Division et Modulo

Gabriel-Andrew Pollo-Guilbert

Mars 6, 2016

Théorème 1 *Soit $a, b \in \mathbb{Z}$ tel que $a|b$. Alors $a|bc$, $\forall c \in \mathbb{Z}$.*

Soit $a, b \in \mathbb{Z}$ tel que $a|b \Rightarrow \exists k \in \mathbb{Z}$ tel que $b = ak$. Donc $bc = akc$, $\forall c \in \mathbb{Z}$. Puisque $kc \in \mathbb{Z} \Rightarrow a|bc$.

Théorème 2 *Soit $a, b, c \in \mathbb{Z}$ tel que $a|b$ et $b|c$, alors $a|c$.*

Soit $a, b, c \in \mathbb{Z}$ tel que $a|b$ et $b|c \Rightarrow \exists s, t \in \mathbb{Z}$ tel que $b = as$ et $c = bt$. Donc $b = \dfrac{c}{t} \Rightarrow \dfrac{c}{t} = as \Rightarrow c = a(st)$. Puisque $st \in \mathbb{Z} \Rightarrow a|c$.

Théorème 3 *Soit $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. Si $\exists k \in \mathbb{Z}$ tel que $a = b + km$, alors $a \equiv b \mod m$.*

Soit $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ tel que $a \equiv b \mod m \Rightarrow \exists r \in \mathbb{N}$ et $s, t \in \mathbb{Z}$ tel que $a = sm + r$ et $b = tm + r$. Donc $a - sm = b - tm \Rightarrow a = b + (s - t)m$. Puisque $s - t \in \mathbb{Z} \Rightarrow a = b + km$, $k \in \mathbb{Z}$.

Théorème 4 *Soit $a, b, c, d \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. Si $a \equiv b \mod m$ et $c \equiv d \mod m$, alors $(a + c) \equiv (b + d) \mod m$.*

Soit $a, b, c, d \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ tel que $a \equiv b \mod m$ et $c \equiv d \mod m \Rightarrow \exists s, t \in \mathbb{Z}$ tel que $a = b + sm$ et $c = d + tm$. Par addition, $a + c = b + sm + d + tm \Rightarrow (a+c) = (b+d) + (s+t)m$. Puisque $(s+t) \in \mathbb{Z} \Rightarrow (a+c) \equiv (b+d) \mod m$.

Théorème 5 *Soit $a, b, c, d \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. Si $a \equiv b \mod m$ et $c \equiv d \mod m$, alors $ac \equiv bd \mod m$.*

Soit $a, b, c, d \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ tel que $a \equiv b \mod m$ et $c \equiv d \mod m \Rightarrow \exists s, t \in \mathbb{Z}$ tel que $a = b + sm$ et $c = d + tm$. Par multiplication, $ac = (b + sm)(d + tm) \Rightarrow ac = bd + m(bt + ds + stm)$. Puisque $(bt + ds + stm) \in \mathbb{Z} \Rightarrow ac \equiv bd \mod m$.