Université Gaston BERGER de Saint-Louis
UFR Sciences Appliquées et de Technologie

Licence Mathématique Appliquées

Correction du TD1 de Arithmétique

Tutorat : P.O. CISSE

Exercice 1

Sachant que l'on a 96842=256×375+842, déterminer, sans faire la division, le reste de la division du nombre 96842 par chacun des nombres 256 et 375.

Solution

96842=256×375+842

$96842=256 \times 375 + 256 \times 3 + 74 = 256 \times 378 + 74$

Le reste de la division du nombre 96842 par 256 est **74**

$96842=256 \times 375 + 375 \times 2 + 92 = 258 \times 375 + 92$

Le reste de la division du nombre 96842 par 375 est 92

Exercice 2

Montrer que $\forall$ n $\in$ IN :
n(n+1)(n+2)(n+3) est divisible par 24;
n(n+1)(n+2)(n+3)(n+4) est divisible par 120:

Solution

Montrons que $\forall$ n $\in$ IN :
n(n+1)(n+2)(n+3) est divisible par 24;

Montrons que : $2|n(n+1)$

X	Reste de la division de X par 2	
n	0	1
n + 1	1	0
n(n + 1)	0	0

n(n + 1) est divisible par 2 donc au moins un des facteurs est divisible par 2

Montrons que : $3|n(n+1)(n+2)$

X	Reste de la division de X par 3		
n	0	1	2
n + 1	1	2	0
n + 2	2	0	1
n(n + 1)(n + 2)	0	0	0

n(n + 1)(n + 2) est divisible par 3 donc au moins un des facteurs est divisible par 3

Montrons que : $4|n(n+1)(n+2)(n+3)$

X	Reste de la division de X par 4			
n	0	1	2	3
n + 1	1	2	3	0
n + 2	2	3	0	1
n(n + 1)(n + 2)	3	0	1	2
n(n + 1)(n + 2)(n + 3)	0	0	0	0

n(n + 1)(n + 2)(n + 3) est divisible par 4 donc au moins un des facteurs est divisible par 4

$\boxed{\text{Donc } 2 \times 3 \times 4|n(n+1)(n+2)(n+3)} \Longrightarrow \boxed{24|n(n+1)(n+2)(n+3)}$

Montrons que ∀ n ∈ IN :
n(n+1)(n+2)(n+3)(n+4) est divisible par 120;

Exercice 3
Montrer que si n est un entier naturel somme de deux carrés d'entiers alors le reste de la division euclidienne de n par 4 n'est jamais égal à 3.

Solution
Soit n, a et b des entiers tel que $n = a^2 + b^2$

X	Reste de la division de X par 4			
a	0	1	2	3
b	0	1	2	3
a^2	0	1	0	1
b^2	0	1	1	1
$n = a^2 + b^2$	0	2	1	2

$\boxed{\text{Le reste de la division de n par 4 est égal à 0, 1 ou 2}}$

Exercice 4

Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est impair ; dans le cas n pair, donner le reste de sa division par 8.

Solution

- Montrons que $7^n + 1$ est divisible par 8 si n est impair

n impair $\Longrightarrow \exists\, k \in \mathbb{Z}$ / $\mathbf{n = 2k + 1}$

on a : $7 \equiv -1 \pmod 8 \Longrightarrow 7^2 \equiv 1 \pmod 8 \Longrightarrow 7^{2k} \equiv 1 \pmod 8 \Longrightarrow 7^{2k+1} \equiv 7 \pmod 8$

$$\Longrightarrow 7^{2k+1} + 1 \equiv 8 \pmod 8 \quad \Longrightarrow \mathbf{7^{2k+1} + 1 \equiv 0 \pmod 8}$$

$\boxed{\text{Donc } 7^{2k+1} + 1 \text{ est divisible par 8}}$

- Si n pair $\Longrightarrow \exists\, k \in \mathbb{Z}$ / $\mathbf{n = 2k}$

On a : $\boxed{7^{2k} \equiv 1 \pmod 8} \Longrightarrow \boxed{\text{le reste de la division de } 7^{2k} \text{ par 8 est 1}}$

Exercice 5

Trouver le reste de la division par 13 du nombre 100^{1000}.

Solution

$10 \equiv -3 \pmod{13} \Longrightarrow 100 \equiv 9 \pmod{13} \Longrightarrow 100^2 \equiv 3 \pmod{13}$

$\Longrightarrow 100^{10} \equiv 3^5 \pmod{13} \Longrightarrow 100^{10} \equiv 243 \pmod{13} \Longrightarrow 100^{10} \equiv 9 \pmod{13}$

$100^{20} \equiv 81 \pmod{13} \Longrightarrow 100^{20} \equiv 3 \pmod{13}\,) \Longrightarrow 100^{100} \equiv 3^5 \pmod{13}$

$\Longrightarrow 100^{100} \equiv 9 \pmod{13} \Longrightarrow 100^{200} \equiv 3 \pmod{13} \Longrightarrow 100^{1000} \equiv 3^5 \pmod{13}$

$\Longrightarrow 100^{1000} \equiv 9 \pmod{13}$

$\boxed{100^{1000} \equiv 9 \pmod{13}} \Longrightarrow \boxed{\text{le reste de la division de } 100^{1000} \text{ par 13 est 9}}$

Exercice 6

1. Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair est 1.
2. Montrer de même que tout nombre pair vérifie $x^2 \equiv 0 \pmod 8$ ou $x^2 \equiv 4 \pmod 8$:
3. Soient a;b;c trois entiers impairs. Déterminer le reste modulo 8 de $a^2+b^2+c^2$ et celui de 2(ab+bc+ca):
4. En déduire que ces deux nombres ne sont pas des carrés puis que ab+bc+ca non plus.

Solution

1. n est impair $\Longrightarrow \exists\, k \in \mathbb{Z} \,/\, n = 2k + 1$

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$

On a : $2|k(k+1) \Longrightarrow 4 \times 2|4k(k+1) \Longrightarrow 8|4k(k+1)$

$4k^2 + 4k \equiv 0 \pmod 8 \quad \Longrightarrow 4k^2 + 4k + 1 \equiv 1 \pmod 8$

$\boxed{\text{Si n est impair, le reste de la division de } n^2 \text{ par 8 est 1}}$

n est pair $\Longrightarrow \exists\, k \in \mathbb{Z} \,/\, n = 2k \quad \Longrightarrow \quad n^2 = 4k^2$

X		Reste de la division de X par 8						
k	0	1	2	3	4	5	6	7
k^2	0	1	4	1	0	1	0	1
$4k^2$	0	4	0	4	0	4	0	4

$\boxed{\text{Si n est pair, le reste de la division de } n^2 \text{ par 8 est 0 ou 4}}$

2. a impair $\Longrightarrow a^2 \equiv 1 \pmod 8$; b impair $\Longrightarrow b^2 \equiv 1 \pmod 8$; c impair $\Longrightarrow c^2 \equiv 1 \pmod 8$

$\boxed{\text{d'où } a^2+b^2+c^2 \equiv 3 \pmod 8} \Longrightarrow \boxed{\text{le reste modulo 8 de } a^2+b^2+c^2 \text{ est 3}}$

➢ $(a+b+c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ac) \Longrightarrow 2(ab + bc + ac) = (a+b+c)^2 - (a^2 + b^2 + c^2)$

$(a+b+c)$ est impair $\Longrightarrow (a+b+c)^2 \equiv 1 \pmod 8$

$(a+b+c)^2 \equiv 1 \pmod 8$ et $a^2+b^2+c^2 \equiv 3 \pmod 8 \Longrightarrow (a+b+c)^2 - (a^2 + b^2 + c^2) \equiv -2 \pmod 8$

$\boxed{2(ab + bc + ac) \equiv -2 \pmod 8} \Longrightarrow \boxed{\text{le reste modulo 8 de } 2(ab + bc + ac) \text{ est - 2}}$

3. soit n, un entier le reste modulo 8 de n^2 est 0, 1 ou 4

$\boxed{\text{Le reste modulo 8 de } a^2+b^2+c^2 \text{ est 3 qui est différent de 1, 0 et 4 donc } a^2+b^2+c^2 \text{ n'est pas un carré}}$

Le reste modulo 8 de 2(ab + bc + ac) est -2 qui est différent de 1, 0 et 4 donc 2(ab + bc + ac) n'est pas un carré

$2(ab + bc + ac) \equiv -2 \pmod 8 \implies ab + bc + ac \equiv -1 \pmod 8$

Le reste modulo 8 de ab + bc + ac est – 1 qui est différent de 1, 0 et 4 donc ab + bc + ac n'est pas un carré

Exercice 7

Calculer le pgcd des nombres suivants :

1. 126, 230.
2. 390, 720, 450.
3. 180, 606, 750.

Solution

1. Calculons le pgcd de 126 et 230

$230 = 126 \times 1 + 104$
$126 = 104 \times 1 + 22$
$104 = 22 \times 4 + 16$
$22 = 16 \times 1 + 6$
$16 = 6 \times 2 + 4$
$6 = 4 \times 1 + 2$
$4 = 2 \times 2 + 0$

$\boxed{\text{pgcd } (126 ; 230) = 2}$

2. Calculons le pgcd de 390 , 720 et 450

390	2
195	3
65	5
13	13
1	

720	2
360	2
180	2
90	2
45	3
15	3
5	5
1	

450	2
225	3
75	3
25	5
5	5
1	

$390 = 2 \times 3 \times 5 \times 13$

$720 = 2^4 \times 3^2 \times 5$
$450 = 2 \times 3^2 \times 5^2$

$\boxed{\text{pgcd } (390, 720, 450) = 2 \times 3 \times 5 = 30}$

3. Calculons le pgcd de 180, 606 et750

180	2
90	2
45	3
15	3
5	5
1	

606	2
303	3
101	101
1	

750	2
375	3
125	5
25	5
5	5
1	

$180 = 2^2 \times 3^2 \times 5$
$606 = 2 \times 3 \times 101$
$750 = 2 \times 3 \times 5^3$

$\boxed{\text{pgcd } (180, 606, 750) = 2 \times 3 = 6}$

Exercice 8
Déterminer les couples d'entiers naturels de pgcd 18 et de somme 360. De même avec pgcd 18 et produit 6480.

Solution

- a et b des entiers naturels tel que pgdc(a, b) = 18 et a + b = 360

a = 18a' et b = 18b', avec a',b' ∈ Z et pgcd(a',b') = 1

$a + b = 360 \Longrightarrow 18a' + 18b' = 360 \Longrightarrow a' + b' = 20$
les couples (a', b') sont: (1 , 19) ; (3 , 17) ; (7 , 13) ; (9 , 11)

$\boxed{\text{les couples d'entiers naturels de pgcd 18 et de somme 360 sont : } (18, 342) ; (54, 306) ; (126, 234) ; (162, 198)}$

- a et b des entiers naturels tel que pgdc(a, b) = 18 et ab = 6480

a = 18a' et b = 18b', avec a',b' ∈ Z et pgcd(a',b') = 1

$ab = 6480 \Longrightarrow 324a'b' = 6480 \Longrightarrow a'b' = 20$
les couples (a', b') sont: (1 , 20) ; (4 , 5)

$\boxed{\text{les couples d'entiers naturels de pgcd 18 et de produit 6480 sont : } (18, 360) ; (72, 90)}$

Exercice 9
Calculer par l'algorithme d'Euclide : pgcd(18480;9828). En déduire une écriture de 84 comme combinaison linéaire de 18480 et 9828.

Solution
Calculons le pgcd de 18480 et 9828
$18480 = 9828 \times 1 + 8652$
$9828 = 8652 \times 1 + 1176$
$8652 = 1176 \times 7 + 420$
$1176 = 420 \times 2 + 336$
$420 = 336 \times 1 + 84$
$336 = 84 \times 4 + 0$

$\boxed{\text{pgcd } (18480 ; 9828) = 84}$

pgcd (18480 ; 9828) = 84 $\Longrightarrow \exists$ u et v $\in$ Z tel que : $18480u + 9828v = 84$

$84 = 420 - 336 = 420 - (1176 - 420 \times 2) = 420 \times 3 - 1176 = (8652 - 1176 \times 7) \times 3 - 1176$
$= 3 \times 8652 - 22 \times 1176 = 3 \times 8652 - 22\,(9828 - 8652) = 25 \times 8652 - 22 \times 9828$

$= 25(18480 - 9828) - 22 \times 9828 = 25 \times 18480 - 47 \times 9828$

$\boxed{25 \times 18480 - 47 \times 9828 = 84}$

Exercice 10
Notons a = 1 111 111 111 et b = 123 456 789.
1. Calculer le quotient et le reste de la division euclidienne de a par b.
2. Calculer p = pgcd(a;b).
3. Déterminer deux entiers relatifs u et v tels que au+bv = p.

Solution

1. $1\,111\,111\,111 = 123\,456\,789 \times 9 + 10$

2. Calculons le pgcd de 1 111 111 111 et 123 456 789
$1\,111\,111\,111 = 123\,456\,789 \times 9 + 10$
$123\,456\,789 = 10 \times 123\,456\,78 + 9$
$10 = 9 \times 1 + 1$
$1 = 1 \times 1 + 0$

$\boxed{\text{pgcd } (1\,111\,111\,111 ; 123\,456\,789) = 1}$

3. pgcd (1 111 111 111 ; 123 456 789) =1 $\Longrightarrow \exists$ u et v $\in$ Z tel : 1 111 111 111u + 123 456 789v = 1

1 = 10 – 9 = 10 – (123 456 789 – 10 $\times$ 123 456 78) = 10 $\times$ 123 456 79 – 123 456 789
= 123 456 79(1 111 111 111 - 123 456 789 $\times$ 9) - 123 456 789
= 123 456 79 $\times$ 1 111 111 111 - 111 111 111 $\times$ 123 456 789 - 123 456 789
= 123 456 79 $\times$ 1 111 111 111 - 111 111 112 $\times$ 123 456 789

123 456 79 $\times$ 1 111 111 111 - 111 111 112 $\times$ 123 456 789 = 1

$\boxed{u = 12\ 345\ 679 \quad \text{et} \quad v = 111\ 111\ 112}$

Exercice 11
Résoudre dans Z : 1665x + 1035y = 45

Solution
1665x + 1035y = 45 $\Longrightarrow$ 333x + 207y = 9 $\Longrightarrow$ 37x + 23y = 1

37 = 23 $\times$ 1 + 14
23 = 14 $\times$ 1 + 9
14 = 9 $\times$ 1 + 5
9 = 5 $\times$ 1 + 4
5 = 4 $\times$ 1 + 1
4 = 4 $\times$ 1 + 0

pgdc(37 ; 23) = 1

pgdc(37 ; 23) = 1 et 1|1 $\Longrightarrow$ l'équation 37x + 23y = 1 admet des solutions dans Z

1 = 5 – 4 = 5 – (9 – 5) = 2 $\times$ 5 – 9 = 2(14 – 9) – 9 = 2 $\times$ 14 - 3 $\times$ 9
= 2 $\times$ 14 - 3 (23 – 14) = 5 $\times$ 14 - 3 $\times$ 23 = 5(37 – 23) - 3 $\times$ 23
= 5 $\times$ 37 - 8 $\times$ 223

5 $\times$ 37 - 8 $\times$ 23 = 1 $\Longrightarrow$ $(x_0, y_0) = (5, -8)$ est solution de : 37x + 23y = 1

37x + 23y = 1 et $37x_0 + 23y_0 = 1$
$37(x - x_0) + 23(y - y_0) = 0 \Longrightarrow 37(x - x_0) = -23(y - y_0)$

$37 | -23(y - y_0)$ et pgdc(37 ; 23) = 1 $\Longrightarrow 37 | -(y - y_0)$

$37 | -(y - y_0) \Longrightarrow \exists$ k $\in$ Z tel que : $y_0 - y = 37k$
$\Longrightarrow y = y_0 - 37k$

$37(x - x_0) = -23(y - y_0) \Longrightarrow 37x - 37x_0 = -23(y_0 - 37k - y_0) \Longrightarrow x - x_0 = 23k$
$\Longrightarrow x = x_0 + 23k$

$$\begin{cases} x = 5 + 23k \\ y = -8 - 37k \end{cases} \quad \text{avec k un entier}$$

Les couples $\binom{x}{y} = \binom{5 + 23k}{y = -8 - 37k}$ avec $k \in Z$ sont solutions de : $1665x + 1035y = 45$

Exercice 12
Combien 15! admet-il de diviseurs ?

Solution
$15! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 \times 13 \times 14 \times 15$

$15! = 2 \times 3 \times 2^2 \times 5 \times (2 \times 3) \times 7 \times 2^3 \times 3^2 \times (2 \times 5) \times 11 \times (3 \times 2^2) \times 13 \times (2 \times 7) \times (3 \times 5)$

$15! = 2^{11} \times 3^6 \times 5^3 \times 7^2 \times 11 \times 13$

Nombre	2^{11}	3^6	5^3	7^2	11	13
Nombre de diviseurs	12	7	4	3	2	2

Le nombre diviseurs de 15! est égal à : 12×7×4×3×2×2 = **4032**

Exercice 13

Démontrer que, si a et b sont des entiers premiers entre eux, il en est de même des entiers a+b et ab.

Solution

Supposons a et b sont premier entre eux alors il existe u et v élément de Z tels que au + bv =1.

Si a+b et ab sont premiers entre eux alors il existerait α et β tels que (a+b)α+ abβ = 1 c.-à-d.

(a+b)α + abβ =au + bv d'où $\beta = \frac{u-\alpha}{b} + \frac{v-\alpha}{a}$. Il reste à prouver qu'il existe k et k' tels que u – α =kb et v – α = k'a α = u – kb et α = v – k'a,u – kb = v – k'a ; u – v = kb – k'a.

Or au + bv = 1 donc u – v = (u – v)(au + bv) = au(u – v) + bv(u – v) d'où k = v(u –v) et k' = -u(u – v).

α = u – v(u – v)b et β = v(u – v) – u(u – v) = - (u – v)^2.

$\boxed{au + bv =1} \Longrightarrow \boxed{\alpha(a + b) + \beta ab = 1 \quad \text{avec } \alpha = u - v(u-v)b \text{ et } \beta = -(u-v)^2.}$

Exercice 14

Soient a;b des entiers supérieurs ou égaux à 1. Montrer :

1. $(2^a - 1) | (2^{ab} - 1)$
2. $2^p - 1\, premier \Rightarrow p\, premier$
3. $pgcd\big((2^a - 1), (2^b - 1)\big) = 2^{pgcd(a,b)} - 1$

Solution

Soient a;b des entiers supérieurs ou égaux à 1. Montrer :

1. Soit n un diviseur de $2^a - 1$ alors $2^a \equiv 1[n] \Rightarrow (2^a)^b \equiv 1[n] \Rightarrow 2^{ab} - 1 \equiv 0[n] \Rightarrow$ n est un diviseur de $2^{ab} - 1$. Tout diviseur de $2^a - 1$ est aussi diviseur de $2^{ab} - 1$ comme $2^a - 1$ est son propre diviseur alors $2^a - 1$ divise $2^{ab} - 1$.

2. Supposons $2^p - 1$ premier et p = ab alors $2^p - 1 = 2^{ab} - 1$ donc $2^a - 1$ divise $2^n - 1$ or $2^n - 1$ est premier donc $2^a - 1 = 1$ ou $2^a - 1 = 2^p - 1$ c'est-à-dire a = 1 ou a = p donc p est premier.

3. Supposons $a \geq b$.

On sait que $pgcd(a;\ b) = pgcd(a - b; b)$.
Donc $pgcd(2^a - 1; 2^b - 1) = pgcd(2^a - 2^b; 2^b - 1)$. Mais $2^a - 2^b = 2^b(2^{a-b} - 1)$
d'où $pgcd(2^a - 1; 2^b - 1) = pgcd\big(2^b(2^{a-b} - 1);\ (2^b - 1)\big) = pgcd\big((2^{a-b} - 1);\ (2^b - 1)\big)$
Nous avons montrer : $pgcd(2^a - 1; 2^b - 1) = pgcd\big((2^{a-b} - 1);\ (2^b - 1)\big)$.
Cette formule est à mettre en parallèle $pgcd(a;\ b) = pgcd(a - b; b)$
En itérant cette formule nous obtenons que si $a = bq + r$ alors :
$pgcd(2^a - 1; 2^b - 1) = pgcd(2^{a-bq} - 1; 2^b - 1) = pgcd(2^r - 1; 2^b - 1)$
à comparer avec $pgcd(a; b) = pgcd(a - bq; b) = pgcd(r; b)$.
Nous avons notre première étape de l'algorithme d'Euclide.
En itérant l'algorithme d'Euclide pour $(a;\ b)$, nous nous arrêtons au dernier reste non nul :

$pgcd(a; b) = pgcd(b;\ r) = \cdots = pgcd(r_n; 0) = rn$.
Ce qui va donner $pgcd(2^a - 1; 2^b - 1) = pgcd(2^{a-bq} - 1; 2^r - 1) = \cdots = pgcd(2^{r_n} - 1; 2^0 - 1)$
Donc $pgcd(2^a - 1; 2^b - 1) = 2^{pgcd(a;b)} - 1$