La théorie des nombres dans la vie courante

Phong (Nguyễn)

« La mathématique est la reine des sciences, et l'arithmétique est la reine des mathématiques. »

Gauss

1940


HARDY
L'APOLOGIE
D'UN MATHÉMATICIEN
UN SAVANT, UNE ÉPOQUE


L'HOMME QUI DÉFIAIT
L'INFINI

Dans la vie courante…

Ce soir

- Détection d'erreur
- Détection de fraude
- L'échange de secret

Détection d'erreurs

L'invasion des nombres

- Mais comment détecter des erreurs de transmission ?

Détection d'erreurs

- Beaucoup de nombres sont formatés pour détecter les erreurs.

M = 

- On veut H(m)≠H(m') si m' proche de m.
- En recevant M, on recalcule H(m).

Quelles Erreurs ?

- Erreurs de chiffre : 5 → 7
- Erreurs de transposition : 38 → 83

Numéros de livre

m_{13}	m_{12}	...	m_4	m_3	m_2	H(m) = m_1

- Code ISBN à 13 chiffres.
- **Equation de vérification :**

  $m_{13}+3m_{12}+m_{11}+3m_{10}+m_9+\ldots+3m_2+m_1 \equiv 0 \pmod{10}$

- $9+3\times7+8+3\times3+1+3\times6+1+3\times4+8+3\times4+1+3\times0+0\equiv0 \pmod{10}$

9	**7**	**8**	**3**	**1**	**6**	**1**	**4**	**8**	**4**	**1**	**0**	**0**

Numéros de livre

m_{13}	m_{12}	...	m_4	m_3	m_2	H(m)

- Th: $m_{13}+3m_{12}+m_{11}+3m_{10}+\ldots+m_1 \equiv 0 \pmod{10}$ devient invalide si un seul chiffre m_i est modifié.
- Car $f(n)=3n \pmod{10}$ est une permutation des chiffres : pourquoi ?

Numéros de livre

- Mais $m_{13}+3m_{12}+m_{11}+3m_{10}+\ldots+m_1 \equiv 0 \pmod{10}$ peut rester valide si deux chiffres consécutifs sont échangés.

9	7	8	3	1	6	1	4	8	4	1	0	0
9	7	**3**	**8**	1	6	1	4	8	4	1	0	0
9	7	8	3	**6**	**1**	1	4	8	4	1	0	0

- Car $8+3\times3 \equiv 3+3\times8$ et $1+3\times6 \equiv 6+3\times1$.

- **Th**: ISBN ne peut détecter les erreurs de transposition (0,5), (1,6), (2,7), (3,8) and (4,9).

Améliorer l'équation pour détecter plus ?

- $m_{13}+3m_{12}+m_{11}+3m_{10}+\ldots+m_1 \equiv 0 \pmod{10}$

9	7	8	3	1	6	1	4	8	4	1	0	0

Numéros Visa/Mastercard

m_{16}	m_{15}	...	m_4	m_3	m_2	H(m)

4	2	2	2	0	7	6	9	6	1	4	8	2	3	5	7

- **Equation de vérification :**

  $f(m_{16})+m_{15}+f(m_{14})+m_{13}+\ldots+f(m_2)+m_1 \equiv 0 \pmod{10}$

  où $f(n) = 2n+\lfloor n/5 \rfloor \pmod{10}$.

n	0	1	2	3	4	5	6	7	8	9
f(n)	0	2	4	6	8	1	3	5	7	9

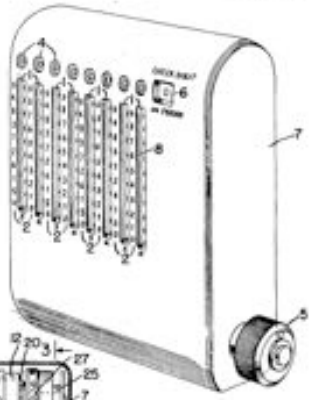
Breveté par Luhn (1960)

Aug. 23, 1960 H. P. LUHN 2,950,048

COMPUTER FOR VERIFYING NUMBERS

Filed Jan. 6, 1954 3 Sheets-Sheet 1

FIG. 1



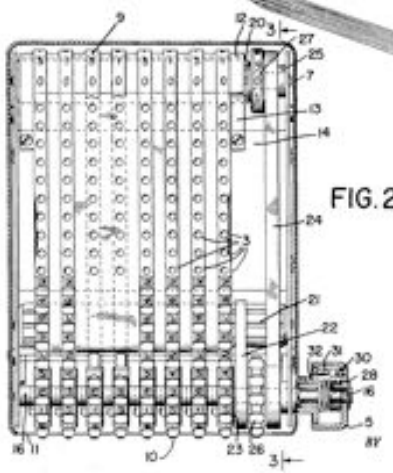


FIG. 2

INVENTOR.
HANS P. LUHN
BY
ATTORNEYS

United States Patent Office 2,950,048 Patented Aug. 23, 1960

1

2,950,048

COMPUTER FOR VERIFYING NUMBERS

Hans P. Luhn, Armonk, N.Y., assignor to International Business Machines Corporation, New York, N.Y., a corporation of New York

Filed Jan. 6, 1954, Ser. No. 402,491

5 Claims. (Cl. 235—61)

This invention relates to a hand computer for computing a check digit for numbers or for verifying numbers which already have a check digit appended.

The principal object of the invention is to provide a simple, inexpensive and portable computer for computing check digits and to provide a simple device for verifying numbers which have a check digit appended.

A further object of the invention is to provide apparatus for computing, in a fast and simple manner, check digits to append to the numbers or to verify numbers with check digits attached.

Pursuant to the invention, a visual check is provided for use at the time of verification. Stamping means is also preferably provided for recording the verified number and for preserving the visual check, which may be appended to the number.

The apparatus of my invention is used in a checking system for multi-digit numbers to indicate whether, in transmitting a number, an error has been made, such as a transposition of the digits. It may be used, for example, where a great many parts are ordered, manufactured, invoiced, shipped, and billed by multi-digit numbers. When a number is first assigned to a new part a check digit is computed, as will be explained hereinafter, and this check digit is appended to the righthand end of the part number. Thereafter whenever the correctness of that part number is in question the number can always be easily and quickly verified by my invention.

The particular mathematical system of number checking preferably embodied in my invention is one in which a single digit, called the check digit, is appended to the righthand end of the original or true number. The value of this check digit is so computed that in verifying the number by cross addition of the multiple digits of the number and the check digit, in accordance with a rule of substitution, the result will be a zero. This zero will appear as such on the computer. If the stamping or printing means of my device is utilized, a check mark may be used to indicate that the number is correct.

Specific illustrations of my invention are shown in the accompanying drawings illustrating two embodiments of the invention, and in which:

Figure 1 is a front perspective view of one of the said embodiments of my device;

Figure 2 is a front elevation of one of the said embodiments partially in cross section;

Figure 3 is a cross-section of one of the said embodiments on the line 3—3 in Figure 2;

Figure 4 is a perspective view of a portion of the same, partly in cross section;

Figure 5 is a front elevation of another embodiment of my invention; and

Figure 6 is a sectional view taken on the line 6—6 in Figure 5.

For convenience of description, the operation of the apparatus of my invention, first in computing a check digit and secondly in verifying a number with a check digit appended, will be set forth to facilitate a complete understanding of the function and purpose of the apparatus. This will be followed by a description of the apparatus and its operation.

It is commonly known that in copying a number comprised of a plurality of digits it often happens that an error occurs by transposing two of the digits. This common error is detected by the invention herein described by the cross addition of digits, the alternate digits being replaced by "substitute" digits, prior to the cross addition. It should be understood that other systems of cross addition checking could be utilized but the system used herein is described as a practical example. In such a method of cross addition for checking a number, it is readily seen that the straight cross addition of the original digits of a number would fail to give any information concerning erroneous transposition because the sum would be the same regardless of the relative placement of the digits. However, if every other digit is a substitute digit in accordance with the system herein set forth, such an error will be detected.

The substitute digit equals twice the original digit plus an end around carry (an end around carry in this system means the addition of any digit standing in the tens position to the digit standing in the units position in the doubled number, as shown below). Thus the substitute digit for an original –3– is –6–(–2–)(–3–=–6–). The substitute digit for an original –6–, illustrating the end around carry, is –3–(–2–)(–6–=–12–=–1–+–2–=–3–).

The following table gives the substitute for each digit according to this system.

Original .... –0– –1– –2– –3– –4– –5– –6– –7– –8– –9–
Substitute... –0– –2– –4– –6– –8– –1– –3– –5– –7– –9–

Applying this system of substitute digits to determine the check digit for a number of seven digits (which is the number of digits provided for in the particular embodiment of the invention hereinafter described), such as –4872148–, first a check digit will be determined, and secondly the number with the check digit appended will be verified. In accordance with the substitution system utilized in my invention, the first digit of the number reading from left to right is a substitute digit, the second digit is an original digit and then this order is repeated until all of the digits have been accounted for. The first digit of the example number, the original –4–, is replaced by its substitute digit, an –8–. This –8– is added to the next digit –8–, an original digit, resulting in the sum of –16– which becomes a –6– by casting out tens in the usual manner. The next digit is an original –7– which is replaced by its substitute digit, a –5–. This –5– is added to the –6– resulting in a –1–. This cross addition, if continued in accordance with the above, across the remaining four digits of the sample number would result in a sum of –6–. This can be determined from the following table giving the original and alternate substitute digits for the number in question.

Original ---------- –4 8 7 2 1 4 8–
Alternate Substitute ... –8+8+5+2+2+4+7– = –6–

Once this sum of –6– has been computed the check digit to be appended is derived by adding to this sum its tens complement or in this case the digit –4–, this being the amount to be added to –6– to produce ten. If this –4– is added to the sum –6– as an original number, the total in the last column will be a –0–. The significance of this particular end result will become apparent in the explanation of the verification of a number having a check digit appended.

It should be realized that the check digit should be added in as an original number. This is accomplished by starting out by using either the original or the substitute digit for the first digit of the alternate substitute

Mieux qu'ISBN

4	2	2	2	0	7	6	9	6	1	4	8	2	3	5	7

- $f(m_{16})+m_{15}+f(m_{14})+m_{13}+\ldots+f(m_2)+m_1 \equiv 0 \pmod{10}$ devient invalide si :
  - Un seul chiffre est modifié.
  - Ou deux chiffres consécutifs sont échangés, sauf 09 ou 90 car f(0)=0 and f(9)=9. C'est 98% des erreurs de transposition.

Erreurs de transposition

- $n+f(m) \equiv m+f(n)$ ssi $f(m)-m \equiv f(n)-n$.

n	0	1	2	3	4	5	6	7	8	9
3n-n	0	2	4	6	8	0	2	4	6	8
f(n)-n	0	1	2	3	4	6	7	8	9	0

- Luhn détecte plus d'erreurs de transpositions qu'ISBN.

Question

- Pour détecter toutes les erreurs de chiffre et de transposition, il faut une permutation f de {0,1,...,9} telle que $n \longmapsto f(n)-n \pmod{10}$ soit aussi une permutation.

Est-ce que f existe ?

Réponse

- **Th**: Il n'y a aucune permutation f de {0,1,…,9} telle que $n \longmapsto f(n)-n \pmod{10}$ soit aussi une permutation.

Améliorer l'équation pour détecter plus ?

- $m_{13}+3m_{12}+m_{11}+3m_{10}+\ldots+m_1 \equiv 0 \pmod{10}$

9	7	8	3	1	6	1	4	8	4	1	0	0

Changer l'addition!

m_n	m_{n-1}	...	m_4	m_3	m_2	H(m)

- **Equation de vérification** :
  $(...((((m_n \oplus m_{n-1}) \oplus m_{n-2}) \oplus m_{n-3}...) \oplus m_1 \equiv 0.$

  Th. [Damm04]: Il existe une opération $\oplus$ sur les chiffres détectant toutes les erreurs de chiffre et transposition.

Changer l'addition!

- **Equation de vérification** :
  $(\ldots((((m_n \oplus m_{n-1}) \oplus m_{n-2}) \oplus m_{n-3} \ldots) \oplus m_1 \equiv 0.$
- Pour détecter toutes les erreurs de chiffre et transposition :
  - $\oplus$ forme un carré latin.
  - $a \oplus b = b \oplus a$ si et seulement si $a=b$
  - $(c \oplus a) \oplus b = (c \oplus b) \oplus a$ si et seulement si $a=b$

$*_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	2	6	0	4	1	7	9	5	3	8
2	3	9	7	0	5	2	8	1	6	4
3	4	5	1	8	0	6	3	9	2	7
4	5	8	6	2	9	0	7	4	1	3
5	6	4	9	7	3	1	0	8	5	2
6	7	3	5	1	8	4	2	0	9	6
7	8	7	4	6	2	9	5	3	0	1
8	9	2	8	5	7	3	1	6	4	0
9	1	0	3	9	6	8	4	2	7	5

Plus loin

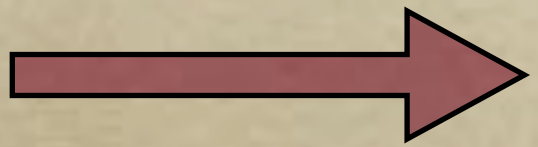
- Détection d'erreur pour des nombres beaucoup plus grands.
- Correction d'erreur : polynômes, algèbre…

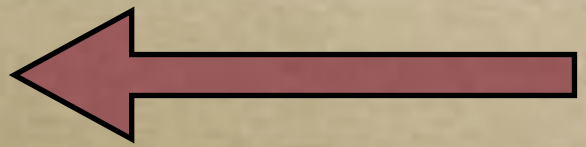
Détection de fraude

Authentification de jeux vidéo

- 1985: Nintendo Entertainment System (NES)

nombre aléatoire m





Vérifier que
$c=H_k(m)$

$c=H_k(m)$

Authentification de jeux vidéo

- 1986: Console Atari 7800

Jeu m

Signature s

Vérifier que s est une signature de m.
Aucun secret : tout est public.

La cryptographie d'Atari

- Chaque console Atari contenait ce nombre de 288 chiffres (956 bits):

  N =

  372763642186038806257268716646134295445276919770501371632454989813933011717
  191815478227077666354717093229568663134016637150236330535225150892192538221
  159833191692967632985205532866327828781379842477084956795255916389772921854
  26539445105636090901552389504405454480086852903016020974765727 3.

- Vérification : $H(m) == s^2 \bmod N$

Jeu *Signature*

La cryptographie d'Atari

- Atari connaissait deux nombres premiers p et q tels que $N=pq$ et $p \equiv q \equiv 3 \bmod 4$.
- Pour chaque jeu m, Atari calculait:
  - $s := a(h^{(p+1)/4} \bmod p) + b(h^{(q+1)/4} \bmod q)$
    où $h = H(m)$, $a = q(p^{-1} \bmod q)$
    et $b = p(q^{-1} \bmod p)$.
  - Alors $s^2 = h \bmod N$ si h est un carré.

La cryptographie d'Atari

- Aucun secret dans la console, ni dans la cartouche.
- Les nombres premiers étaient cachés chez Atari.
- La securité repose sur la difficulté de factoriser de grands entiers.

Record de factorisation

- Février 2020 : N=pq de 250 chiffres (829 bits).
- Temps de calcul du meilleur algorithme connu :

$$(\log N)^{1.923\left(\frac{\log N}{\log\log N}\right)^{1/3}}$$

Cryptographie à base de factorisation

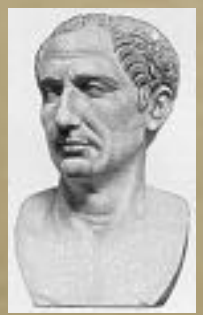
Comment échanger un secret

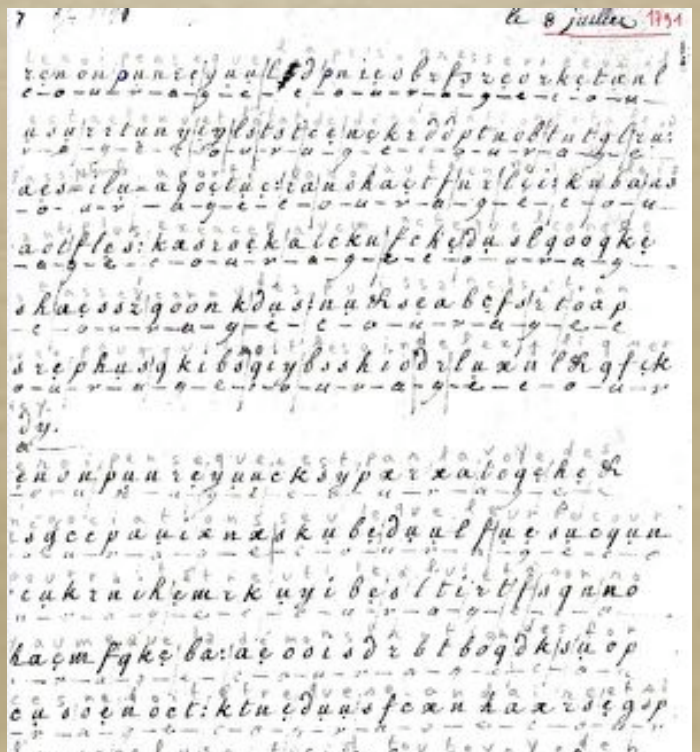
L’irruption de la théorie des nombres en cryptographie

Cryptographie

- 2000 ans avant J.C.

- Jusqu'aux années 1980, utilisé surtout par l'armée et la diplomatie.



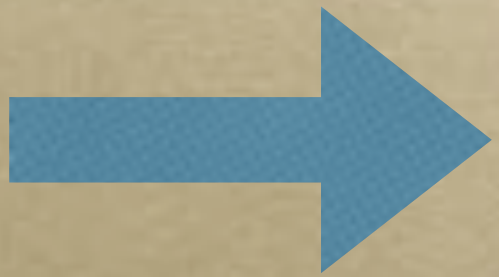


Chiffrement

- On transforme un message pour le rendre inintelligible. L'opération inverse est le déchiffrement.

Message

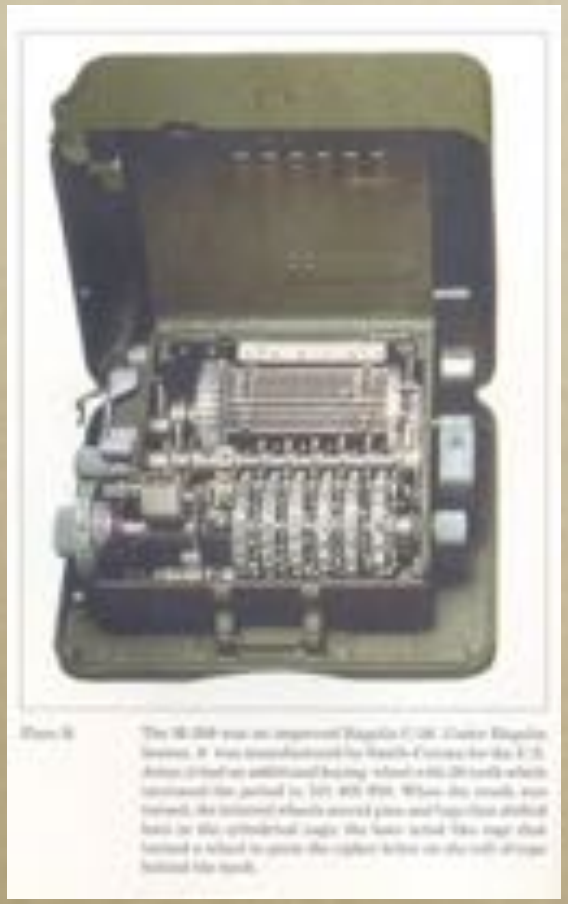
Chiffrement



01000110010

Texte chiffré

Machines de chiffrement



Tous ces systèmes nécessitent de se mettre d'accord sur un secret

Echange de clef

- Inventé par Diffie et Hellman en 1976.

2015

Puissances modulo p

- Si p est premier, il existe un entier g tel que la fonction puissance $n \longmapsto g^n \bmod p$ soit une permutation de {1,2,3,...p-1}.
  Facile à calculer, mais difficile à inverser.

n	1	2	3	4	5	6	7	8	9	10
$2^n \bmod 11$	2	4	8	5	10	9	7	3	6	1

Echange de clé Diffie-Hellman

Alice choisit $a \in \{1,..,p-1\}$

Bob choisit $b \in \{1,..,p-1\}$

$g^a \bmod p$

$g^b \bmod p$

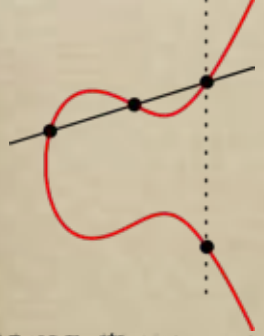
- Alice et Bob peuvent calculer $g^{ab} \bmod p$
  car $g^{ab} = (g^a)^b = (g^b)^a$
- Mais ceux qui ne connaissent ni a ni b...

Efficacité de Diffie-Hellman

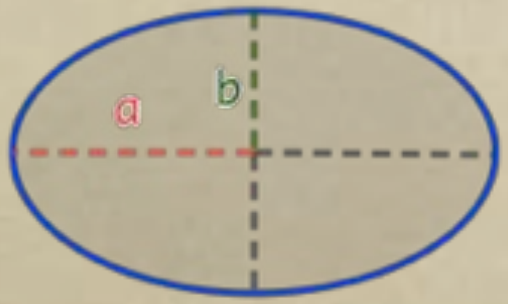
- Pour la sécurité, il faut des nombres premiers p aussi grands que des nombres N difficiles à factoriser : au moins 600 chiffres !
- Peut-on éviter de si grands nombres ?

Changer de monde

- Dans les années 80, Koblitz et Miller ont proposé de remplacer la multiplication modulo p par l'« addition » sur une courbe elliptique modulo p.



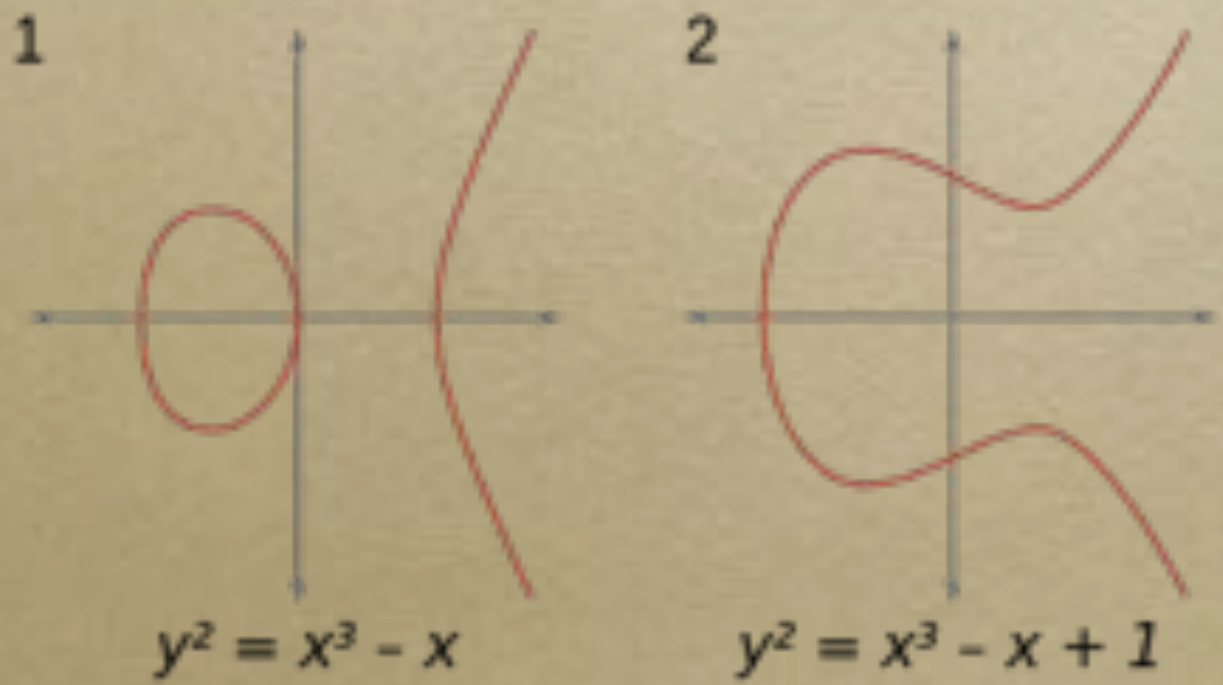
Courbes elliptiques



- Pas une ellipse.
  Mais liées aux fonctions elliptiques, qui proviennent du périmètre d'une ellipse.
- Utilisées pour démontrer le grand théorème de Fermat : $x^n+y^n=z^n$.
- L'un des sept problèmes du millénaire concerne les courbes elliptiques.

Courbes elliptiques

- C'est l'ensemble des solutions (x,y) à une équation de la forme $y^2=x^3+ax+b$.

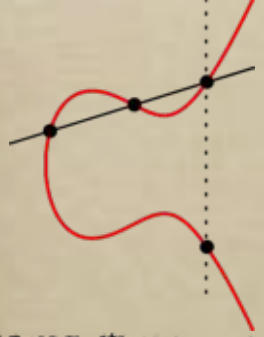


Avis et communications

AVIS DIVERS

PREMIER MINISTRE

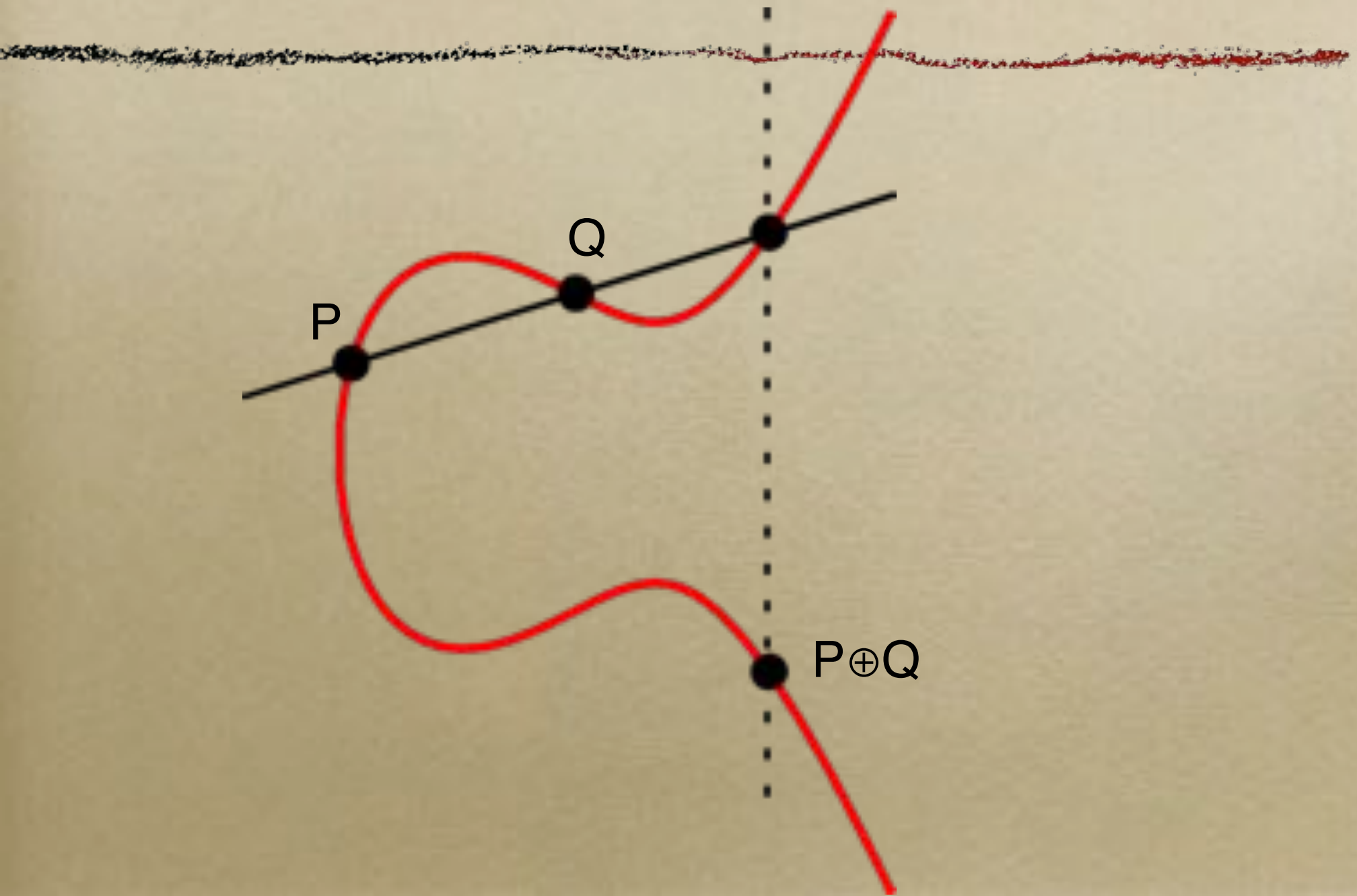
Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français



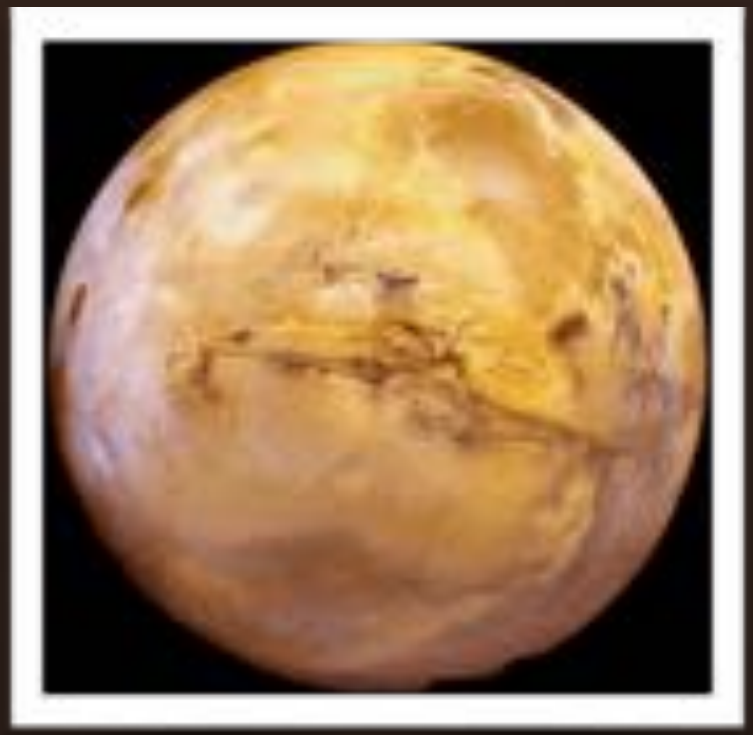
Courbes elliptiques

- En 2011, la France a publié une courbe elliptique : un nombre premier p de 77 chiffres, un entier b, et deux entiers x et y tels que $y^2 \equiv x^3 - 3x + b \pmod{p}$.
- Il existe une opération $\oplus$ qui permet de fabriquer d'autres points (x,y) :
  $(x,y) \oplus (x,y) \oplus \ldots \oplus (x,y)$.
  C'est l'analogue de $g^n \bmod p$.

Comment additionner deux points



Conclusion



Et dans le futur ?

- [Shor1994] a démontré qu'un ordinateur quantique pouvait casser la cryptographie à base de factorisation et de courbes elliptiques.