Corrigé feuille 7 : Arithmétique

Exercice 7-1 Les diviseurs de -12 sont les mêmes que ceux de $12 = 2^2 * 3^1$. Il y en a donc $(2+1)*(1+1) = 6, (1, 2, 3, 4, 6, 12)$ dans $\mathbb{N}$ et 12 dans $\mathbb{Z}$.

Exercice 7-2 Non. Si m et n sont congru à 0 modulo 5, $m+n$ l'est aussi, mais par exemple $2+3$ est congru à 0 modulo 5.

Exercice 7-3 $3^{2n} - 2^n \equiv 9^n - 2^n \equiv 2^n - 2^n \equiv 0$ [7]

Exercice 7-4

1. Comme $35 = 5 * 7$ et $210 = 2 * 3 * 5 * 7$ on a $(35, 210)$, $(70, 105)$, $(105, 70)$ et $(210, 35)$.
2. Comme $64 = 2^6$ et les couples (a, b) solutions sont de la forme $a = 64a'$ et $b = 64b'$ avec a', b' premiers entre eux et $a' + b' = 18$ on a donc pour a',b' les possiblités suivantes : $(1, 17)$, $(5, 13)$, $(7, 11)$ et les symétriques.
3. Comme la somme vaut 1152 et le pgcd est 17, le ppcm est donc $102 = 2 * 3 * 17$. On a donc $(17, 102)$, $(34, 51)$, $(51, 34)$ et $(102, 17)$.

Exercice 7-5

$210 = 4 * 48 + 18$, $48 = 2 * 18 + 12$,et $18 = 12 + 6$, donc le pgcd est 6. On a alors $6 = 18 - 12 = -48 + 3 * 18 = 3 * 210 - 13 * 48$. Les couples solutions de $210x + 48y = 6$ sont alors $(3 + 8k, -13 - 35k)$ pour $k \in \mathbb{Z}$.

$237 = 2 * 81 + 75$, $81 = 75 + 6$ et $75 = 12 * 6 + 3$, donc le pgcd est 3. On a alors $3 = 75 - 12 * 6 = 13 * 75 - 12 * 81 = 13 * 237 - 38 * 81$. Les couples solutions de $237x + 81y = 3$ sont alors $(13 + 27k, -38 - 79k)$ pour $k \in \mathbb{Z}$.

Exercice 7-6

On fait une récurrence. C'est vrai pour $u_0 = a$ et $u_1 = b$. Supposons que que c'est vrai pour u_{n-1} et u_n, donc il existe (k, l) tel que $ku_{n-1} + lu_n = 1$ d'où $ku_{n+1} + (l - k)u_n = 1$ et donc c'est vrai pour u_{n+1} et u_n.

Exercice 7-7

1. Le pgcd d de a et b divise a et b donc $ax + by = c$. Réciproquement Bezout donne une solution pour le pgcd et donc pour tout multiple du pgcd.
2. On a $58 = 2 * 29$ et $21 = 3 * 7$. Donc $58x + 21y = 0$ a pour solution $(21k, -58k)$ pour $k \in \mathbb{Z}$. On a $1 = 16 - 3 * 5 = 4 * 16 - 3 * 21 = 4 + 58 - 11 * 21$, donc les solutions de $58x + 21y = 1$ sont $(4 + 21k, -11 - 58k)$ pour $k \in \mathbb{Z}$.
   Comme $35 = 2 * 14 + 7$ les solutions de $14x + 35y = 21$ sont $(-6 + 5k, 3 - 2k)$ pour $k \in \mathbb{Z}$. On a $637 = 595 + 42$ et $595 = 14 * 42 + 7$ le pgcd est donc 7 qui ne divise pas 29 donc la dernière n'a pas de solutions.

Exercice 7-8

1. $9 \equiv 1$ [8], donc $\forall k \in \mathbb{N}$, $9^k \equiv 1$ [8]. Ainsi $3^{2k} + 1 \equiv 9^k + 1 \equiv 2$ [8] et $3^{2k+1} + 1 \equiv 3 * 9^k + 1 \equiv 4$ [8].
2. Comme $2^m = 3^n + 1$ on a nécéssairement $m \leq 2$ car $8 = 2^3$.
3. Pour $m = 0$ il faut que $3^n + 1 \equiv 0$ [8] ce qui est impossible. Pour $m = 1$ il faut que $3^n + 1 \equiv 2$ [8] on a donc la solution $(1, 0)$, et pour $m = 2$ il faut que $3^n + 1 \equiv 4$ [8] on a alors la solution $(2, 1)$.

Exercice 7-9 Parmi 4 entiers successifs, l'un au moins est un multiple de 3 et donc le produit est divisible par 3. De même deux sont pairs dont l'un des deux est un multiple de 4, donc le produit est divisible par 8. Ainsi le produit est divisible par $24 = 3 * 8$.

Exercice 7-10

1. 7 étant premier, 16 et 7 sont premiers entre eux et on a $1 = 7 - 3 * 2 = 7 * 7 - 3 * 16$.
2. Le ppcm est donc $112 = 16 * 7$.
3. $-3 * 16 \equiv 4 * 16 \equiv 1$ [7]. Donc 64 est une solution.
4. Une solution de (E) est donc $832 = 64 * 13$, et l'ensemble des solutions est $\{832 + 112k, k \in \mathbb{Z}\}$.

Exercice 7-11

1. Le reste de a est 31 donc la clef est 66.
2. Il suffit de regarder les restes des 10^k pour $k \in \{0 \dots 13\}$ modulo 97.
3. La il suffit de regarder les differences de deux restes consécutifs.

Exercice 7-12

1. $(n - x)^2 - x^2 = n(n - 2x)$
2. D'après la question précédente l'application n'est pas injective, elle n'est donc pas non plus surjective.
3. Les images sont dans l'ordre : $0, 1, 4, 2, 2, 4, 1$.
4. On a $x^2 - 6xy + 2y^2 = (x - 3y)^2 - 7y^2 \equiv (x - 3y)^2$ [7]. Or $7003 \equiv 3$ [7], donc l'équation n'a pas de solution.

Exercice 7-13

1. $x^2 \equiv 1$ [7] $\Leftrightarrow (x - 1)(x + 1) = 7k$ donc 7 divise $x - 1$ ou $x + 1$ est donc x est congru à 1 ou $-1 \equiv 6$ modulo 7.
2. Dans $(p - 1)!$, en dehors de 1 et $(p - 1)$ les termes se regroupent 2 par 2 pour donner la classe de 1 modulo p, grâce à Bezout. Donc on a $(p - 1)! \equiv p - 1 \equiv -1$ [p], d'où le résultat.

Exercice 7-14

1. Toutes le puissances de 10 sont congrues à 1 modulo 3 ou 9.
2. Pour $k > 0$, 10^k est congru à 0.
3. Pour $k > 1$, 10^k est congru à 0.
4. Les puissances paires sont congrues à 1 et les puissances impaires à-1.

Exercice 7-15

1. a) $256 + 128 + 32 + 8 + 1 = 425$ b) $6561 + 2187 + 243 + 9 + 1 = 9001$ c) $512 + 3 * 64 + 6 * 8 + 7 = 759$ d) $125 + 4 * 25 + 2 = 227$
2. a) 11111111 b) 773 c) 10