# Démonstrations :

## Existence de ? :

k est premier avec ?(n) donc d'après Bezout on a :

? ? et a tels que, k*? + a*?(n) = 1.

Et donc k*? = 1 mod [?(n)].

## Preuve de $c^{?} = m \bmod [n]$ :

$c = m^k \bmod [n] \Rightarrow n$ divise $c-m^k$.

Or $c^{?} - m^{k*?} = (c - m^k) * (c^{?-1} + c^{?-2}m^k + c^{?-3}m^{2*k} + \dots + m^{k*(?-1)})$.

On en déduit que n divise $c^{?} - m^{k*?}$.

Petit Théorème de Fermat :

$p$ premier $\Rightarrow m^p = m \bmod [p]$.

$\Rightarrow p$ divise $m^p - m$.

$k*? = 1 \bmod [(p-1)*(q-1)]$ donc il existe un entier a tel que :

$k*? - 1 = a*(p-1)*(q-1)$.

$$\begin{aligned} m^{k*?} - m &= m*(m^{k*?-1} - 1) \\ &= m*(m^{a*(p-1)*(q-1)} - 1) \\ &= m*(m^{(p-1)} - 1)*(m^{(a*(q-1)-1)*(p-1)} + m^{(a*(q-1)-2)*(p-1)} + \dots + 1) \\ &= (m^p - m)*(m^{(a*(q-1)-1)*(p-1)} + m^{(a*(q-1)-2)*(p-1)} + \dots + 1). \end{aligned}$$

Donc, d'après le petit théorème de Fermat :

$p$ divise $m^{k*?} - m$.

De même q divise $m^{k*?} - m$ et donc n aussi.

On conclue que, comme $c^{?} - m = (c^{?} - m^{k*?}) + (m^{k*?} - m)$ alors :

n divise $c^{?} - m$ et donc :

$c^{?} = m \bmod [n]$.

Ce qu'il fallait démontrer.

## Petit Théorème de Fermat :

D'après le petit théorème de Fermat on a :

Si p est premier alors, pour tout entier m on peut dire que $m^p = m \bmod [p]$.

Preuve : Par récurrence sur m :

Pour m=0 c'est évident (aussi pour m=1) : 0=0 mod [p].

Supposons la propriété vraie pour m et montrons la pour m+1 :

$(m+1)^p = ? _{i=0..p} (C^i_p . m^i) = 1 + p*Q + m^p$

Car $C^i_p$ est divisible par p, pour $0<i<p$.

(par décomposition en facteurs premiers :

dans $C^i_p = p!/(i!*(p-i)!)$ on a p en haut, or $i<p$ et $p-i<p$)

Et d'après l'hypothèse de récurrence : $m^p = m \bmod [p]$

Or $1=1 \bmod [p]$ et $(p*Q)^p = p*Q' = 0 \bmod [p]$

Et en sommant, $m^p + p*Q + 1 = m+1 \bmod [p]$.

D'où $(m+1)^p = (m+1) \bmod [p]$.

Et le théorème est démontré.

## ?(p*q)= ?(p)* ?(q) avec p et q premiers :

?(n) est le nombres d'entiers premiers avec n et plus petits que n.

Dénombrons le complémentaire :

p , 2*p , 3*p , 4*p , … , (q-1)*p , q*p ne sont pas premiers avec p*q.

De même q , 2*q , 3*q , … , (p-1)*q ce qui fait au total p+q-1 nombres.

Donc ?(p*q)=p*q-p-q+1=(p-1)*(q-1)= ?(p)* ?(q)

car ?(p)=p-1 puisque p est premier.

## Théorème de Bezout :

D'après le théorème de Bezout on a :

a et b sont premiers entre eux ✍ il existe u et v entiers tels que a*u+b*v=1.

Preuve : $a*\mathbf{Z} + b*\mathbf{Z}$ est un sous groupe additif de $\mathbf{Z}$ :

_ non vide.

_ inclus dans $\mathbf{Z}$.

_ stable par + et opposé.

De plus il est non réduit à {0} donc il existe d tel que :

$a*\mathbf{Z} + b*\mathbf{Z} = d*\mathbf{Z}$ et d=pgcd(a,b)

car tout sous-groupe additif G de $\mathbf{Z}$, ?{0} peut s'écrire $n*\mathbf{Z}$.

preuve : soit n le plus petit élément >0 de G.

par double inclusion :

_ $n*\mathbf{Z}$ ? G.

_ si il existe g ? (G-$n*\mathbf{Z}$).

alors g ? ]k*n ; (k+1)*n[ où k? $\mathbf{Z}$.

donc g-k*n? G or g-k*n<n ; contradiction.

Donc $G = n*\mathbf{Z}$.

Ici d=1 donc tout élément de $\mathbf{Z}$ , et à fortiori 1, peut s'écrire a*u+b*v.