Rappel : un nombre premier est premier avec tous les nombres qu'il ne divise pas.

Exercice : Si un entier est premier avec deux entiers, il est premier avec leur produit.

Sol : Soit a un entier premier avec b et c. D'après le théorème de Bézout, il existe deux entiers u et v tels que au+bv = 1 et des entiers u′ et v ′ tels que au′ + cv = 1. On effectue le produit membre à membre. On obtient : (au + bv)(au′ + cv ′) = 1 ⇔ $a^2uu'+acuv'+abvu'+bcvv'=1 \Leftrightarrow a(auu'+cuv'+bvu')+bc(vv')=1$. Comme auu′ + cuv ′ + bv u′ et v v ′ sont des entiers, on en déduit que a et bc sont premiers entre eux

Exemple 4 est premier avec 9 et avec 35, donc 4 est premier avec 315.

Théorème de Gauss (Théorème fondamental de l'arithmétique)

Soient a, b et c trois entiers. Si a divise le produit bc et si a est premier avec b, alors a divise c.

Démonstration

Si a est premier avec b, il existe u et v tels que : au + bv = 1. On en déduit : acu + bcv = c.
Or, a divise acu et bc par hypothèse, donc a divise c.

Exemple : Soient a et b deux entiers tels que 5a = 14b. 14 divise le produit 5a, les entiers 14 et 5 sont premiers entre eux, donc 14 divise a. De même, 5 divise b.

Corollaires

1. Si un entier est divisible par des entiers a et b premiers entre eux, alors il est divisible par leur produit ab.
2. Si un entier <u>premier</u> divise un produit de facteurs ab, alors il divise au moins un des facteurs a et b.

Démonstration

1. Soit n entier divisible par a et b. Il existe des entiers k et k ′ tels que n = ka et n = k ′ b donc n = ka = k ′ b.
a divise donc k ′ b. Comme a et b sont premiers entre eux, on en déduit (d'après le théorème de Gauss) que a divise k ′ donc il existe q tel que k ′ = q a. On a alors n = q ab et n est divisible par ab.
2. Soit p un nombre premier divisant ab.
Si p divise a, alors la condition est vérifiée.
Supposons que p ne divise pas a. Alors a et p sont premiers entre eux (d'après la propriété précédente « <u>Un nombre premier est premier avec tous les nombres qu'il ne divise pas</u>. ») comme p divise ab, alors p divise b d'après le théorème de Gauss.

Exemple 1 : Résoudre une équation 7x + 5y = 0. dans $\mathbb{Z}^2$

Cette équation s'écrit 7x = −5y. 7 et −5 sont premiers entre eux. 7 divise −5y donc 7 divise y d'après le théorème de Gauss. Ainsi y = 7k avec k entier.
En reportant : 7x = −5 × 7k d'où x = −5k. Les solutions sont les couples (−5k ; 7k) où k ∈ Z.

Exemple 2 : Déterminer les entiers x et y tels que 5x + 7y = 1

On remarque que que 5 × 3 − 2× 7 = 1 donc on peut prendre $x_0=3$ et $y_0=-2$. Le couple (3 ; −2) est une solution particulière de notre équation.
Alors : 5x + 7y = 1 ⇔ 5x + 7y = 5 × 3 − 2 × 7 ⇔ 5(x − 3) = 7(−y − 2).
5 divise 7(−y − 2) ; 5 et 7 sont premiers entre eux. D'après le théorème de Gauss, on en déduit que 5 divise −y − 2. Par conséquent : −y − 2= 5k, k ∈ Z, donc y = −2 − 5k.
On reporte dans l'équation 5(x − 3) = 7(−y − 2). On obtient : 5(x − 3) = 7 × 5k d'où x − 3 = 7k soit x = 3 + 7k. Les solutions sont de la forme $(3+7k;-2-5k), k\in\mathbb{Z}$.

<u>Fonction d'Euler</u>

Remarque : i est inversible modulo n → il existe k tel que $k*i\equiv 1\, mod(n)$ → il existe k' tel que k*i-1=k'*n
→ k*i + k'*n =1 → D'après Bézout pgcd(i,n)=1

Définition

Le groupe multiplicatif $\mathbb{Z}^*_n$ est l'ensemble des entiers inversibles modulo n :
$\mathbb{Z}^*_n=\{i\in\mathbb{Z}_n \ / \ pgcd(i,n)=1\}$

Si p est premier alors $\mathbb{Z}^*_p=\{1,2,...,p-1\}$

Définition

La fonction d'Euler φ(n) représente le nombre d'éléments dans $\mathbb{Z}^*_n$: $\varphi(n)=|\mathbb{Z}^*_n|$
→ φ(n) est le nombre d'éléments de $\mathbb{Z}^*_n$ (={0, . . . , n − 1}) qui sont premiers avec n

Si p est premier alors alors φ(n)=p-1

Théorème

Soit $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ l'unique factorisation de n. Alors $\varphi(n)=\prod(p_i^{e_i-1}(p_i-1))$

Si p et q sont premiers alors $\varphi(pq)=(p-1)(q-1)$ (ici $e_1=e_2=1 et\ p_1=p, p_2=q$)

Lemme

p est premier et soit $k\in\{1,2,...p-1\}$ Alors p divise C_p^k : démonstration via Théorème de Gauss

Petit théorème de Fermat

1. p est un nombre premier, a est un entier Alors $a^p\equiv a \mod(p)$.
2. De plus si p^a=1 alors $a^{p-1}\equiv 1 \mod(p)$

Démonstration : Théorème de Gauss & Formule du binôme de Newton pour raisonner par récurrence :

1. Montrons par récurrence que pour tout $a\in\{0,1,2,...p-1\}$ on $a^p\equiv a \mod(p)$:
initialisation vrai pour a=0
supposons vrai pour a et montrons que la formule est vraie pour a+1 :
formule de newton → $(a+1)^p=\sum_{k=0}^{p}C_p^k a^k=a^p+\sum_{k=1}^{p-1}C_p^k a^k+1$. D'après le lemme précédent on $C_p^k\equiv 0 \mod(p)$ et $a^p\equiv a \mod(p)$ (hypothèse) donc $(a+1)^p\equiv a+1 \mod(p)$
2. p divise a^p-a d'après 1 (car p est premier). Comme $a^p-a=a*(a^{p-1}-1)$ et a^p=1 alors d'après théorème de Gauss alors p divise $a^{p-1}-1$ donc $a^{p-1}\equiv 1 \mod(p)$

Exemple : 7 est premier et ne divise pas 12, donc 12^6-1 est divisible par 7.

Remarque (Grand Théorème de Fermat (1650→ 1995-2002): Soit $n\geq 3$ Les solutions de l'équation $x^n+y^n=z^n$ *avec* $x,y,z\in\mathbb{Z}$, vérifient toutes $xyz=0$.

Théorème : Théorème d'Euler
Soient p et q deux nombres premier distincts et $n=pxq$. Pour tout $a\in\mathbb{Z}$ tel que $pgcd(a,n)\equiv 1$ alors $a^{(p-1)(q-1)}\equiv 1 mod(n)$ ($a^{\varphi(n)}\equiv 1 mod(n)$ avec $\varphi(n)=(p-1)(q-1)$

Définition : Inverse modulo
Soit $a\in\mathbb{Z}$. On dit que $x\in\mathbb{Z}$ est l'inverse de a modulo n si $a.x\equiv 1 mod(n)$

Proposition
a admet un inverse modulo n ⇔ $pgcd(a,n)\equiv 1$

Propriété 1
Soit p et q deux nombres premiers. $\varphi(n)=(p-1)(q-1)$ est la fonction indicatrice d'Euler

Si e, tel que 1 < e < $\varphi(n)$, est premier avec $\varphi(n)$ alors il existe d unique tel que 1 < d < $\varphi(n)$ et vérifiant $e\,d \equiv 1\, mod(\varphi(n))$ (d est l'inverse de e modulo $\varphi(n)$)

Démonstration :
a) existence : Si e et $\varphi(n)$ sont premiers entre eux, il existe d'après le théorème de Bézout il existe deux entiers relatifs u_0 et v_0 tels que $u_0 e + v_0 \varphi(n) = 1$. Par la suite (u, v) est solution de $ue + v\varphi(n) = 1$ → $u_0 e + v_0 \varphi(n) = ue + v\varphi(n)$ → $(u - u_0)e = (v_0 - v)\varphi(n)$ (*)
→ e divise $v_0 - v$ donc il existe $k \in \mathbb{Z}$ tel que $v = v_0 + k\,e$ en remplaçant $v - v_0$ par $k\,e$ dans (*) on obtient $u = u_0 + k\,\varphi(n)$ **

le nombre **d** recherché sera la plus petite valeur de u de ** en choisissant la valeur adéquate de k.

Unicité : d est unique car s'il en existait un autre d' , on aura $d\,e = 1 - v\,\varphi(n)$ et $d'e = 1 - v'\varphi(n)$ et donc $e(d - d') = (v' - v)\varphi(n)$ donc $\varphi(n)$ divise e(d-d')

Comme e est premier avec $\varphi(n)$ alors, d'après le théorème de **Gauss**, $\varphi(n)$ divise d-d' $d - d' \equiv 0\, mod(\varphi(n))$. Mais comme on a $1 < d < \varphi(n)$ et $1 < d' < \varphi(n)$ alors $d = d'$.

Propriété 2
Dans les conditions de la propriété 1 et si p et q sont différents (n=p.q) et si $b \equiv a^e\, mod(n)$ alors $b^d \equiv a\, mod(n)$.

Démonstration :

Si $b \equiv a^e\, mod(n)$ alors $b^d \equiv a^{e\,d}\, mod(n)$. comme $ed \equiv 1\, mod(\varphi(n))$ alors il existe un entier $k > 0$ tel que $e\,d = 1 + k\,\varphi(n)$. On obtient donc $a^{e\,d} = a^{1 + k\,\varphi(n)}$ → $a^{e\,d} = a^{1 + k(1-p)(1-q)}$
→ $a^{e\,d} = a\left(\left(a^{p-1}\right)^{q-1}\right)^k$ (*).
Si a est divisible par p alors de façon évidente $a^{e\,d} \equiv a \equiv 0\, mod(p)$ ((car p divise a → il existe j tel que a=j.p → $a \equiv 0\, mod(p)$ → $a^{e\,d} \equiv a.a.a.a...a(ed\,fois)\, mod(p) \equiv 0\, mod(p)$))

Si a n'est pas divisible par p alors d'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \;\; mod(p)$ d'où $a^{e\,d} \equiv a\, mod(p)$ d'après (*) .

De même $a^{e\,d} \equiv a\, mod(q)$.

Il existe donc deux entiers k et k′ tels que $a^{e\,d} = a + k\,p$ et $a^{e\,d} = a + k'q$ → $k\,p = k'q$
→ p|k'q et comme p et q sont premiers et donc premiers entre eux alors p|k' → il existe k'' tel que k'=k''.p → $a^{ed} = a + k'q = a + k''pq = a + k''n$ donc $a^{ed} \equiv a\, mod(\varphi(n))$.

→ $b^d \equiv a^{ed}\, mod(n) \equiv a\, mod(n)$