MT 282
11/09/96

Université Paris 7
U.F.R. de Mathématiques
B. Keller

Un corrigé de l'examen du 11.09.96

1) Soit x le montant du chèque de tante Emilie. D'après les informations fournies, nous avons

$$\begin{aligned} x &\equiv 15 \ (29) \\ x &\equiv 11 \ (99) \\ x &\equiv 53 \ (79). \end{aligned}$$

Les nombres $29, 99, 79$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution x dont la classe modulo $29 \times 99 \times 79 = 226809$ est unique. Pour trouver x, nous déterminons d'abord x_1, x_2, x_3 dont les classes sont les images réciproques de $(1,0,0), (0,1,0), (0,0,1)$ par la projection

$$\mathbf{Z}/226809 \xrightarrow{\sim} \mathbf{Z}/29 \oplus \mathbf{Z}/99 \oplus \mathbf{Z}/79.$$

Nous avons

$7821\,u_1 + 29\,v_1 = 1;$	sol. part.	$7821 \times (-13) + 29 \times 3506 = 1.$	Posons	$x_1 = -101673.$
$2291\,u_2 + 99\,v_2 = 1;$	sol. part.	$2291 \times (-7) + 99 \times 162 = 1.$	Posons	$x_2 = -16037.$
$2871\,u_3 + 79\,v_3 = 1;$	sol. part.	$2871 \times (-38) + 79 \times 1381 = 1$	Posons	$x_3 = -109098.$

Nous avons donc $x \equiv 15 \times (-101673) + 11 \times (-16037) + 53 \times (-109098) \equiv 1001 \ (226809)$. On a donc $x = 1001 + k \times 226809$. Puisque $x \leq 10000$, il s'ensuit que $x = 1001$. *Le montant du chèque était de* 1001 *francs.*

2) a) Nous avons $311 \equiv 3 \ (7)$ et $1000 \equiv -1 \ (7)$. Donc

$$\begin{aligned} a &= 311 + 1000 \times 311 + \cdots + 1000^n \times 311 \\ &\equiv 3 + (-1) \times 3 + \cdots + (-1)^n \times 3 \quad (7) \\ &\equiv \begin{cases} 0 & \text{si } n \text{ est pair} \\ 3 & \text{si } n \text{ est impair} \end{cases} \end{aligned}$$

Donc le reste est $r = 0$ si n est pair et $r = 3$ si n est impair.

b) Le nombre $b = 863$ est premier. D'après le petit théorème de Fermat, nous avons donc $a = 541^{b-1} \equiv 1 \ (b)$. Donc le reste est $r = 1$.

c) Nous avons la décomposition en facteurs premiers $561 = 3 \times 11 \times 17$. Pour l'indicatrice de Carmichael $\lambda(561)$, nous trouvons donc $\lambda(561) = \mathrm{PPCM}\,(2, 10, 16) = 80$. Comme 19 est premier avec 561, nous pouvons appliquer le lemme de Carmichael pour conclure que $19^{80} \equiv 1 \ (561)$. Le reste r vaut donc 1.

d) D'après le petit théorème de Fermat, le reste de $2^{a'}$ modulo 13 ne dépend que de la classe de a' modulo 12. Or, nous avons $5^2 \equiv 1 \ (12)$ et ainsi, la classe de a' modulo 12 ne dépend que de la classe de 7^{11} modulo 2. Or, $7 \equiv 1 \ (2)$ de façon que $7^{11} \equiv 1 \ (2)$. Donc $a' \equiv 5 \ (12)$ et $a \equiv 2^5 \equiv 6 \ (13)$. Finalement, nous trouvons $r = 6$.

3) a) Par récurrence, on voit que

$$x_n = b\,(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Si $a \not\equiv 1 \ (p)$, alors en particulier, nous avons $a \neq 1$ et

$$x_n = b\,\frac{a^n - 1}{a - 1}$$

Dans ce cas, comme p ne divise pas $a - 1$, le nombre x_n est divisible par p ssi le nombre $b\ (a^n - 1)$ est divisible par p. D'après le petit théorème de Fermat, c'est le cas si n est

multiple de $p-1$. Par contre, si $a \equiv 1\ (p)$, nous avons $x_n \equiv nb\ (p)$ et alors x_n est divisible par p ssi n ou b est divisible par p.

b) Si $b \equiv 0\ (p)$, alors p divise x_n pour tout $n \in \mathbf{N}$. Supposons donc que $b \not\equiv 0\ (p)$. Alors, si $a \not\equiv 1\ (p)$, le nombre x_n est divisible par p si et seulement si n divise l'ordre de $\overline{a}$ dans le groupe $(\mathbf{Z}/p\mathbf{Z})^*$. Finalement, si $a \equiv 1\ (p)$, alors p divise x_n si et seulement si p divise n.

4) a) Si p divise y, alors p divise $x^2 = pz^2 - y^2$. Donc p divise x. Ainsi, p^2 divise $pz^2 = x^2 + y^2$ et p doit diviser z. Donc x, y et z sont divisibles par p. Clairement, le triplet $(x/p, y/p, z/p)$ est encore une solution de l'équation $(*)$. Par récurrence on trouve que si p^k divise y, alors p^k divise x et z et $(x/p^k, y/p^k, z/p^k)$ est encore une solution de l'équation $(*)$. En choisissant pour p^k la plus grande puissance de p qui divise y, on construit ainsi une nouvelle solution (x', y', z') telle que p ne divise pas y'.

b) L'équation $(*)$ donne la congruence $x^2 + y^2 \equiv 0\ (p)$. Comme p ne divise pas y, la classe de y modulo p est inversible. Supposons que la classe de y' est son inverse. En multipliant la congruence par y'^2, nous obtenons $(xy')^2 + 1 \equiv 0\ (p)$. Ainsi, la congruence $u^2 + 1 \equiv 0\ (p)$ admet la solution $u = xy'$.

c) D'après b), -1 est un résidu quadratique modulo p, nombre premier impair. On sait que -1 est résidu quadratique modulo p ssi p est congru à 1 modulo 4. D'où l'affirmation.

5) a) Une condition nécessaire est que

$$(\frac{a}{p}) = 1$$

(symbole de Legendre). La démonstration est analogue à celle de 4).

b) Une condition nécessaire est que

$$(\frac{7}{p}) = 1$$

D'après la réciprocité quadratique, si $p \equiv 1\ (4)$, nous avons

$$(\frac{7}{p}) = (\frac{p}{7})$$

ce qui vaut 1 seulement si p est un carré modulo 7, c'est-à-dire que $p \equiv 1, 2, 4\ (7)$. Nous arrivons au système

$$\begin{aligned} p &\equiv 1\ (4) \\ p &\equiv x\ (7) \quad \text{où } x = 1, 2, 4. \end{aligned}$$

Ceci nous donne $p \equiv 1, 9, -3\ (28)$.

Par contre, si $p \equiv -1\ (4)$, nous avons

$$(\frac{7}{p}) = -(\frac{p}{7})$$

ce qui vaut 1 seulement si p est un non carré modulo 7, c'est-à-dire que $p \equiv 1, 2, 4\ (7)$. Nous arrivons au système

$$\begin{aligned} p &\equiv 1\ (4) \\ p &\equiv x\ (7) \quad \text{où } x = 3, 5, 6. \end{aligned}$$

Ceci nous donne $p \equiv 3, -9, 13\ (28)$.

En conclusion, d'après a), l'équation ne peut admettre de solutions non-triviales que si $p \equiv 1, \pm 3, \pm 9$ ou 13 modulo 28.