Université de Rennes 1 Année 2022/2023

Algèbre et géométrie 1
Devoir maison
À rendre *impérativement* pour le mercredi 14 décembre 2022

Il va de soi que, sauf mention explicite du contraire, toute affirmation doit être justifiée et tout énoncé doit être démontré. On pourra cependant bien sûr s'appuyer librement sur les résultats démontrés en cours. On pourra aussi utiliser tout document ou outil comme aide à la décision mais *en aucun cas* comme argument mathématique.

1. Une *écriture binaire* de $n \in \mathbb{Z}_{>0}$ est une égalité de la forme

$$n = 2^k + 2^{k-1}\epsilon_{k-1} + \ldots + 2\epsilon_1 + \epsilon_0 \tag{1}$$

avec $k \in \mathbb{Z}_{\geq 0}$ et $\epsilon_0, \ldots, \epsilon_{k-1} \in \{0, 1\}$. En pratique, on omet les termes avec $\epsilon_i = 0$ et les facteurs $\epsilon_i = 1$. Par exemple, $10 = 2^3 + 2$ est une écriture binaire.

(a) Donner des écritures binaires pour 7 et 11.

Solution: On a $7 = 2^2 + 2 + 1$ et $11 = 2^3 + 2 + 1$.

(b) Montrer que, dans l'équation (1), on a $2^k \leq n < 2^{k+1}$.

Solution: On a

$$n - 2^k = 2^{k-1}\epsilon_{k-1} + \ldots + 2\epsilon_1 + \epsilon_0 \geq 0$$

et donc $2^k \leq n$. On a

$$\begin{aligned} n &= 2^k + 2^{k-2}\epsilon_{k-2} + \ldots + 2\epsilon_1 + \epsilon_0 \\ &\leq 2^k + 2^{k-2} + \ldots + 2 + 1 \\ &= 2^{k+1} - 1 \end{aligned}$$

(progression géométrique) et donc $n < 2^{k+1}$.

(c) En déduire [1] que, dans l'équation (1), on a $k = \lfloor \ln(n)/\ln(2) \rfloor$.

Solution: En effet, on aura $\ln(2^k) \leq \ln(n) < \ln(2^{k+1})$ et donc $k\ln(2) \leq \ln(n) < (k+1)\ln(2)$ si bien que $k \leq \ln(n)/\ln(2) < k + 1$.

1. On désigne par $\lfloor x \rfloor$ la partie entière d'un réel x.

(d) Soit $\mathcal{P}(n)$ une propriété qui dépend d'un entier naturel $n \geq n_0$ et

$$\mathcal{P}'(n) := (\forall m \in \mathbb{N}, n_0 \leq m < n \Rightarrow \mathcal{P}(m)).$$

Montrer que

$$(\forall n \geq n_0, \mathcal{P}'(n) \Rightarrow \mathcal{P}(n)) \Rightarrow (\forall n \geq n_0, \mathcal{P}(n)).$$

Cette méthode s'appelle la *récurrence forte*.

Solution: On suppose que $\mathcal{P}'(n) \Rightarrow \mathcal{P}(n)$ pour tout $n \geq n_0$. On fixe $n \geq n_0$. Par défintion, "$\mathcal{P}'(n)$ et $\mathcal{P}(n) \Leftrightarrow \mathcal{P}'(n+1)$". On en déduit tautologiquement que $\mathcal{P}'(n) \Rightarrow \mathcal{P}'(n+1)$. D'autre part, $\mathcal{P}'(n_0)$ est la condition vide qui est toujours satisfaite. On a donc montré par récurrence que, sous notre hypothèse, si $n \geq n_0$, alors $\mathcal{P}'(n)$ est satisfaite. Mais notre hypothèse implisque alors que $\mathcal{P}(n)$ aussi est satsifaite.

(e) Montrer par récurrence forte que tout $n \in \mathbb{Z}_{>0}$ possède une écriture binaire.

Solution: Soit $n \in \mathbb{Z}_{>0}$. On suppose que m possède une écriture binaire lorsque $0 < m < n$. On effectue la division euclidienne de n par 2 : $n = 2m+\epsilon$ avec $\epsilon \in \{0, 1\}$. Si $m = 0$, alors $n = 1$ et on a fini. Sinon, on a $0 < m < n$ et on peut donc écrire

$$m = 2^k + 2^{k-1}\epsilon_{k-1} + \ldots + 2\epsilon_1 + \epsilon_0$$

avec $k \in \mathbb{N}$ et $\epsilon_0, \ldots, \epsilon_{k-1} \in \{0, 1\}$. On en déduit que

$$n = 2^{k+1} + 2^k\epsilon_{k-1} + \ldots + 2^2\epsilon_1 + 2\epsilon_0 + \epsilon$$

(c'est bien une écriture binaire).

(f) Montrer par la même méthode que cette écriture est unique.

Solution: Soit

$$n = 2^k + 2^{k-1}\epsilon_{k-1} + \ldots + 2\epsilon_1 + \epsilon_0$$

une écriture binaire. Si $k = 0$, celle-ci est clairement unique car $n = 1$, et on suppose maintenant $k > 0$. Si on effectue la division euclidienne de n par 2, on trouve $n = 2m + \epsilon_0$ avec

$$m = 2^{k-1} + 2^{k-2}\epsilon_{k-1} + \ldots + 2\epsilon_2 + \epsilon_1.$$

Par récurrence forte, on voit donc que k et $\epsilon_1, \ldots, \epsilon_{k-1}$ sont uniques. L'unicité de ϵ_0 résulte alors de l'unicité du reste dans la division euclidienne.

(g) Soit $a \in \mathbb{Z}$. On définit par récurrence la suite $a_0 = a$ et $a_{i+1} = a_i^2$. Montrer que pour tout $i \in \mathbb{N}$, on a $a_i = a^{2^i}$. En déduire que si (1) est une écriture binaire et $m \in \mathbb{N}$, alors

$$a^n \equiv a_k a_{k-1}^{\epsilon_{k-1}} \ldots a_1^{\epsilon_1} a_0^{\epsilon_0} \mod m.$$

Solution: Par récurrence : on a bien $a_0 = a^{2^0}$ et si $a_i = a^{2^i}$, on aura $a_{i+1} = a_i^2 = (a^{2^i})^2 = a^{2^i \times 2} = a^{2^{i+1}}$. On en déduit que

$$\begin{aligned} a^n &\equiv a^{2^k + 2^{k-1}\epsilon_{k-1} + \ldots + 2\epsilon_1 + \epsilon_0} && \mod m \\ &\equiv a^{2^k} a^{2^{k-1}\epsilon_{k-1}} \ldots a^{2\epsilon_1} + a^{\epsilon_0} && \mod m \\ &\equiv a_k a_{k-1}^{\epsilon_{k-1}} \ldots a_1^{\epsilon_1} a_0^{\epsilon_0} && \mod m. \end{aligned}$$

Remarque. C'est la méthode d'*exponentiation rapide* : on cherche l'écriture binaire de n, on calcule $a_1, \ldots, a_k$ modulo m, on applique la formule et on simplifie. Considérons par exemple le cas $n = 10$, $m = 11$ et $a = 7$. On a $10 = 2^3 + 2$. On calcule d'autre part

1. $7^2 = 49 \equiv 5 \mod 11$,
2. $5^2 = 25 \equiv 3 \mod 11$,
3. $3^2 = 9 \equiv -2 \mod 11$.

On conclut que $7^{10} \equiv -2 \times 5 = -10 \equiv 1 \mod 11$.

(h) Appliquer la méthode d'exponentiation rapide pour déterminer le reste dans la division de 6^7 par 11.

Solution: On a $7 = 2^2 + 2 + 1$. On calcule ensuite

1. $6^2 = 36 \equiv 3 \mod 11$,
2. $3^2 = 9 \equiv -2 \mod 11$.

On a donc

$$6^7 \equiv -2 \times 3 \times 6 = -36 \equiv 8 \mod 11.$$

(i) Même question avec la division de 8^{11} par 19.

Solution: On a $11 = 2^3 + 2 + 1$. On calcule ensuite

1. $8^2 = 64 \equiv 7 \mod 19$,
2. $7^2 = 49 \equiv -8 \mod 19$,
3. $(-8)^2 = 64 \equiv 7 \mod 19$.

On a donc

$$8^{11} \equiv 7 \times 7 \times 8 \equiv 7 \times 56 \equiv -7 \equiv 12 \mod 19.$$

2. Sauf mention explicite du contraire, toutes les lettres minuscules représentent des entiers relatifs.
   On dit que a' est un *inverse* pour a modulo n si $aa' \equiv 1 \mod n$.

(a) Déterminer un inverse pour 3 modulo 10.

Solution: On a $3 \times 7 = 21 \equiv 1 \mod 10$, ce qui montre 7 est un inverse pour 3 modulo 10.

(b) Montrer que si a est inversible modulo n et $ab \equiv ac \mod n$ alors $b \equiv c \mod n$.

Solution: En effet, on aura $b \equiv a'ab \equiv a'ac \equiv c \mod n$.

(c) Soit a' un inverse pour a modulo n et a'' un entier quelconque. Montrer que a'' est un inverse pour a modulo n si et seulement si $a' \equiv a'' \mod n$.

Solution: Si $a'' \equiv a \mod n$, alors $aa'' \equiv aa' \equiv 1 \mod n$. Réciproquement, si $aa'' \equiv 1 \mod n$, alors $aa' \equiv aa'' \mod n$ et donc $a' \equiv a'' \mod n$ grâce à la question précédente.

(d) Montrer que a est inversible modulo n si et seulement s'il existe u, v tels que $nu + av = 1$ et qu'alors v est un inverse pour a modulo n. En déduire que a est inversible modulo n si et seulement si a est premier avec n.

Solution: Si a possède un inverse a' modulo n, alors $aa' \equiv 1 \mod n$ et il existe donc $k \in \mathbb{Z}$ tel que $aa' = 1 + kn$. Il suffit alors de poser $u = -k$ et $v = a'$. Réciproquement, si $nu + av = 1$ et qu'on pose $a' = v$, on aura $aa' = 1 - nu \equiv 1 \mod n$. La dernière assertion résulte du théorème de Bézout.

(e) Appliquer l'algorithme d'Euclide étendu à 18 et 5 et en déduire un inverse pour 5 modulo 18.

Solution: On a

$$\begin{aligned} 18 &= 1 \times 18 + 0 \times 5 \\ 5 &= 0 \times 18 + 1 \times 5 \\ 3 &= 1 \times 18 - 3 \times 5 \\ 2 &= -1 \times 18 + 4 \times 5 \\ 1 &= 2 \times 18 - 7 \times 5. \end{aligned}$$

On voit donc que -7 (ou 11 si on préfère) est un inverse pour 5 modulo 18.

(f) Soit p un nombre premier. Rappeler l'énoncé du petit théorème de Fermat.

Solution: Si $p \nmid x$, alors $x^{p-1} \equiv 1 \mod p$.

(g) Montrer que si a' est un inverse pour a modulo $p-1$, alors l'équation $x^a \equiv c \mod p$ a pour solution (non unique) $x = c^{a'}$.

Solution: Posons $x = c^{a'}$. Puisque $aa' \equiv 1 \mod p-1$, on peut écrire $aa' = 1 + k(p-1)$ et alors

$$x^a = (c^{a'})^a = c^{aa'} = c^{1+k(p-1)} = c \times (c^{p-1})^k \equiv c \mod p$$

grâce au petit théorème de Fermat (le cas où $p \mid c$ étant immédiat).

(h) Déterminer x tel que $x^3 \equiv 6 \mod 11$ et $0 \leq x < 10$ en utilisant cette méthode (et l'exponentiation rapide).

Solution: Ici on a $p = 11$ et donc $p - 1 = 10$. On a déjà vu que que 7 est un inverse pour 3 modulo 10. On en déduit que $x = 6^7$ est une solution. Par exponentiation rapide, on a aussi montré que $6^7 \equiv 8 \mod 11$. On a donc $x = 8$.

(i) Déterminer de même x tel que $0 \leq x < 19$ et $x^5 \equiv 8 \mod 19$.

Solution: On a vu que 11 est un inverse pour 5 modulo 18. On en déduit que $x = 8^{11}$ est solution. Or on a aussi vu que $8^{11} \equiv 12 \mod 19$. On a donc $x = 12$.