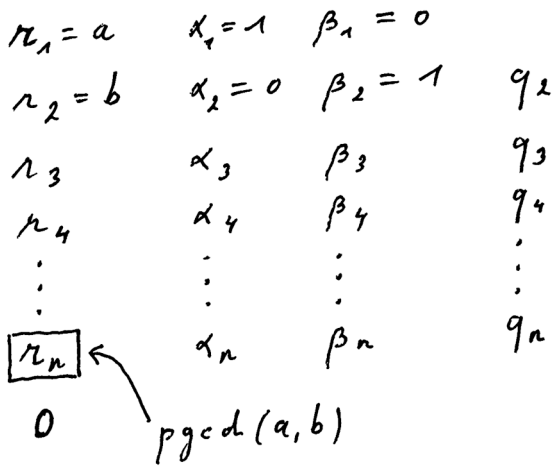
JUSTIFICATION DE L'EXTENSION DE L'ALGORITHME D'EUCLIDE

Considérons le tableau produit par l'algorithme étendu :



On doit prouver que $r_n = \alpha_n a + \beta_n b$.
Pour cela, on établit par récurrence que $r_i = \alpha_i a + \beta_i b$ pour tout $i \in \{1, 2, \ldots, n\}$.
C'est évidemment vrai pour $i = 1$ et $i = 2$.

Il suffit maintenant de montrer que si :

$$r_k = \alpha_k a + \beta_k b \qquad (1)$$
$$\text{et} \quad r_{k+1} = \alpha_{k+1} a + \beta_{k+1} b \qquad (2)$$

alors : $r_{k+2} = \alpha_{k+2} a + \beta_{k+2} b$

En faisant $(1) - q_{k+1} \cdot (2)$, on obtient :

$$r_k - q_{k+1} r_{k+1} = (\alpha_k - q_{k+1}\alpha_{k+1})a + (\beta_k - q_{k+1}\beta_{k+1})b$$

Or :

a) $r_k - q_{k+1} r_{k+1} = r_{k+2}$ puisque r_{k+2} est le reste de la division de r_k par r_{k+1} et que q_{k+1} en est le quotient ;

b) $\alpha_{k+2} = \alpha_k - q_{k+1}\alpha_{k+1}$ parce que α_{k+2} provient d'une combinaison linéaire de coefficients 1 et $-q_{k+1}$;

c) $\beta_{k+2} = \beta_k - q_{k+1}\beta_{k+1}$ parce que β_{k+2} provient d'une combinaison linéaire de coefficients 1 et $-q_{k+1}$.

Ainsi $r_{k+2} = \alpha_{k+2} a + \beta_{k+2} b$, ce qu'il fallait démontrer.

LE THÉORÈME DE BÉZOUT

Théorème

Soient $a, b \in \mathbb{Z}$. Si d est le pgcd de a et b, il existe deux entiers α et β tels que

$$\alpha a + \beta b = d$$

Preuve

L'algorithme d'Euclide étendu nous donne les coefficients α et β.

Remarque. Les coefficients de Bézout, α et β, ne sont pas uniques.

Corollaire

Deux entiers a et b sont premiers entre eux (c'est-à-dire sans diviseur commun supérieur à 1) si et seulement si il existe $\alpha, \beta \in \mathbb{Z}$ tels que :

$$\alpha a + \beta b = 1$$

Epitaphe d'Etienne Bézout

CY GIT

ETIENNE BEZOUT DE L'ACADEMIE (ROYALE) DES SCIENCES ET DE CELLE DE LA MARINE,
EXAMINATEUR DES GARDES DU PAVILLON ET DE LA MARINE ET DES ELEVES ET
ASPIRANTS AU COPRS (ROYAL) D'ARTILLERIE, CENSEUR (ROYAL),
NE A NEMOURS, LE 31 MARS 1730, ET MORT AUX BASSES-LOGES LE 27 7bre 1783.

GEOMETRE SCAVANT, PHILOSOPHE PAISIBLE,
PERE, EPOUX, CITOYEN, AMI TENDRE ET SENSIBLE
SON SCAVOIR FUT PROFOND, SON ESPRIT PENETRANT.
IL CONNUT LES PLAISIRS QUE DONNE LA SAGESSE ;
IL VECUT POUR LES SIENS, CULTIVA LEUR TENDRESSE
ET FIT DE LEUR BONHEUR, SON BONHEUR LE PLUS GRAND.
POUR SAUVER DE L'OUBLI SON NOM ET SA MEMOIRE
CE MARBRE ETAIT SANS DOUTE UN TEMOIN SUPERFLU ;
MAIS DES REGRETS QUE LAISSE APRES LUI SA VERTU
L'AMITIE SE CONSOLE EN PARLANT DE SA GLOIRE.

L'EUROPE A VU PERIR ET PRESQUE AU MEME TEMPS,
EULER SI RENOMME CHEZ LES GERMAINS SCAVANS
BEZOUT ET D'ALEMBERT NON MOINS CHERS A LA FRANCE
O ! QUEL SIECLE FECOND EN VERTUS, EN TALENS
POURRA DE CERTAINS NOMS REMPLIR LE VUIDE IMMENSE.

QU'IL REPOSE EN PAIX

L'ÉQUATION AX + BY = C

Soient a, b, c des *entiers*, a ou b étant non nul.

On cherche tous les couples $(x, y) \in \mathbb{Z}^2$ vérifiant $ax + by = c$.

Soit d le pgcd de a et b.

1. Si d ne divise pas c, l'équation est impossible, car d divise $ax + by$.

2. Si d divise c, l'algorithme d'Euclide étendu donne $(\alpha, \beta) \in \mathbb{Z}^2$ tel que $a\alpha + b\beta = d$; en multipliant cette relation par l'entier c/d, on trouve $a\left(\frac{c}{d}\alpha\right) + b\left(\frac{c}{d}\beta\right) = c$. On a donc obtenu une solution de l'équation : $(x_0, y_0) = \left(\frac{c}{d}\alpha, \frac{c}{d}\beta\right) \in \mathbb{Z}^2$.

A partir de la solution (x_0, y_0), on obtient toutes les autres comme indiqué à l'exercice 316 :

$$S = \left\{ (x, y) \in \mathbb{Z}^2 \;\middle|\; \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + k \begin{pmatrix} b/d \\ -a/d \end{pmatrix},\ k \in \mathbb{Z} \right\}$$

CHIFFREMENT AFFINE

La fonction de chiffrement, de $\mathbb{Z}_{26}$ dans $\mathbb{Z}_{26}$, est du type $f : x \mapsto ax + b$.

Achtung !

> La fonction $f : x \mapsto ax + b$ est bijective si et seulement si a est inversible dans $\mathbb{Z}_{26}$.

Si a est inversible, donc premier à 26, on trouve la réciproque ${}^{r}f$ comme suit :

$$\begin{aligned} y &= ax + b \\ ax &= y - b \quad \| \cdot a^{-1} \\ x &= \left(a^{-1}\right)y + \left(-ba^{-1}\right) \\ {}^{r}f &: \; y \mapsto a^{-1}y - ba^{-1} \end{aligned}$$

Réciproquement, on peut montrer que si a n'est pas inversible, alors f n'est pas bijective. (Voir par exemple l'exercice 327.)

Les 12 inversibles modulo 26 et leurs inverses

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

MULTIPLICATIVITÉ DE LA FONCTION D'EULER

Pour tout $n \in \mathbb{N}^*$ notons $I(n)$ l'ensemble des inversibles de $\mathbb{Z}_n$. On rappelle que $\left|I(n)\right| = \varphi(n)$.

Remarque préliminaire. Si $x \in I(n)$ et si d divise n, alors le reste r de x mod d appartient à $I(d)$. En effet, si r n'était pas inversible modulo d, il existerait un premier p divisant r et d. Or x peut s'écrire $x = dq + r$ (division euclidienne) ce qui montre que p diviserait également x et d et donc x et n, ce qui contredit l'inversibilité de x modulo n.

Théorème

Soient n_1 et n_2 des entiers ≥ 1, premiers entre eux, et $n = n_1 n_2$. L'application f définie comme suit est ***bijective***.

$$f : I(n) \to I(n_1) \times I(n_2)$$
$$x \mapsto (r_1 , r_2)$$

où r_1 (resp. r_2) désigne le reste modulo n_1 (resp. n_2) de x.

Preuve

1) L'application f est bien définie en vertu de la *remarque préliminaire*.

2) f est injective : Soient x et x' tels que $f(x) = f(x')$ c'est-à-dire tels que $x \equiv x'$ mod n_1 et $x \equiv x'$ mod n_2. On a donc $x - x' \equiv 0$ mod n_1 et $x - x' \equiv 0$ mod n_2. Il existe donc des entiers s et t tels que $x - x' = sn_1 = tn_2$, ce qui montre que $x - x'$ est un multiple du ppcm de n_1 et n_2, soit de $n = n_1 n_2$ puisque n_1 et n_2 sont premiers entre eux. Ainsi $x - x' \equiv 0$ mod n et, par suite, $x = x'$.

3) f est surjective : Soit (r_1 , r_2) dans $I(n_1) \times I(n_2)$. Cherchons x dans $I(n)$ tel que x mod n_1 = r_1 et x mod n_2 = r_2. On doit donc trouver des entiers s et t vérifiant $r_1 + sn_1 = r_2 + tn_2$, qui équivaut à $sn_1 - tn_2 = r_2 - r_1$. Comme n_1 et n_2 sont premiers entre eux, Bézout fournit s et t. On pose donc $x = r_1 + sn_1 = r_2 + tn_2$ mod n, et il ne reste plus qu'à montrer que x est inversible modulo n. S'il ne l'était pas, il existerait un premier p divisant x et n. p diviserait donc aussi n_1 ou n_2, disons n_1 pour fixer les idées. Si p divise x et n_1, il divise aussi x et r_1 puisque $x \equiv r_1 + sn_1$ mod n. Cela contredit l'inversibilité de r_1 modulo n_1.

Corollaire. Si les entiers ≥ 1 n_1 et n_2 sont premiers entre eux,

$$\boxed{\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)}$$

Preuve. La bijection f nous assure que $\left|I(n)\right| = \left|I(n_1) \times I(n_2)\right|$. D'où :

$$\varphi(n_1 n_2) = \varphi(n) = \left|I(n)\right| = \left|I(n_1) \times I(n_2)\right| = \left|I(n_1)\right| \cdot \left|I(n_2)\right| = \varphi(n_1)\varphi(n_2)$$

LE THÉORÈME D'EULER

Théorème

Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{N}$ inversible modulo n. Alors :

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Preuve

Considérons l'ensemble $I = \left\{ r_1, r_2, ..., r_{\varphi(n)} \right\}$ des inversibles de $\mathbb{Z}_n$.

L'ensemble I est égal à $I_a = \left\{ ar_1, ar_2, ..., ar_{\varphi(n)} \right\}$. En effet :

- les ar_i sont inversibles, comme produit de deux inversibles ;
- les ar_i sont distincts, car $ar_i \equiv ar_j \Rightarrow a^{-1}ar_i \equiv a^{-1}ar_j \Rightarrow r_i \equiv r_j \Rightarrow i = j$.

Le produit de tous les éléments de I est donc égal à celui de tous les éléments de I_a. Il en résulte que $r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(n)} = a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(n)}$. Il suffit maintenant de multiplier cette égalité par $r_1^{-1} \cdot r_2^{-1} \cdot ... \cdot r_{\varphi(n)}^{-1}$ pour obtenir $a^{\varphi(n)} \equiv 1 \bmod n$.

Corollaire *(Petit théorème de Fermat)*

Soit p un nombre premier et $a \in \mathbb{N}$ non congru à 0 modulo p. Alors :

$$a^{p-1} \equiv 1 \bmod p$$

Preuve

L'hypothèse $a \not\equiv 0 \bmod p$ implique que a est inversible modulo p. Donc, par le théorème d'Euler, $a^{\varphi(p)} \equiv 1 \bmod p$. Mais $\varphi(p) = p - 1$. Ainsi $a^{p-1} \equiv 1 \bmod p$.

LE THÉORÈME RSA

H : p et q premiers, $p \neq q$

$n = pq$

e inversible modulo $\varphi(n)$

$d = e^{-1} \bmod \varphi(n)$

$$[de \equiv 1 \bmod \varphi(n)]$$

C : La fonction $x \longmapsto x^e$ de $\mathbb{Z}_n$ dans $\mathbb{Z}_n$ est bijective et sa réciproque est $x \longmapsto x^d$

$$\mathbb{Z}_n \underset{()^d}{\overset{()^e}{\rightleftarrows}} \mathbb{Z}_n$$

Preuve suivra.

$$(x^e)^d = x \qquad (x^d)^e = x$$

DÉMONSTRATION DU THÉORÈME RSA

Hypothèse : p, q premiers distincts, $n = pq$;
e, d entiers tels que $ed \equiv 1 \mod \varphi(n)$.

Conclusion : Quel que soit l'entier x, $\left(x^e\right)^d \equiv x \mod n$ et $\left(x^d\right)^e \equiv x \mod n$

Démonstration :

Il suffit d'établir que $x^{ed} \equiv x \mod n$.

Comme $ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$, on a $x^{ed} = x\left(x^{(p-1)(q-1)}\right)^k$.

Or le Petit Fermat nous dit que $x^{p-1} \equiv \left\{\begin{matrix} 1 \text{ si } x \not\equiv 0 \\ 0 \text{ si } x \equiv 0 \end{matrix}\right\} \mod p$.

Ainsi $x^{(p-1)(q-1)} = \left(x^{p-1}\right)^{q-1} \equiv \left\{\begin{matrix} 1 \text{ si } x \not\equiv 0 \\ 0 \text{ si } x \equiv 0 \end{matrix}\right\} \mod p$.

On a donc $x^{ed} \equiv x \mod p$ et, de même, $x^{ed} \equiv x \mod q$.

Il existe alors des entiers α et β tels que $x^{ed} = x + \alpha p = x + \beta q$. Cette dernière égalité montre que p divise β. Alors : $x^{ed} = x + \beta q = x + \gamma pq$ et, finalement, $x^{ed} \equiv x \mod n$.

CHIFFREMENT ET DÉCHIFFREMENT RSA

- Chaque personne désirant envoyer ou recevoir une information sécurisée doit avoir une clé publique (n, e), où n est le produit de deux premiers distincts p et q, et e est un entier inversible modulo $\varphi(n) = (p-1)(q-1)$. Les nombres p et q sont gardés secrets (clé privée).

- Si Alice veut envoyer un message à Bob, elle utilise la clé publique de Bob ; elle transforme son message en un nombre $m \in \mathbb{Z}_n$ et le chiffre ainsi :

$$\boxed{c = m^e} \ (\text{dans } \mathbb{Z}_n)$$

- Bob déchiffre en calculant $d = e^{-1} \bmod \varphi(n)$, puis :

$$\boxed{m = c^d} \ (\text{dans } \mathbb{Z}_n)$$

Exemple

La clé publique de Bob est $(n, e) = (55, 3)$.
Alice veut envoyer le message $m = \boxed{19} \in \mathbb{Z}_{55}$. Chiffrement, dans $\mathbb{Z}_{55}$:

$c = m^e = 19^3 = \boxed{39}$.

Pour déchiffrer, Bob — qui connaît p et q — calcule :

$\varphi(n) = \varphi(55) = \varphi(5 \cdot 11) = 4 \cdot 10 = 40$;
$d = e^{-1} \bmod \varphi(n) = 3^{-1} \bmod 40 = 27$ (via l'algorithme d'Euclide) ;
$m = c^d = 39^{27} = \boxed{19} \ (\text{dans } \mathbb{Z}_{55})$.

Remarques

1) Pour casser le code, il faudrait trouver $\varphi(n) = (p-1)(q-1)$, donc p et q ; c'est pratiquement impossible si p et q sont très grands.

2) Si $e = 1$: $c = m$; $e = 2$ ne convient pas puisque non premier à $\varphi(n)$, qui est ici toujours pair ; on prend donc pratiquement $e \geq 3$.

CHIFFREMENT RSA PAR BLOCS

Prenons par exemple la clé RSA $(n, e) = (25'937, 143)$, avec $n = pq = 37 \cdot 701$. On veut transmettre le message « I see a bee ».

Le message est d'abord découpé à partir de la gauche en blocs de taille

$$k = \max\left\{ i \in \mathbb{N} \;\middle|\; 26^i \le n \right\}$$

Il faut en effet pouvoir crypter le plus gros mot de longueur k : $ZZ...Z = (25, 25, ..., 25)_{26} = 26^k - 1$.

Dans notre exemple, on a $k = 3$, puisque $26^3 = 17'576 < n < 26^4 = 456'976$.

Le chiffrement se fait ainsi :

Texte clair :	I S E	E A B	E E (A)
En base 26 :	$(8, 18, 4)$	$(4, 0, 1)$	$(4, 4, 0)$
En base 10 :	$m_1 = 5880$	$m_2 = 2705$	$m_3 = 2808$
$m^e \bmod n$:	$c_1 = 16921$	$c_2 = 8797$	$c_3 = 19101$
En base 26 :	$(0, 25, 0, 21)$	$(0, 13, 0, 9)$	$(1, 2, 6, 17)$
Texte crypté :	A Z A V	A N A J	B C G R

Remarque : Lorsqu'on calcule les c_i en base 26, on ajoute si nécessaire des zéros à gauche afin que tous les blocs chiffrés soient de taille $k+1$. La taille $k+1$ est requise, car certains c_i peuvent être supérieurs à 26^k. Les c_i sont par contre toujours inférieurs à 26^{k+1} puisque celui-ci est strictement supérieur à n.

Pour le déchiffrement, on calcule d'abord $\varphi(n) = (p-1)(q-1)$ et $d = e^{-1} \bmod \varphi(n)$; ici : $\varphi(n) = 25'200$ et $d = 11'807$. Puis le cryptogramme est découpé depuis la gauche en blocs de taille $k+1$ auxquels on applique la méthode habituelle :

Texte crypté :	A Z A V	A N A J	B C G R
En base 26 :	$(0, 25, 0, 21)$	$(0, 13, 0, 9)$	$(1, 2, 6, 17)$
En base 10 :	$c_1 = 16921$	$c_2 = 8797$	$c_3 = 19101$
$c^d \bmod n$:	$m_1 = 5880$	$m_2 = 2705$	$m_3 = 2808$
En base 26 :	$(8, 18, 4)$	$(4, 0, 1)$	$(4, 4, 0)$
Texte clair :	I S E	E A B	E E (A)

I see
A bee

SIGNATURE ÉLECTRONIQUE

Un protocole possible via RSA et une fonction de hachage

Alice envoie un message à Bob.

Clé publique d'Alice : $(n_A,\ e_A)$; clé publique de Bob : $(n_B,\ e_B)$.

1. Phase d'encryptage et de signature (par Alice)

- Alice crypte le message signé m à l'aide de la clé publique e_B de Bob, lequel reçoit c.
- Elle calcule la valeur hachée $h(m)$ du message, puis $h = h(m) \bmod n_A$, et crypte h au moyen de sa clé privée d_A : $h^{d_A} \bmod n_A = s$. s est la signature électronique du message m.

2. Phase de décryptage et de vérification (par Bob)

- Bob décrypte le message c au moyen de sa clé privée d_B et obtient m.
- Il calcule $h(m)$, puis $h = h(m) \bmod n_A$, et vérifie la signature d'Alice à l'aide de la clé publique e_A d'Alice en déterminant $s^{e_A} \bmod n_A$; si s^{e_A} n'est pas égal à h, il est sûr que le message ne provient pas d'Alice. Et dans le cas contraire, il est quasi certain que le message est bien d'Alice.

$c = m^{e_B} \bmod n_B$ $h = h(m) \bmod n_A$ $s = h^{d_A} \bmod n_A$
$m = c^{d_B} \bmod n_B$ $h = h(m) \bmod n_A$ $?\left(s^{e_A} \bmod n_A = h\right)?$

Note sur les fonctions de hachage

- Pour une définition, voir : http://fr.wikipedia.org/wiki/Fonction_de_hachage.
  Une fonction de hachage est « résistante aux collisions » et « à sens unique ».
- Deux fonctions de hachages répandues : « MD5 » et « SHA-1 ».
- Dans nos exercices, pour simplifier et éviter l'usage de l'ordinateur, on utilisera toujours la *pseudo* fonction de hachage définie par :

$$h(x) = x^2 \bmod 100$$