MT 282
17/01/96

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

Un corrigé du 2^e examen partiel

1) Les nombres $13, 15, 17$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution x dont la classe modulo $13 \times 15 \times 17 = 3315$ 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

$$\mathbf{Z}/3315 \xrightarrow{\sim} \mathbf{Z}/13 \oplus \mathbf{Z}/15 \oplus \mathbf{Z}/17.$$

Nous avons

$$\begin{array}{llll} 255\,u_1 + 13\,v_1 = 1; & \text{sol. part.} & 255 \times 5 + 13 \times -98 = 1. & \text{Posons} \quad x_1 = 1275. \\ 221\,u_2 + 15\,v_2 = 1; & \text{sol. part.} & 221 \times (-4) + 15 \times 59 = 1. & \text{Posons} \quad x_2 = -884. \\ 195\,u_3 + 17\,v_3 = 1; & \text{sol. part.} & 195 \times (-2) + 17 \times 23 = 1 & \text{Posons} \quad x_3 = -390. \end{array}$$

Nous avons donc $x \equiv 11 \times 1275 + 5 \times (-884) + 11 \times (-390) \equiv 5315 \equiv 2000 \ (3315)$.

2) a) D'après le lemme chinois (appliqué à $15 = 3 \times 5$ et $35 = 5 \times 7$), le système donné est équivalent à

$$\begin{aligned} x &\equiv a \ (3) \\ x &\equiv a \ (5) \\ x &\equiv b \ (5) \\ x &\equiv b \ (7) \end{aligned}$$

Ce dernier système est contradictoire, sauf si $a \equiv b \ (5)$. Si cette condition est remplie, le système est équivalent au système

$$\begin{aligned} x &\equiv a \ (3) \\ x &\equiv a \ (5) \\ x &\equiv b \ (7) \end{aligned}$$

qui admet une solution puisque $3, 5, 7$ sont premiers entre eux deux à deux. En conclusion, *le système admet une solution si et seulement si* $a \equiv b \ (5)$.

b) Si les conditions sont remplies, le dernier système est équivalent à

$$\begin{aligned} x &\equiv a \ (15) \\ x &\equiv b \ (7) \end{aligned}$$

L'équation de Bézout $15 - 2 \times 7 = 1$ montre que

$$x \equiv -14\,a + 15b \ (105).$$

3) a) On a $2^4 \equiv -1 \ (17)$ et donc $2^8 \equiv 1 \ (17)$. Ainsi,

$$a = \sum_{k=0}^{999} 2^k = 2^{1000} - 1 \equiv 1 - 1 \equiv 0 \ (17).$$

Donc $r = 0$.

b) Le nombre $p = 113$ est premier. Par le petit théorème de Fermat, il s'ensuit que $r = 1$.

c) Nous avons $b = 323 = 17 \times 19$ et donc $\phi(b) = \phi(17)\,\phi(19) = 16 \times 18 = 288$. Ainsi, nous avons $243^{288} \equiv 1 \ (323)$ d'après le théorème d'Euler. D'où $243^{289} \equiv 243 \ (323)$ et $r = 243$.

d) Nous avons $b = 25 \times 13$. D'après le lemme chinois, il suffit de déterminer les restes de r modulo 25 et 13. Puisque

$$\begin{aligned} 80 &\equiv 5 \ (25) \\ 80 &\equiv 2 \ (13) \end{aligned}$$

il s'ensuit que

$$\begin{aligned} 80^{206} &\equiv 0 \ (25) \\ 80^{206} &\equiv 2^{206} \ (13). \end{aligned}$$

(Pour la première congruence, nous avons utilisé que $5^2 \equiv 0 \ (25)$). D'après le petit théorème de Fermat, nous avons $2^{12} \equiv 1 \ (13)$. Puisque $206 \equiv 2 \ (12)$, il s'ensuit que $2^{206} \equiv 2^2 \ (13)$. Donc

$$\begin{aligned} a &\equiv 0 \ (25) \\ a &\equiv 4 \ (13) \end{aligned}$$

Par l'équation de Bézout $-25 + 2 \times 13 = 1$, nous trouvons que

$$a \equiv 4 \times (-25) \equiv -100 \equiv 225 \ (325).$$

Donc $r = 225$.

4) a) Si k ou l contient un facteur carré, alors kl contient un facteur carré et les deux côtés s'annulent. Si $k = 1$ ou $l = 1$, l'affirmation est triviale. Finalement, si $k = p_1 \dots p_r$ et $l = q_1 \dots q_s$ où les p_i et les q_j sont des nombres premiers distincts, alors

$$kl = p_1 \dots p_r q_1 \dots q_s$$

où tous les facteurs sont distincts (car k et l sont premiers entre eux). Donc $\mu(kl) = (-1)^{r+s} = \mu(k)\,\mu(l)$.

b) Soit $s(n) = \sum_{d|n} \mu(d)$ et $p_1, \dots, p_r$ les facteurs premiers (sans répétition) de n. On a $s(n) = s(p_1 \dots p_r)$, car les diviseurs qui contiennent une puissance > 1 d'un p_i ne contribuent pas à $s(n)$. On peut donc supposer que $n = p_1 \dots p_r$. Soit D l'ensemble des diviseurs de $p_2 \dots p_n$. Alors nous avons clairement

$$s(n) = \sum_{d \in D} \mu(d) + \sum_{d \in D} \mu(p_1 d).$$

Or par la multiplicativité de μ, nous avons $\mu(p_1 d) = \mu(p_1)\mu(d) = -\mu(d)$ pour tout $d \in D$, car p_1 est premier avec $p_2 \dots p_r$. D'où $s(n) = 0$.

c) Nous avons

$$\begin{aligned} \sum_{d|n} \mu(\frac{n}{d})\, g(d) &= \sum_{d|n} \mu(\frac{n}{d})\, (\sum_{d'|d} f(d')) = \sum_{d'|d|n} \mu(\frac{n}{d})\, f(d') = \sum_{d'd''|n} \mu(d') f(d'') \\ &= \sum_{d''|n} f(d'') \sum_{d'|n/d''} \mu(d') = f(n) + \sum_{d''|n, d''<n} f(d'') \sum_{d'|n/d''} \mu(d') \\ &= f(n)\,, \end{aligned}$$

où nous avons utilisé b) pour la dernière égalité.

d) Nous savons que

$$n = \sum_{d|n} \phi(d).$$

Si nous appliquons c) à la fonction $f(n) = \phi(n)$, nous trouvons donc

$$g(n) = n$$

et par conséquent

$$\phi(n) = f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d) = \sum_{d|n} \mu(\frac{n}{d}) d.$$