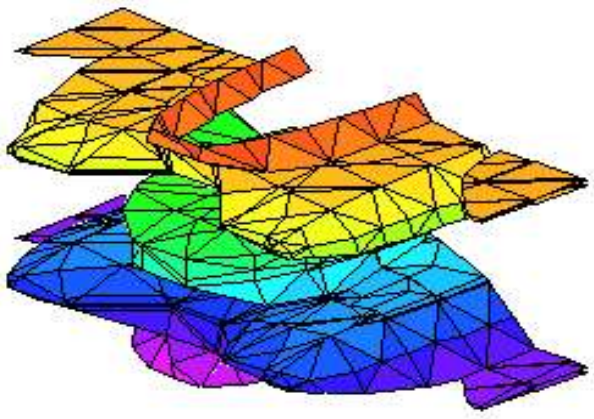
UNIVERSITE D'EVRY VAL D'ESSONNE

Tests de primalité et cryptographie

Latifa Elkhati

Chargé de TER :
Mr.Abdelmajid.BAYAD



composé d'une courbe de Weierstrass et la fonction (exp(x), cos (y), cos(z))

Maîtrise de

Mathématiques
2001-2002

Tests de primalité et cryptographie

Un grand remerciement au professeur d'algèbre monsieur Abdelmajid.BAYAD qui a accepté de prendre sur son temps pour être le chargé de ce TER.

2001-2002

Introduction

Jusqu'à ces dernières années, il aurait fallu (même en utilisant un gros ordinateur un siècle pour savoir si un nombre de 100 chiffres est premier ou non. Aujourd'hui une minute suffit.

Depuis Euclide, les problèmes de théorie des nombres reliés à la primalité d'un nombre ont fasciné les mathématiciens.

Pour beaucoup de mathématiciens, la théorie des nombres est « la reine des mathématiques », en partie parce que ses démonstrations sont d'une beauté compliquée mais aussi parce que son étude est croyait-on une forme de contemplation pure dépourvue de conséquences pratiques.

Bien sûr rien n'est longtemps inutile en mathématique et l'on s'est aperçu, depuis 1977, que la théorie des nombres peut avoir des applications très importantes en cryptographie.

En effet, quelques idées brillantes et paradoxales, fonction à sens unique, clés publiques, puisant leur inspiration dans la théorie des nombres, ont fait basculer la cryptographie d'une culture séculaire du secret vers une véritable étude scientifique de la confidentialité.

Ce TER est ainsi consacré à l'étude des tests de primalité et de leurs applications en cryptographie.

Le premier chapitre est consacré à la cryptographie moderne sans oublier de citer quelques exemples de la cryptographie classique pour voir ainsi l'évolution de celle-ci qui a stimulé la recherche en théorie des nombres.

Le deuxième chapitre est consacré à l'étude de différent testes de primalité, qu'il s'agit de tests probabilistes ou de tests certifiant la primalité : il constitue ainsi le cœur de ce TER.

Le troisième chapitre s'intéresse en particulier aux courbes elliptiques et à leurs nombreuses applications en cryptographie comme en théorie des nombres, on ne peut pas parler des différents tests de primalité sans, bien évidement faire intervenir les courbes elliptiques.

Chapitre 1

Introduction à la cryptographie

A l'heure de l'explosion des nouvelles technologies de l'information et de la communication, la Cryptographie est aujourd'hui essentielle pour le développement du commerce électronique, des cartes à puce, de la téléphonie mobile, et particulièrement cruciale dans le secteur bancaire, elle est devenue une discipline à deux facettes multiples qui concerne un public de plus en plus important.

La cryptographie traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire. Le message à envoyer est appelé message ou texte *en clair* et, sous sa forme déguisée, message *chiffré* (codé et non pas sous forme de chiffres) ou *cryptogramme.*

Le codage est une transformation mathématique particulière, en général bijective, et la fiabilité de la plupart des cryptosystèmes modernes dépend essentiellement de la difficulté de cette transformation, dans le sens où le retour en arrière pour retrouver le message en clair nécessiterait, d'un éventuel indiscret, des moyens très coûteux.

I-.Exemples historiques

1-.Chiffrement par décalage ou par substitution

Le message chiffré se déduit du message en clair par un décalage des lettres de l'alphabet :

Exemple : décalage de 7,

Longtemps ⇨ svunaltwz

2-.chiffrement par permutation ou transposition

Dans ce cas on ne modifie pas les symboles du texte en clair, mais on les permute. Le texte en clair est d'abord découpé en bloc de n symboles et chaque clé K est une permutation de {1, 2,..., n}.

Exemple : soit n=5 et la clé K= $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$

Longtemps  ntolgp mes

On remarque bien que les deux systèmes sont bien peu résistants : le décalage est restreint par le chiffre, et la substitution ne résiste pas à une analyse des fréquences(« q » par exemple est souvent suivi par « u » etc..).

Pour rendre le déchiffrement plus difficile, il est important de concevoir des systèmes tels que le texte chiffré ait un aspect aléatoire, cette idée a dû attendre le XX-iémme siècles pour sa mise en application.

3. Le système de Vernam ou, « one-time pad »

Ce système trouvé en 1926 fonctionne de la manière suivante : Les messages en clair où chiffrés, s'écrivent sur un même alphabet, que l'on présentera par Z_m (où m est le nombre des alphabets). Un message $M = (x_i)_{i<n}$ se chiffre par la k-transformation :

$$y_i = x_i + k_i \bmod m .$$

Le $K = (k_i)_{i<n}$ constitue la clé de la transformation, et est choisi aléatoirement dans Z_m (la clef K n'est jamais réutilisée, d'où l'appellation « one-time » et « pad » pour dire bloc, pas). Le système de Vernam peut être considéré comme l'aboutissement de la cryptographie traditionnelle.

Si les quantités d'information à échanger sont importantes, ce système devient très lourd à mettre en pratique car il faut à chaque fois engendrer des clés aléatoires très longues et les mettre simultanément à la disposition de l'émetteur et du destinataire Il reste parfois utilisé, cependant, si la confidentialité est très importante car ce système garanti une confidentialité « parfaite » d'après ce qu'a démontré Shannon en 1949. D'ailleurs la ligne téléphonique directe Krémlin-maison blanche a longtemps été protégée par un « one-time pad ».

4. Les méthodes DES(Data Encyption Standard)

Avec l'expansion de l'informatique et des télécommunications, le besoin se fit sentir

de disposer de système de chiffrement grand public, bon marché, simples à réaliser tant du point de vue matériel que logiciel, et très rapide d'exécution. C'est à dire que les algorithmes de chiffrement et de déchiffrement seraient publiés et normalisés, seules leurs clés seraient sécurisées.

Le DES est une méthode, dont l'essentiel de recherche a été mené par Horst Feistel, en 1967, est basé sur la combinaison de chiffrement par substitution et par transposition. Avant les ordinateurs, la transposition était difficile à mécaniser et trop complexe à effectuer manuellement. L'augmentation de la mémoire des ordinateurs permit d'utiliser ce cryptosystéme.

Le DES est un chiffrement par blocs. Un chiffrement par blocs prend un certain nombre de lettres et il les code tous en même temps. Le DES emploie aussi un mode de chaînage quand la longueur d'un message est plus longue qu'un bloc.

Le DES, standard de cryptographie publique depuis 1977, a résisté aux assauts des ans. Cet algorithme étant fort, les cryptanalystes ne pouvaient qu'attaquer les clés. Les progrès du matériel informatique ont toutefois compromis la force et la sécurité du DES. Il devient en effet plus facile de parcourir toutes ces clés aujourd'hui qu'en 1977.

II-. Cryptographie moderne

L'arithmétique des congruences modulo m joue un grand rôle dans la cryptographie moderne car elle transforme des fonctions monotones en fonctions qui ne le sont pas, introduisant de ce fait un facteur de confusion dans le calcul de leurs inverses. Considérons la fonction simple $f(x)=4x$. Lorsque x augmente de manière très régulière, il en résulte que si l'on connaît un nombre $y=f(x)$, il n'est pas difficile, de déterminer c sans même résoudre l'équation $y=4x$. Par contre si on considère la fonction de codage $f(x) \equiv 4x \bmod 7$, lorsque x augmente, les valeurs de $f(x)$ « sautent » de manière quasiment aléatoire. Même dans un cas aussi simple les congruences donnent un meilleur codage qu'une fonction monotone.

1-.L'exponentiation modulaire

La fonction à sens unique est un élément indispensable dans la cryptographie moderne. Une fonction considérée comme difficilement inversible est l'exponentiation modulo un nombre premier. On l'appelle exponentielle discrète ou modulaire. La fonction est définie par :

$$\begin{array}{ccc} Z_p & \longrightarrow & Z_p \\ x & \longrightarrow & f(x) = a^x \end{array}$$

Avec p un nombre premier et a un nombre primitif modulo p (de préférence on le choisit primitif pour que f soit bijective). Tous les algorithmes connus pour inverser cette fonction,

c'est à dire calculer le logarithme discret, nécessitent un temps non polynomial en *log p* – surtout quand *p* est très grand.

2-.Le protocole de Diffie-Hellman

Ce cryptosystéme basé sur le principe de la fonction à sens unique a connu son véritable début lors de l'apparition de l'article de Diffie-Hellman en 1976. Les auteurs y résolvent, grâce à l'exponentielle discrète, un problème de partage de secret considéré jusqu'alors insoluble.

Le problème est le suivant :

Alice et Bob ne disposent pour communiquer d'aucun moyen sûr et ils souhaitent, cependant, communiquer confidentiellement. Il leur faut se mettre d'accord publiquement sur un procédé de communication assurant la confidentialité, une confidentialité garantie par la limitation de la puissance de calcul adverse.

La solution est la suivante :

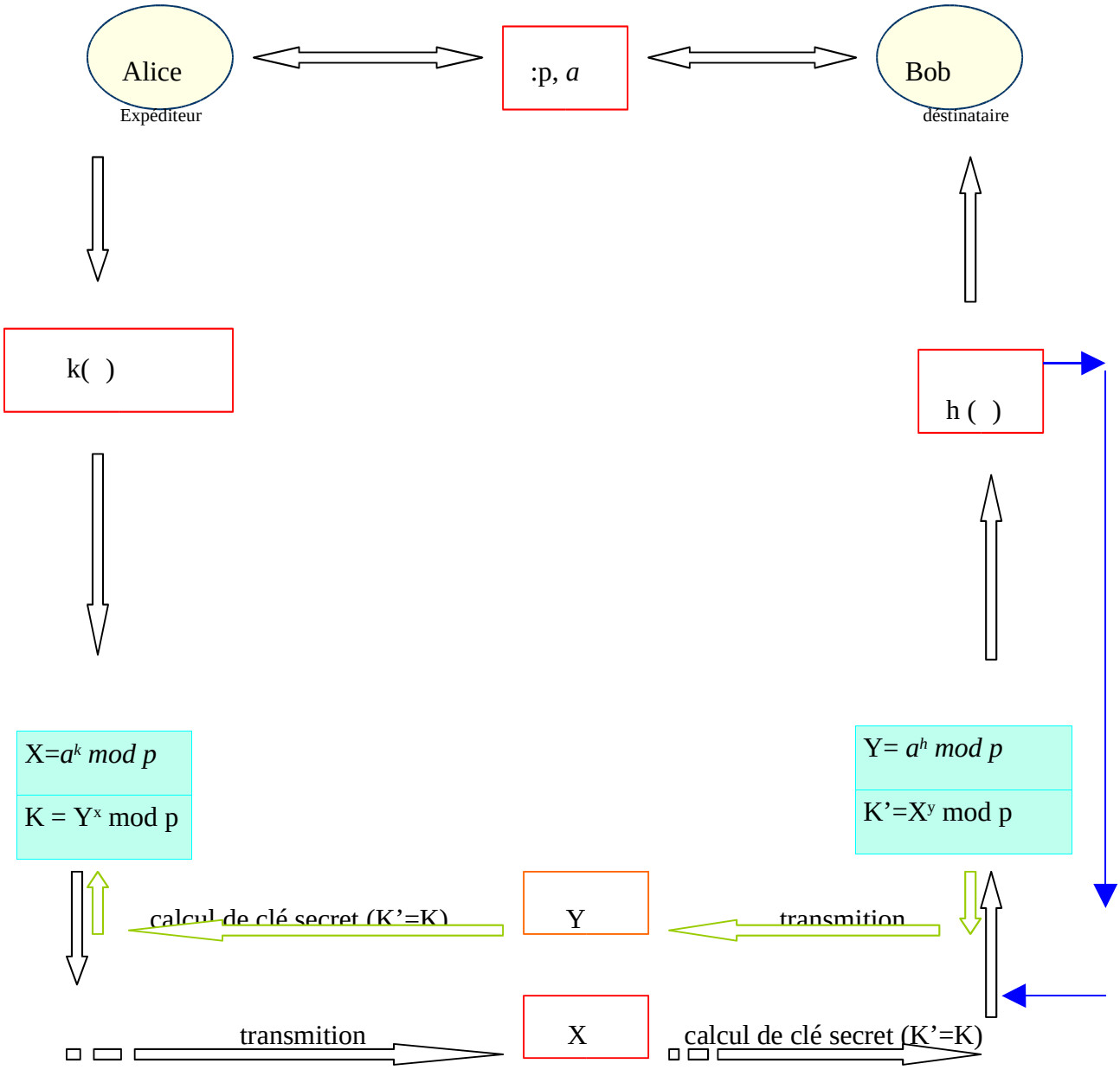
Il suffit qu'Alice et Bob se mettent d'accord sur un nombre secret S qui leur servira, par exemple, de clé pour un système de chiffrement traditionnel, S doit rester, bien entendu, discret. Alice et Bob commencent par se mettre d'accord publiquement sur un grand nombre premier p, et une racine primitive modulo p, soit a. Alice choisit secrètement et aléatoirement un nombre k, qu'elle gardera pour elle seule. Mais elle transmet à Bob, même publiquement, le nombre a^k *mod p. Bob se choisit de même un nombre secret h et transmet* a^h*. Alice et Bob décident ensuite que leur secret commun sera*

$$S = a^{kh} \bmod p.$$

Comme ça Alice accède à S en enlevant a^h *à la puissance son nombre secret k. Et Bob pareil !*

On remarque bien que l'exponentielle serve comme un bon candidat de ces deux propriétés qui sont la difficulté de l'inverser et la commutativité.

Schéma de Diffie-Helman



Codage de Diffie-Helman classique

3-. Le système d'El Gamal

Grâce au protocole de Diffie-Hellman la voix a été ouverte à d'autres séries d'algorithmes cryptographiques. On a alors réalisé un système dit « à clé publique » ou

« asymétrique » : seul le destinataire possède le secret permettant de déchiffrer. C'est le grand avantage de ce protocole, ne plus se préoccuper du partage du secret, chose généralement délicate.

Les principes de ce système :

Bob dans ce cas possède deux clés, une secrète S, et une autre clé publique a^S, avec a un nombre primitif modulo un nombre premier p(p, a et a^S seront publiques). Donc pour envoyer un message M à Bob on tire au hasard un nombre k modulo p, et on calcule $C_1 = a^k \bmod p$, et $C_2 = M\,(a^S)^k \bmod p$, le message chiffré est le couple (C_1, C_2). Si l'on est le destinataire légitime du message, et que l'on dispose de la clé secrète S, on trouve

$$M = (C_2 / C_1^S) \bmod p.$$

Un défaut de ce système est que le message chiffré est deux fois plus longue que le message original. Par conséquent le grand avantage est que chacun déchiffre le message par sa propre clé secrète.

A l'aide du même genre d'idée on réalise un schéma de signature, pour résoudre le problème d'authenticité. C'est à dire que l'on souhaite apporter au destinataire de M (Bob) une preuve que le message a bien était envoyée par Alice, et non pas par Amélie. Alors on procède de la façon suivante :

En gardant les même principes cités ci-dessus, Alice choisit au hasard un entier k premier avec p-1, puis elle calcule

$$U = a^k \bmod p$$

Ensuite Alice calcule l'unique solution v de l'équation

$$M = us + kv \bmod (p-1).$$

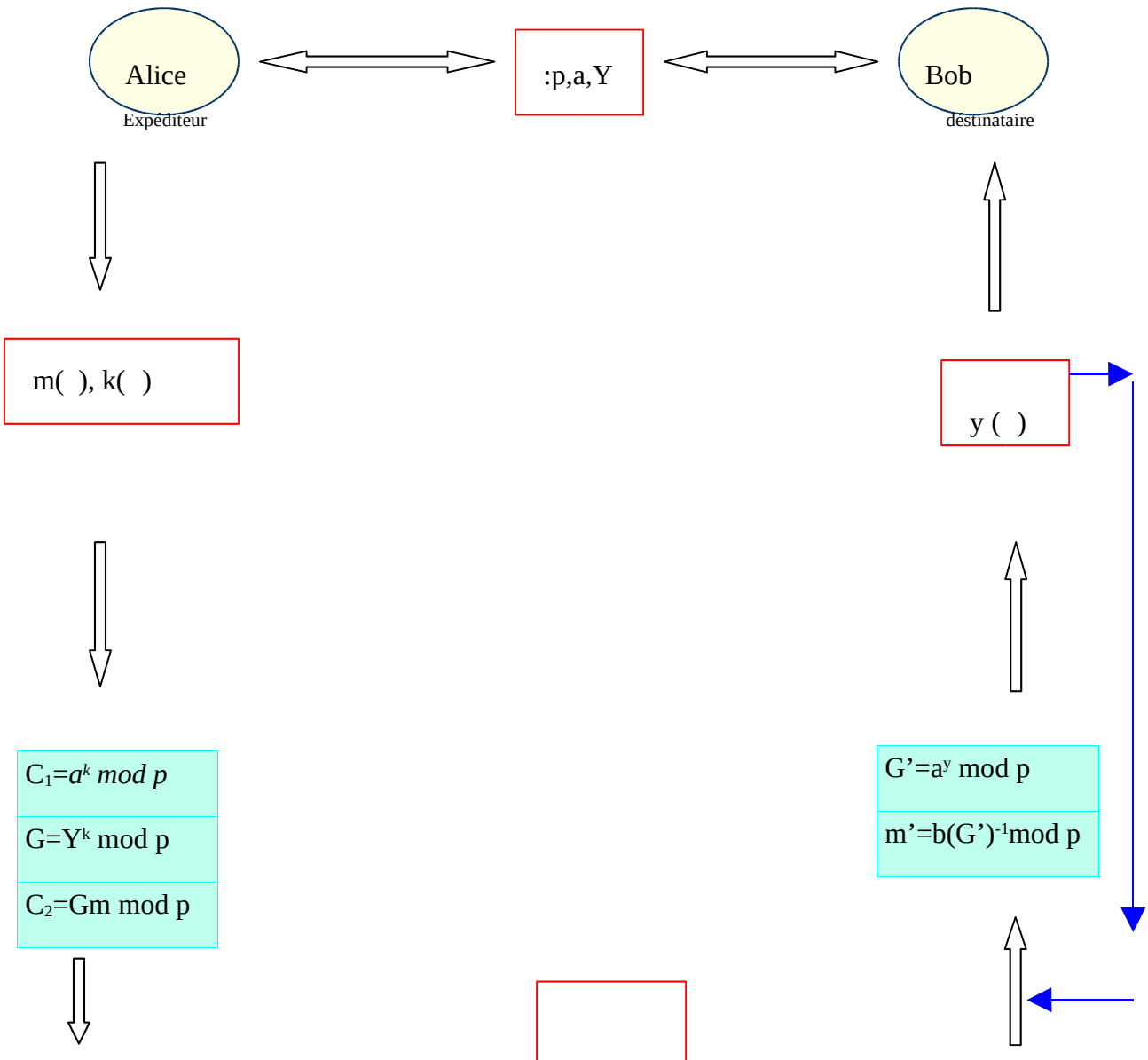
Finalement Alice « signe » son message M par S=(u, v). Si l'on exponentie, on obtient

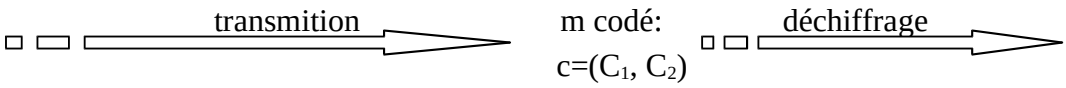
$$A^M = (a^S)^u\, u^v \bmod p.$$

Bob vérifie donc l'authenticité de la signature en calculant et en comparant les deux termes de la dernière égalité. Sauf que là aussi on se retrouve confronté à un problème algorithmiquement difficile, à savoir la recherche de (u, v) vérifiant l'équation..

Transfert de l'information

Codage d'El-Gamal





Codage d'El-Gamal classique

4-. Le système RSA

le système à clé publique à avoir été inventé, et le plus utilisé actuellement, est le système RSA (Rivest, schamir, Adleman). Il est fondé sur la difficulté de factoriser des grands nombres.

Son principe est le suivant :

La clé secrète est constituée du produit de grands nombres premiers n = pq, ainsi que d'un entier e inversible modulo (n)(c'est à dire inférieur à n et sans facteurs communs avec le produit (p-1)(q-1)). Le chiffrement se fait par la transformation :

$$M \longrightarrow M^e \bmod n.$$

Et pour déchiffrer, on calcule

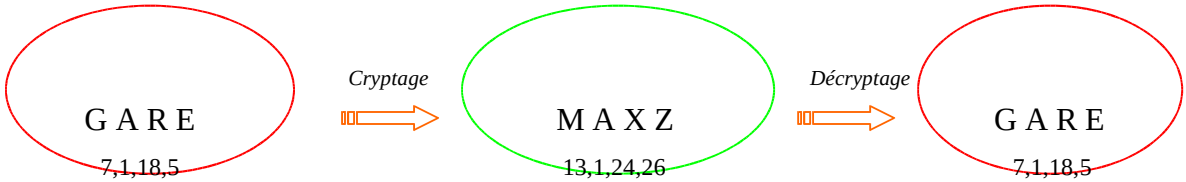
$$M \longrightarrow M^d \bmod n.$$

Où d est l'inverse de e modulo (n).

Exemple :

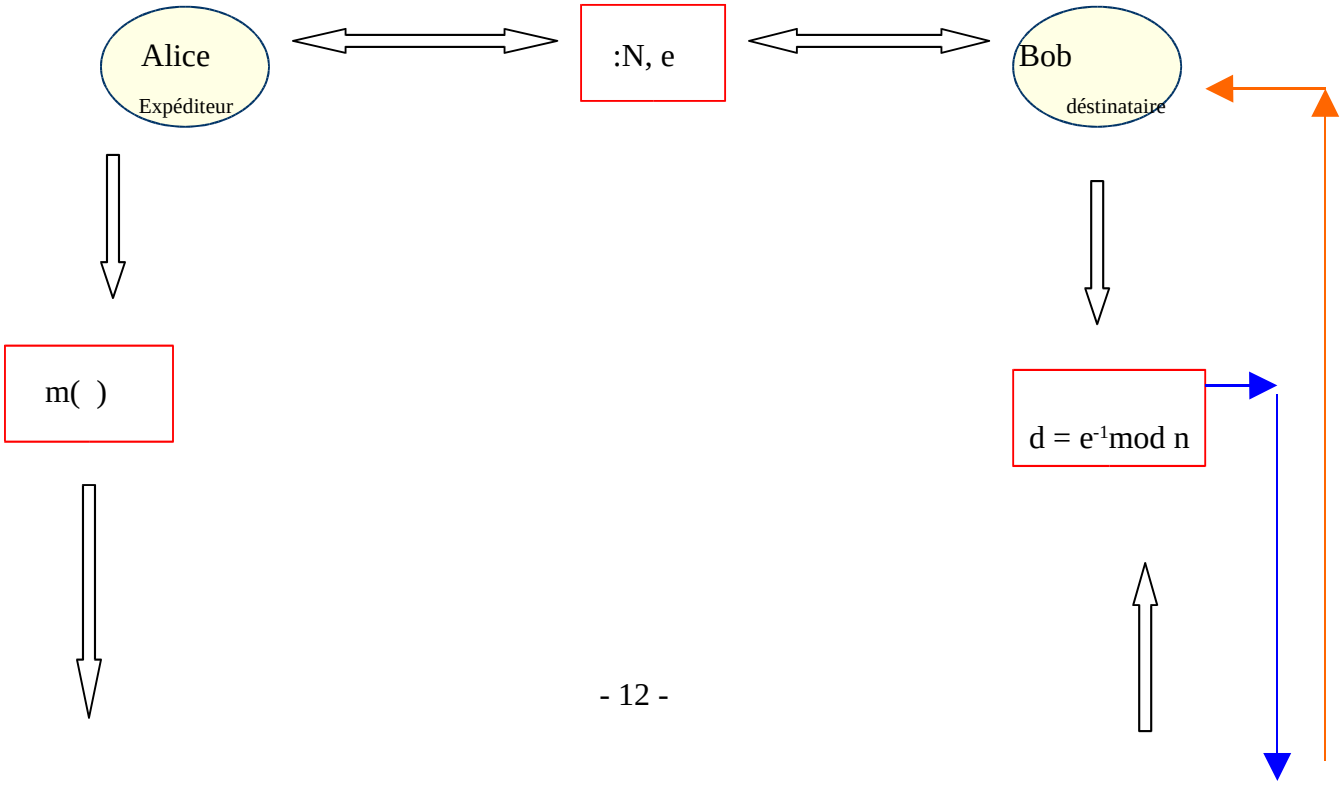
*Si p=3, q=11, d'où N=33, et e=3 (qui est sans facteurs communs avec 2*10=20).*
Alice communique à Bob n=33 et e=3, qui constituent les clefs publiques, pour crypter un G par exemple c'est à dire que m=7 (le rang de G, représenté par 7), on calcule $7^3=343$, dont le reste de la division par n=33 vaut c=13. Le G est donc représenté, après cryptage par le nombre 13, qui correspond à la lettre M.

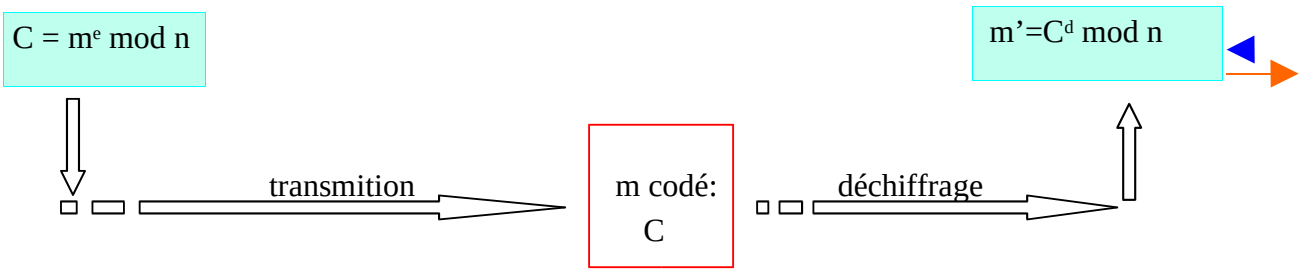
Par ailleurs Alice a calculé l'entier positif d inférieur à N tel que le reste de la division de ed par (p-1)(q-1) soit égal à 1 c'est à dire 7(=d). Alice doit garder les nombres p, q et d secrets. Pour déchiffrer Alice calcule $c^d=13^7$, dont le reste de la division par n=33 est égal à 7, qui correspond à la lettre G.



Connaître (n) équivaut à connaître la factorisation de n. Comme on ne sait pas factoriser efficacement les grands entiers, accéder à *(n)* où à *d* reste difficile.

Schéma de RSA





Codage RSA

5-.Résumé :

Au niveau réalisation pratique, quelques questions restent en suspens. Comment choisit-on concrètement de grands entiers *p* et *q* ? De quelle taille faut-il les prendre ? Pour quelle garantie de sécurité ?

La meilleur des méthodes consiste à les choisir aléatoirement et tester leur prima lité. Mentionnons, tout de même, que le nombre moyen de choix qu'il faut effectuer avant de tirer effectivement un nombre premier est tout à fait acceptable. Cela est affirmé par le théorème des nombres premiers suivant :

Théorème : *Le nombre des nombres premiers* $\leq x$, *noté* $\pi(x)$, *vérifie*

$$\pi(x) \sim x/\ln(x).$$

Ceci veut dire tout simplement que si l'on choisit au hasard des entiers de 500 bits, on aura un nombre premier au bout d'environ 350 tentatives en moyenne. Ce qui veut dire qu'il nous reste maintenant que les tests de primalités.

Chapitre 2

Les tests de primalité

Les nombres premiers sont, pour la multiplication, ce qu'on pourrait appeler les »atomes » des nombres. Tout nombre entier supérieur à 1 est soit premier soit décomposable.

Comment savoir si un nombre donné est premier ou pas ? On peut toujours essayer de chercher parmi les nombres inférieurs à ce nombre ses diviseurs ou essayer la méthode du crible d'Eratosthène. Cependant ces algorithmes restent incapables de déterminer, en un temps raisonnable, la primalité d'un nombre. A titre d'exemple, Harry Nelson et David Slowinski ont démontré que le nombre $2^{44\,497} - 1$ (qui a 13 395 chiffres)est premier, avec ces méthodes même un ordinateur qui effectue un million de division par seconde, il aurait fallu 10^{6684} années pour avoir un résultat !

Depuis Euclide, les problèmes de théorie des nombres reliés à la primalité d'un nombre ont fasciné les mathématiciens. Jusqu'à présent, toutes les méthodes connues pour tester la primalité d'un nombre sans essayer de le factoriser sont issues d'un théorème énoncé par Pierre de Fermat dans une lettre écrite à son ami Bernard Frénicle de Bessy en 1640. Un théorème qui va être démontré plus tard par Euler en 1736.

1-. Critère de Fermat

Théorème (le petit théorème de Fermat) : *Soit un nombre premier. Tout entier a satisfait à* $a^p \equiv a \bmod p$. *De plus, si a n'est pas divisible par p, alors* $a^{p-1} \equiv 1 \bmod p$.

Démonstration : (i) Considérons le cas où p ne divise pas *a*, alors $a \in IF_p^{*¿}$. Donc $a^{p-1} \equiv 1 \bmod p$

¿

Si on multiplie les deux membres par *a*, on trouve la thèse.
(ii) Si p divise *a*, alors $a \equiv 0 \bmod p$ et la thèse est retrouvée.

Pour les tests de primalité le point important est : si $a^n - a$ n'est pas un multiple de n, le nombre n est décomposé. Exemple si $n=4$ et $a=3$ comme le reste de la division de 78 par 4 donne 2 alors 4 n'est pas premier.

Mais que dire de la réciproque ? Est-il vraie que si $a^{n-1} \equiv 1 \bmod n$ alors n est premier ?Plusieurs exemples suggèrent que la réponse soit oui : 2^2-2 est un multiple de 2, 2^3-2 est multiple de 3,..et 2 et 3 sont premiers. Il y a 2500 ans les mathématiciens chinois avaient découvert cette propriété, et affirmé que si 2^n-2 est divisible par n, alors n est premier. Gottfried Leibniz croyait ce résultat exact. En 1819, le mathématicien Pierre Sarrus a remarqué que 2^{341}-2 est multiple de 341 bien que 341 ne soit pas premier(=11*31).

Test de Fermat. Choisir *a* au hasard, calculer $a^{n-1} \bmod n$. L'entier n satisfait au test si

$$a^{n-1} \equiv 1 \bmod n.$$

Définition :Un nombre pseudo-premier en base b est un nombre composé impair n qui ne divise pas b et tel que

$$b^{n-1} \equiv 1 \bmod n.$$

Mesurer l'efficacité du test revient à comparer la densité des nombres pseudo-premiers en base *a*, à celle des nombres premiers. En effet grâce au résultat de Pomerance(1981) on a

$$e^{(lnx)} \leq p_2(x) \leq xe^{-1/2(lnxlnlnlnx)/lnlnx}$$

si l'on compare cette estimation avec $x/lnx \leq (x)$, on obtient que le rapport $p_2(x)/(x)$ tende vers zéro quand x tend vers l'infini, avec une rapidité satisfaisante ; par exemple pour $x = 2^{200}$ on a

$$p_2(x)/(x) \leq 2.6 .10^{-8}$$

C'est à dire qu'il faut être malchanceux pour tomber sur un pseudo-premier. Ceci dit, il existe des nombres sur lesquels le test ne réussit pas tel est le cas des nombres de Carmichael (appelés ainsi en hommage au mathématicien américain Carmichael qui a découvert leurs propriétés en 1909).

Définition(nombre de Carmichael) ***:*** *un nombre de Carmichael est un nombre composé pseudo-premier pour toute base.*

Théorème ***:*** *un entier n est un nombre de Carmichael si et seulement si n est non premier, sans facteur carré, et tout diviseur premier p de n est tel que (p-1)divise (n-1).*

Par exemple on peut obtenir un de ces nombres sous la forme

$n=(6t+1)(12t+1)(18t+1)$

Si *6t+1, 12t+1, 18t+1 sont tous les trois des nombres premiers(par expemple) : 1729=7.13.19).*
Ces nombres restent rares, grâce à un résultat trouvé en 1994 on sait que pour tout *x* suffisamment grand, il existe au moins $x^{2/7}$ nombres inférieurs à *x*.

Cependant on peut envisager d'adopter ce critère souvent connu sous le non de *test de Fermat* comme test probabiliste de primalité.

2-.Critère de Miller-Rabin :

La difficulté crée par les nombres de Carmichael peut être levée par la remarque suivante, due à Miller : si on trouve $a^{(n-1)/2} \equiv 1 \bmod n$ et si *(n-1)/2* est pair, on peut recommencer, et ainsi de suite.

Propriété : *soit p>2, un nombre premier. Ecrivons p-1=* $2^s t$ *avec t impair. Soit a un entier non divisible par p. Alors ou bien* $a^t \equiv 1 [p]$ *, ou bien il existe un entier i avec 0* $\leq i < s$ *et* $a^{2^i t} \equiv -1 [n]$.

Démonstration *:* Posons $a_i \equiv a^{2^i t} [p]$ pour i=0, …,s. On a a_s =1 d'après Fermat. Ainsi, de deux choses l'une : ou bien tous les a_i et en particulier a_0 sont égaux à 1, ou bien il existe i avec $0 \leq i < s$, $a_i \neq 1$ et $a_{i+1} = 1$ .Mais, puisque $a_{i+1} = a_i^2$ et que p est premier, cela implique a_i = -1.

Corollaire *Soit n>1 un entier impair. Ecrivons n-1=* $2^s t$ *avec t impair .Supposons qu'il existe un entier a avec 1< a < n,* $a^t \neq 1 [n]$ et $a^{2^i t} \neq -1 [n]$ *pour i=0,1…,s-1.Alors n est composé.*
(Appelons un tel entier a un témoin de Miller).

Propriété *:Si le nombre impair n est composé, au moins les trois quarts des n-2 entiers a tels que 1< a < n sont des témoins de Miller pour n.*

Théorème(Rabin) : *Soit n un entier impair composé tél que n>9. Posons n-1=* $2^s t$ *avec t impair. Les entiers a compris entre 1 et n et qui satisfont à la condition* $a^t \equiv 1 [n]$ *ou à l'une des conditions* $a^{2^i t} \equiv -1 [n]$ *pour i=0,1…, s-1 sont en nombre au plus* $\varphi(n)/4$ *(avec* $\varphi(n)$ *l'indicateur d'Euler).*

Exemple :

Prenons l'exemple du nombre de Carmichael 561, pour lequel on a $a^{560} \equiv 1 \bmod 561$ pour tout *a* premier à 561 (on peut prendre a=2). Mais on a $560 = 2^4.35$, $2^{2^3.35} \equiv 1 \bmod 561$ et $2^{2^2.35} \equiv 67 \bmod 561$, de sorte que 2 est un témoin de Miller.

3-.Test de primalité à la lehmer :

Grâce au test de Fermat, d'autre variété de test a été mise au point. Dans ce test on suppose donnée une décomposition en facteurs premiers de p-1.

Proposition (critère de lehmer): *soit n>1 un enter impair tel qu'on connaît tous les facteurs premiers de n-1.Les conditions suivantes sont équivalentes :*

(i) *n est premier*

(ii) *Il existe un entier a tel que* $a^{n-1} \equiv 1 \left[\bmod n\right]$ et $a^{(n-1)/q} \neq 1 \left[\bmod n\right]$ *pour tout facteur premier q de n-1.*

Démonstration : pour démontrer que (i) implique (ii) il suffit de prendre pour *a* une primitive de l'unité.

(ii) implique (i) : Supposons inversement (ii) satisfaite, alors l'ordre de l'élément *a mod n* de $(\quad /n \quad)^{¿}$ divise *n-1*, mais ne divise aucun des *(n-1)/q*. Il est donc égal à *n-1*. Par conséquent, possède au moins *n-1* élément(les puissances de *a* modulo *n*)et *n* est premier.

Corollaire : *soit n>2 un entier impair. Les conditions suivantes sont équivalentes :*

(i) n est premier ;

(ii) il existe un entier a tel que $a^{n-1/2} \equiv -1 \left[\bmod n\right]$ *et* $a^{(n-1)/q} \neq 1 \left[\bmod n\right]$ *pour tout facteur premier impair q de n-1.*

Démonstration : En effet, dans un corps, le seul élément distinct de 1 et de carré 1est -1.La conjonction des conditions $a^{n-1} \equiv 1 \left[\bmod n\right]$ et $a^{(n-1)/2} \neq 1 \left[\bmod n\right]$ peut donc être remplacée par $a^{(n-1)/2} \equiv -1 \left[\bmod n\right]$.

Lemme(critère de Pocklington): *soit n un entier >1.Ecrivons n-1=* $q^r m$ *, avec q premier et r≥1. Supposons qu'il existe un entier a avec* $a^{q^r} \equiv 1 \left[\bmod n\right]$ et $\text{pgcd}(a^{q^{r-1}} - 1, n) = 1$. *Alors tout facteur premier de n est congru à 1 modulo* q^r .

Démonstration : Soit p un facteur premier de n. On a $a^{q^r} \equiv 1 \pmod{p}$ et $a^{q^{r-1}} \neq 1 \pmod{p}$. Cela signifie que l'ordre de *a* modulo *p* dans le groupe (/n)¿ divise q^r et ne divise pas q^{r-1}, donc est égal à q^r. Donc q^r divise p-1(théorème de Lagrange).

Proposition(critère de Lehmer-Pocklington) :*Soit n un entier >1.Ecrivons n-1= uv, les facteurs premiers de u étant connus. Supposons qu'il existe pour chaque facteur premier q de u, en désignant par q^r la plus grande puissance de q qui divise u, un entier a_q avec*

$$a_q^{q^r} \equiv 1 \pmod{n} \text{ et } \operatorname{pgcd}(a_q^{q^{r-1}} - 1, n) = 1 \quad .$$

Alors tout facteur premier p de n est congru à 1 modulo u. Si on a de plus $v \leq u+1$,alors n est premier.

Démonstration *:* Soit *u*= $q_1^{r_1} \cdots q_s^{r_s}$ la décomposition de *u* en facteurs premiers et soit *p* un facteur premier de *n*. D'après le lemme précédent, p-1est divisible par chacun des $q_i^{r_i}$, donc est divisible par *u*. Cela implique en particulier que *p>u* ; si on a $v \leq u+1$, on a $n = 1+ uv < (u+1)^2 \leq p^2$.
Par conséquent, tout facteur premier *p* de *n* est > $\sqrt{n}$, et *n* est premier.

Les nombres de Fermat

Ce qui précède fait apparaître le cas particulier des nombres de Fermat : ce sont les nombres premiers p qui ont les certificats de primalité les plus courts, autrement dit ceux pour lesquels p-1 est une puissance de deux. Alors p = 2^m +1 , mais m est à son tour une puissance de 2(si *m* peut s'écrire sous forme de *m=ab* avec a impaire, alors 2^m +1 = $(2^b)^a$ +1 est divisible par 2^b +1). Tout nombre premier de Fermat est donc de la forme

$$Fer_n = 2^{2^n} + 1 \quad .$$

Pour les nombres de Fermat, le critère de Lehmer devient :

Lemme **:** *Pour que Fer_n soit premier, il faut et il suffit qu'il existe a avec* $a^{(Fer_n - 1)/2} \equiv -1 \pmod{Fer_n}$.

4-.Critére de Lucas :

En 1876 le mathématicien Edouard Lucas énonce une méthode irréfutable permettant de déterminer si un nombre n est premier. Par exemple le nombre n=257, n-1=256 =2^8, pour montrer que n est premier, il suffit de trouver un nombre b tel que b^{256} est congru à 1 modulo 257 et tel que $b^{256/2}$ n'est pas congru à 1 modulo 257. Le nombre b est choisit au hasard.

Cependant, la méthode de Lucas n'est applicable qu'à des nombres ayant une forme spéciale : elle ne s'applique que si on détermine les facteurs premier de n-1.

a-.Suites de Lucas

Définition :*Soient A un anneau (dont on notera* 1_A *son élément neutre pour la multiplication) et a un élément de A.On appelle suite de Lucas associée à a la suite* $\left(V_n\right)_{(n\geq 0)}$ *d'éléments de A définie par récurrence par* $V_0=2\,.1_A$, $V_1=a$ et $V_{n+1}=aV_n-V_{n-1}$

Proposition :*On a pour tout n>0 les relations*

$$V_{2n-1}=V_nV_{n-1}-a,$$

$$V_{2n}=V_n^{\,2}-2\ ,$$

$$V_{2n+1}=aV_n^{\,2}-V_nV_{n-1}-a\ .$$

Démonstration :On peut donc supposer l'existence d'un x dans A comme ci-dessus, ce qui donne par exemple

$$V_nV_{n-1}=(x^n+x^{-n})(x^{n-1}+x^{-n+1})=(x^{2n-1}+x^{-2n+1})+(x+x^{-1})=V_{2n-1}+a.$$

La deuxième relation se prouve de manière analogue et la troisième se déduisent des deux premières par la formule de récurrence.

b-.Le critère de primalité de Lucas-Lehmer

Nous énonçons ici le critère, du à Lucas(1878) et Lehmer(1930), qui permet d'étudier la primalité d'un entier *n* lorsqu'on connaît la décomposition en facteurs premiers de *n+1*.

Nous établirons un résultat qui nous sera bien utile. Soient p un nombre premier impair et a un entier. Notons IF_p le corps fin Z/pZ à p éléments et considérons comme ci-dessus l'anneau quotient

$$k = IF_p[x]/(x^2 - ax + 1)$$

et soit la classe de X dans k. On a par construction la relation $^2 - a + 1_k = 0$, qui s'écrit aussi

$$+ \ ^{-1} = a.1_k = a \bmod p,$$

ou encore $X^2 - aX + 1_k = (X -)(X - \ ^{-1})$. Posons $= a^2 - 4$. On a $(- \ ^{-1})^2 =$ mod p. Supposons premier à p. Alors le petit théorème de Fermat implique $^{p-1} \equiv 1$ mod p, donc $^{(p-1)/2} \equiv \pm 1$ mod p.

Lemme :*Supposons* p ≠ 2 et *premier à p.*

a)- On a, ou bien $(p-1)/2 \equiv 1 \ [\bmod p]$

et alors $p-1 \equiv 1_k$ *ou bien* $(p-1)/2 \equiv -1 \ [\bmod p]$ *et alors* $p+1 \equiv 1_k$.

b) Pour un entier m, les relations

$^m \equiv 1_k$ et $^m + \ ^{-m} = 2.1_k$

sont équivalentes.

Démonstration *:* Puisque p est impair, 2 est inversible modulo p. On a par construction

(- $a/2$)$^2 =$ /4

. En élevant à la puissance (p-1)/2, en multipliant par

- $a/2$ et en posant pour simplifier

$=$ $^{(p-1/2}$ on

en déduit

(- $a/2$)$^p =$ (

En utilisant le résultat suivant :

Soient x et y deux éléments d'un anneau commutatif A tels que pxy=0. Alors $(x+y)^p = x^p + y^p$

Et le petit théorème de Fermat(pour et pour 2), on en tire

$^{p}-a/2=$ (-$a/2$)

.

Si

$\equiv 1$, on obtient $^{p}=$

. Si $\equiv -1$, on obtient

$^{p}=a$ – = $^{-1}$

.Cela prouve a).

Prouvons b) :

La relation

$^{m}+$ $^{-m}=2$ équivaut à ($^{m}-1\,)^{2}=0$

. Il suffit donc de prouver que dans l'anneau k la relation $x^2=0$ implique x=0. Si l'on pose x = u +v, on a

$x^2=u^2$ $^{2}+$ 2uv

.

Il s'agit donc de voir que dans $/p$ le système des deux équations (u + v)(u - v) = 0 et u(2v + au) = 0 n'a comme solution que u = v = 0. Mais cela est immédiat puisqu'il s'agit d'un corps dans lequel $a + 2$ et $a - 2$ sont inversible par hypothèse.

Proposition (critère de primalité de Lucas-Lehmer) : *soit n>1 un entier impair tel qu'on connaît la décomposition de n+1 en facteurs premiers. Soit a un entier tel que n et* $a^2 - 4$ *soient premiers entre eux, et soit* (V_n) *la suite de Lucas définie par*

$V_0=2,\ \mathrm{V}_1=a,\ \mathrm{V}_{i+1}=aV_i-\mathrm{V}$

i-1.

¿¿¿¿¿¿

Si $V_{n+1}\equiv 2[n]$ et si $\mathrm{pgcd}(V_{(n+1)/q}-2,n)=1$ *pour tout facteur premier q de n+1, alors n est premier.*

Démonstration : Soit *p* un facteur premier de *n*. Considérons l'anneau k et l'élément introduit ci-dessus. On a d'après le lemme $^{p\pm1}=1$. D'autre part, pour tout entier *m>0*, la relation $^{m}=1$ équivaut à

$^{m}+$ $^{-m}=2$,

donc d'après la définition elle-même des suites de Lucas $V_m \equiv 2\ [p]$. L'hypothèse faite implique donc que

$^{n+1}=1,$ et $^{(n+1)/q} \neq 1$

pour tout facteur premier *q* de *n+1*. Mais cela signifie que l'ordre de dans le groupe multiplicatif k^* est égal à *n+1*.

Puisque $^{p\pm1}=1$, il en résulte que *n+1* divise $p\pm1$;

Puisque *p* est au plus égal à *n*, cela implique *n+1= p+1*, donc *n = p* et *n* est premier.

c-.Critère de primarité des nombres de Mersenne :

1-.Nombre de Mersenne

Le test de Lucas-Lehmer est extrêmement rapide, ce test a servi à montrer qu'un grand nombre d'entier de la forme 2^p-1, où p est premier, sont premiers. Ces nombres sont appelés nombres de Mersenne en l'honneur du mathématicien du XVII^e siècle qui a donné une liste de nombre premiers p.

En vertu du fait que 2^{a} -1 divise 2^{ab} - *1* , un tel nombre ne peut être premier que si s est premier. La détermination des nombres de Mersenne premiers est un très ancien défi. En fait, on ne connaît que 33 nombres de Mersenne premiers. Le plus grand nombre de Mersenne premier dernièrement connu est $2^{13466917}$ -1, qui en a plus de 4053946 chiffres décimaux (découvert par Cameron, Woltman et Kurowski en 2001).

Corollaire : *Soient s > 1 et a deux entiers. Définissons la suite* $(L_i)_{i\geq 1}$ *par* $L_1 = a,\ L_{i+1} = L_i^2 - 2$. *Supposons qu'on ait* $L_{s-1} \equiv 0\ [\mathrm{mod}\ 2^s - 1\ ]$ *et que* $a^2 - 4$ *soit premier à* $2^s - 1$ *.Alors le nombre de Mersenne* $2^s - 1$ *est premier.*

Démonstration : En effet, on a pour tout i la relation $L_i = V_{2^{i-1}}$. La relation donnée implique donc modulo $2^s - 1$ la congruence $V_{2^{s-2}} \equiv 0$, d'où l'on tire $V_{2^{s-1}} \equiv 0^2 - 2 = -2,$ puis $V_{2^s} \equiv (-2)^2 - 2 = 2$ .On applique alors la proposition.

Exemple :

Prenons par exemple s = 5, donc $2^s - 1 = 31$, et a = 4. On a successivement $L_1 = 4$, $L_2 = 14$, $L_3 = 14^2 - 2 = 194 \equiv 8$, $L_4 \equiv 8^2 - 1 \equiv 0$ et 31 est premier. Pour s = 11, donc $2^s - 1 = 2047$, on trouve modulo 2047 la suite 4, 14, 194, 788, 701, 119, -170, 240, 282, et en

définitive, $L_{10} \equiv -311$. Le critère ne permet donc pas (heureusement !)de conclure à la primalité de 2047. Mieux, il implique sa non primalité, car l'unique essai avec a = 4 suffit à détecter tous les nombres de Mersenne premiers, en vertu du théorème suivant :

2-.Théorème de Lucas :

Théorème (Lucas) : *Soit s un entier impair >1, et soit n =* 2^s-1. *Définissons une suite* (L_i) *d'entier modulo n par* $L_1 = 4$ *et* $L_{i+1} \equiv L_i^2 - 2$ *.Pour que n soit premier, il faut et il suffit qu'on ait* $L_{s-1} \equiv O[\text{mod } n]$.

Démonstration : Notons d'abord qu'on a $n \equiv 7[\text{mod}12]$; en effet, on a

$$n \equiv -1[\text{mod } 4] \text{ et } n \equiv -2[\text{mod } 3].$$

Pour *a* = 4, on a pgcd(a^2-4 , n) = pgcd(12,n) = pgcd(12,7)=1. On peut donc appliquer le corollaire précédent et la condition est bien suffisante pour que n soit premier. Il nous reste à prouver la réciproque, et nous supposons désormais que n est premier.
Nous utiliserons les deux faits suivants, d'ailleurs équivalents, et tous deux conséquences de la congruence $n \equiv 7[\text{mod}12]$:

(a) 3 n'est pas un carré modulo n,

(b) on a $3^{(n-1)/2} \equiv -1 [\text{mod } n]$, ainsi que le suivant, qui résulte, lui de la congruence $n \equiv -1[\text{mod } 8]$

(c) On a $2^{(n-1)/2} \equiv 1 [\text{mod } n]$.

D'après (a), le polynôme X^2-3 est irréductible sur le corps Z/*n*Z et l'anneau $(Z/nZ)[X]/(X^2-3)$ est un corps. Notons β la classe de X (on a donc

^{2}=3 et posons =2 +

, de sorte que

$^2-4$ +1 = 0.

Par définition de suite de Lucas associé à *a* = 4 et en remplaçant, on trouve $2^{\frac{n+1}{2}} L_s \equiv 2(1+3^{\frac{n+1}{2}})$ (puisque n est premier et impair).
D'après (b) et (c) ci-dessus, on trouve que $L_s \equiv -2[\text{mod } n]$. Ce qui implique $L_{s-1} \equiv 0[\text{mod } n]$.

5-.Le critère de primarité de Solovay et Strassen

On aurait pu souhaiter que pour tout *n* composé, il existe une proportion indépendante de *n* du choix de *a* donnant une réponse négative au test de Fermat. Ce n'est pas le cas, cependant, comme le montre l'existence des nombres de Carmichael. Le test suivant est plus efficace car il évite cet inconvénient.

Soit *n* un entier impair >2.Si *n* est premier, on a $\left(\frac{a}{n}\right)\equiv a^{(n-1)/2}[\mathrm{mod}\quad n]$ pour tout entier *a* premier à *n* .Inversement :

Propriété (Solovay-Strassen) :*Soit n un entier impair >2 tel que* $\left(\frac{a}{n}\right)\equiv a^{(n-1)/2}[\mathrm{mod}\quad n]$ *pour tout entier a premier à n .Alors n est premier.*

Démonstration : On a pour tout *a* tel que *(a,n)=1* la relation $a^{n-1}[\mathrm{mod}\quad n]\equiv\left(\frac{a}{n}\right)^2=1$, ainsi si *n* n'est pas premier, c'est un nombre de Carmichael donc un produit de facteurs premiers tous différents, soit $n= p_1 \ldots p_r$ avec r ≠ 1. Soit *a* un entier premier à *n*, c'est à dire premier à chacun des p_i ; notons α_i sa classe modulo p_i .On a d'une part : $\left(\frac{a}{n}\right)=\left(\frac{a}{p1}\right)\ldots\left(\frac{a}{pr}\right)=\left(\frac{\alpha 1}{p1}\right)\ldots\left(\frac{\alpha r}{p1}\right)$, d'autre part, réduisant (modulo p_1) l'égalité initiale, on obtient $\left(\frac{a}{n}\right)\equiv$ $^{(n-1)/2}_{1}$ $[\mathrm{mod}\quad p_1]$ donc

$$\left(\frac{\quad}{p_1}^{1}\right)\ldots\left(\frac{\quad}{p_1}^{r}\right)=$$

.

D'après le théorème chinois on peut choisir les différents $_i$ indépendants. Mais le second membre ne dépend que de $_1$, tendis qu'on peut changer le signe du premier sans modifier $_1$, par exemple en modifiant α_r .Cela est absurde et contredit l'hypothèse r ≠ 1.

Corollaire :*Soit n entier impair >2*

(a) *Si n est premier on a* $\left(\frac{a}{n}\right)\equiv a^{(n-1)/2}[\mathrm{mod}\quad n]$ *pour tout entier a premier à n.*

(b) *Si n est composé, l'ensemble des a premier à n tels que 0 < a < n et* $\left(\frac{a}{n}\right)\equiv a^{(n-1)/2}[\mathrm{mod}\quad n]$ *a au plus φ(n)/2 éléments.*

Remarquons que parmi les avantages de ce test ,c'est que pour tout n composé il existe une proportion indépendante de n du choix de « *a* » donnant une réponse négative au test de Fermat , donc il est plus efficace.

6-.Résumé :

Remarquons que cela ne donne aucune certitude. Mais si n est composé chaque test a une probabilité de réussite ≤ α et une série de N tests à une probabilité de réussite

^{N} ainsi le risque d'erreur est majoré par

^{N} .et remarquons aussi que généralement un test de Miller-Rabin implique le test de Solovay et Strassen.

Finalement pour tester la primalité d'un grand nombre que l'on a choisi soi-même, le test de Fermat est en pratique suffisant. Il ne l'est plus, cependant, s'il s'agit d'un nombre dont on ne connaît pas l'origine. Dans ce cas là on applique le test de Solovay-Strassen ou de Miller-Rabin.

7-.Factorisation

Le théorème de décomposition en facteurs :

Théorème : *Soient A un anneau factoriel et P un système représentatif d'éléments extrémaux de A. Pour tout élément x =0 de A, il existe un unique élément inversible* $u \in$ A *et une unique famille d'entiers naturels* $(n_p)_{p\in P}$ *nuls à l'exception d'un nombre fini d'entre eux tels qu'on ait* $x = u\prod_{p\in P} p^{n_p}$.

Démonstration : Par définition d'anneau factoriel on a :

(i) Si x est inversible il s'écrit x=x ; sinon il s'écrit $q_1 \ldots q_m$ où chaque q_i peut s'écrire sous la forme vp avec $v \in$ A et p ∈ P .

(ii) Si on suppose qu'on a $x = u\prod_{p\in P} p^{n_p} = u_1 \prod_{p_1\in P} p_1^{n_p}$ si $n_{p_0} < n_{1\,p_0}$ alors $x/p^{n_{p_0}}$ est divisible par p_0 ce qui est contradictoire car le terme de gauche est produit d'élément inversible et d'éléments extrémaux non associés à p_0 donc d'élément non divisible par p_0 .

Malheureusement, en pratique ce théorème ne sert pas à grand chose quand il s'agit de grands nombres.

Mentionnons d'abord que tout les algorithmes performants de factorisation suivent une démarche probabiliste ; C'est à dire qu'il cherche à minimiser le temps de moyen de

calcul des facteurs d'un nombre n. L'essentiel des efforts, en matière de factorisation de grands nombres, a porté sur la recherche de raffinements de l'approche.

L'idée de base remonte à Fermat : pour factoriser un nombre n, il suffit de trouver deux entiers x et y modulo n, distincts et non opposée modulo n, tels que

$$X^2 \equiv y^2 \ mod \ n.$$

Puisque (x+y)(x-y) est un multiple de n, on voit aisément que le calcul de pgcd(n, x+y) ou de pgcd(n, x-y) nous donne un diviseur non trivial de n.

La méthode de Fermat consiste à calculer les carrés modulo n d'entiers x légèrement supérieurs à la partie entière de la racine carrée de n afin de tomber sur un carré parfait y^2, ce qui nous donnera un diviseur non trivial de n.

Chapitre 3

Courbes elliptiques

Les tests probabilistes de primalité que nous avons détaillés dans le chapitre précédent sont tout à fait suffisants pour les applications cryptographiques. Cependant, après s'être convaincu qu'un entier *n* est très probablement premier car il a passé avec succès une multitude de tests, on a la certitude qu'il est premier que si on a une factorisation de *n-1* et si on réussi le test de Lucas. Mais en général trouver une factorisation complète de *n-1* est difficile !

Les courbes elliptiques figurent parmi les objets mathématiques les plus étudiées. Elles ont la particularité de s'appliquer à la cryptographie de façon diverse, pas seulement en fabriquant des fonctions à sens unique mais aussi du fait qu'elles offrent un algorithme performant pour la factorisation, dont la complexité est sous-exponentielle.

1-. Le groupe d'une courbe elliptique

Soit un corps commutatif K, de caractéristique différente de 2 et 3.
Soit un polynôme $x^3 + ax + b$ (avec *a*, *b* deux élément de K qui n'a pas de racine multiple dans K (càd $4a^3 + 27b^2 \neq 0$). Une courbe elliptique sur K est définie comme étant l'ensemble des couples(x, y), avec x, y dans K, vérifiant l'équation :

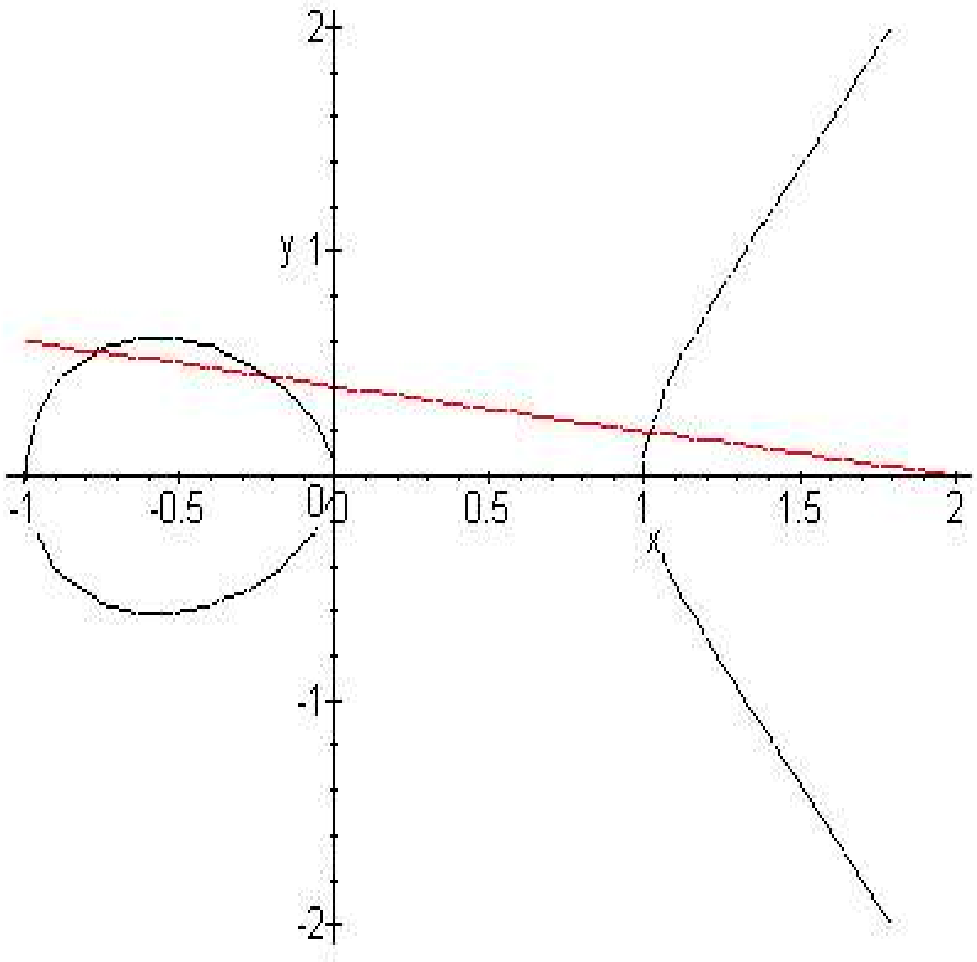
$$y^2 = x^3 + ax + b$$

et augmenté d'un élément supplémentaire que l'on notera O et qu'on appelle le « point à l'infini ». Les courbes elliptiques ont la particularité d'être munies d'une structure de groupe commutatif. C'est dû au fait qu'une droite qui passe par deux points d'une courbe elliptique la recoupe en exactement un point supplémentaire. On peut alors définir ce groupe de la façon suivante :

1. Le point à l'infini est l'élément neutre.
2. P+Q+R=0 si les points P, Q, R sont alignés.

Par conséquent on peut définir la loi de groupe de la manière suivante (on considère que K est l'ensemble des réels):

1. Pour tout P de la courbe, on convient que P+O=P; O sera l'élément neutre de la loi.
2. Si P ≠O est le point (x, y) et Q est le point (x, -y) symétrique de P par rapport à l'axe des x, on convient que P+Q=O. P et Q seront donc opposés.
3. Si P et Q deux points différents de O, avec des abscisses différentes, la courbe coupe la droite (PQ) en exactement un point R
4. Si P=Q et P ≠Q alors P+P=R, où R est l'intersection de la courbe avec la tangente en P



La courbe elliptique $y^2 = x^3 – x$.

2-.L'exponentielle elliptique

Toute loi de groupe fini est susceptible de donner naissance à une fonction exponentielle qu'on note :

$$\{0, 1, .., m-1\} \rightarrow H$$
$$k \rightarrow k.P = P+P+\ldots+P(k \text{ fois})$$

où $P = (x, y)$ est un point d'une courbe elliptique définie sur IF_p. h est le sous groupe d'ordre m de E_p engendré par P.

Exemple :

Soit la courbe $y^2 = x^3 + x + 1$ sur IF_{17}. Le groupe de la courbe est un groupe cyclique d'ordre 18 et p=(0, 1)en est un générateur. On a alors :

k	1	2	3	4	5	6	7	8	9
$k.P$	(0,1)	(-4,1)	(4, -1)	(-8, -5)	(-1,4)	(-7, -5)	(6,6)	(-2, -5)	(11,0)

k	10	11	12	13	14	15	16	17	18
$k.P$	(-2,5)	(6, -6)	(-7,5)	(-1, -4)	(-8,5)	(4,1)	(-4, -1)	(0, -1)	0

La question qu'on peut se poser est la cardinalité du groupe associé, le théorème dû à Hasse (1934) répond à cette question

Théorème de Hasse: *Le nombre de points d'une courbe elliptique sur IF_p est compris entre* $p + 1 - 2\sqrt{p}$ et $p + 1 + 2\sqrt{p}$.

Preuve : Notons $m=\#E(IF_p)$.

(i) Si $p=2$ ou $p=3$, alors la propriété est vérifiée car O appartient à la courbe et à chaque abscisse x correspond au plus deux ordonnées y.

(ii) Supposons maintenant que la courbe est donnée par l'équation de Weierstrass

$$E : y^2 = x^3 + ax + b \text{ ¿ } O = (0, 1, 0)$$

1) Considérons la courbe elliptique

$$Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b} \cup O = (0, 1, 0) \qquad (*)$$

avec X et Y deux éléments de IF_p, le corps des fractions rationnelles à coefficients dans IF_p. L'ensemble des solutions de (*) forme un groupe commutatif et comme $(x, 1)$ et $(x^p, (x^3+ax+b)^{(1/2)(p-1)}$ sont solution de (*), donc

$$S_n = (x^p, (x^3+ax+b)^{(1/2)(p-1)} + n(x, 1)$$

Vérifie aussi (*).
Soit la suite (d_n) définie par :

$$\begin{cases} d_n=0 & \text{si } S_n=O, \\ d_n=\max(d°(\text{numérateur}(X_n)), d°(\text{dénominateur}(X_n))) & \text{si } S_n=(X_n, Y_n) \end{cases}$$

où X_n est telle que

pgcd(numérateur(X_n), dénumérateur(X_n))=1.

Pour une forme elliptique donnée sous la forme

$$E_1 : F(X, Y) = Y^2 - \frac{X^3+aX+b}{x^3+ax+b} . \qquad (**)$$

Soient $P=(P_1, P_2)$ et $Q=(Q_1, Q_2)$ deux points disjoints de E_1, tous deux différent de O et tels que $R=(R_1, R_2)=P+Q \neq O$. L'inverse de point P est donnée par

$$-P= (P_1, -P_2), \qquad (1)$$

Notons $cX+d$ la sécante passant par Pet Q avec

$$c=(Q_2-P_2)/(Q_1-P_1) \text{ et } d=P_2-cP_1.$$

En substituant dans (**), on trouve :

$$F(X, cX+d)=\frac{-X^3}{x^3+ax+b}+(cX)^2+\left[2cd-\frac{a}{x^3+ax+b}\right]X+\left[d^2-\frac{b}{x^3+ax+b}\right]$$

$$= k(X - P_1)(X - P_2)(X - P_3)$$
$$= kX^3 - k(P_1 + Q_1 + R_1)X^2 + k(Q_1 R_1 + P_1 Q_1 + P_1 R_1)X - kP_1 Q_1 R_1.$$

Comme $k = -(x^3 + ax + b)^{-1}$ et $-k(P_1 + Q_1 + R_1) = c^2$, et

$$R_1= c^2(x^3 + ax + b) - P_1 - Q_1, \qquad (2)$$

$$R_2 = -(cR_1 + d) \qquad (3)$$

Si $P = Q$, alors la sécante devient tangente et

$$c = \frac{\frac{\partial F}{\partial X}(P_1, P_2)}{\frac{\partial F}{\partial Y}(P_1, P_2)} = \frac{3P_1^2 + a}{2P_2(x^3 + ax + b)} \qquad (4)$$

2) maintenant on veut montrer que $d_{-1} - d_0 = m\text{-}p$.
par (*), on a $d_0 = p$. Il reste à démontrer que $d_{-1} = m$. par (1) et (2) on a

$$X_{-1} = (x^p, (x^3 + ax + b)^{(p-1)/2} + (x, -1)$$
$$= \underbrace{\left| \left(\frac{-1 - (x^3 + ax + b)^{(p-1)/2}}{x - x^p} \right)^2 \right| (x^3 + ax + b) - x^p - x.}_{= L}$$

Simplifions L. Dans (Z/pZ), le dénominateur de L se factorise en

$$(x - x^p)^2 = \prod_{u \in (Z/pZ)} (x - u)^2 .$$

Les facteurs de la forme (x – u) du numérateur de L sont ceux pour lesquels ce dénominateur s'annule en u. Cela apparat quand

$$(u^3 + ax + b = 0 \quad \Leftrightarrow \quad \left(\frac{u^3 + au + b}{p} \right) = 0.$$

Après simplification on trouve que les dénominateurs restants sont

$$(x - u)^2 \quad si \quad \left(\frac{u^3 + au + b}{p} \right) = 1$$

$$(x - u) \quad si \quad \left(\frac{u^3 + au + b}{p} \right) = 0,$$

ce qui correspond au nombre de solution affines de $E(IF_p)$ et donc

$$d^\circ (dénominateur(L) = m - 1).$$

Or,

$$X_{-1} = \left(\frac{x^{2p+1} + R(x)}{(x - x^p)^2} \right)$$

Où le degré de R(x) est strictement inférieur à $2p+1$; donc

$$d^\circ(\text{numérateur}(X_{-1})) = d^\circ(\text{dénominateur}(X_{-1})) + 1$$

et

$$d_{-1} = d^\circ(\text{dénominateur}(L)) + 1 = m.$$

3) montrons que $d_{n-1} + d_{n+1} = 2d_n + 2$, pour tout n de Z.

(i) Considérons d'abord le cas où S_{n-1}, S_n ou S_{n+1} est le point O. Si $S_{n-1} = O$, alors $d_{n-1} = 0$ et, par (2) et (4),

$$S_n = (x, 1) \text{ et } S_{n+1} = (x, 1) + (x, 1) = \left(\frac{x^4 - 2\,ax^2 - 8\,bx + a^2}{4\,(x^3 + ax + b)}, Y_{n+1} \right),$$

Donc $d_n = 1$ et $d_{n+1} = 4$ et la formule est vérifiée. Si $S_n = O$, alors $d_n = 0$ et $S_{n+1} = (x, 1)$ et $S_{n-1} = -(x, 1) = (-x, 1)$, et donc $d_{n+1} = d_{n-1} = 1$ et la formule est vérifiée. Si $S_{n+1} = O$, alors $d_{n+1} = O$ et $S_n = -(x, 1) = (-x, 1)$ et

$$S_{n-1} = (-x, 1) - (x, 1) = 2(-x, 1) = \left(\frac{17x^4 + 14ax^2 + 8\,bx + a^2}{4\,(x^3 + ax + b)}, Y_{n-1} \right),$$

et donc $d_n = 1$ et $d_{n-1} = 4$ et la formule est vérifiée.

(ii) Si les trois points S_{n-1}, S_n, et S_{n+1} sont tous différents de O. notons

$$X_{n-1} = \frac{A}{B}, \; X_n = \frac{P}{Q}, \; X_{n+1} = \frac{C}{D}$$

De sorte que les dénominateurs et les numérateurs n'aient pas de facteur commun, i.e.

Pgcd(A, B) = pgcd(P, Q) = pgcd(C, D) = 1.

Par les formulas (1) et (2), on a alors

$$X_{n-1} = \frac{Q^3(1+Y_n)^2(x^3+ax+b)-(Qx-P)^2(P+Qx)}{(Qx-P)^2Q},$$

(6)

$$X_{n+1} = \frac{Q^3(1-Y_n)^2(x^3+ax+b)-(Qx-P)^2(P+Qx)}{(Qx-P)^2Q}.$$

(7)

En multipliant et en additionnant les deux égalités précédentes, nous obtenons

$$X_{n-1}\,X_{n+1} = \frac{(Px-aQ)^2-4\,bQ(P+Qx)}{(Qx-P)^2} = \frac{AC}{BD}, \quad (8)$$

$$(X_{n-1} + Xn_{+1}) = \frac{2\,[PQx^2+P^2x+axQ^2+2\,bQ^2+aPQ]}{(Qx-P)^2} = \frac{AD+BC}{BD}$$

(9)

Soit H=pgcd(AC, BD), alors par (8) et (9) on a

$$AC = H[(Px - aQ)^2 - 4bQ(Qx + P)], \quad (10)$$
$$BD = H(Qx - P)^2, \quad (11)$$
$$AD + BC = 2H[PQx^2 + P^2x + axQ^2 + 2bQ^2 + Apq]. \quad (12)$$

Si F est un facteur premier de H, alors, par les relations précédentes, on a

$$F \quad AC, \; F \quad BD \; \text{et} \; F \quad (AD + BC) \qquad (13)$$

Supposons que F B (le cas F divise D est symétrique), alors F ne divise pas A car pgcd(A, B) = 1. De plus, comme $F\ AC$, il vient que $F\ C$ et donc $F\ BC$. Enfin, comme $F\ (AD+BC)$, il s'ensuit que F$A\,D$ *et* $F\ D$ car F ne divise pas *A.* On vient de démontrer que FC *et* $F\ D$, par conséquent F = 1 car pgcd(C, D)=1. Par les équations (10), (11) et (12), cela implique que

$$AC = (Px - aQ)^2 - 4bQ(Qx + P), \quad (14)$$
$$BD = (Qx - P)^2, \quad (15)$$
$$AD + BC = 2[PQx^2 + P^2x + axQ^2 + 2bQ^2 + Apq]. \quad (16)$$

Démontrer que $d_{n-1} + d_{n+1} = 2d_n + 2$ équivaut à démontrer que

$$\max(d°(A), d°(B)) + \max(d°(C), d°(D)) = 2\max(d°(P),d°(Q)) + 2.$$

(a) Si $d_{n-1} = d°(A)$ et si $d_{n+1} = d°(C)$, alors, par (14),

$$d_{n-1} + d_{n+1} = d°(AC) = d°[(Px-aQ)^2 – 4bQ(Qx + P)].$$

Par l'absurde, supposons que $d°(P) < d°(Q)$. Alors, par (15),

$$d°(BD) = 2d°(Q) + 2.$$

De plus,

$d°(AC) \leq \max(2d°(P) + 2, 2d°(Q), 2d°(Q) + 1, d°(PQ)) = 2d°(Q) + 1 < d°(BD)$,

ce qui est impossible. Donc, $d°(P) \geq d°(Q)$ et

$$d°(AC) = d°(Px^2) = d_n + 2,$$

ce qui démontre 3).

(b) Si $d_{n-1} = d°(B)$ et si $d_{n+1} = d°(D)$, alors, par (15),

$$d_{n-1} + d_{n+1} = d°(BD) = d°[(Qx – P)^2].$$

Par l'absurde, supposons que $d°(Q)<d°(P)$. Alors, par (14),

$$D°(AC) = d°(P^2x^2)>d°5BD),$$

Ce qui est impossible. Donc, $d°(Q)\geq d°(P)$ et

$$d°(BD) = d°(Q^2x^2) = d_n + 2,$$

Ce qui démontre le 3).

(c) Si $d_{n-1} = d°(A)$ et $d_{n+1} = d°(D)$ avec $d°(A) > d°(BC)$ et $d°(D)>d°(C)$, alors, par(16),

$$d°(AD) = d°(AD+BC) \text{ car } d°(AD)>d°(BC) = d°\{2[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]\} = d°(PQx^2).$$

Si $d°(P) \geq d°(Q)$, alors

$d°(AD) < d°(Q^2x^2) = d°(BD)$,

Ce qui est impossible. Le cas © ne se rencontre jamais.

(d) Si $d_{n-1} = d°(B)$ et si $d_{n+1} = d°(C)$ avec $d°(B) > d°(A)$ et $d°(C) > d°5D$), (alors, par (16),

$$d°(BC) = d°(AD+BC) \text{ car } d°(AD) < d°(BC)$$
$$= d°\{2[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]\}$$
$$= d°(PQx^2)$$

Si $d°(P) \geq d°(Q)$, alors

$$d°(BC) < d°(P^2x^2) = d°(AC),$$

ce qui impossible.

Sinon, si $d°(P) < d°(Q)$, alors

$$d°(BC) < d°(Q^2x^2) = d°(BD),$$

ce qui impossible.

(4) Par induction, montrons que $d_n = n^2 – (d_{-1} – d_0 – 1)n + d_0$.

Pour $n=-1$ ou $n=0$, la relation est vérifiée. Supposons que $d_{n-2} = (n-2)^2 –(d_{-1} – d_0 – 1)(n-1) + d_0$ et que $d_{n-1} = (n-1)^2$, alors par 3),

$$d_n = 2d_{n-1} – d_{n-2} + 2$$
$$= 2[(n-1)^2 – (d_{-1} – d_0 – 1)(n-1) + d_0]$$
$$– [(n-2)^2 –(d_{-1} – d_0 – 1)(n-2) + d_0] + 2$$
$$= n^2 -(d_{-1} – d_0 – 1)n + d_0.$$

En remplaçant d_{-1} et d_0 par leurs valeurs déjà calculées en 2), donc on a

$$d_n = n^2 + a_pn + p,$$

Où $a_p = p + 1 – m$.

Considérons la fonction

$$f : IR \rightarrow IR$$
$$r \rightarrow r^2 + a_pr + p.$$

Si cette fonction a deux racines distinctes r_1 et r_2 avec $r_1 < r_2$, alors pour tout r dans $]r_1,r_2[$: $f < 0$

Car $f'''(r)>0$. Or comme $r_2 - r_1 =$ $= (a_p)^2 - 4p, > 0$ et que a_p est entier, on a $r_2 - r_1 \geq 1$. Il existe donc un entier n tel que d_n consécutifs ne peuvent pas s'annuler simultanément. Ce qui implique que $d_n < 0$, ce qui st impossible car d_n est le degré d'un polynome. Par conséquent,

$$= (a_p)^2 - 4p \geq 0 \text{ et donc } | a_p | = | p + 1 - \#E(IF_p) | \leq 2\sqrt{p} .$$

L'attrait principal de l'exponentielle elliptique revient aux deux avantages suivants :

-Elle est à peine plus difficile à calculer que l'exponentielle modulaire.

-Elle semble plus difficile à inverser : elles necissitent un nombre d'opération dans IF_p exponentielle en $\log p$.

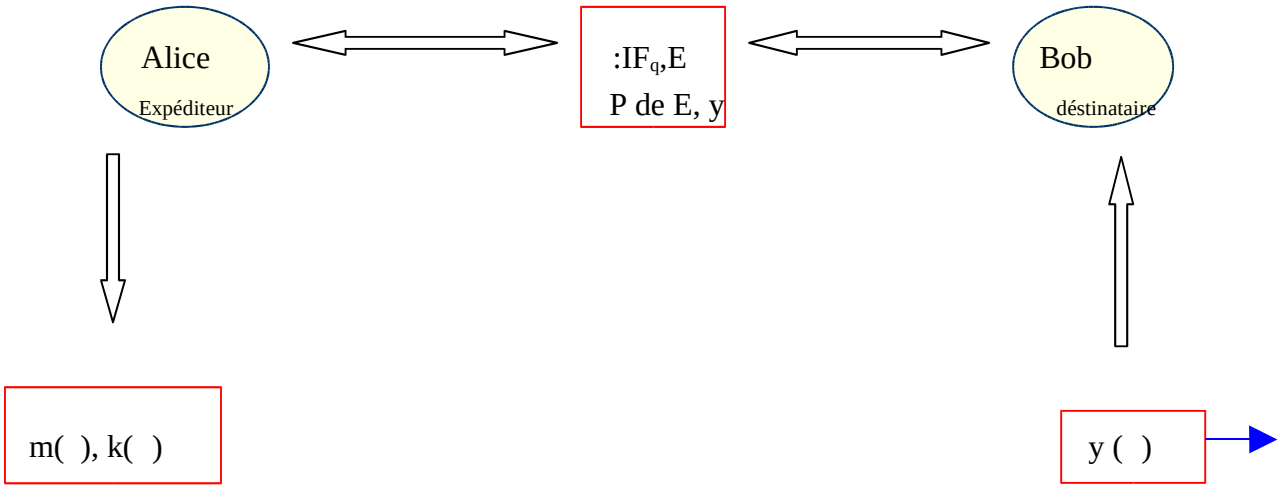
3-.Cryptographie et courbes elliptiques

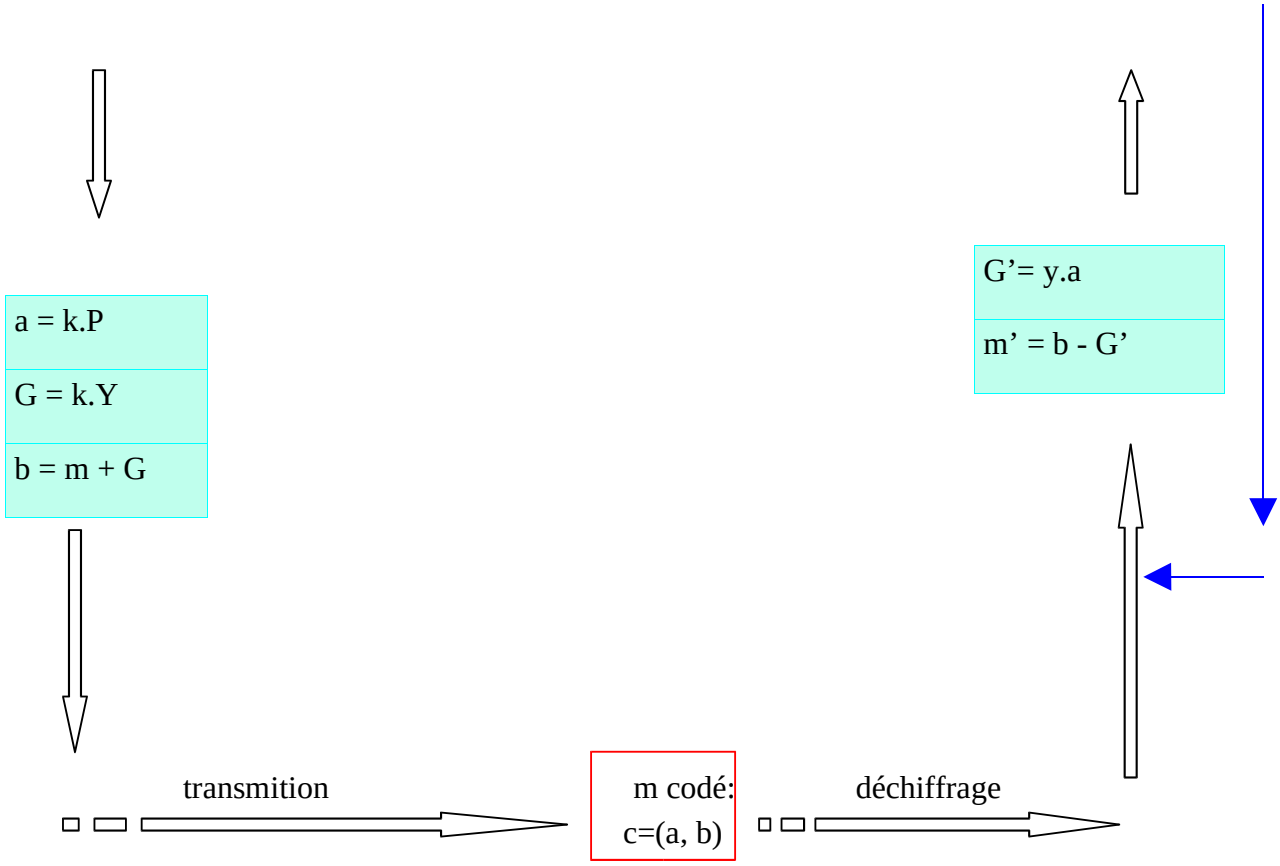
Tout système cryptographique fondé sur l'exponentielle modulaire est candidat à être transformé en un système elliptique après des adaptations.

Exemple du système El-Gamal :

Dans le système El-Gamal, en l'adaptant à ce système on obtient :

Le destinataire Bob rend public un nombre premier p, une courbe elliptique E_p sur IF_p, un point P qui sera la base de l'exponentielle, et un point (s.P) avec s la clé secrète de Bob. Un message M, en clair, est un point de la courbe, et pour le chiffrer, Alice choisit un entier aléatoire k, calcule k. P, et transmet le couple de point (C_1, C_2) où C_1=k. P et C_2=M+k. (s.P). Pour déchiffrer, Bob calcule $M=C_2 - s.C_1$.





Codage d'El-Gamal elliptique

Exemple du système deDiffie-Hellman :

Une façon de faire de la cryptographie en utilisant des courbes elliptiques consiste à appliquer le même principe à l'algorithme Diffie-Hellman
Alice dispose de sa courbe elliptique et de deux points. Elle dispose aussi d'un nombre d, mais le garde secret. Son nombre d n'est qu'un nombre aléatoire.

Clé publique d'Alice : p, a, b, P, Q_{Alice}

Clé privée d'Alice : d_{Alice}

Bob reçoit la clé publique d'Alice et calcule la sienne. Il s'agit simplement d'une valeur aléatoire. Il trouve ensuite un point Q en multipliant dP.

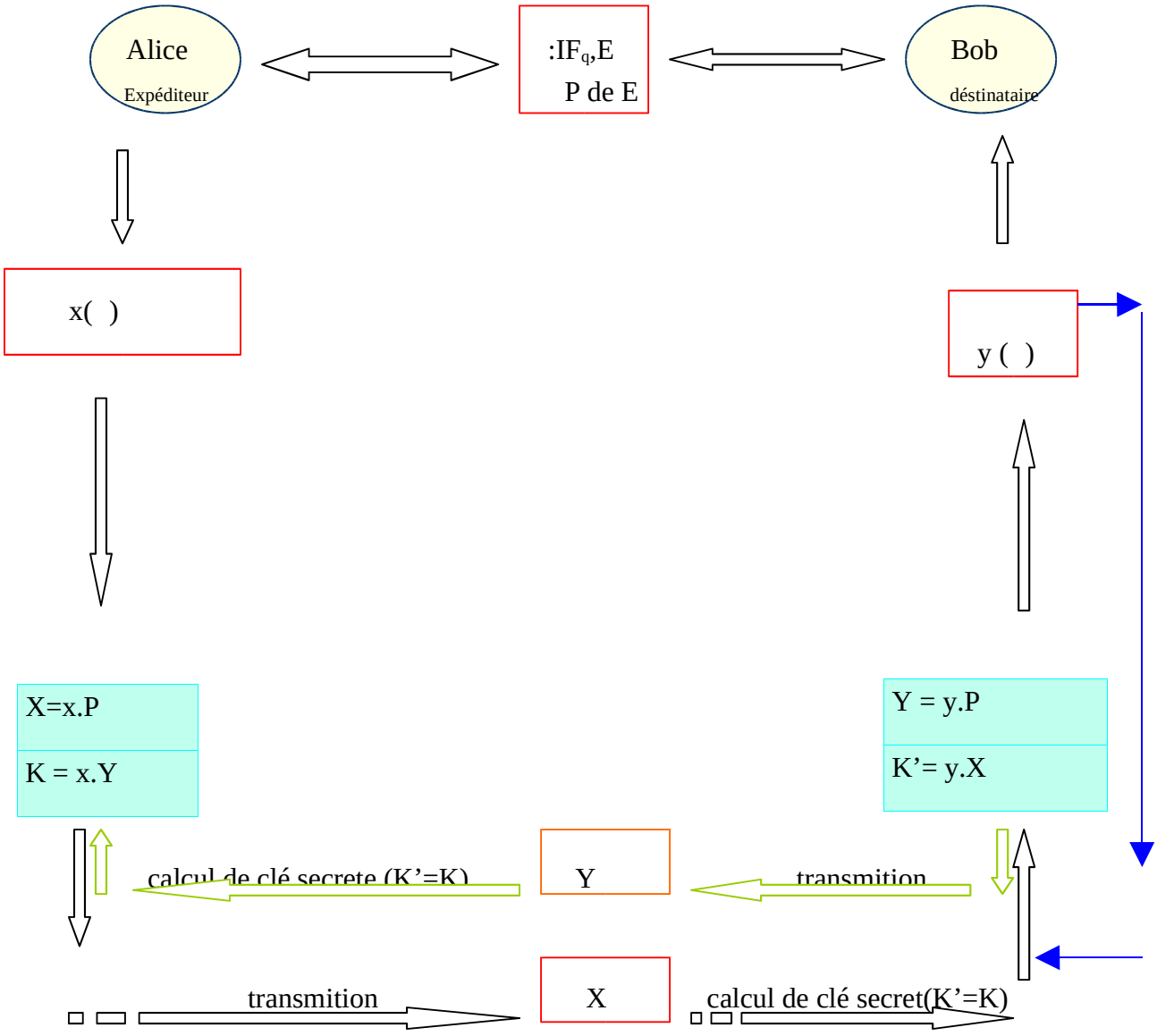
Clé publique de Bob : p, a, b, P, Q_{Bob}

Clé privée de Bob : d_{Bob}

Bob multiplie alors son nombre d par le nombre Q d'Alice.

Valeur secrète : $S=d_{Bob}Q_{Alice}$. (avec $Q_{Alice}=d_{Alice}P$)

Bob envoie maintenant à Alice son nombre Q. Et Alice effectue ses calculs à partir de ce nombre Q.



Codage de Diffie-Helman elliptique

Pourquoi la cryptographie par courbe elliptique ?

Pour des raisons de performances, tout simplement. En effet la taille des clés et la taille de la transmission de données sont plus petites. Mais un des inconvénients de cette méthode est que vous pouvez signer vite ou économiser de l'espace de stockage, mais pas les deux en même temps.
A l'heure actuelle, dans la course aux standards, la cryptographie RSA tient la corde car cette dernière s'appuie sur une infrastructure bien développée en matière de certificats chose qui manque à la méthode des courbes elliptique car il est difficile de développer des certificats numériques en passant par la cryptographie par courbes elliptiques.

4-.factorisation et courbes elliptiques

On se sert aussi de l'exponentielle elliptique pour trouver des algorithmes de factorisation.

Exemple de « L'algorithme p-1 de Pollard » :

Supposons que l'on veut trouver un diviseur non trivial d'un entier n qui admet comme facteur premier p(avec p-1 suffisamment ''friable''. Ce qui signifie que tous les facteurs premiers de p-1 sont inférieurs à un certain entier $A << n$). Alors A! est un multiple de p-1(presque sûrement). Dans ce cas, d'après le petit théorème de Fermat on a pour tout a :

$$a^{A!} \equiv 1 \bmod p .$$

C'est à dire que $a^{A!} - 1$ est un multiple de p. Donc l'idée est de choisir un entier a, au hasard, calculer $a^{A!}$ modulo n puis évaluer en utilisant l'algorithme d'Euclide, le pgcd(n, $a^{A!} \equiv 1 \bmod n$).

Exemple de L'algorithme de Lenstra :

Il est clair que le calcul peut devenir prohibitif dans certain cas. Vers 1986, Lenstra a pensé faire appel aux courbes elliptiques sur IF_P pour les diviseurs premiers p de n. L'intérêt est qu'il y a plus de groupes de courbes elliptiques que de diviseurs premiers p de n ce qui veut dire qu'on peut espérer en essayer beaucoup pour espérer tomber sur un dont la cardinalités soit friable.

Concrètement, on s'arrange pour trouver une équation d'une courbe elliptique, c à d vérifiant $4a^3 + 27b^2$ sur n'importe quel corps fini IF_p où p divise n ; pour cela il suffit de vérifier que $pgcd(n, 4a^3 + 27b^2) = 1$(si ce n'est pas le cas, on obtient gratuitement un diviseur de n). En même temps on choisit un (x, y) vérifiant l'équation modulo n, ce qui veut dire que qu'en réduisant (x, y) modulo un diviseur p premier de n, on aura un point de la courbe. Ensuite on choisit un entier suffisamment grand(comme dans l'algorithme de p-1 de Pollard, et on effectue le calcul de A!.P modulo n (grâce à l'équation de la courbe), ce qui nous

permet d'obtenir un couple (X, Y) qui s'il était réduit modulo p, donnerait le point A!.P de la courbe elliptique.

Remarquons que cett méthode à l'avantage d'être calculable en un temps relativement inférieur.

Exemple :

Factorisons le nombre N = 540143 par la méthode de Lenstra. Soit la famille de courbes paramétrées par a

$$E_a : y^2 = x^3 + ax + 1 \text{ ¿ } O.$$

Le point P = (0, 1) ≠O appartient toujours à E_a pour toute valeur de *a*. Le discriminant vaut $-16(4a^3 + 27)$. Prenons *a* = 1, alors pgcd(, N) = 1 et la courbe E_1 est bien une courbe elliptique sur IF_p *où p* est un facteur premier de N. Nous savons que tout facteur premier p de N est inférieur à

5-.Courbes elliptiques et primalité :

Savoir si un nombre est probablement premier ou pas est une chose et être sûr qu'il est premier est une autre chose. Peut-on obtenir un véritable certificat de primalité ? On sait que si on trouve une factorisation de n-1, alors on peut appliquer le théorème de Lucas pour certifier sa primalité. Comme le théorème de Lucas repose sur l'exponentiation modulaires, on peut trouver alors une version elliptique.

Le théorème suivant est la version elliptique de théorème de Lucas :

Théorème (critère de Goldwasser-Kilian): *Soit n un entier impair non divisible par 3. Soit m un entier et q un diviseur premier de m tel que* $q>(n^{1/4}+1)^2$.

Soit l'équation $y^2 = x^3 + ax + b$ *où* $4a^3 + 27b^2 \neq 0 \bmod n$. *Soit* $P=(x_1, y_1)$ *un point satisfaisant l'équation modulo n. Si, par application répétée des formules d'addition suivantes :*

$$\begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 (x_1 - x_3) \end{cases} \quad \text{Et} \quad \begin{cases} x_3 = \left(\dfrac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\dfrac{3x_1^2 + a}{2y_1}\right)^2 (x_1 - x_3) \end{cases}$$

prises modulo n, on trouve que :

1. $m.P=0$
2. $\left(\frac{m}{q}\right).P=(X, Y)$ *où au moins une des deux coordonnées X et Y est inversible modulo n,*

alors n est premier.

Preuve **:** Supposons p le plus petit diviseur premier de *n*. L'équation nous définit une courbe elliptique E_p sur IF_p. Les hypothèses impliquent que $m.P=0$ et $(m/q).P\neq 0$ dans E_p. On en déduit, parce que *q* est premier, que *q* divise l'ordre de *P*.Donc *q* divise l'ordre du groupe $\#E_p$. En particulier $q \leq \#Ep$. Mais le théorème de Hasse nous dit : $\#E_p \leq (\sqrt{p}+1)^2$. Or l'hypothèse $q > (n^{1/4} + 1)^2$ implique alors $\sqrt{n} < p$, mais ceci contredit le choix de *p*.

Exemple ***:***

Appliquons ce test pour prouver la primalité de 1283. Comme 1283 est relativement premier avec 6, considérons la courbe

$$y^2 = x^3 + ax + b \pmod{1283} \text{ ¿ } O.$$

Choisissons $x=121$, $y=30$ et $a=-1$. Nous calculons alors $b=30^2 - 121^3 + 21 \bmod 1283 = 0$. Le point $P=(121, 30)$ appartient à la courbe

$$E : y^2 = x^3 - x \pmod{1283} \text{ ¿ } O.$$

Cette courbe est non singulière car son disciminant est égal à 64 qui est non nul. Nous devons maintenant calculer le nombre de points de cette courbe. Remarquons que

$$((-x)^3 - (-x)) = (-1)(x^3 - x) = -(x^3 - x)$$

car 1283 = 3 mod 4 et donc

$$\sum_{x \in IF_{1283}} (x^3 - x) = (0) = 0.$$

La cardinalité m de la courbe vaut 1283+1=1284. Comme m=1284=12.107, vérifions les hypothèses de la proposition avec q=107 :

1. 107 est premier et $107 > ((1283)^{1/4} + 1)^2$ ¿ 49 ;
2. 1284P=2(2(P + 2(2(2(2(2(2(P+2(2P)))))))))=…=O;
3. $\frac{1284}{107}$ P = 12P = 2(2(P + 2P)) = 2(2((121,30) + (1066,377)))
   = 2(2(1083,1155))=2(704,284)=(903,1038) ≠O.

Comme les hypothèses du théorème sont vérifiées, on peut constater que 1283 est premier.

Cette idée d'utiliser les courbes elliptiques dûe à Goldwasser et Kilian (1986), a comme principal problème le calcul de nombre de points sur une courbe elliptique. La méthode a été améliorée de manière significative par Atkin qui choisit la courbe non pas au hasard mais parmi une certaine famille de courbes pour lesquelles le décompte des points est beaucoup plus facile. Au bout du compte on obtient un test déterministe de primalité finalement mis au point par Morain, et qui prouve sans problème la primalité d'entiers de 500 chiffres décimaux et même parfois beaucoup plus.

6-.Representation d'un message

Il reste un point très important concernant la représentation d 'un message *m* sur une courbe elliptique. A vrai dire, il n'existe pas de méthode déterministe pour représenter un message. Par contre ce qui reste possible c'est de fixer la probabilité d'échec. Si on considère la courbe elliptique sur IF_q suivante :

$$E : y^2 = x^3 + ax + b \text{ ¿ } O,$$

Et soit k tel que 2^{-k} est la probabilité qu'on ne puisse pas représenter le message m. Supposons que

(i) m<M et (ii) q>Mk.

Nous représentons le message m comme un élément de IF_q par

$$X' = mk + j,\ 1 \le j \le k.$$

On remarque que $x' \le (M - 1)k + k = Mk < q$. Nous avons alors :

$$Y' = x'^3 + ax' + b.$$

Avec y' un carré (on essaye j=1, 2, …, k). Donc pour retrouver m, on calcule la partie entière inférieure de (x'-1)/k.
Comme il y a approximativement une chance sur deux pour qu'y' soit un carré, la probabilité d'échec est de l'ordre de 2^{-k}.

Table des matières