ n'est PAS un groupe.

En effet, 2 n'a pas d'inverse. Supposons qu'il existe n tel que $2n \equiv 1 \pmod 6$.
Alors, $2n \times 3 \equiv 1 \times 3 \equiv 3 \pmod 6$. Mais, $2n \times 3 \equiv 6n \equiv 0 \pmod 6$.

CONTRADICTION

L'ensemble $\{a \pmod n : a$ et n n'ont pas de diviseur commun autre que $1\}$
est un groupe pour la multiplication

Exemple de groupe

Petit théorème de Fermat

Si p et q sont deux nombres premiers distincts. L'ensemble

$Z_{pq}^{\times} = \{a \pmod{pq} : a \text{ n'est divisible ni par } p \text{ ni par } q\}$

est un groupe pour la multiplication

On pose $\varphi = (p-1)(q-1)$.

Alors, si $a \in Z_{pq}^{\times}$, on a $a^{\varphi} \equiv 1 \pmod{pq}$.

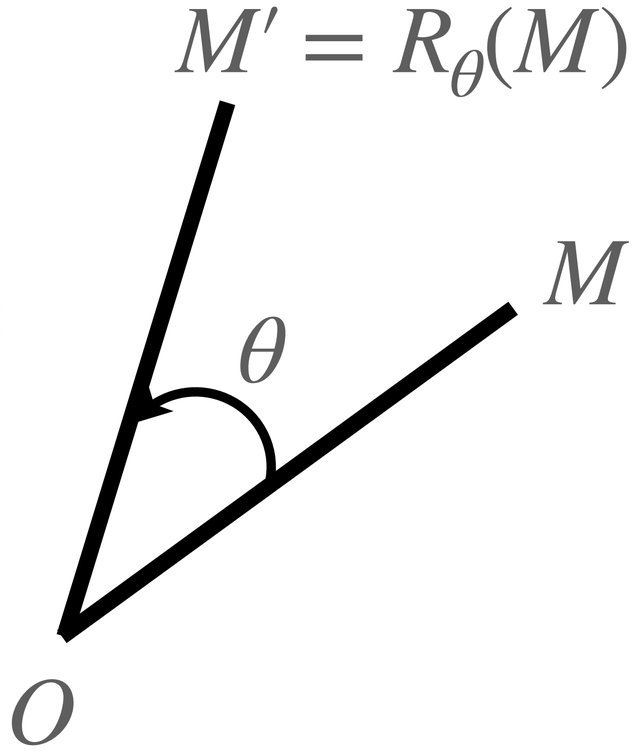
Pour tout $a \in \{1,5\}$ on a $a^2 \equiv 1 \pmod{6}$.

Exemple de groupe

Les rotations

R_θ : rotation d'angle θ autour de O :

- $OM = OM'$
- $\text{Angle}(\overrightarrow{OM}, \overrightarrow{OM'}) = \theta$



Si on fait une rotation d'angle θ_2 autour de O
suivie d'une rotation d'angle θ_1 autour de O
alors, on a fait une rotation d'angle $\theta_1 + \theta_2$ autour de O

$$R_{\theta_1} \circ R_{\theta_2} = R_{\theta_1+\theta_2}$$

Exemple de groupe

Les rotations

$$R_{\theta_1} \circ R_{\theta_2} = R_{\theta_1+\theta_2}$$

$R_\theta \circ R_0 = R_{\theta+0} = R_\theta$ et $R_0 \circ R_\theta = R_{0+\theta} = R_\theta$ R_0 est l'élément neutre

$R_{\theta_1} \circ \left(R_{\theta_2} \circ R_{\theta_3} \right) = R_{\theta_1+(\theta_2+\theta_3)} = R_{(\theta_1+\theta_2)+\theta_3} = \left(R_{\theta_1} \circ R_{\theta_2} \right) \circ R_{\theta_3}$ Associativité

$R_\theta \circ R_{-\theta} = R_{\theta-\theta} = R_0$ et $R_{-\theta} \circ R_\theta = R_{-\theta+\theta} = R_0$ $R_{-\theta}$ est l'inverse de R_θ.

Exemple de groupe

Une opération sur les couples de réels

Si a, b, c, d sont quatre réels on définit le produit du couple (a, b) par le couple (c, d) :

$$(a, b) \odot (c, d) = (ac - bd, ad + bc)\,.$$

Élément neutre $(1,0)$

$$(a, b) \odot (1,0) = (a, b) = (1,0) \odot (a, b)\,.$$

Exemple de groupe

Une opération sur les couples de réels

$$(a,b) \odot (c,d) = (ac - bd, ad + bc)$$

Associativité

$$\begin{aligned}
\big((a,b) \odot (c,d)\big) \odot (e,f) &= (ac - bd, ad + bc) \odot (e,f) \\
&= \big((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e\big) \\
&= (ace - bde - adf - bcf, acf - bdf + ade + bce)
\end{aligned}$$

$$\begin{aligned}
(a,b) \odot \big((c,d) \odot (e,f)\big) &= (a,b) \odot (ce - df, cf + de) \\
&= \big(a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)\big) \\
&= (ace - adf - bcf - bde, acf + ade + bce - bdf)
\end{aligned}$$

Exemple de groupe

Une opération sur les couples de réels

$$(a,b) \odot (c,d) = (ac - bd, ad + bc)$$

Inverse

$$(a,b) \odot \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right) = \left(\frac{a^2}{a^2+b^2} - \frac{b(-b)}{a^2+b^2}, \frac{-ab}{a^2+b^2} + \frac{ba}{a^2+b^2} \right) = (1,0)$$

$$\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right) \odot (a,b) = \left(\frac{a^2}{a^2+b^2} - \frac{(-b)b}{a^2+b^2}, \frac{ab}{a^2+b^2} + \frac{a(-b)}{a^2+b^2} \right) = (1,0)$$

Si $(a,b) \neq (0,0)$ alors (a,b) à un inverse : c'est $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right)$.

Exemple de groupe

$$(a,b) \odot (c,d) = (ac - bd, ad + bc)$$

Une opération sur les couples de réels

Pour l'opération $\odot$ l'ensemble

$$\{(a,b) \in \mathbb{R}^2 : (a,b) \neq (0,0)\}$$

est un groupe.

Le reconnaissez-vous ?

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).

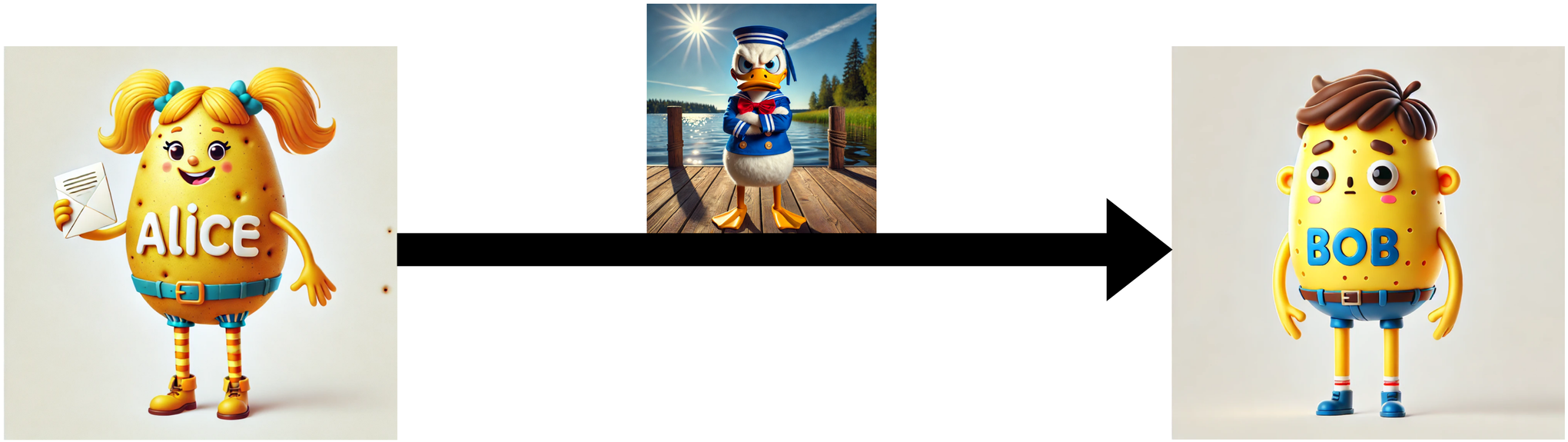
Une grande figure de cette histoire est Emmy Noether dont l’impact a aussi été majeur en physique.

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

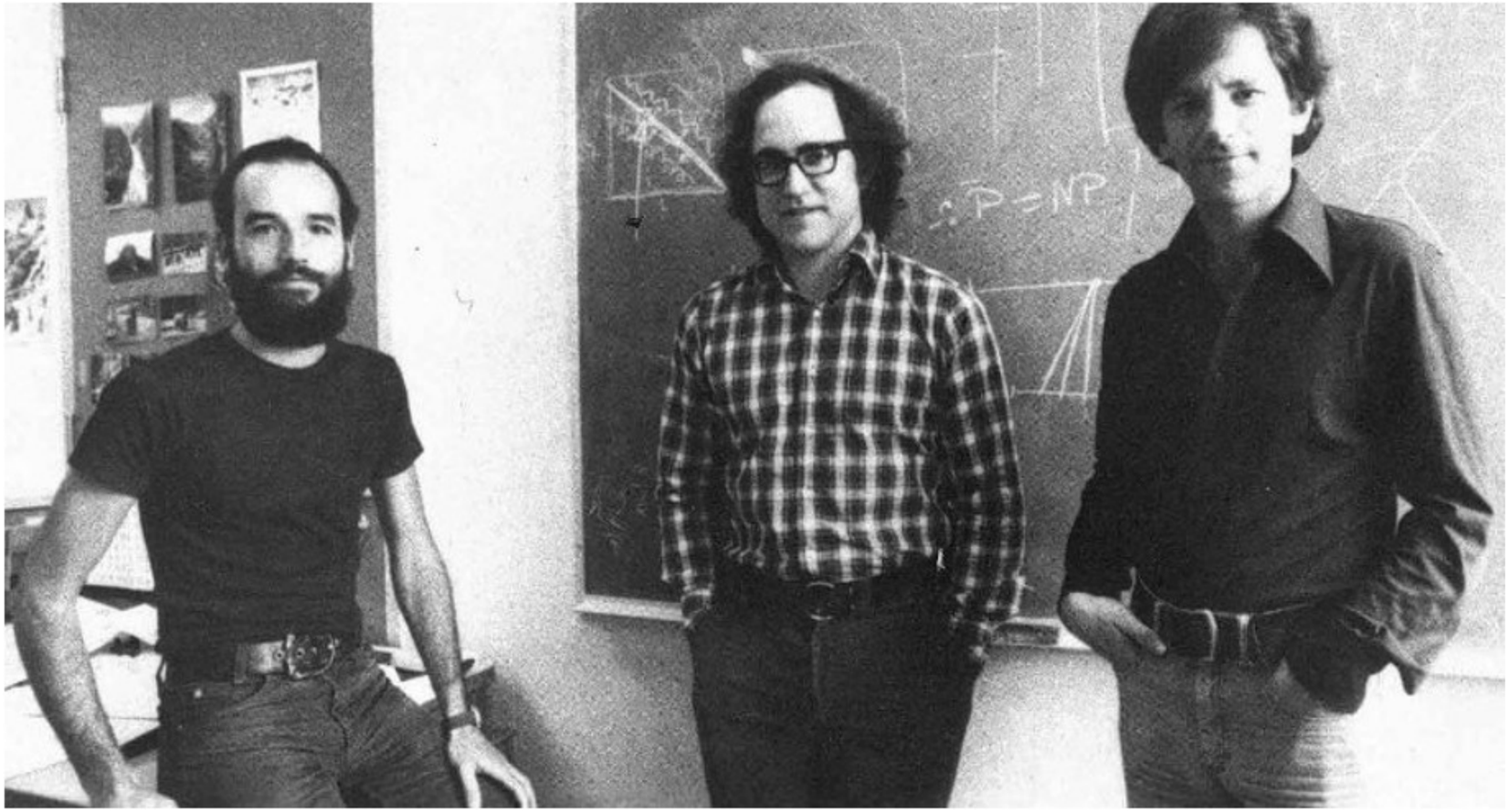
Communiquer en secret avec un inconnu…



Alice veut écrire à Bob qu'elle ne connaît pas et seul Bob doit pouvoir lire le message.
Donald voudrait bien connaître le message d'Alice.
Par exemple en remplaçant chaque lettre par sa place dans l'alphabet, le message est un nombre : $A \to 1; B \to 2...$

Utilisation en cryptographie

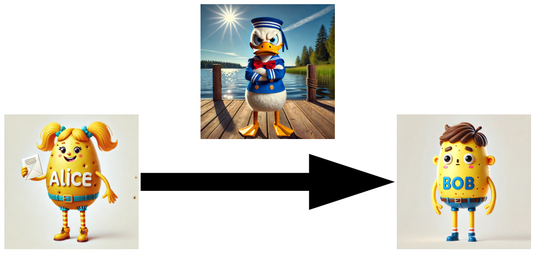
Communiquer en secret avec un inconnu…



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



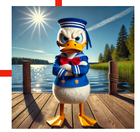
En secret Bob

- 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 $M^{\varphi} \equiv 1 \pmod{n}$.

Donald ne connait pas d. Pour le calculer, il doit connaître φ. Pour cela elle doit connaître p et q, donc factoriser n.



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

BOB 

SECRET	PUBLIC
p, q	
$n = pq$	n
$\varphi = (p-1)(q-1)$	
e tel que $e \leq \varphi$ premier à φ	e
d tel que $de \equiv 1 \pmod{\varphi}$	

ALICE 

SECRET	PUBLIC
Message	
$T = (\text{Message})^e$	T

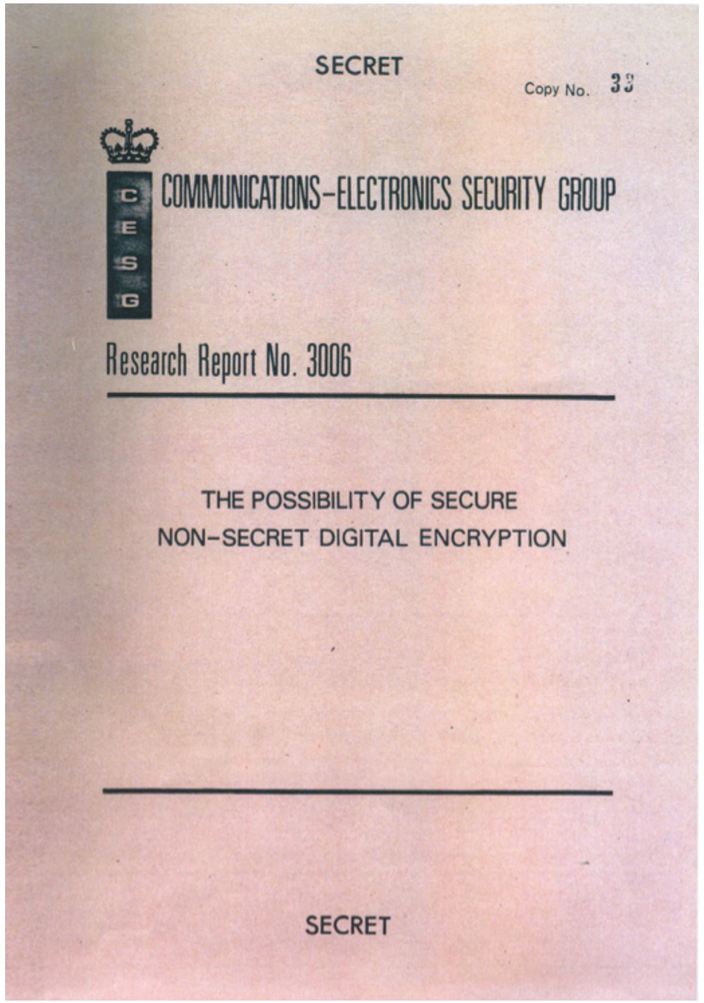
BOB 

$$T^d = \text{Message}^{\varphi} = \text{Message}\,.$$

Donald doit calculer d et donc φ. Pour cela il a besoin de p et q et donc FACTORISER n. C'est compliqué.

Avant RSA

Découvertes antérieurs d'Ellis, Cocks & Williamson… restés secrets jusqu'en 1997



SECRET

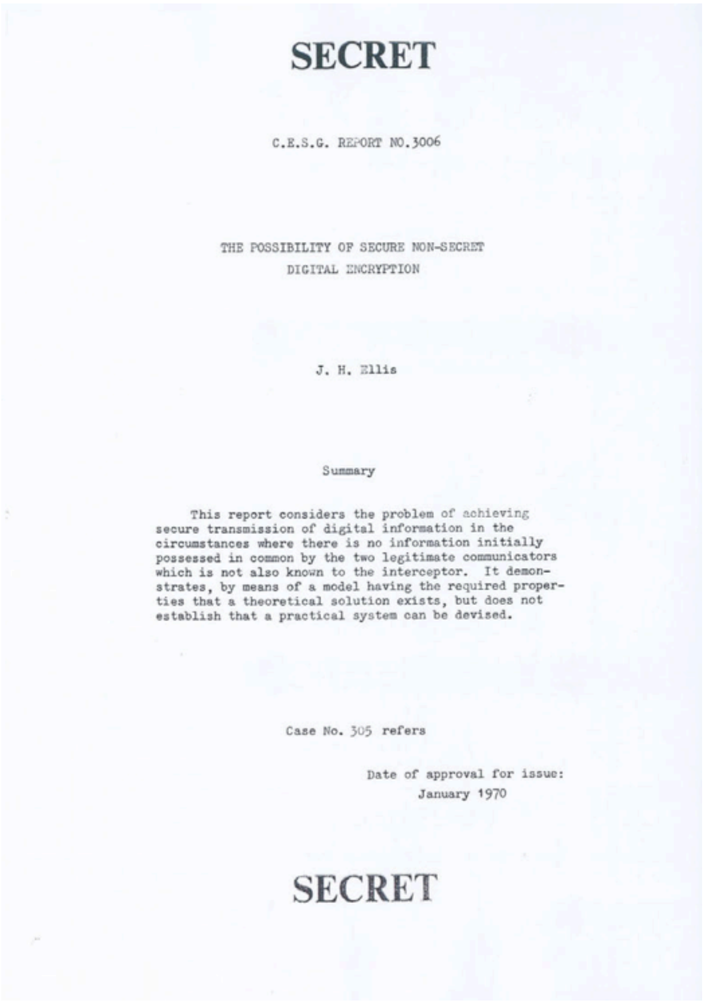
Copy No. 33

COMMUNICATIONS-ELECTRONICS SECURITY GROUP

Research Report No. 3006

THE POSSIBILITY OF SECURE
NON-SECRET DIGITAL ENCRYPTION

SECRET



SECRET

C.E.S.G. REPORT NO.3006

THE POSSIBILITY OF SECURE NON-SECRET
DIGITAL ENCRYPTION

J. H. Ellis

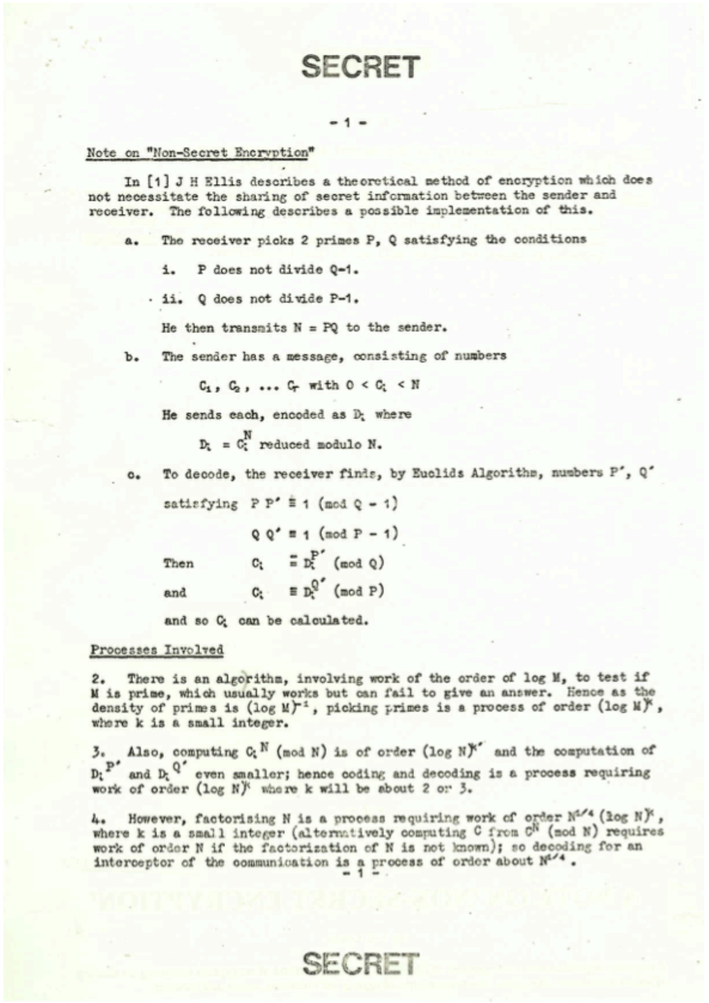
Summary

This report considers the problem of achieving secure transmission of digital information in the circumstances where there is no information initially possessed in common by the two legitimate communicators which is not also known to the interceptor. It demonstrates, by means of a model having the required properties that a theoretical solution exists, but does not establish that a practical system can be devised.

Case No. 305 refers

Date of approval for issue:
January 1970

SECRET



SECRET

- 1 -

Note on "Non-Secret Encryption"

In [1] J H Ellis describes a theoretical method of encryption which does not necessitate the sharing of secret information between the sender and receiver. The following describes a possible implementation of this.

a. The receiver picks 2 primes P, Q satisfying the conditions

i. P does not divide Q-1.

ii. Q does not divide P-1.

He then transmits N = PQ to the sender.

b. The sender has a message, consisting of numbers

$C_1, C_2, \ldots C_r$ with $0 < C_i < N$

He sends each, encoded as D_i where

$D_i = C_i^N$ reduced modulo N.

c. To decode, the receiver finds, by Euclids Algorithm, numbers P', Q' satisfying $P P' \equiv 1 \pmod{Q-1}$

$Q Q' \equiv 1 \pmod{P-1}$

Then $C_i \equiv D_i^{P'} \pmod{Q}$

and $C_i \equiv D_i^{Q'} \pmod{P}$

and so C_i can be calculated.

Processes Involved

2. There is an algorithm, involving work of the order of log M, to test if M is prime, which usually works but can fail to give an answer. Hence as the density of primes is $(\log M)^{-1}$, picking primes is a process of order $(\log M)^k$, where k is a small integer.

3. Also, computing $C_i^N \pmod{N}$ is of order $(\log N)^{k'}$ and the computation of $D_i^{P'}$ and $D_i^{Q'}$ even smaller; hence coding and decoding is a process requiring work of order $(\log N)^k$ where k will be about 2 or 3.

4. However, factorising N is a process requiring work of order $N^{1/4}(\log N)^k$, where k is a small integer (alternatively computing C from $C^N \pmod{N}$ requires work of order N if the factorization of N is not known); so decoding for an interceptor of the communication is a process of order about $N^{1/4}$.

- 1 -

SECRET

Exercice : factoriser 234 497

Le nombre RSA_{250} donné par

2140324650240744961264423072839333563008614715144755017797754
9208814180234471401366433455190958046796109928518724709145876
8739626192155736304745477052080511905649310668769159001975940
5693457452230589325976697471681738069364894699871578494975937
497937

n’a été factorisé qu’en 2020 par une équipe de mathématiciennes et mathématiciens franco—états-unienne : Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé et Paul Zimmermann.

Donald doit calculer d et donc φ. Pour cela il a besoin de p et q et donc FACTORISER n. C’est compliqué.

$$p = 6413528947707158027879019017057738908482501474294344720811685963202453234463023862359875266834770873766192558569463979885336 7$$

$$q = 3337202759497815655622601060535511422794076034476755466678452098702384172921003708025744867329688187756571898625803693206271 1$$

$$\mathrm{RSA}_{250} = pq$$

Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment*

Fabrice Boudot[1], Pierrick Gaudry[2], Aurore Guillevic[2], Nadia Heninger[3], Emmanuel Thomé[2], and Paul Zimmermann[2]

[1] Université de Limoges, XLIM, UMR 7252, F-87000 Limoges, France
[2] Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France
[3] University of California, San Diego, USA

In memory of Peter L. Montgomery

Abstract. We report on two new records: the factorization of RSA-240, a 795-bit number, and a discrete logarithm computation over a 795-bit prime field. Previous records were the factorization of RSA-768 in 2009 and a 768-bit discrete logarithm computation in 2016. Our two computations at the 795-bit level were done using the same hardware and software, and show that computing a discrete logarithm is not much harder than a factorization of the same size. Moreover, thanks to algorithmic variants and well-chosen parameters, our computations were significantly less expensive than anticipated based on previous records.
The last page of this paper also reports on the factorization of RSA-250.

1 Introduction

The Diffie-Hellman protocol over finite fields and the RSA cryptosystem were the first practical building blocks of public-key cryptography. Since then, several other cryptographic primitives have entered the landscape, and a significant amount of research has been put into the development, standardization, cryptanalysis, and optimization of implementations for a large number of cryptographic primitives. Yet the prevalence of RSA and finite field Diffie-Hellman is still a fact: between November 11, 2019 and December 11, 2019, the ICSI Certificate Notary [21] observed that 90% of the TLS certificates used RSA signatures, and 7% of the TLS connections used RSA for key exchange. This holds

Un défi

Factoriser l'entier RSA_{260} donné par

2211282552952966643528108525502623092761208950247001539441374831912882294140200198651272972656974659908590033003140005117074220456085927635795375718595429883895870922923849100670303412462054578456641366454068421436129301769402084639106587591479425143514445819

Factoriser l'entier RSA_{2048} donné par

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035 7

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

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

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

ou

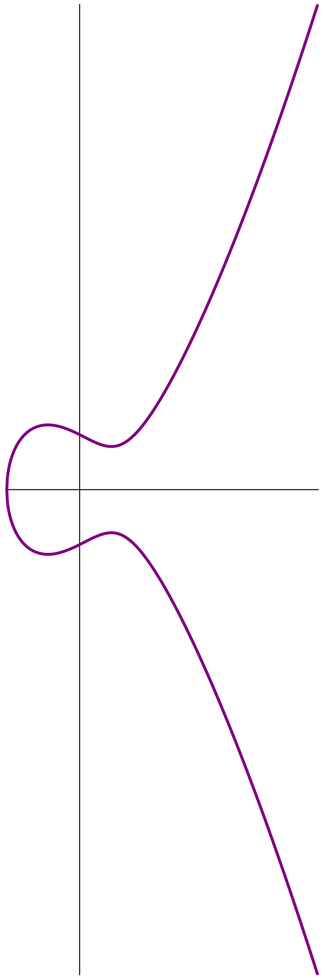
$$y = -\sqrt{x^3 + ax + b}.$$

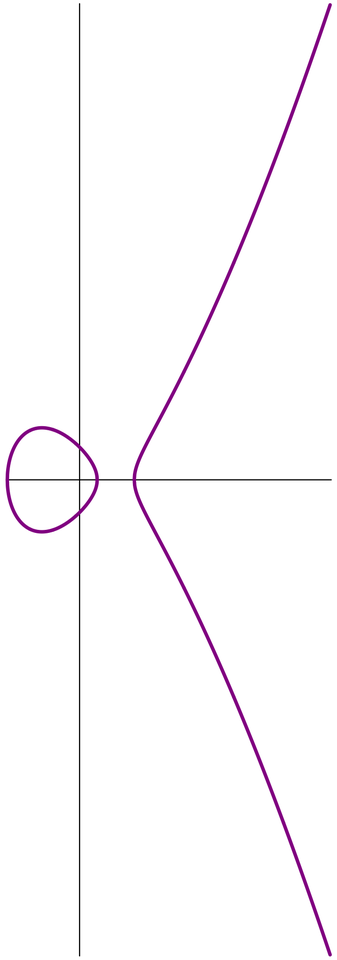
On a donc une courbe avec $y > 0$ et son symétrique par rapport à l'axe des abscisses.

Courbes elliptiques

Deux types de graphes

$\Delta > 0$





$\Delta < 0$

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

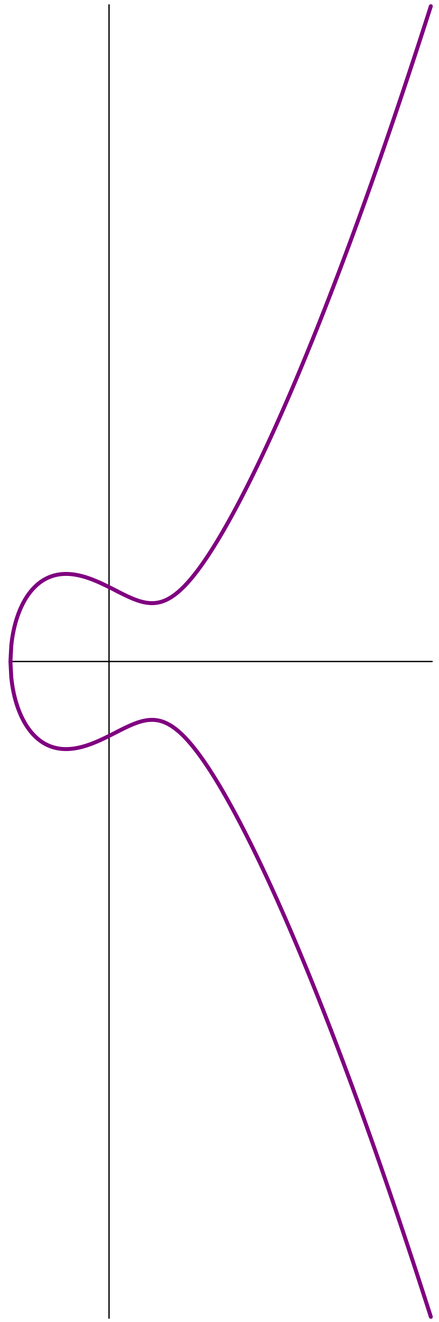
Courbes elliptiques

Deux types de graphes

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

$a = -1 \qquad b = 1$

$$\Delta > 0$$



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

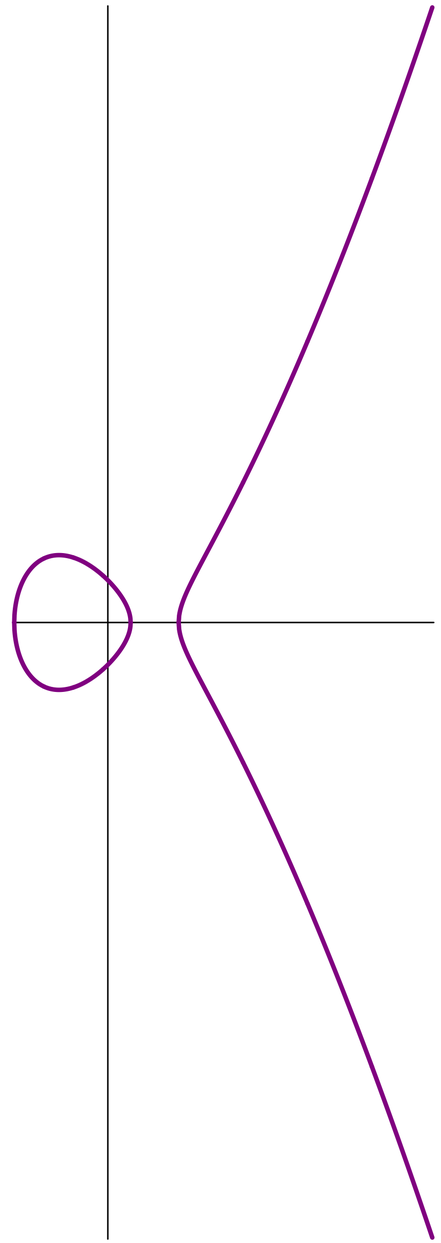
Courbes elliptiques

Deux types de graphes

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

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

$$\Delta < 0$$

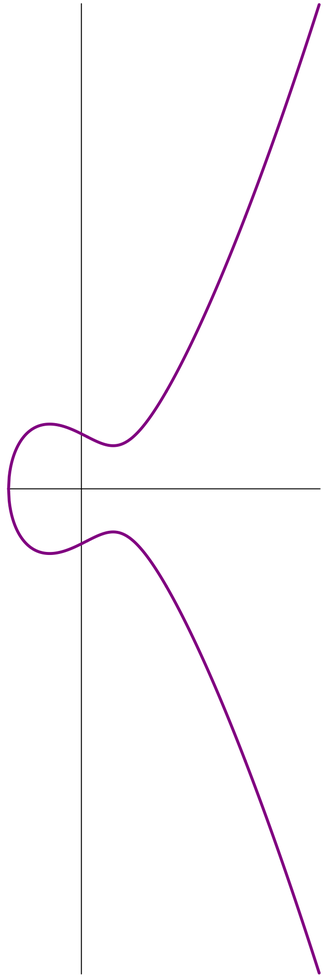


$$\Delta = 4 \times (-1)^3 + 27 \times \left(\frac{1}{4}\right)^2 = -4 + 27 \times \frac{1}{16}$$

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

Courbes elliptiques

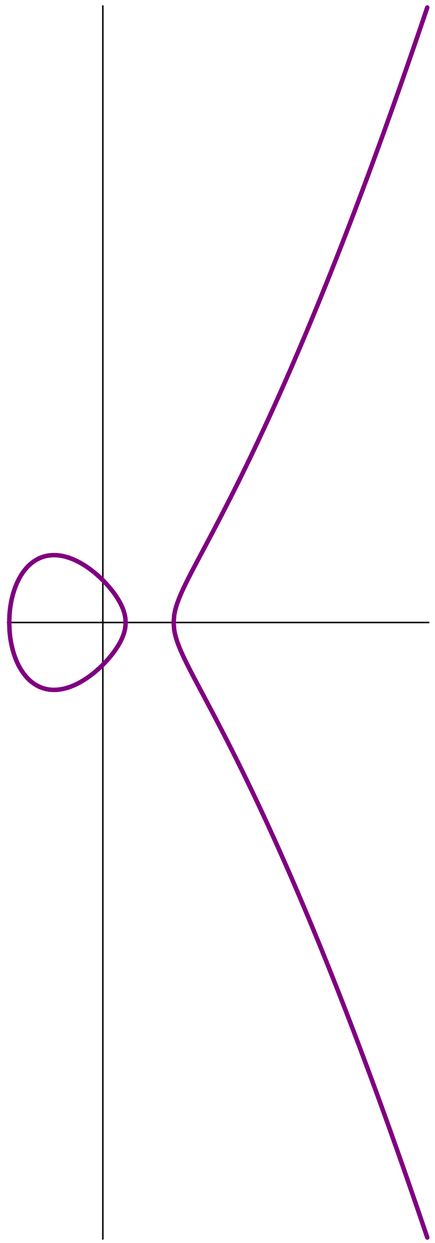
Un groupe !



On sait construire une addition des points des courbes elliptiques pour en faire un groupe !

On sait décrire les points des courbes dont les coordonnées sont des nombres entiers.

Si on regarde les points modulo un nombre premier, on a alors un groupe fini.



Courbes elliptiques

Additionner des points distincts

Pour additionner le point P et le point Q

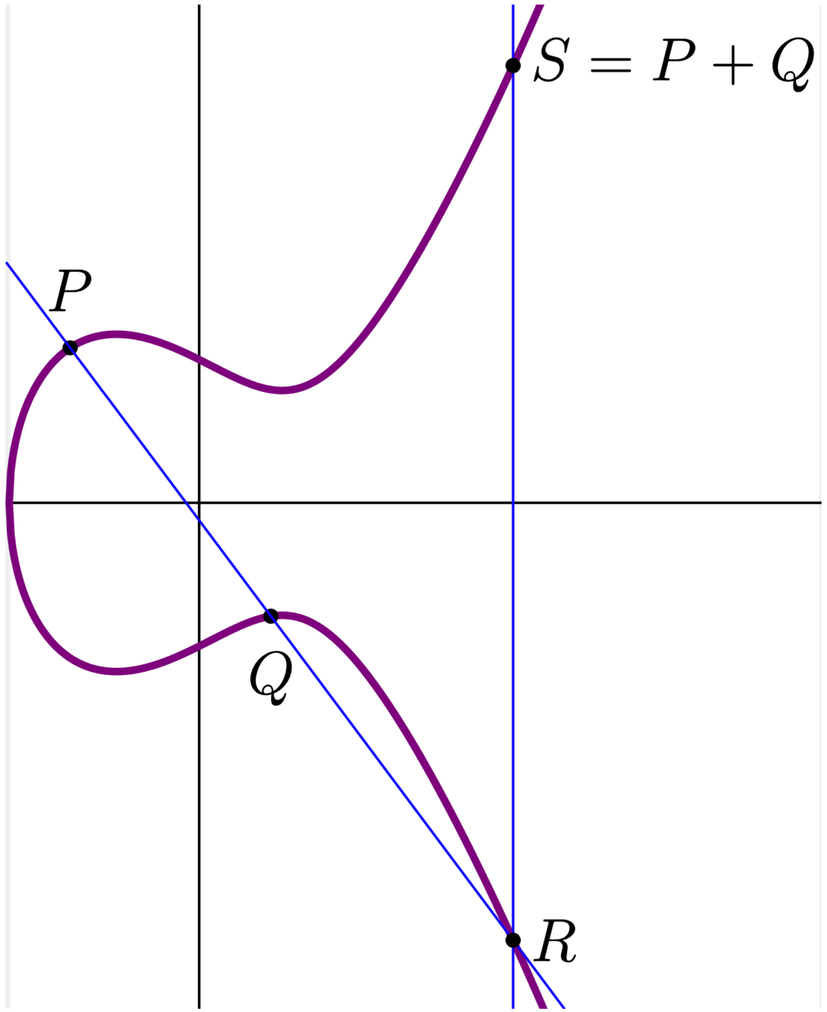
1. Tracer la droite (PQ)
2. Tracer le point R intersection de (PQ) avec la courbe
3. Tracer le point S symétrique de R par rapport à l'axe des abscisses.

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. Ce point S est $P + Q$.

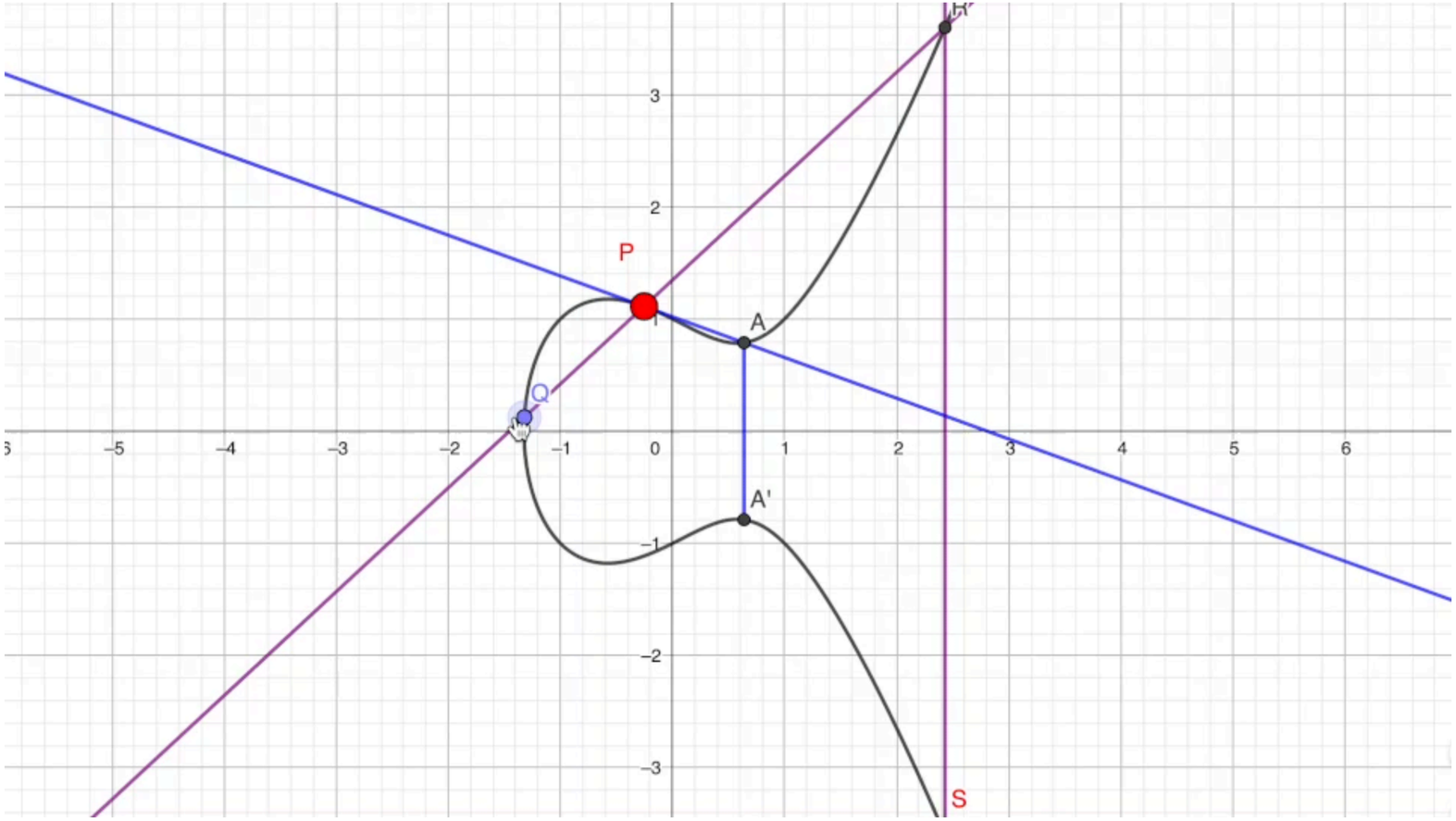


L'opposé d'un point est son symétrique par rapport à l'axe des abscisses.
Par exemple $R = -S$.

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

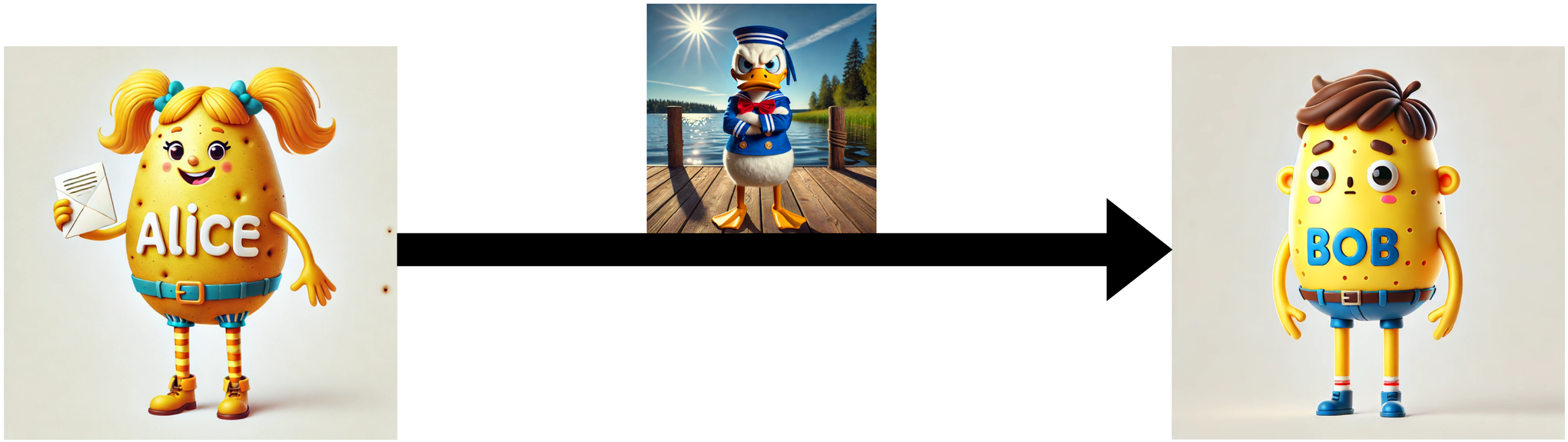
Additionner un point avec lui même

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

Problème du logarithme discret

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.

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 $M + kQ - kQ = M$.

BOB 

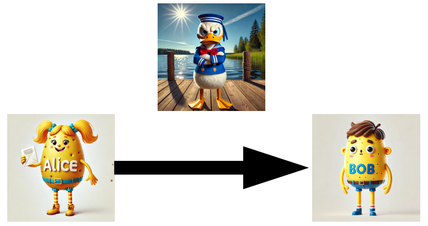
SECRET	PUBLIC
	Courbe E
	Point P de E
Entier n	
$Q = nP$	Point Q de E

ALICE 

SECRET	PUBLIC
$M =$ Message	
Entier k	
$M_1 = kP$	Point M_1 de E
$M_2 = M + kQ$	Point M_2 de E

BOB 

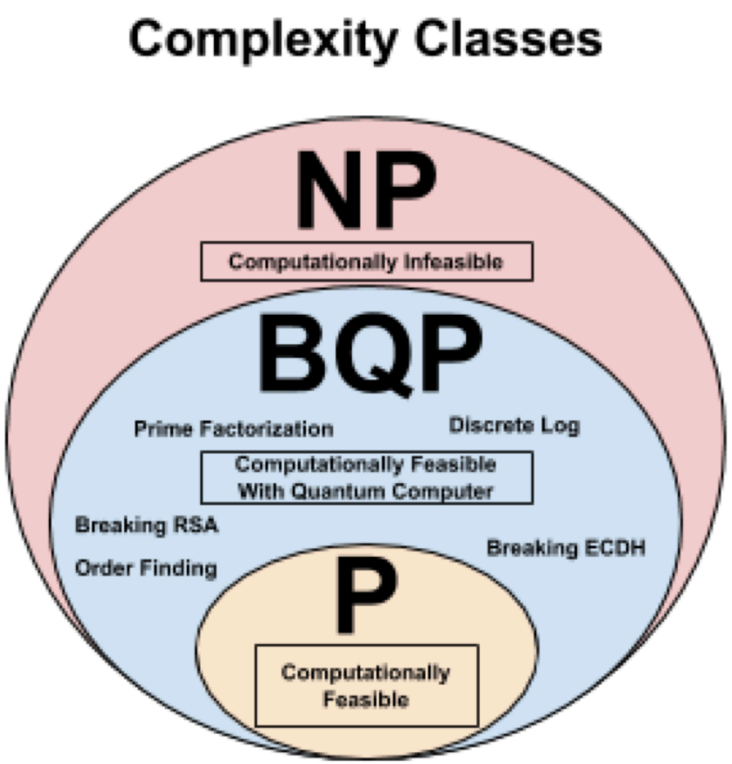
$$M_2 - nM_1 = M + kQ - nkP = M + kQ - kQ = M$$



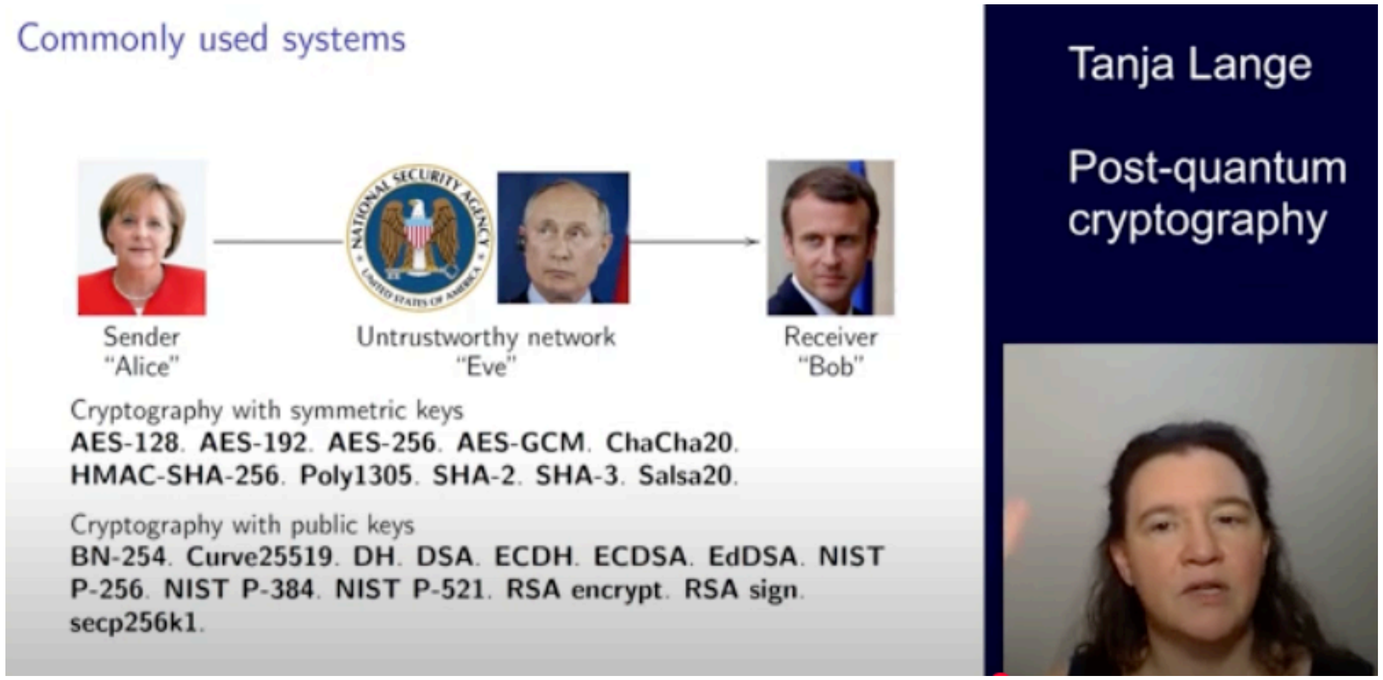
Donald doit calculer n et donc trouver le nombre par lequel il doit multiplier P pour obtenir Q. C'est TRÈS LONG à moins de trouver une méthode qu'aujourd'hui personne ne connaît.

Et après ?

Cryptographie post-quantique



Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers, J. Tibbetts, 2019.



https://youtu.be/dEpk4ZxceeY?si=JjO2eAjdvEa0wIoc

Tanja Lange, professeure à l'université de Eindhoven