UNIVERSITÉ DE RENNES 1

UFR DE MATHÉMATIQUES

Licence – portail MIPE

NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES, PERMUTATIONS (*A2*)

Examen du 16 décembre 2004 (2 heures)

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits.
Vous pouvez utiliser les résultats du cours sans les redémontrer.

PROBLÈME

1 Énoncer le théorème de décomposition en facteurs premiers.

2 Décomposer 187 en facteurs premiers.

3 Combien y a-t-il d'entiers compris entre 1 et 187 qui sont premiers avec 187 ?
Quels sont les 3 plus petits entiers strictement positifs qui ne sont pas premiers avec 187 ?

4 Dire si les assertions suivantes sont vraies ou fausses. Justifier chaque réponse par une démonstration si l'assertion est juste ou un contre-exemple si elle est fausse.

a) Pour tout entier x, $x^{186} \equiv 1 \pmod{187}$.
b) Pour tout entier x, $x^{187} \equiv x \pmod{187}$.
c) Pour tout entier x premier à 187, $x^{160} \equiv 1 \pmod{187}$.
d) Pour tout entier x premier à 187, $x^{187} \equiv x \pmod{187}$.
e) Pour tout entier x, $x^{161} \equiv x \pmod{187}$.

5 Soit a un entier relatif ; montrer qu'il existe un unique entier relatif x tel que $|x| \leqslant 93$ et $x \equiv a \pmod{187}$.

6 Trouver tous les entiers x tels que $|x| \leqslant 100$ et $7x \equiv 11 \pmod{187}$. (On commencera par montrer qu'un tel entier x est multiple de 11, puis on posera $x = 11y$.)

7 Soit (x_n) la suite définie par récurrence par $x_1 = 2$ et $x_{n+1} = -x_n(1 + 2x_n^2)$. Montrer par récurrence que pour tout $n \geqslant 1$, $x_n^2 \equiv -1 \pmod{5^n}$. (On pourra introduire l'entier u tel que $x_n^2 + 1 = 5^n u$.)

Veuillez rédiger les questions suivantes sur une nouvelle feuille.

8 Démontrer que 691 est un nombre premier.

9 Écrire l'entier 691 en base 7.

10 Existe-t-il une base $b > 5$ dans laquelle $\overline{2004}^{(b)}$ représente un nombre premier ?

11 Soit n un entier $\geqslant 1$. Calculer le dernier chiffre du développement décimal de 3^n. (Distinguer suivant le reste de la division euclidienne de n par 4.) Calculer le dernier chiffre du développement décimal de 3^{3^3}.

12 Soit A l'ensemble $\{0, 1, \ldots, 9\}$. Soit f l'application de A dans lui-même qui associe à x le dernier chiffre de $7x$. Montrer que f est une permutation de A. Calculer ses orbites et sa décomposition en cycles. Quelle est sa signature ?

13 Soit p un nombre premier. Si $1 \leqslant k \leqslant p-1$, démontrer que le coefficient binomial $\binom{p}{k}$ est multiple de p.
Soit a et b des entiers tels que $a \equiv b \pmod{p}$. Montrer que $a^p \equiv b^p \pmod{p^2}$.

14 Démontrer, pour tout entier relatif a, la congruence $a^{13} \equiv a \pmod{2730}$. (Commencer par décomposer 2730 en facteurs premiers.)

NOMBRES ENTIERS ET RATIONNELS,
CONGRUENCES, PERMUTATIONS (*A2*)
Corrigé de l'examen du 16 décembre 2004 (2 heures)
Sujet proposé (et corrigé) par A. Chambert-Loir

SOLUTION DU PROBLÈME.

1 Soit n un entier >1. Il existe un entier $r \geqslant 1$ et des nombres premiers $p_1, \dots, p_r$ vérifiant $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$ tels que $n = p_1 \dots p_r$. Il y a de plus unicité : si $s \geqslant 1$ et si $q_1 \leqslant \cdots \leqslant q_s$ sont des nombres premiers tels que $n = q_1 \dots q_s$, on a $r = s$ et $p_i = q_i$ pour tout i.

2 On a $187 = 11 \times 17$.

3 On a $\varphi(187) = 160$ (cf. le cours sur RSA), donc il y a $187 - 160$ entiers compris entre 1 et 187 qui ne sont pas premiers avec 187.
On peut le redémontrer. Les entiers qui ne sont pas premiers avec 187 sont ceux qui sont multiples de 11 ou de 17. Entre 1 et 187, il y a 17 multiples de 11, 11 multiples de 17, et 187 qui est multiple à la fois de l'un et de l'autre. Parmi les entiers compris entre 1 et 187, exactement 27 ne sont pas premiers à 187.
Les trois plus petits sont 11, 17 et 22.

4

a) Fausse pour $x = 0$.

b) Fausse pour $x = 2$. En effet, comme 2 est premier à 11, on a $2^{10} = 1 \pmod{11}$. D'où $2^{180} = 1 \pmod{11}$ et

$$2^{187} \equiv 2^7 \equiv 4 \times 32 \equiv 4 \times (-1) \equiv -4 \pmod{11},$$

donc $2^{187} \not\equiv 1 \pmod{11}$. Comme 11 divise 187, a fortiori, $2^{187} \not\equiv 1 \pmod{187}$.

c) Vrai, c'est le théorème d'Euler (on a $\varphi(187) = 160$).

d) Faux, $x = 2$ est encore un contre exemple.

e) Vrai, c'est démontré dans le cours sur RSA, car $187 = 11 \times 17$ est le produit de deux nombres premiers distincts.

5 Notons que la condition $x \equiv a \pmod{187}$ s'écrit aussi « il existe $k \in \mathbf{Z}$ tel que $a = 187k + x$ ».
Montrons d'abord l'unicité : si $a = 187k + x = 187k' + x'$, avec k et $k' \in \mathbf{Z}$ et $a, a' \in \mathbf{Z}$ de valeurs absolues $\leqslant 93$, $x - x' = 187(k' - k)$ est multiple de 187. Mais on a aussi $\left|x - x'\right| \leqslant |x| + |x|' \leqslant 2 \times 93 = 186$. Le seul multiple de 187 qui soit inférieur à 186 en valeur absolue est 0, donc $x = x'$.
Montrons maintenant l'existence. Soit $a = 187q + r$ la division euclidienne de a par 187. Si $r \leqslant 93$, on pose $x = r$; si $r > 93$, on écrit $a = 187(q+1) + (r - 187)$ et on remarque que l'on a $-94 < r - 187 < 0$. Comme $r - 187$ est un entier, on a $-93 \leqslant r - 187 \leqslant -1$, d'où $|r - 187| \leqslant 93$ et $x = r - 187$ convient dans ce cas.

6 D'après le théorème chinois, la congruence $7x = 11 \pmod{187}$ équivaut à la conjonction des deux congruences $7x = 11 \pmod{11}$ et $7x = 11 \pmod{17}$.

Si $7x = 11 \pmod{187}$, on a en particulier $7x = 11 = 0 \pmod{11}$; autrement dit $7x$ est multiple de 11. Comme 7 et 11 sont premiers entre eux, il résulte du lemme de Gauss que x est multiple de 11. On peut donc écrire $x = 11y$.
Les deux congruences mod. 11 et 17 s'écrivent alors $7 \times 11y = 11 \pmod{11}$, toujours vérifiée, et $7 \times 11y = 11 \pmod{17}$, qui équivaut à $7y = 1 \pmod{17}$ puisque 7 et 17 sont premiers entre eux. Pour déterminer un inverse de 7 modulo 17, on peut utiliser l'algorithme d'Euclide étendu, ou remarquer que $5 \times 7 = 35 = 2 \times 17 + 1$. En multipliant la relation $7y = 1 \pmod{17}$ par 5 on trouve ainsi $y \equiv 5 \pmod{17}$. Finalement, il existe $z \in \mathbf{Z}$ tel que $y = 5 + 17z$, puis $x = 55 + 187z$.
Inversement tous les entiers x de la forme $55+187z$, avec $z \in \mathbf{Z}$ vérifient la congruence $7x = 11 \pmod{187}$. On ne s'intéresse qu'à ceux dont la valeur absolue est $\leqslant 100$. L'inégalité $55+187z \leqslant 100$ implique $z \leqslant 0$; l'inégalité $55 + 187z \geqslant -100$ entraîne $187z \geqslant -155$, donc $z \geqslant 0$.
L'unique solution est $x = 55$.

7 On a $x_1^2 = 4 = -1 \pmod{5}$. Supposons que l'on ait $x_n^2 \equiv -1 \pmod{5^n}$ (où $n \geqslant 1$) et démontrons que l'on a $x_{n+1}^2 \equiv -1 \pmod{5^{n+1}}$. Soit u l'entier tel que $x_n^2 + 1 = 5^n u$. Alors, $1 + 2x_n^2 = -1 + 2u5^n$, donc

$$\begin{aligned} x_{n+1}^2 &= x_n^2(1 + 2x_n^2)^2 = (-1 + u5^n)(-1 + 2u5^n)^2 \\ &= (-1 + u5^n)(1 - 4u5^n + 4u^2 5^{2n}) = -1 + u5^n + 4u5^n - 4u^2 5^{2n} + (-1 + u5^n)(4u^2 5^{2n}) \\ &\equiv -1 + 5u5^n \pmod{5^{2n}} \equiv -1 \pmod{5^{n+1}}. \end{aligned}$$

Cela démontre l'assertion au rang $n+1$.
Par récurrence, l'assertion est vraie pour tout $n \geqslant 1$.

8 691 n'est pas pair, n'est pas multiple de 3 (somme des chiffres congrue à 1 mod 3), ni de 5. Comme $691 = 700 - 9$, il n'est pas multiple de 7 ; comme $691 = 671 + 20$ et que $671 = 11 \times 7$, il n'est pas multiple de 11. On a $691 = 13 \times 53 + 2$, donc il n'est pas multiple de 13. Il n'est pas non plus multiple de 17 car $691 = 17 \times 40 + 11$, ni de 19 étant donné que $691 = 19 \times 30 + 141 = 19 \times 37 + 8$. Reste 23, mais $69 = 3 \times 23$, donc $691 = 30 \times 23 + 1$, puis 29 mais $29^2 = (30-1)^2 = 841 > 691$. Par suite, 691 n'a aucun facteur premier $< \sqrt{691}$, donc est un nombre premier.

9 On effectue des divisions euclidiennes par 7 : $691 = 7 \times 98 + 5$, $98 = 7 \times 14 = 7^2 \times 2$, donc 691 s'écrit $\overline{2005}^{(7)}$ en base 7.

10 Non car pour toute base b, $\overline{2004}^{(b)} = 2 \times \overline{1002}^{(b)}$.

11 On a $3^2 = 9$, et $3^3 = 27 \equiv 7 \pmod{10}$, et enfin $3^4 = 81 \equiv 1 \pmod{10}$. Soit $n = 4q + r$ la division euclidienne de n par 4 ; on a donc $3^n \equiv 3^r \pmod{10}$. Si $r = 0$, le dernier chiffre de 3^n est 1, si $r = 1$, c'est 3, si $r = 2$ c'est 9 et si $r = 3$ c'est 7.
Comme $3^3 = 27 \equiv 3 \pmod{4}$, le dernier chiffre de 3^{3^3} est 7.

12 Montrons que f est injective. Soit x et y des éléments de A tels que $f(x) = f(y)$ et montrons que $x = y$. Par hypothèse $7x$ et $7y$ ont même dernier chiffre, ce qui signifie que $7(x-y)$ est

multiple de 10. Comme 7 et 10 sont premiers entre eux, $x-y$ est multiple de 10. Comme x et y appartiennent à A, $0 \leqslant x, y \leqslant 9$ et il n'y a pas d'autre possibilité que $x = y$.
D'après un résultat du cours, une application injective d'un ensemble fini dans lui même est bijective. Autrement dit, f est une permutation de A.
On peut calculer f explicitement :

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix}.$$

On voit bien que chaque chiffre arrive une fois et une seule sur la seconde ligne, ce qui confirme que f est une permutation.
L'orbite de 0 est $\{0\}$; l'orbite de 1 est $\{1, 7 = f(1), 9 = f(7), 3 = f(9)\}$; celle de 2 est $\{2, 4 = f(2), 8 = f(4), 6 = f(8)\}$ et celle de 5 est $\{5\}$. La décomposition de f en cycles est ainsi

$$f = (1,7,9,3)(2,4,8,6).$$

Un cycle de longueur paire est de signature -1 ; la signature de f est donc $+1$.

13 On a $\binom{p}{k} = p!/k!(p-k)!$, d'où $k!(p-k)!\binom{p}{k} = p!$. Comme $1 \leqslant k \leqslant p-1$, $k!$ est produit d'entiers qui ne sont pas multiples de p, donc n'est pas multiple de p ; de même, $(p-k)!$ n'est pas multiple de p. Comme le produit $k!(p-k)!\binom{p}{k}$ est multiple de p, le lemme d'Euclide entraîne que $\binom{p}{k}$ est multiple de p.
On écrit $a = b + pn$, avec $n \in \mathbf{Z}$. D'après la formule du binôme, on a

$$a^p = \sum_{k=0}^{p} \binom{p}{k} b^k (pn)^{p-k}.$$

Le terme pour $k = 0$ est $p^p n^p$, donc est multiple de p^2 car $p \geqslant 2$. Si $1 \leqslant k \leqslant p-1$, $p-k \geqslant 1$, donc $(pn)^{p-k}$ est multiple de p, et $\binom{p}{k}$ est multiple de p ; le terme correspondant est multiple de p^2. Enfin, le terme pour $k = p$ vaut b^p. Par suite, a^p est la somme de b^p et d'un multiple de p^2, ce qui montre la congruence voulue.

14 Décomposons 2730 en facteurs premiers ; on a

$$2730 = 2 \times 1365 = 2 \times 3 \times 455 = 2 \times 3 \times 5 \times 91 = 2 \times 3 \times 5 \times 7 \times 13.$$

D'après le théorème chinois, il suffit de montrer la congruence $a^{13} \equiv a \pmod{p}$ pour chacun des nombres premiers $p \in \{2, 3, 5, 7, 13\}$.
Si a est multiple de p, la congruence $a^{13} \equiv a \pmod{p}$ est vérifiée, les deux membres étant congrus à 0 modulo p. Si a n'est pas multiple de p, on sait que $a^{p-1} \equiv 1 \pmod{p}$ (petit théorème de Fermat). Or, 12 est multiple de $p-1$ dans chacun des cas considérés ($12 = 12\times1 = 6 \times 2 = 3 \times 4 = 2 \times 6 = 1 \times 12$), donc $a^{12} \equiv 1 \pmod{p}$, puis $a^{13} \equiv a \pmod{p}$.