Arithmétique

Solution de quelques exercices

O. Simon, Université de Rennes I

Théorème chinois. Soient m, n deux entiers premiers entre eux, $p,\ p_1,\ p_2$ les applications quotients de $\mathbb{Z}$ dans les anneaux $\mathbb{Z}/nm\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ alors il existe un isomorphisme f d'anneaux de $\mathbb{Z}/nm\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, tel que $f\ o\ p = (p_1, p_2)$.

$$\begin{array}{ccc} & \overset{p}{} & \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/nm\mathbb{Z} \\ (p_1,p_2)\ \searrow & & \swarrow\ f \\ & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \end{array}$$

Si m et n ne sont pas premiers entre eux, il existe un unique homomorphisme f vérifiant $f\ o\ p = (p_1, p_2)$, d'après la propriété universelle du quotient d'anneaux, mais il n'est ni surjectif, ni injectif.

Etude des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Exercice 19

1. Comme 17 est un nombre premier, $\mathbb{Z}/17\mathbb{Z}$ est un corps et $U(17)$ est un groupe multiplicatif d'ordre 16. On a les puissances de la classe de 3 dans le tableau suivant :

k	0	1	2	3	4	5	6	7	8
3^k	1	3	9	10	13	5	15	11	16

   L'ordre de tout élément d'un groupe est un diviseur de l'ordre du groupe. Comme l'ordre de 3 est supérieur strictement à 8, il est égal à 16 et 3 engendre $U(17)$.

2. On a la décomposition en facteurs premiers $15 = 3 \times 5$, ainsi $\phi(15) = \phi(3) \times \phi(5) = 8$ et

$$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

   Les éléments 2, 8, 7 et 13 sont d'ordre 4, les éléments 4, 11 et 14 sont d'ordre 2. Le groupe $U(15)$ n'est pas cyclique.

3. On a la décomposition en facteurs premiers $10 = 2 \times 5$, ainsi $\phi(10) = \phi(2) \times \phi(5) = 4$ et

$$U(10) = \{1, 3, 7, 9\}$$

   La classe de 3 est d'ordre 4, donc $U(10)$ est cyclique engendr par 3.

Pour le vocabulaire,
- on a trouvé que 3 est racine primitive de 17 et aussi de 10, par contre, 15 n'admet pas de racine primitive.
- dans $U(17)$, l'indice de 13 relativement à 3 ou le logarithme discret de base 3 de 13 est 4.

Exercice 20 On va résoudre dans $\mathbb{Z}/17\mathbb{Z}$, les équations suivantes :

$$6x^{10} = 4 \text{ et } 6x^{10} = 7$$

Comme 6 est inversible, (on a $6 \times 3 = 1$ *modulo* 17, les deux équations sont équivalentes à

$$x^{10} = 3 \times 4 = 12 \text{ et } x^{10} = 3 \times 7 = 4 \textit{ modulo } 17$$

Dans les deux cas, 0 n'est pas solution, il suffit donc de les résoudre dans $U(17) = \mathbb{Z}/17\mathbb{Z} - \{0\}$. En utilisant le générateur 3, on cherche des solutions de la forme $x = 3^k, k \in \{0, 1, ..., 15\}$.

1. La première équation devient : $3^{10k} = 3^{13}$ *modulo* 17. On a donc à résoudre

$$10k = 13 \textit{ modulo } 16$$

2. La deuxième équation devient $3^{10k} = 3^{12}$ *modulo* 17. On a donc à résoudre

$$10k = 12 \text{ } modulo \text{ } 16$$

Comme 10 n'est pas inversible dans $\mathbb{Z}/16\mathbb{Z}$, la multiplication par 10 n'est pas bijective, on a les valeurs atteintes :

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$10k$	0	10	4	14	8	2	12	6	0	10	4	14	8	2	12	6

On constate que 13 n'est pas atteint et que 12 est atteint deux fois.
Ainsi, la première équation n'a pas de solution,
la seconde en a deux : $x_1 = 3^6 = 15$ et $x_2 = 3^{14} = 2$ dans $\mathbb{Z}/17\mathbb{Z}$

Résidus quadratiques

Exercice 28 Soit $a \in \mathbb{Z}$.
Si a est un résidu quadratique modulo mn, alors il existe $x \in \mathbb{Z}$ tel que

$$a = x^2 + \lambda mn = x^2 + (\lambda m)n = x^2 + (\lambda n)m$$

donc a est un résidu quadratique modulo m et modulo n.
Réciproquement, si $a = x^2 + \lambda m$ et $a = y^2 + \lambda n$, en utilisant l'isomorphisme f du théorème chinois, soit $z \in \mathbb{Z}$ tel que $f \text{ } o \text{ } p(z) = (p_1(x), p_2(y))$. Alors

$$\begin{cases} z = x \text{ } modulo \text{ } m \\ z = y \text{ } modulo \text{ } n \end{cases} \text{ et donc } \begin{cases} z^2 = x^2 \text{ } modulo \text{ } m \\ z^2 = y^2 \text{ } modulo \text{ } n \end{cases}$$

$$f \text{ } o \text{ } p(a) = (p_1(a), p_2(a)) = (x^2, y^2) = (p_1(z^2), p_2(z^2)) = f \text{ } o \text{ } p(z^2) = f \text{ } o \text{ } (p(z))^2$$

Ainsi $a = z^2$ *modulo* mn.

Si $n = 3,\ m = 5,\ a = 2$, on constate que 2 n'est pas un carré dans $\mathbb{Z}/3\mathbb{Z}$, que 2 n'est pas un carré dans $\mathbb{Z}/5\mathbb{Z}$ et que 2 n'est pas un carré dans $\mathbb{Z}/15\mathbb{Z}$. Ainsi, on a l'inégalité pour les symboles de Legendre

$$\left(\frac{2}{3 \times 5}\right) = -1 \neq \left(\frac{2}{3}\right) \times \left(\frac{2}{5}\right) = -1 \times -1 = 1$$

Exercice 29 Soit p un nombre premier impair.
D'une part, pour tout x dans $\mathbb{Z}/p\mathbb{Z} - \{0\}$, on a $x^2 = (p-x)^2$ et comme p est impair x et $p - x$ sont deux éléments distincts.Donc il y a au plus $\dfrac{p-1}{2}$ résidus quadratiques.
D'autre part, si $x^2 = y^2$ alors $x^2 - y^2 = (x+y)(x-y) = 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, on a $x + y = 0$ ou $x - y = 0$, c'est-à-dire $y = x$ ou $y = -x$. Il y a donc exactement $\dfrac{p-1}{2}$ résidus quadratiques.
Remarque : Il y a $\dfrac{p-1}{2}$ valeurs de a dans $\mathbb{Z}/p\mathbb{Z}$, pour lesquelles le polynôme $X^2 - a$ n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$ et est donc irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 30
Exercice 31
Exercice 32
Exercice ??