TD9 : Arithmétique sur $\mathbb{Z}$ - Corrigé

Exercice 1

Indication :

Pour résoudre une équation diophantienne $ax+by=c$ avec $a,b,c\in\mathbb{Z}$, on applique la méthode :

1. On applique l'algorithme d'Euclide pour trouver $u,v\in\mathbb{Z}$ tel que $au+bv=pgcd(a,b)$. Si $PGCD(a,b)$ divise c alors $c=PGCD(a,b)\times d$ et (du,dv) est une solution particulière. Sinon l'équation n'admet aucune solution dans $\mathbb{Z}^2$.
2. On résout l'équation homogène $ax_0+by_0=0$. Si a et b sont premiers entre eux alors le théorème de Gauss montre l'existence d'un entier $k\in\mathbb{Z}$ tel que $x_0=bk$ puis $y_0=-ak$. Sinon en divisant par le pgcd, on se ramène au cas où ils sont premiers entre eux.
3. On applique le principe de superposition en $(x,y)=(x_p,y_p)+(x_0,y_0)$ avec (x_p,y_p) une solution particulière et (x_0,y_0) n'importe quelle solution homogène.

Solution :

On a $26=15\times1+11, 15=11\times1+4$ et $11=4\times3-1$ donc PGCD$(26,15)=1$.
La remontée d'Euclide donne $1=3\times4-11=3(15-11)-11=3\times15-4\times(26-15)=7\times15-4\times26$.
Une solution particulière est $\binom{x_p}{y_p}=\binom{-4}{7}$.

Puis on recherche les solutions homogènes $26x_0+15y_0=0$, on a $26|26x_0=-15y_0$ avec PGCD$(26,15)=1$. Donc d'après le thm de Gauss $26|y_0$. Il existe $k\in\mathbb{Z}$ tel que $y_0=26k$ puis $x_0=-15k$. Donc on obtient $\binom{x_0}{y_0}\in\mathbb{Z}\binom{-15}{26}$ puis l'ensemble des solutions est $\binom{-4}{7}+\mathbb{Z}\binom{-15}{26}$.

Exercice 2

Indication :

On se ramène à l'exercice précédent en résolvant un système de deux équations diophantiennes.

Solution :

On résout le système $\begin{cases}2x+3y &= n\\ 5n+7z &= 11\end{cases}$

On commence par l'équation diophantienne $5n+7z=11$.
On trouve $\binom{n_p}{z_p}=11\binom{3}{-2}$ et $\binom{n_0}{z_0}=k\binom{7}{-5}$ pour $k\in\mathbb{Z}$.
Donc $z=-22-5k$ et $n=33+7k$.

Puis on résout $2x+3y=33+7k$.
On trouve $\binom{x_p}{y_p}=(33+7k)\binom{-1}{1}$ et $\binom{x_0}{y_0}=l\binom{3}{-2}$ pour $l\in\mathbb{Z}$.
Donc $x=-33-7k+3l$ et $y=33+7k-2l$.

Ainsi $\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}-33\\33\\-22\end{pmatrix}+k\begin{pmatrix}-7\\7\\-5\end{pmatrix}+l\begin{pmatrix}3\\-2\\0\end{pmatrix}$.

Exercice 3

Indication :

On raisonne par double implication.
($\Rightarrow$) avec le théorème de Bézout.
($\Leftarrow$) avec la propriété ($p|ab$ ssi $p|a$ ou $p|b$) pour p un nombre premier.

Solution : ($\Rightarrow$) On suppose que PGCD$(a+b,ab)=1$ d'après le thm de Bézout, ils existent des entiers $u,v\in\mathbb{Z}$ tel que $u(a+b)+vab=1$.
Donc $au+b(u+va)=1$. D'après à nouveau le thm de Bézout, a et b sont premiers entre eux.

($\Leftarrow$) On suppose que PGCD$(a+b,ab)\neq1$ alors il existe un diviseur commun premier $p>1$ tel que $p|(a+b)$ et $p|ab$. Or $p|ab$ et p premier donc $p|a$ ou $p|b$.
1er cas : $p|a$ alors $p|(a+b)-a=b$ et $p|$PGCD(a,b).
2eme cas : $p|b$ alors $p|(a+b)-b=b$ et $p|$PGCD(a,b).
Dans tous les cas, on obtient PGCD$(a,b)\neq1$.

Exercice 4

Indication :

On utilise le calcul modulaire avec la propriété ($d|a$ ssi $a \equiv 0[d]$).

Solution :

a) On a $7^{8n+1} + 10(-1)^n = 7(49^{4n}) + 10(-1)^n$
$= 7(-2)^{4n} + 10(-1)^n[17]$ car $49 = 51 - 2 = 3 \times 17 - 2$.
$= 7(16)^n + 10(-1)^n$
$= 7(-1)^n + 10(-1)^n[17]$ car $16 = 17 - 1$.
$= 17(-1)^n = 0[17]$.
Donc 17 divise $7^{8n+1} + 10(-1)^n$.

b) De même $9^{5n+2} - 4 = (-2)^{5n+2} - 4[11]$ car $9 = 11 - 2$.
$= (-2)^2(-32)^n - 4$ car $-32 = -3 \times 11 + 1$.
$= 4(1^n) - 4 = 0[11]$
Donc 11 divise $9^{5n+2} - 4$.

c) On a $10^{3n+2} - 4^{n+1} = 0 - 0[2]$ donc 2 divise $10^{3n+2} - 4^{n+1}$.
Et $10^{3n+2} - 4^{n+1} = 1^{3n+2} - 1^{n+1} = 0[3]$ donc 3 divise $10^{3n+2} - 4^{n+1}$.
Donc 6 divise $10^{3n+2} - 4^{n+1}$.

Exercice 5

Indication :

La définition de la division euclidienne est composée de :
$\boxed{\text{l'égalité } A = BQ + R}$ et $\boxed{\text{l'inégalité } 0 \leq R \leq B - 1}$.

Solution :

On écrit la division euclidienne $a - 1 = bq + r$ avec $0 \leq r \leq b - 1$.
Donc $ab^n - 1 = (bq + r + 1)b^n - 1 = b^{n+1}q + b^n(r + 1) - 1$.
Or $1 \leq r + 1 \leq b$ donc $b^n \leq b^n(r + 1) \leq b^{n+1}$.
Ainsi $R = b^n(r + 1) \in [b^n - 1, b^{n+1} - 1]$ est bien un entier tel que $0 \leq R < b^n$.
Donc $ab^n - 1 = b^{n+1}q + R$ est la division euclidienne de $ab^n - 1$ par b^n.
Par unicité de la division euclidienne, son quotient est q.

Exercice 6

Indication :

On adapté la démonstration classique de $\sqrt{2}$ est irrationnel.
Elle repose sur le résultat ($2|n$ ssi $2|n^2$) qui se généralise pour $p = 2$ un autre nombre premier.

Solution :

a) Par l'absurde, on suppose $\sqrt{2} = p/q$ avec $p, q \in \mathbb{N}^*$ premier entre eux.
On a $p^2 = 2q^2$ donc p^2 est pair puis $p = 2k$ avec $k \in \mathbb{N}^*$ est pair.
Donc $2q^2 = p^2 = 4k^2$ donne $q^2 = 2k^2$ est pair puis q est pair.
Ceci est absurde car 2 divise p et q qui sont premiers entre eux.

b) Par l'absurde, on suppose $\sqrt{3} = p/q$ avec $p, q \in \mathbb{N}^*$ premier entre eux.
On a $p^2 = 3q^2$ donc $3|p^2$ puis $3|p$ car 3 est un nombre premier.
Donc $p = 3k$ permet d'obtenir $3q^2 = p^2 = 9k^2$ donne $3|q^2 = 3k^2$ et de même $3|q$.
Ceci est absurde car 3 divise p et q qui sont premiers entre eux.

c) Par l'absurde si $\sqrt{2} + 1 \in \mathbb{Q}$ alors $\sqrt{2} = (\sqrt{2} + 1) - 1 \in \mathbb{Q}$ comme somme de rationnels.
Donc $\sqrt{2} + 1$ est irrationnels.

d) Si $\sqrt{6} = p/q$ alors $p^2 = 6q^2$ donc $2|p$.
En écrivant $p = 2k$, on trouve $3q^2 = 2k^2$ donc $2|q$ car 2 et 3 sont premiers entre eux.
Ceci est absurde car 2 divise p et q que l'on peut supposer premiers entre eux.

e) Si $r = \sqrt{2} + \sqrt{3}$ est rationnel alors $r^2 = 5 + 2\sqrt{6}$ est rationnel. Puis $\sqrt{6} = \frac{r^2 - 5}{2}$ est rationnel ce qui est absurde.

Exercice 7

Solution :

a) Soit $k \in [\![1, p-1]\!]$. On a $p|p! = \binom{p}{k} k!(p-k)!$ avec p premier avec $k!$ et $(p-k)!$. Donc d'après le théorème de Gauss p divise $\binom{p}{k}$.

b) On démontre par récurrence sur $n \in \mathbb{N}$ que $p|n^p - n$.

Initialisation $n = 0$ on a $p|0^p - 0 = 0$.

Hérédité Soit $n \in \mathbb{N}$. On suppose que $p|n^p - n$.

On a $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k$ d'après la formule du binôme.

$\equiv 1 + 0 + ... + 0 + n^p \quad [p]$ d'après le a)

$\equiv 1 + n \quad [p]$ par HR.

Donc $(n+1)^p - (n+1) \equiv 0 \quad [p]$ et $p|(n+1)^p - (n+1)$.

Si $p = 2$ alors (n est pair ssi $n^2 = n^p$ est pair) donc $n^2 \equiv n[2]$.

Si p premier impair alors $(-n)^p = (-1)^p n^p = -n^p \equiv -n[p]$.

Ainsi la relation s'étend sur $\mathbb{Z}$ les entiers relatifs.

Exercice 8

Solution :

a) On sait que $X^2 - SX + P$ est la forme développée du polynôme avec S la somme et P le produit des racines. Donc $p = n + m$ et $q = mn$.

b) On peut suppose $m \leq n$. L'équation $q = mn$ donne $m = 1$ et $n = q$ car q est un nombre premier. Puis $p = n + m = q + 1$ est premier. Or les seuls nombres premiers consécutifs sont 2 et 3. Donc $q = 2$ et $p = 3$.

Exercice 9

Indication :

On utilise la formule de factorisation $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$.

Solution :

a) On le démontre par contraposée.

On suppose $a > 2$. On a $a^n - 1 = (a-1)\sum_{k=0}^{n-1} a^k = (a-1)N$. Or $a - 1 \neq 1$ car $a > 2$ et $a - 1 \neq a^n - 1$ car $n \neq 1$. Donc la factorisation n'est pas triviale et $a^n - 1$ n'est pas premier.

b) Par contraposé, on suppose que $n = bc$ avec $b \notin \{1, n\}$ n'est pas premier.

Alors $a^n - 1 = a^{bc} - 1 = (a^c)^b - 1$ n'est pas premier d'après a) car $b \geq 2$ et $a^c > 2$.

c) Ceci impose la forme $N_p = 2^p - 1$ avec p premier pour la recherche de grand nombre premier.

On a $N_2 = 3, N_3 = 7, N_5 = 31, N_7 = 127$ sont premiers.

Mais $N_{11} = 2047 = 23 \times 89$ n'est pas premier.

La réciproque est donc fausse.

Exercice 10

Solution :

a) On montre le résultat par récurrence sur $n \in \mathbb{N}$.

Initialisation $n = 0$ $F_0 = 3$ et $F_1 = 5$ donc $F_0 = F_1 - 2$.

Hérédité Soit $n \in \mathbb{N}$ tel que $\prod_{k=0}^{n} F_k = F_{n+1} - 2$.

On a $F_{n+2} - 2 = 2^{2^{n+2}} - 1 = 2^{2.2^{n+1}} - 1 = \left(2^{2^{n+1}}\right)^2 - 1 = [2^{2^{n+1}} - 1][2^{2^{n+1}} + 1]$

$= [F_{n+1} - 2]F_{n+1} = [\prod_{k=0}^{n} F_k]F_{n+1} = \prod_{k=0}^{n+1} F_k$.

b) Montrer F_n et F_m deux nombres de Fermat avec $m < n$.

On a $2 = F_n + \prod_{k=0}^{n-1} F_k = F_n + AF_m$ avec $A \in \mathbb{N}$ un entier. Donc d'après le Thm de Bézout un diviseur commun est divisible par 2. Or F_n et F_m sont impairs. Donc ils sont premiers entre eux.

c) Par construction, il existe une infinité de nombres de Fermat. Ils ne sont pas toujours premiers mais tous leurs facteurs sont premiers entre eux. Donc on peut considérer $p_n > 1$ le plus petit diviseur de F_n. C'est un nombre premier. Les nombres p_n et p_m pour $m < n$ sont premiers entre eux donc $p_n \neq p_m$. Donc la suite $(p_n)_{n\geq 0}$ est une suite infinie de nombres premiers 2 à 2 distincts.

Exercice 11

Solution : On note $Div(n) = \{d \in \mathbb{N}^* \text{ tel que } d|n\}$ et $\sigma_1(n) = \sum_{d|n} d$ leur somme.
Ainsi n est parfait ssi $\sigma_1(n) = 2n$.

a) On a $Div(6) = \{1, 2, 3, 6\}$ et $\sigma_1(6) = 12$. Donc 6 est parfait.
On a $Div(28) = \{1, 2, 4, 7, 14, 28\}$ et $\sigma_1(28) = 56$. Donc 28 est parfait.
On a $Div(496) = \{1, 2, 4, 8, 16, 31, 62, 124, 248, 496\}$ et $\sigma_1(496) = 992$. Donc 496 est parfait.

b) On a $6 = 2^1 \times 3$ avec $3 = 2^2 - 1$ est premier.
Puis $28 = 2^2 \times 7$ avec $7 = 2^3 - 1$ est premier.
Et $496 = 2^4 \times 31$ avec $31 = 2^5 - 1$ est premier.

c) Soit $n \in \mathbb{N}$.
($\Rightarrow$) On suppose $p = 2^{n+1} - 1$ premier.
Alors pour $N = 2^n p$, on a $Div(N) = \{2^a p^b \text{ avec } 0 \leq a \leq n \text{ et } 0 \leq b \leq n\}$.
D'où $\sigma_1(N) = \sum_{a=0}^{n}(2^a + 2^a p) = (1 + p)\frac{2^{n+1}-1}{2-1} = 2^{n+1}(2^{n+1} - 1) = 2N$. Donc N est parfait.
($\Leftarrow$) Par contraposée, on suppose que $p = 2^{n+1} - 1$ n'est pas premier.
Alors il existe un diviseur d non trivial de p. Puis $Div(N) \supset= \{2^a p^b \text{ avec } 0 \leq a \leq n \text{ et } 0 \leq b \leq n\} \cup \{d\}$.
Le même calcul donne $\sigma_1(N) \geq 2N + d > 2N$. Donc N n'est pas parfait.

d) On a N parfait ssi il existe $n \in \mathbb{N}$ tel que $N = 2^n(2^{n+1} - 1)$ avec $2^{n+1} - 1$ premier.
Le sens ($\Leftarrow$) est donné par la question précédente.
($\Rightarrow$) On suppose N parfait et on écrit $N = 2^n m$ avec m impair. On a $D|N$ ssi $D = 2^a d$ avec $0 \leq a \leq n$ et $d|m$ (Gauss avec $\text{PGCD}(2, m) = 1$)
Donc $\sigma_1(N) = \sum_{a=0}^{n} \sum_{d|m} 2^a d = (\sum_{a=0}^{n} 2^a) \left(\sum_{d|m} d\right) = (2^{n+1} - 1)\sigma_1(m)$.
Donc $2^{n+1}m = 2N = \sigma_1(N) = (2^{n+1} - 1)\sigma_1(m)$. Or $2^{n+1} - 1$ et 2 sont premiers entre eux.
Donc $2^{n+1} - 1$ divise m. Il existe $k \in \mathbb{N}^*$ tel que $m = k(2^{n+1} - 1)$.
On veut aboutir à $k = 1$. Par l'absurde, on suppose $k > 1$ donc
$\sigma_1(m) \geq 1 + k + (2^{n+1} - 1)k = 1 + k2^{n+1} > k2^{n+1}$.
Donc $2^{n+1}(2^{n+1} - 1)k = 2^{n+1}m = (2^{n+1} - 1)\sigma_1(m) > (2^{n+1} - 1)k2^{n+1}$ absurde.

Exercice 12

Indication :
Il s'agit d'un cas particulier du Lemme des restes chinois : Pour montrer une congruence modulo $N = ab$ avec a et b premier entre eux, il suffit de le démontrer modulo a et modulo b.
On démontre donc que $p^2 = 1[3]$ et $p^2 = 1[8]$.

Solution : On sait que 3 ne divise pas p donc $p \neq 0[3]$ ainsi $p = 1[3]$ ou $p = 2[3]$ donc $p^2 = 1 = 4[3]$.
Puis p n'est pas divisible par 2 donc il est impair $p = 2k + 1$ pour $k \in \mathbb{N}$.
Donc $p^2 - 1 = (p+1)(p-1) = (2k+2)(2k) = 4k(k+1)$. Or k et $k+1$ sont des entiers consécutifs.
Donc l'un est pair et l'autre impair. Leur produit $k(k + 1)$ est alors pair.
Donc $8|p^2 - 1$ et $3|p^2 - 1$ donc $24|p^2 - 1$ car 8 et 3 sont premiers entre eux (Thm de Gauss).
Ainsi $p^2 = 1[24]$.