NOMBRES PREMIERS, CONGRUENCES

I. Division euclidienne dans $\mathbb{Z}$

1. Diviseur
   On dit que l'entier a est un diviseur de l'entier b s'il existe un entier k tel que $b=k\,a$. Dans ce cas, on dit aussi que a divise b et que b est un multiple de a et on note $a|b$.
2. Quelques propriétés
   a. Si $a|b$ et $b|c$ alors $a|c$.
   b. Si $a|b$ et $b|a$ alors $a=b$ ou $a=-b$.
   c. Si $a|b$ et $a|c$ alors, quels que soient les entiers β et γ, $a|(\beta b+\gamma c)$.
3. Division euclidienne.
   Étant donnés un entier a et un entier b non nul, il existe un unique couple $(q;r)$ d'entiers tels que $a=qb+r$ avec $0\le r<|b|$. q est appelé quotient et r est appelé reste de la division euclidienne de a par b.

II. Nombres premiers

1. Définition
   On dit que l'entier naturel p est premier s'il admet exactement deux diviseurs positifs, 1 et p.
   Remarque : 0 et 1 ne sont pas des nombres premiers.
2. Décomposition en produit de facteurs premiers
   Tout entier naturel n se décompose de façon unique sous la forme :
   $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}$
   avec, p_i premier $(1\le i\le m)$ et $p_i<p_j$ pour $i<j$. Cette écriture est appelée décomposition de n en produit de facteurs premiers.
3. Nombres premiers entre eux
   On dit que les entiers a et b sont premiers entre eux si leurs seuls diviseurs communs sont 1 et -1

III. Congruences

1. Définition
   Étant donnés trois entiers, a, b et n avec $n\ge 2$, on dit que a est congru à b modulo n si $n|(a-b)$. On note $a\equiv b(n)$.
   Exemple : $4\equiv 19(5)$ car $19-4=15$ et $5|15$.
   Remarque : 1) $a\equiv b(n)$ équivaut à dire que a et b ont le même reste pour la division euclidienne par n. $a\equiv 0(n)\Leftrightarrow n|a$.
   2) Il existe un unique entier r tel que $0\le r<n$ et $a\equiv r(n)$.
2. Propriétés
   a. Si $a\equiv b(n)$ et si $n'|n$ ($n'\ge 2$) alors $a\equiv b(n')$.
   b. Si $a\equiv a'(n)$ et $b\equiv b'(b)$ alors $a+b\equiv a'+b'(n)$, $a-b\equiv a'-b'(n)$ et $ab\equiv a'b'(n)$.
   Conséquence : pour tout entier $p\ge 1$, $a\equiv b(n)\Rightarrow a^p\equiv b^p(n)$.