UNIVERSITÉ d'ORLÉANS SCL1 MA02
Département de mathématiques 2008-9

Arithmétique : Corrigé Feuille 4 (Congruences).

Exercice 1. Calculons le reste de 7^8 divisé par 6 i.e on cherche $0 \leq x < 6$ tel que $7^8 \equiv x$ [6]. Modulo 6, on a :

$$7^8 \equiv (7^2)^4 \equiv (49)^4 \equiv (6 \times 8 + 1)^4 \equiv (1)^4 \equiv 1.$$

Le reste est donc 1.

Calculons le reste de 3^{15} divisé par 11. Modulo 11, on a

$$\begin{aligned} 3^{15} \equiv (3^3)^5 = (27)^5 \equiv (2 \times 11 + 5)^5 \equiv 5^5 \equiv (5^2)^2 \times 5 \equiv (25)^2 \times 5 \equiv (2 \times 11 + 3)^2 \times 5 \\ \equiv 3^2 \times 5 \equiv 9 \times 5 \equiv 45 \equiv 4 \times 11 + 1 \equiv 1. \end{aligned}$$

Le reste est donc 1. (On n'a pas besoin de calculer explicitement la puissance).

Exercice 2. Montrons que $2x + 9y \equiv 0$ [8] implique $10x - 3y \equiv 0$ [8]. On a (modulo 8) $2x \equiv -9y$ donc $5 \times 2x \equiv -5 \times 9y \equiv -45y \equiv (-6 \times 8 + 3)y \equiv 3y$. Ainsi $10x \equiv 3y$ et donc $10x - 3y \equiv 0$ [8].

Exercice 3. Trouvrons tous les entiers y tels que $2y \equiv 5$ [7]. On calcule $pgcd(2, 7) = 1$. Ainsi 2 et 7 sont premiers entre eux et que $7 = 3 \times 2 + 1$. Ainsi $(1) \times 7 + (-3) \times 2 = 1$. Ce qui donne $(-3) \times 2 \equiv 1$ [7]. On pose $x_0 = -3$ alors $2 \times x_0 \equiv 1$ [7]. En multipliant par 5: $2 \times (5x_0) \equiv 5$ [7]. Ainsi une solution particulière de $2y \equiv 5$ [7] est $y_0 = 5x_0 = -15$. Pour trouver toutes les solutions de $2y \equiv 5$ [7], on "retranche" la solution particulière y_0 ainsi $2(y - y_0) \equiv 5 - 5 \equiv 0$ [7]. Ce qui équivaut à: 7 divise $2(y - y_0)$. Puisque 2 et 7 sont premiers entre eux, on a par le lemme de Gauss, que 7 divise $(y - y_0)$ i.e. il existe $k \in \mathbb{Z}$ tel que $y - y_0 = 7k$. On conclut que $y = y_0 + 7k = -15 + 7k$ avec $k \in \mathbb{Z}$. Réciproquement, on vérifie que tout y de la forme $y = -15 + 7k$ avec $k \in \mathbb{Z}$ vérifie aussi $2y \equiv 5$ [7]. L'ensemble des solutions S est égal à $S = \{-15 + 7k, k \in \mathbb{Z}\}$.

Exercice 4. Trouvons tous les entiers y tels que $3y \equiv 12$ [33]. On calcule $pgcd(3, 33) = 3$. L'équation $3y \equiv 12$ [33] équivaut à $\frac{3}{3}y \equiv \frac{12}{3}$ $[\frac{33}{3}]$ (Voir cours) i.e. $y \equiv 4$ [11]. Ainsi $y = 11k + 4$ avec $k \in \mathbb{Z}$. L'ensemble des solutions S est égal à $S = \{11k + 4, k \in \mathbb{Z}\}$.

Exercice 5. Trouvons tous les entiers x tels que

$$\begin{cases} x \equiv 3 \ [11] \\ x \equiv 5 \ [7]. \end{cases}$$

On commence par chercher une solution particulière x_0 du système à résoudre. On suit la méthode du cours à la lettre. On a $pgcd(11, 7) = 1$. Par Bezout, $1 = (2) \times 11 + (-3) \times 7$. On pose $x_0 = (2) \times 5 \times 11 + 3 \times (-3) \times 7 = 47$ (Attention à bien placer le 3 et le 5: voir cours). On vérifira toujours explicitement que x_0 est une solution particulière. En effet, on a modulo 11, $x_0 \equiv 3 \times [(-3) \times 7] \equiv 3[1 - 2 \times 11] \equiv 3 - 3 \times (2) \times 11 \equiv 3$. Et modulo 7, on a :

$x_0 \equiv (2) \times 5 \times 11 \equiv 5[1-(-3) \times 7 \equiv 5 - 5 \times (-3) \times 7] \equiv 5.$

On a que

$$\begin{cases} x \equiv x_0 \equiv 3\ [11] \\ x \equiv x_0 \equiv 5\ [7]. \end{cases}$$

Ainsi par différence,

$$\begin{cases} x - x_0 \equiv 0\ [11] \\ x - x_0 \equiv 0\ [7]. \end{cases}$$

Ainsi $x - x_0$ est multiple de 11 et 7. Puisque 11 et 7 sont premiers entre eux alors $x - x_0$ est multiple de $11 \times 7 = 77$. D'où $x = x_0 + 77k = 47 + 77k$ pour un $k \in \mathbb{Z}$. Réciproquement, tous les x de la forme $x = 47 + 77k$ pour un $k \in \mathbb{Z}$ sont solutions. L'ensemble des solutions est $S = \{47 + 77k, k \in \mathbb{Z}\}$.

Exercice 6. a) Montrons que 223 est un nombre premier. Il suffit de voir si les nombres premiers $\leq \sqrt{225} = 15$ (i.e. $3, 5, 7, 11, 13$) divise 223. On vérifie facilement que non. Donc 223 est premier.

b) Calculons 1998^{1998} modulo 223. On ne calcule évidemment pas 1998^{1998} explicitement. On utilise le corollaire de Fermat pour tout $x \in \mathbb{N}$, $x^{p-1} \equiv 1\ [p]$ pour p premier et x non divisible par p.
On en déduit $1998^{222} \equiv 1\ [223]$. On effectue la division euclidienne de 1998 par 222, on a $1988 = 9 \times 222$. Ainsi modulo 223, on a $1998^{1998} \equiv ((1998)^{222})^9 \equiv (1)^9 \equiv 1$.

Exercice 7. Trouver tous les entiers x tels que

$$\begin{cases} x \equiv -1\ [8] \\ x \equiv 7\ [13]. \end{cases}$$

Exercice 8. a) Factorisons 455 en produit de nombres premiers. On a $455 = 5 \times 91 = 5 \times 7 \times 13$.

b) Soient a et n des entiers naturels. Montrons que l'on a $a^n \equiv 1\ [455]$ si et seulement si $a^n \equiv 1\ [5]$, $a^n \equiv 1\ [7]$ et $a^n \equiv 1\ [13]$.

Supposons que $a^n \equiv 1\ [455]$ i.e. $a^n - 1$ est multiple de 455 alors $a^n - 1$ est multiple de 5, de 7 et de 13 d'après a). Réciproquement, supposons $a^n \equiv 1\ [5]$, $a^n \equiv 1\ [7]$ et $a^n \equiv 1\ [13]$ i.e. $a^n - 1$ est multiple de 5, de 7 et de 13. Alors $a^n - 1 = 5q_1$ pour $q_1 \in \mathbb{N}$. Puisque 7 divise $a^n - 1$ i.e. $5q_1$ et que 5 et 7 sont premiers entre eux alors par le lemme de Gauss, 7 divise q_1 i.e. $q_1 = 7q_2$ avec $q_2 \in \mathbb{N}$. Donc $a^n - 1 = 5 \times 7 \times q_2$. Puisque 13 est premier avec 5×7 et que 13 divise $a^n - 1$ alors par le lemme de Gauss, 13 divise q_2 i.e. $q_2 = 13q_3$ avec $q_3 \in \mathbb{N}$. Ainsi $a^n - 1 = 5 \times 7 \times 13q_3 = 455q_3$. Donc $a^n - 1$ est bien multiple de 455 i.e. $a^n \equiv 1\ [455]$.

c) Soit a un entier tel que $pgcd(a, 455) = 1$. Montrons que l'on a $a^{12} \equiv 1\ [455]$. Ceci est équivalent à montrer que $a^{12} \equiv 1\ [5]$, $a^{12} \equiv 1\ [7]$ et $a^{12} \equiv 1\ [13]$ (avec $n = 12$).

Puisque $pgcd(a, 455) = 1$ implique $pgcd(a, 5) = 1$, $pgcd(a, 7) = 1$ et $pgcd(a, 13) = 1$. Par le corollaire de Fermat, $a^4 \equiv 1$ [5] donc $a^{12} \equiv (a^4)^3 \equiv 1$ [5] et $a^6 \equiv 1$ [7] donc $a^{12} \equiv (a^6)^2 \equiv 1$ [7]. puis $a^{12} \equiv 1$ [13]. Ce qui donne le résultat.

Exercice 9. Soient p un nombre premier et a un entier positif non multiple de p.

a) Montrons qu'il existe un plus petit entier positif k tel que $a^k \equiv 1$ [p]. D'aprés le corollaire de Fermat $a^{p_1} \equiv 1$ [p]. L'ensemble de $\ell \in \mathbb{N}^*$ vérifiant $a^\ell \equiv 1$ [p] n'est pas vide puisqu'il contient $p-1$. Cet ensemble est non vide et minoré donc il existe un plus petit entier $k \geq 1$ tel que $a^k \equiv 1$ [p].

Soit $n \in \mathbb{N}$. Notons r le reste de la division euclidienne de n par k.

b) Montrons que l'on a $a^n \equiv 1$ [p] si et seulement si n est multiple de k. Supposons que $a^n \equiv 1$ [p]. Avec $n = qk + r$, on obtient $a^n \equiv (a^k)^q a^r \equiv a^r$ [p] car $a^k \equiv 1$ [p]. Ainsi $0 \leq r < k$ vérifie $a^r \equiv 1$ [p]. donc $r = 0$ sinon $1 \leq r$ serait plus petit que k (contradiction).

c) Soit $p = 5$ et $a = 4$. Vérifions que $a^4 \equiv 4^4 \equiv (16^2) \equiv (15+1)^2 \equiv 1^2 \equiv 1$ [5]. Cherchons le plus petit entier k tel que $4^k \equiv 1$ [5]. On a $4^1 \equiv 4$ [5] et $4^2 \equiv 15+1 \equiv 1$ [5] ainsi $k = 2$. Notons que $k < (p-1)$ ici.

Exercice 10. a) Soit $a \in \mathbb{Z}$. Montrons que a^2 est congru à 0, 1 ou 4 modulo 8.
On a $a \equiv x$ [8] pour $0 \leq x < 8$. On fait la liste des cas:
Si $a \equiv 0; [8]$ alors $a^2 \equiv 0; [8]$.
Si $a \equiv 1; [8]$ alors $a^2 \equiv 1; [8]$.
Si $a \equiv 2; [8]$ alors $a^2 \equiv 4; [8]$.
Si $a \equiv 3; [8]$ alors $a^2 \equiv 9 \equiv 1; [8]$.
Si $a \equiv 4; [8]$ alors $a^2 \equiv 16 \equiv 0; [8]$.
Si $a \equiv 5; [8]$ alors $a^2 \equiv 25 \equiv 24 + 1 \equiv 1; [8]$.
Si $a \equiv 6; [8]$ alors $a^2 \equiv 36 \equiv 32 + 4 \equiv 4; [8]$.
Si $a \equiv 7; [8]$ alors $a^2 \equiv 49 \equiv 48 + 1 \equiv 1; [8]$.

b) Soit n un entier positif. Montrons que $a^2 + b^2 + c^2 \neq 8n - 1$, pour tous $a, b, c \in \mathbb{Z}$. On interpréte cette dernière équation dans le language de la congruence: $a^2 + b^2 + c^2$ n'est pas congru à -1 modulo 8 ou encore $a^2 + b^2 + c^2$ n'est pas congru à $8 - 1 = 7$ modulo 8.

On considère tous les cas posssibles (27 cas) en considérant a^2 est congru à 0 ou 1 ou 4 modulo 8 et b^2 est congru à 0 ou 1 ou 4 modulo 8 et c^2 est congru à 0 ou 1 ou 4 modulo 8.

Par exemple, a^2 est congru à 4, b^2 est congru à 1 et c^2 est congru à 1 ainsi $a^2+b^2+c^2$ est congru à $4 + 1 + 4 = 9$ i.e. à 1 modulo 8. (Les autres cas sont laissés à faire).

Exercice 11. a) Factorisons 1729 en produit de nombres premiers. On teste les diviseurs premiers $\leq 41 \leq \sqrt{1729}$. $1729 = 7 \times 13 \times 19$.

b) Soient a et n des entiers positifs. Montrons que l'on a $a^n \equiv 1\ [1729]$ si et seulement si $a^n \equiv 1\ [7]$, $a^n \equiv 1\ [13]$ et $a^n \equiv 1\ [19]$.

La preuve est analogue à celle de l'exo. 8. L'argument principal est le fait que les nombres $7, 13, 19$ sont des nombrers premiers.

c) Soit a un entier positif tel que $pgcd(a, 1729) = 1$. Démontrer que l'on a $a^{1728} \equiv 1\ [1729]$. La preuve est analogue à celle de l'exo. 8.

Exercice 12. Trouvons tous les entiers x tels que

$$\begin{cases} 7x \equiv 5\ [19] \\ 3x \equiv 1\ [11]. \end{cases}$$

Solutions: Le système équivaut à

$$\begin{cases} 3 \times 7x \equiv 3 \times 5\ [3 \times 19] \\ 7 \times 3x \equiv 7 \times 1\ [7 \times 11]. \end{cases}$$

i.e.

$$\begin{cases} 21x \equiv 15\ [57] \\ 21x \equiv 7\ [77]. \end{cases}$$

On pose $y = 21x$ et on résoud

$$\begin{cases} y \equiv 15\ [57] \\ y \equiv 7\ [77]. \end{cases}$$

On applique la méthode du cours (voir aussi l'exercice 7). On a $pgcd(57, 77) = 1$ car par Bezout $1 = (20) \times 77 + (-27) \times 57$. Un solution particulière $y_0 = (20) \times 15 \times 77 + (-27) \times 7 \times 57 = 12327$ (Attention où on place 15 et 7). La solution générale y satisfait

$$\begin{cases} y - y_0 \equiv 0\ [57] \\ y - y_0 \equiv 0\ [77]. \end{cases}$$

qui équivaut à

$$y - y_0 \equiv 0\ [57 \times 77]$$

car 57 et 77 sont premiers entre eux. D'où l'ensemble de solutions S' pour y,
$S' = \{y = 12327 + 4389k, k \in \mathbb{Z}\}$. On en déduit l'ensemble de solutions S pour x,
$S = \{x = 587 + 209k, k \in \mathbb{Z}\}$ (car $x = y/21$).

$\triangle$