Correction du contrôle continu du mercredi 11 mars 2020

Durée : 2 heures.

Remarques générales

- **Rédigez !** Trop de copies ressemblent à des idées que vous auriez notées sur un brouillon. Expliquez ce que vous entreprenez, utilisez des connecteurs logiques pour mettre en valeur les déductions.
- Rappel : chercher « l'inverse de a modulo m » revient à chercher b tel que $a \times b \equiv 1 \mod m$. Par exemple, l'inverse de 2 modulo 7 est 4 car : $2 \times 4 = 8$ et 8 est congru à 1 modulo 7.
  Si l'inverse n'est pas « évident », on peut utiliser l'algorithme d'Euclide pour trouver une relation de Bézout et en déduire l'inverse. (Méthode détaillée dans la démo du Théorème 1.42 du poly de cours.)
- Si a et b sont deux entiers et que d est leur pgcd, alors les entiers a' et b' tels que $a = da'$ et $b = db'$ sont **premiers entre eux**.
- Résoudre une équation revient à trouver **toutes** les solutions. Et pas seulement *une* solution particulière.

Exercice 1 (3 pts). Résoudre dans $\mathbb{Z}$ l'équation $1124x + 1004y = 12$.

Rappel sur la méthode Pour résoudre une équation de type $ax + by = c$.

1. Calculer le PGCD de a et b, ou bien à l'aide de l'algorithme d'Euclide ou bien (si la décomposition en facteurs est évidente) avec la décomposition en facteurs premiers.
   $\rightarrow$ L'équation a des solution ssi $\mathrm{pgcd}(a, b)$ divise c.
2. Dans le cas où $\mathrm{pgcd}(a, b)$ divise c : on cherche d'abord une solution particulière à l'équation
   $$ax + by = \mathrm{pgcd}(a, b),$$
   ou bien en exhibant une solution évidente, ou bien en remontant l'algorithme d'Euclide. On note (x_0, y_0) cette solution particulière.
3. On pose k l'entier tel que $c = k \times \mathrm{pgcd}(a, b)$. Une solution particulière de
   $$ax + by = c,$$
   est alors $(x_1, y_1) = (k \times x_0, k \times y_0)$.
4. Soient $a', b' \in \mathbb{Z}$ tq $a = \mathrm{pgcd}(a, b)a'$ et $b = \mathrm{pgcd}(a, b)b'$. Les solutions générales sont données par la formule [a] :
   $$\mathcal{S} = \{(x_1 + kb', y_1 - ka')\, k \in \mathbb{Z}\}\,.$$

[a]. Établie page 10 du poly de cours.

1. Calculons le PGCD de 1124 et 1004 à l'aide de l'algorithme d'Euclide.

$$\begin{aligned}
1124 &= 1004 \times 1 + 120 \\
1004 &= 120 \times 8 + 44 \\
120 &= 44 \times 2 + 32 \\
44 &= 32 \times 1 + 12 \\
32 &= 12 \times 2 + 8 \\
12 &= 8 \times 1 + 4 \\
8 &= 4 \times 2 + 0.
\end{aligned}$$

   Le PGCD étant le dernier reste non-nul, nous obtenons $\mathrm{pgcd}(1004, 1124) = 4$. Comme 4 divise 12, l'équation a des solutions.

2. Cherchons d'abord une solution particulière à l'équation $1124x + 1004y = 4$. Une réécriture de l'algorithme d'Euclide donne :

$$\begin{aligned}
1124 - 1004 &= 120 \\
1004 - 120 \times 8 &= 44 \\
120 - 44 \times 2 &= 32 \\
44 - 32 \times 1 &= 12 \\
32 - 12 \times 2 &= 8 \\
12 - 8 &= 4
\end{aligned}$$

   Ainsi :

$$\begin{aligned}
4 = 12 - 8 = 12 - (32 - 12 \times 2) &= -32 + 3 \times 12, \\
&= -32 + 3 \times (44 - 32), \\
&= 3 \times 44 - 4 \times 32, \\
&= 3 \times 44 - 4 \times (120 - 44 \times 2), \\
&= -4 \times 120 + 11 \times 44, \\
&= -4 \times 120 + 11 \times (1004 - 120 \times 8), \\
&= 11 \times 1004 - 92 \times 120, \\
&= 11 \times 1004 - 92 \times (1124 - 1004), \\
&= 103 \times 1004 - 92 \times 1124.
\end{aligned}$$

   Une solution particulière est donc $(x_0, y_0) = (-92, 103)$.

3. Une solution particulière de l'équation $1124x + 1104y = 12$ est donc :

$$(x_1, y_1) = (3 \times (-92), 3 \times 103) = (-276, 309).$$

4. Comme $1124 = 4\times$ **281** et $1004 = 4\times$**251** l'ensemble des solutions est :

$$\mathcal{S} = \left\{(-276 + \mathbf{251}k, 103 - \mathbf{281}k) \;\middle|\; k \in \mathbb{Z}\right\}.$$

Exercice 2 (2+2 pts).

1. Montrer que pour tout $n \in \mathbb{N}$ impair, $7^n + 1$ est divisible par 8.

Soit $n \in \mathbb{N}$ impair. Alors, il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$. Ainsi :

$$7^n = 7^{2k+1} = \left(7^2\right)^k \times 7.$$

Mais $7^2 = 49 \equiv 1 \mod 8$, donc :

$$\left(7^2\right)^k 7 \equiv 1^k \times 7 \equiv 7 \mod 8.$$

Ainsi, $7^n + 1 \equiv 7 + 1 \equiv 8 \equiv 0 \mod 8$.

Le fait que 8 divise $7+1$, 7^3+1, 7^5+1, 7^7+1 **n'**est **pas** une preuve que 8 divise 7^n+1 **pour tout n impair**.
De manière générale : **ce n'est pas parce qu'une propriété est vraie pour quelques cas qu'elle est vraie en toute généralité.**

2. Montrer que pour tout $a, b \in \mathbb{Z}$, 4 ne divise jamais $a^2 + b^2 - 3$.

Étudions les valeurs possible d'un carré modulo 4. Soit $n \in \mathbb{N}$, nous avons le tableau de congruence suivant :

$n \mod 4$	0	1	2	3
$n^2 \mod 4$	0	1	0	1

Ainsi, pour $a, b \in \mathbb{Z}$ les valeurs possibles de (a^2, b^2) modulo 4 sont

$$(0,0)\ (0,1)\ (1,0) \text{ et } (1,1).$$

Si $a^2 \equiv 0 \mod 4$ et $b^2 \equiv 0 \mod 4$, alors $a^2 + b^2 - 3 \equiv -3 \equiv 1 \mod 4$.
Si $a^2 \equiv 1 \mod 4$ et $b^2 \equiv 0 \mod 4$, alors $a^2 + b^2 - 3 \equiv 1 - 3 \equiv 2 \mod 4$. Le cas $a^2 \equiv 0 \mod 4$ et $b^2 \equiv 1 \mod 4$ est analogue.
Si $a^2 \equiv 1 \mod 4$ et $b^2 \equiv 1 \mod 4$, alors $a^2 + b^2 - 3 \equiv 2 - 3 \equiv -1 \equiv 3 \mod 4$.
Dans tous les cas, $a^2 + b^2 - 3$ n'est pas congru à 0 modulo 4 donc n'est pas divisible par quatre.

Exercice 3 (1.5+1.5 pts).

1. Trouver le reste de la division par 47 du nombre $2020^{123456789}$.

La division euclidienne de 2020 par 47 donne :

$$2020 = 47 \times 42 + 46.$$

Donc, $2020 \equiv -1 \mod 47$ et alors $2020^2 \equiv (-1)^2 \equiv 1 \mod 47$.
Or 123456789 est impair, c'est à dire qu'il existe $k \in \mathbb{Z}$ tel que $123456789 = 2k+1$. Ainsi :

$$\begin{aligned} 2020^{123456789} &= 2020^{2k+1} = \left(2020^2\right)^k 2020, \\ \Rightarrow 2020^{123456789} &\equiv \left(2020^2\right)^k 2020 \equiv 1^k \times (-1) \equiv -1 \equiv 46 \mod 47. \end{aligned}$$

Le reste dans la division euclidienne par 47 de $2020^{123456789}$ est donc 46.

Remarque : On rappelle que le reste d'un division Euclidienne est un entier *positif* et *strictement inférieur au nombre par lequel on divise*. Donc même s'il est vrai que $2020^{123456789}$ est congru à -1 modulo 47, le reste de la division euclidienne par 47 n'est pas -1.

2. Quel est le chiffre des unités dans l'écriture en base 2 de 45675413247^{61} ?

Le chiffre des unités dans l'écriture en base 2 d'un nombre est le *reste de la division euclidienne par* 2. Or, 45675413247 est impair. Donc :

$$45675413247 \equiv 1 \mod 2 \Longrightarrow 45675413247^{61} \equiv 1^{61} \equiv 1 \mod 2.$$

Ainsi, le reste dans la division euclidienne de 45675413247^{61} par 2 est 1. Le chiffre des unités en base deux de 45675413247^{61} est donc 1.

Exercice 4 (4 pts). Résoudre dans $\mathbb{Z}$ le système suivant :

$$S : \begin{cases} x & \equiv 1 \mod 10, \\ 4x & \equiv 9 \mod 15. \end{cases}$$

Rappel sur la méthode[a] Pour résoudre un système du type :

$$\begin{cases} cx & \equiv a_1 \mod m, \\ dx & \equiv b_1 \mod n. \end{cases}$$

1. Inverser c modulo n et d modulo m pour se ramener à un système de la forme :

$$\begin{cases} x & \equiv a_2 \mod m, \\ x & \equiv b_2 \mod n. \end{cases}$$

$\rightarrow$ Le système admet des solutions ssi $\text{pgcd}(m, n)$ divise $(b_2 - a_2)$.

2. On cherche ensuite une solution particulière au système en cherchant une solution (u_0, v_0) à l'équation de Bézout :

$$mu + nv = \text{pgcd}(m, n).$$

(Si cette solution n'est pas évidente, passer par l'algorithme d'Euclide pour l'obtenir.)

3. Une solution particulière du système est alors :

$$x_0 = b_2 u_0 m' + a_2 v_0 n',$$

où $m = \text{pgcd}(m, n)m'$ et $n = \text{pgcd}(m, n)n'$

4. Cette solution étant unique modulo **ppcm(m,n)**, l'ensemble des solutions est :

$$\mathcal{S} := \{x_0 + k \times ppcm(m, n) \mid k \in \mathbb{Z}\}.$$

[a] Poly de cours pages 14 et 15.

1. Inversons tout d'abord 4 modulo 15. On remarque :

$$4 \times 4 = 16 \equiv 1 \mod 15.$$

Donc

$$4x \equiv 9 \mod 15 \iff 4 \times 4x \equiv 4 \times 9 \mod 15 \iff x \equiv 6 \mod 15.$$

Le système est donc équivalent à :

$$\begin{cases} x & \equiv 1 \mod 10, \\ x & \equiv 6 \mod 15. \end{cases}$$

Or $\mathrm{pgcd}(10, 15) = 5$ et divise bien $6 - 1$. Donc le système admet des solutions.
2. Cherchons une solution à l'équation $15u + 10v = 5$. Une solution évidente est $(u_0, v_0) := (1, -1)$.
3. On remarque que 10= $\mathbf{2} \times 5$ et 15= $\mathbf{3} \times 5$, alors, une solution particulière du système de départ est :

$$x_0 := 1 \times 1 \times \mathbf{3} + 6 \times (-1) \times \mathbf{2} = -9$$
4. Comme $ppcm(10, 15) = 30$, l'ensemble des solutions est donc :

$$\mathcal{S} := \{-9 + k \times 30 \mid k \in \mathbb{Z}\}.$$

Exercice 5 (1+2 pts). Déterminer l'ensemble des x dans $\mathbb{Z}$ qui sont solutions de l'équation (E) dans chacun des cas suivants :

Rappel sur la méthode [a]

Dans une équation de type $ax \equiv b \mod c$,

1. Si a n'est pas premier avec c :
   - Si le $\mathrm{pgcd}(a, c)$ ne divise pas b, alors il n'y a pas de solution.
   - Si le $\mathrm{pgcd}(a, c)$ divise b, alors l'équation est équivalente à

     $$a'x \equiv b' \mod c',$$

     où $a = \mathrm{pgcd}(a, c)a'$ et $b = \mathrm{pgcd}(a, c)b'$ et $c = \mathrm{pgcd}(a, c)c'$. Dans ce cas, a' est alors premier avec c' et on applique ce qui suit à la nouvelle équation.
2. Si a est premier avec c, on cherche d'abord à « inverser » a modulo c. Pour se ramener à un équation de type $x \equiv d \mod c$.
3. On exprime les solutions sous la forme :

$$\mathcal{S} = \{ck + d \mid k \in \mathbb{Z}\}.$$

a. Voir page 13 du poly, Proposition 1.44 et Exemple 1.46.

1. $(E) : 2x \equiv 4 \mod 17.$

(a) On remarque que 2 et 17 sont premiers entre eux.

(b) Cherchons l'inverse de 2 modulo 17. On a :

$$9 \times 2 = 18 \equiv 1 \mod 17.$$

Donc,

$$2x \equiv 4 \mod 17 \iff 9 \times 2x \equiv 9 \times 4 \mod 17 \iff x \equiv 2 \mod 17.$$

(c) Les solutions sont donc $\mathcal{S} = \{17k + 2 \mid k \in \mathbb{Z}\}$.

2. $(E) : 6x \equiv 2 \mod 8$.

(a) On remarque que $\mathrm{pgcd}(6, 8) = 2$. L'équation est alors équivalente à $3x \equiv 1 \mod 4$.

(b) On cherche alors l'inverse de 3 modulo 4. On a :

$$3 \times 3 = 9 \equiv 1 \mod 4.$$

Donc :

$$\begin{aligned} 3x \equiv 1 \mod 4 &\Leftrightarrow 3 \times 3x \equiv 3 \times 1 \mod 4, \\ &\Leftrightarrow x \equiv 3 \mod 4. \end{aligned}$$

(c) Les solutions de (E) sont : $\mathcal{S} = \{4k + 3 \mid k \in \mathbb{Z}\}$.

Exercice 6 (1+2 pts).

1. Enoncer le théorème de Bézout.

Soient a, b des entiers relatifs qui ne sont pas tous les deux nuls. Alors il existe des entiers relatifs u et v tels que $au + bv = \mathrm{pgcd}(a, b)$.

2. Soient a, b, c trois entiers non nuls, et soit $d = \mathrm{pgcd}(a, b)$. Montrer que si c est un diviseur commun de a et de b, alors c divise d.

Par le théorème de Bézout : il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$.
Si c divise a et b, alors il existe a' et b' des entiers tels que $a = ca'$ et $b = cb'$. Ainsi :

$$au + bv = d \Rightarrow ca'u + cb'v = d \Rightarrow c\,(ua' + vb') = d.$$

Comme $ua' + vb' \in \mathbb{Z}$, on a bien que c divise d.

Exercice 7 (Bonus, 2pts). Soient a et b deux entiers positifs distincts et premiers entre eux. Calculer $\mathrm{pgcd}(a + b, a - b)$, en discutant selon les parités de a et de b.

Voir correction de l'exercice 15, question 5 sur la feuille de TD 1.