EUCLIDE, GAUSS, BÉZOUT

I. PGCD et PPCM

1. Définitions
   a. Le $PGCD$ de deux entiers naturels non nuls est leur plus grand diviseur commun. Le $PGCD$ de a et b se note $PGCD(a;b)$.
   Si a et b sont deux entiers relatifs, $PGCD(a;b) = PGCD(|a|;|b|)$.
   Remarque : a et b premiers entre eux équivaut à $PGCD(a;b) = 1$.
   b. Le $PPCM$ de deux entiers naturels est leur plus petit multiple commun. Le $PPCM$ de a et b se note $PPCM(a;b)$.
   Si a et b sont deux entiers relatifs, $PPCM(a;b) = PPCM(|a|;|b|)$.
2. Propriétés
   a. Si $b|a$, $PGCD(a;b) = |b|$ et $PPCM(a;b) = |a|$.
   b. Si $c|a$ et $c|b$ alors $c|PGCD(a;b)$. Si $a|c$ et $b|c$ alors $PPCM(a;b)|c$
   c. Pour tout entier relatif $k \neq 0$,
   $PGCD(ka;kb) = |k|PGCD(a;b)$ et $PPCM(ka;kb) = |k|PPCM(a;b)$.
   d. Pour tous entiers relatifs a et b non nuls, $PGCD(a;b) \times PPCM(a;b) = |ab|$.
3. Décomposition en facteurs premiers
   Si $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}$ et si on pose $\gamma_i = min(\alpha_i;\beta_i)$ et $\delta_i = max(\alpha_i;\beta_i)$, alors $PGCD(a;b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_m^{\gamma_m}$ et $PPCM(a;b) = p_1^{\delta_1} p_2^{\delta_2} \dots p_m^{\delta_m}$.

II. Algorithme d'Euclide

1. Principe
   Si r est le reste de la division euclidienne de a par b (a et b non nuls), alors, si r est non nul, $PGCD(a;b) = PGCD(b;r)$ et si r est nul, $PGCD(a;b) = b$.
   Remarque : Si on prend $a > b$, alors le calcul du $PGCD$ de a et b se ramène au calcul du $PGCD$ de deux nombres plus petits.
2. Algorithme
   Pour calculer le $PGCD$ de deux nombres on applique en « boucle » le principe précédent jusqu'à obtenir un reste nul.

III. Théorème de Gauss

Si a, b et c sont trois entiers naturels non nuls tels que $a|bc$ et a et b sont premiers entre eux, alors $a|c$.

IV. Théorème de Bézout

1. Théorème
   Quels que soient les entiers relatifs non nuls a et b, il existe deux entiers relatifs u et v tels que $au+bv = PGCD(a;b)$.
2. Conséquence
   Si a et b sont premiers entre eux, il existe u et v tels que $au+bv = 1$.