Ecole Polytechnique Fédérale de Lausanne

Sciences de l'information

Série 7

Olivier Cloux

7.1

1. Rappelons nous qu'une classe de congruence $[a]_m$ est inversible si et seulement s'il existe une classe de congruence $[b]_m$ telle que $[a]_m \cdot [b]_m = [1]_m$; le théorème 8.5 nous dit aussi que Soient a et m deux entiers avec $m > 2$. $[a]_m$ est inversible si et seulement si a et m sont premiers entre eux.
   (a) 3 et 7 sont premiers (donc premiers entre eux), donc cette classe est inversible ; $([3]_7)^{-1} = \boxed{[5]_7}$ car $[3]_7 \cdot [5]_7 = [3 \cdot 5]_7 = [15]_7 = [1]_7$
   (b) 3 et 9 ne sont pas premiers entre eux ($pgcd(3, 9) = 3$), donc cette classe de congruence n'est pas inversible.
   (c) 4 et 8 ne sont pas premiers entre eux ($pgcd(4, 8) = 4$), donc cette classe de congruence n'est pas inversible.
   (d) Les i qui ne sont pas inversibles sont 2, 4, 5, 6, 8 (car ils ne sont pas premiers avec 10 ; les pairs ont 2 comme multiple commun avec 10, et 5 a 5). Pour les autres i :
   i=1 Son inverse est lui-même : $[1]_{10} \cdot [1]_{10} = [1]_{10}$
   i=3 Son inverse est 7 : $[7]_{10} \cdot [3]_{10} = [21]_{10} = [1]_{10}$
   i=7 Son inverse est 3 : $[7]_{10} \cdot [3]_{10} = [21]_{10} = [1]_{10}$
   i=9 Son inverse est lui-même : $[9]_{10} \cdot [9]_{10} = [81]_{10} = [1]_{10}$
2. Nous résolvons avec les opérations standard, et le concept d'inverse :
$$\left.\begin{array}{ll} & [3]_9 x + [4]_9 = [1]_9 \\ \iff & [3]_9 x = [1]_9 - [4]_9 \\ \iff & [3]_9 x = [-3]_9 = [6]_9 \\ \iff & [1]_3 x = x = [2]_3 \end{array}\right\} \text{Donc } x = 3k + 2 \ \forall k \in \mathbb{Z}$$
Mais nous le voulons dans la classe 9. Il faut donc regarder nos éléments avec le modulo 9 ((2 mod 3) mod 9). Les éléments de 2 mod 3 sont 2,5,8,11,14,17,20,... En prenant le modulo 9 de ces chiffres, nous obtenons 2,5,8,2,5,8,... Nous voyons une boucle. Ainsi, $\boxed{x = \{2, 5, 8\}}$. Nous

pouvons vérifier en les entrant dans notre équation de base :

$$[3]_9 \cdot [2]_9 + [4]_9 = [10]_9 = [1]_9 \surd$$
$$[3]_9 \cdot [5]_9 + [4]_9 = [19]_9 = [1]_9 \surd$$
$$[3]_9 \cdot [8]_9 + [4]_9 = [28]_9 = [1]_9 \surd$$

Nous avions donc raison quant à notre x !

7.2

Soient nos deux équations de base :

$$4[x]_{17} = [1]_{17} \quad (1)$$
$$3[x]_5 = [2]_5 \quad (2)$$

Calculer x dans (1) revient à calculer l'inverse de $[4]_{17}$ (car cette équation correspond à la définition de l'inverse). Nous trouvons donc que $x = [13]_{17}$ (car $[4]_{17} \cdot [13]_{17} = [68]_{17} = [1]_{17}$), donc $x = 17k+13 \; \forall k \in \mathbb{Z}$

De même, pour trouver x dans (2), il faut d'abord trouver l'inverse de $[3]_5$, qui est $[2]_5$ (car... vous savez pourquoi, j'en suis sur). Donc

$$\begin{aligned} 3[x]_5 = [2]_5 &\iff [2]_5[3]_5[x]_5 = [2]_5[2]_5 \\ &\iff [x]_5 = [2 \cdot 2]_5 \\ &\iff x = [4]_5 \end{aligned}$$

Ainsi, x doit satisfaire deux équation : (pour tout $k \in \mathbb{Z}$)

$$[x]_{17} = [13]_{17} \iff x = 17k + 13 \quad (3)$$
$$[x]_5 = [4]_5 \iff x = 5k + 4 \quad (4)$$

Afin de pouvoir travailler sur nos équations, nous les multiplions pour avoir la même classe. Nous multiplions chacune afin d'arriver à leur *ppmc* (comme 5 et 17 sont premiers entre eux, $ppmc(5, 17) = 5 \cdot 17 = 85$). Ainsi, nous allons chercher un x dans une classe de congruence 85 ($[x]_{85}$). En modifiant (1) et (2) (en les multipliant par respectivement 5 et 17), nous obtenons :

$$20[x]_{85} = [5]_{85} \iff 20x = 5 \mod 85 \quad (5)$$
$$51[x]_{85} = [34]_{85} \iff 51x = 34 \mod 85 \quad (6)$$

Pour ensuite trouver le reste, nous cherchons un chiffre entre 0 et 85, qui soit en commun dans les équations (3) et (4). Après une rapide investigation, nous trouvons l'unique chiffre 64 ($= 17 \cdot 3 + 13 = 5 \cdot 12 + 4$). Les augures semblent indiquer donc que $x = [64]_{85}$.

Pour le vérifier, nous n'avons qu'à injecter notre x dans (5) et (6). Cela nous donne :

$$20 * 64 \equiv 1280 \equiv 5 \mod 85$$
$$51 * 64 \equiv 3264 \equiv 64 \mod 85$$

ce qui correspond bien aux résultats attendus. Cela confirme donc les augures ; ainsi, $\boxed{x = [64]_{85}}$

7.3

1. Si un nombre est divisible par 2 et par 7, cela signifie qu'il a, parmi sa liste de facteurs premiers, $2^{\alpha_1} \cdot 7^{\alpha_2}$ (au moins), avec $\alpha_{1,2} \geq 1$. De ce fait, nous pouvons "mettre en évidence" un 14, ce qui

fait que ce chiffre est divisible par 14.

De même, si un nombre est divisible par 14, cela signifie qu'il a, dans ses facteurs premiers, $2^{\alpha_1} \cdot 7^{\alpha_2}$ (au moins), avec $\alpha_{1,2} \geq 1$. De ce fait, nous pouvons sans problème diviser par 2 et par 7.

Les deux énoncés sont donc vrais. Cela s'explique par le fait que $14 = 2 \cdot 7$. Diviser par 14 ou par 2 et 7 est totalement égal, sans aucuns différence.

2. Pour qu'on nombre soit divisible par 6 $(2 \cdot 3)$ et par 8 (2^3), il doit donc être divisible par $ppmc(6, 8) = 24 = 2^3 \cdot 3 = (3 \cdot 2^2) \cdot 2 = (3 \cdot 4) \cdot 2 = 12 \cdot 2$. Donc le nombre est forcément divisible par 12.

   En revanche, si notre nombre est divisible par 12, cela signifie qu'il est divisible par $3 \cdot 2^2$. Pour être divisible par 6 et 8, il doit être divisible, nous l'avons vu avant, par $24 = 2^3 \cdot 3$. Nous voyons bien que c'est impossible dans bien des cas. Pour s'en convaincre, nous pouvons prendre un exemple : 12. Ce nombre est bien divisible par 12 et est divisible par 6 mais il n'est pas divisible par 8.

   Ainsi, notre premier énoncé est correcte, mais sa réciproque est fausse.

3. La somme des chiffres de ce 561 est un multiple de 3, donc il est divisible par 3. De plus, la somme du premier et dernier chiffre donne le chiffre du milieu, il est donc divisible par 11. En divisant par 33 nous voyons que le résultat est 17. Ce chiffre n'est donc pas premier car il vaut $3 \cdot 11 \cdot 17$ (un produit de nombres premiers différents de lui-même et 1).

4. Pour commencer, notons que a et p sont premiers entre eux (selon le théorème 7.6.2). Comme $0 < a < p$ et que p est premier, nous pouvons assurer que $a \mod p = a$ (grâce au théorème 8.6). Maintenant, prouvons par l'absurde que $a, 2a, 3a, \ldots, (p-1)a$ sont distincts (mod p) :
   Posons deux entiers distincts $k, k' \in]0, (p-1)[\subset \mathbb{Z}$. Imaginons, tels des fous, qu'il existe une telle paire d'entiers, tels que le modulo de leurs multiples de a ne sont pas distincts, autrement dit que

$$\begin{aligned} & ka \mod p = k'a \mod p \\ \iff & (ka - k'a) \mod p = 0 \mod p \\ \iff & a(k - k') \mod p = 0 \mod p \end{aligned}$$

   Cette dernière égalité ne peut être vraie que dans 3 cas :

   a) Si $a(k - k') = p$
   b) Si $a = 0$
   c) Si $k - k' = 0$

   Le premier cas est impossible, car p est premier, donc ne peut pas être le produit d'autres entiers (différents de 1 et lui-même). Le second cas est également impossible par donnée (on veut que $0 < a < p$). Seul le 3ème cas est envisageable. Mais cela implique que $k = k'$, ce que nous avions posé comme faux au début. Nous voulons donc deux entiers distincts égaux. Comme cela est impossible, notre proposition (il existe deux entiers distincts tels que[...]) est fausse. Cela implique que $a, 2a, 3a, ..., (p-1)a$ sont tous distincts (mod p)

   Maintenant, attaquons nous à la preuve : nous savons que, l'inverse de $a \mod p$ est entre 0 et p (non inclus), soit dans une plage de $p - 1$ éléments. Nous savons également que l'inverse d'un nombre est unique. Nous savons aussi que le produit de $a, 2a, 3a, ..., (p-a)a = a^{p-1}(p-1)!$. Par le pigeonhole principle, nous pouvons déduire que $a^{-1} \neq (2a)^{-1} \neq (3a)^{-1} \neq ... \neq ((p-1)a)^{-1}$ et que $(a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a) \mod p = (p-1)! \mod p$ (car nous avons le produit de $p - 1$

éléments distincts, sur une plage de $p-1$ éléments ; quel que soit l'ordre nous auront le produit de ces éléments).
De plus, nous pouvons trouver que les inverses de $a, 2a, 3a, ...$ sont tous distincts sur $p-1$. Cela implique que l'inverse de $(p-1)!$ est lui-même ! En mettant cela en équations, nous avons

$$\begin{aligned} a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \mod p &= (p-1)! \mod p \\ \iff a^{p-1}(p-1)! \mod p &= (p-1)! \mod p \\ \iff a^{p-1} \underbrace{(p-1)!(p-1)!}_{=1} \mod p &= \underbrace{(p-1)!(p-1)!}_{=1} \mod p \\ \iff \boxed{a^{p-1} \equiv 1 \mod p} & \end{aligned}$$