3.2.2

Soit $m, n, r \in \mathbb{Z}$. Montrer que

a) si $m \mid n$ et $m \mid r$, alors $m \mid (n - r)$;

b) si $m \mid n$ alors $m \mid r\,n$;

c) si $r \neq 0$, alors $m \mid n$ si et seulement si $r\,m \mid r\,n$.

Déf: $a \mid b$ s'il existe $c \in \mathbb{Z}$ tel que $a \cdot c = b$

a) Ex : $5 \mid 30$ et $5 \mid 75$ $\Rightarrow$ $5 \mid (\underbrace{30 - 75}_{-45})$

① $m \mid n \Rightarrow$ il existe $x \in \mathbb{Z}$ tel que $m \cdot x = n$

② $m \mid r \Rightarrow$ il existe $y \in \mathbb{Z}$ tel que $m \cdot y = r$

③ $n - r = mx - my = m(\underbrace{x - y}_{z})$. Posons $z = x - y$.

$m \cdot z = n - r \Rightarrow m \mid (n - r)$

b) si $m \mid n$ alors $m \mid r\,n$;

$m \mid n \Rightarrow \exists\, x \in \mathbb{Z}$ tq $mx = n$,

On a $rn = mx \cdot r = m \cdot (\underbrace{xr}_{z}) = mz \Rightarrow mz = rn \Rightarrow m \mid rn$.

c) si $r \neq 0$, alors $m \mid n$ si et seulement si $r\,m \mid r\,n$.

① $r \neq 0$, si $m \mid n \Rightarrow rm \mid rn$

② $r \neq 0$, si $rm \mid rn \Rightarrow m \mid n$

① $m \mid n \Rightarrow \exists\, x \in \mathbb{Z}$ tel que $mx = n$. Comme $r \neq 0$, on a

$mx \cdot r = r \cdot n \Rightarrow (rm) \cdot x = rn \Rightarrow rm \mid rn$

② $rm \mid rn \Rightarrow \exists\, x \in \mathbb{Z}$ tel que $(rm) \cdot x = rn \Rightarrow m \cdot (rx) = rn \overset{r \neq 0}{\Rightarrow}$

$r \cdot (mx) = r \cdot n \Rightarrow mx = n \Rightarrow m \mid n$.

Théorème fondamental de l'algèbre

3.1.7 Tout entier n peut se décomposer en produit de facteurs premiers (sauf 0 et 1).

$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_r}^{\alpha_r}$$

avec p_j des nombres premiers distincts et α_j des entiers naturels non nuls.

$100 = 4 \cdot 25 = 2^2 \cdot 5^2$

$120 = 2^3 \cdot 3 \cdot 5$

120	2
60	2
30	2
15	3
5	5
1	

Soit a, b dans $\mathbb{Z}$ avec $b > 0$. Soit encore q et r les deux entiers uniques qui satisfont

$$a = b\,q + r \quad \text{et} \quad 0 \leq r < b$$

On définit

$$a \mod b = r$$

Autrement dit, $a \mod b$ désigne le reste de la division de a par b.

$a = 1200$, $b = 7$. Trouvez q et r.

$$1200 = 7 \cdot \underbrace{171}_{q} + \underbrace{3}_{r}$$

$$1200 \equiv 3 \pmod 7$$

Le reste de la division de 1200 par 7 est égal à 3

3.2.21 Soit n un entier positif et a et b deux entiers quelconques.

a) Démontrer que

$$(a+b) \mod n = ((a \mod n) + (b \mod n)) \mod n$$

b) Démontrer que

$$(a \cdot b) \mod n = ((a \mod n) \cdot (b \mod n)) \mod n$$

a) $a = 17$, $b = 8$, $n = 7$

① $17 + 8 \equiv 25 \equiv 4 \pmod 7$

2.1 $17 \equiv 3 \pmod 7$

2.2 $8 \equiv 1 \pmod 7$

2.3 $3 + 1 \equiv 4 \pmod 7$

b) ① $17 \cdot 8 \equiv 3 \pmod 7$

2.3 $3 \cdot 1 \equiv 3 \pmod 7$

3.2.12 On donne un nombre naturel a. Chercher son reste après division par n.

a) $a = 111\,;\ n = 2, 3, 4, \ldots, 12\,;$

b) $a = 123456789 \cdot 987654321\,;\ n = 2,\ n = 9,\ n = 11\,;$

c) $a = 22^{22},\ n = 3,\ n = 9,\ n = 10,\ n = 11\,;$

d) $a = 1234^5,\ n = 9,\ n = 11,\ n = 99\,;$

e) $a = 2^{64} - 1,\ = 2,\ n = 3,\ n = 9.$

a) $111 \equiv 1 \pmod 2$

$111 \equiv 0 \pmod 3$

$111 \equiv 3 \pmod 4$

$111 \equiv 1 \pmod 5$

$111 \equiv 3 \pmod 6$

$111 \equiv 6 \pmod 7$

$111 \equiv 7 \pmod 8$

$111 \equiv 3 \pmod 9$

$111 \equiv 1 \pmod{10}$

$111 \equiv 1 \pmod{11}$

$111 \equiv 3 \pmod{12}$

b) $a = 123456789 \cdot 987654321$; $n = 2$, $n = 9$, $n = 11$;

$$a = 123456789 \cdot 987654321 \equiv 1 \pmod 2$$

$$123456789 \cdot 987654321 \equiv 0 \cdot 0 \equiv 0 \pmod 9$$

$$123456789 \cdot 987654321 \equiv 5 \cdot 5 \equiv 25 \equiv 3 \pmod{11}$$

$$\begin{array}{r|l} 1\,2\,3\,4\,5\,6\,7\,8\,9 & 11 \\ \hline & 11223344 \\ \hline \text{reste: } (5) & \end{array}$$

c) $a = 22^{22}, n = 3, n = 9, n = 10, n = 11;$

$22^{22} \equiv 1^{22} \equiv 1 \pmod 3$

$22^{22} \equiv 4^{22} \equiv ? \pmod 9$

$4^1 \equiv 4 \pmod 9$

$4^2 \equiv 7 \pmod 9$

$4^4 \equiv 7^2 \equiv 49 \equiv 4 \pmod 9$

$4^8 \equiv 4^2 \equiv 7 \pmod 9$

$4^{16} \equiv 7^2 \equiv 4 \pmod 9$

$4^{22} \equiv 4^{16+4+2} \equiv 4^{16} \cdot 4^4 \cdot 4^2$

$\equiv 4 \cdot 4 \cdot 7$

$\equiv 7 \cdot 7 \equiv 4 \pmod 9$

C'est l'exponentiation modulaire A finir pour le 10.03.26