UNIVERSITÉ DE RENNES 1

UFR DE MATHÉMATIQUES

Licence – portail MIPE

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

Examen du 2 décembre 2005 (1 heure)

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits.
Justifiez toutes vos réponses

NOM : **Prénom :**

EXERCICE 1

1 Décomposer 120 en facteurs premiers.
2 Montrer que $\varphi(120) = 4 \times 2 \times 4 = 32$.
3 En développant $(2n+1)^4$, montrer que pour tout nombre impair x, $x^4 \equiv 1 \pmod{16}$.
4 Montrer que pour tout entier x qui n'est multiple ni de 2, ni de 3, ni de 5, on a $x^4 \equiv 1 \pmod{120}$.

EXERCICE 2

Soit n un entier naturel. Montrer que $2^n - 1$ est multiple de 7 si et seulement si n est multiple de 3.

EXERCICE 3

On pose $m = 6499$ et $n = 3007$.
1 Calculer le pgcd de m et n, ainsi que leur ppcm.
2 Décomposer m et n en facteurs premiers.

EXERCICE 4

Soit P le polynôme $P(x) = x^3 + x^2 + 3x - 5$.
1 Trouver toutes les racines réelles de P. (Il y a une racine évidente.)
2 Résoudre l'équation $P(x) \equiv 0 \pmod{7}$.
3 Résoudre l'équation $P(x) \equiv 0 \pmod{9}$.
4 Résoudre l'équation $P(x) \equiv 0 \pmod{4}$.
5 Résoudre l'équation $P(x) \equiv 0 \pmod{168}$.

NOMBRES ENTIERS ET RATIONNELS,
CONGRUENCES, PERMUTATIONS (*A2*)
Corrigé de l'examen du 2 décembre 2005 (1 heure)
Sujet proposé (et corrigé) par A. Chambert-Loir

SOLUTION DE L'EXERCICE 1.

1 On a $120 = 2^3 \times 3 \times 5$.

2 Un entier est premier à 120 si et seulement si il n'est multiple ni de 2 ni de 3 ni de 5. Il y a donc 4 restes possibles modulo 8, 2 modulo 3 et 4 modulo 5. D'après le théorème chinois, on a donc $\varphi(120) = 4 \times 2 \times 4 = 32$.

3 D'après la formule du binôme de Newton,

$$(2n+1)^4 = 16n^4+4\times 8n^3+6\times 4n^2+4\times 2n+1 = 16n^4+32n^3+24n^2+8n+1 = 16(n^4+2n^3+n^2)+8(n^2+n)+1.$$

De plus, $n^2+n = n(n+1)$; comme le produit de deux entiers consécutifs est pair (l'un des deux facteurs est pair), n^2+n est pair, donc $8(n^2+n)$ est multiple de 16. Par conséquent,

$$(2n+1)^4 \equiv 1 \pmod{16}.$$

4 Soit x un entier qui n'est multiple ni de 2, ni de 3, ni de 5. Déjà, x est impair, donc $x = 2n+1$ pour un certain n et $x^4 = (2n+1)^4 \equiv 1 \pmod{16}$. De plus, x n'est pas multiple de 3, donc $x^2 \equiv 1 \pmod 3$ en vertu du petit théorème de Fermat. A fortiori, $x^4 \equiv 1 \pmod 3$. Enfin, comme x n'est pas multiple de 5, $x^4 \equiv 1 \pmod 5$. Donc $x^4 - 1$ est multiple de 16, 3 et 5. Comme ces entiers sont premiers entre eux deux à deux, x^4-1 est multiple de leur produit qui vaut 240. Donc $x^4 \equiv 1 \pmod{240}$. Comme 120 divise 240, on a aussi $x^4 \equiv 1 \pmod{120}$.

SOLUTION DE L'EXERCICE 2.

On a $2^0 \equiv 1 \pmod 7$, $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$ et $2^3 = 8 \equiv 1 \pmod 7$. Soit $n = 3q + r$ la division euclidienne de n par 3, avec $0 \leqslant r < 2$. On a donc

$$2^n = 2^{3q}2^r = 8^q 2^r \equiv 1^q 2^r \equiv 2^r \pmod 7.$$

Par conséquent, $2^n \equiv 1 \pmod 7$ si et seulement si $r = 0$, c'est-à-dire si et seulement si n est multiple de 3.

SOLUTION DE L'EXERCICE 3.

1 On a $6499 = 2 \times 3007 + 485$, $3007 = 6 \times 485 + 97$ et $485 = 97 \times 5$. Par conséquent, le pgcd de 6499 et 3007 est égal à 97. Le ppcm de 6499 et 3007 est, quant à lui, égal à

$$\frac{6499 \times 3007}{97} = 6499 \times 31 = 201469.$$

2 On a $6499 = 97 \times 67$ et $3007 = 97 \times 31$. Montrons que 31, 67 et 97 sont des nombres premiers. Il suffit de vérifier qu'ils ne sont divisible par aucun nombre premier inférieur à leur racine carrée, disons par aucun nombre premier inférieur à 10, car $10^2 > 97$; les nombres premiers concernés sont 2, 3, 5 et 7. Déjà, 31 n'est divisible ni par 2, ni par 3 ni par 5, ni par 7. De même, $61 = 2 \times 30 + 1 = 3 \times 20 + 1 = 12 \times 5 + 1 = 7 \times 8 + 5$, donc 61 est premier. Enfin, $97 = 2 \times 48 + 1 = 3 \times 32 + 1 = 5 \times 19 + 2 = 7 \times 14 + 1$, donc 97 est premier. Ce sont les décompositions en facteurs premiers cherchées.

SOLUTION DE L'EXERCICE 4.

1 On a $P(1) = 1 + 1 + 3 - 5 = 0$, donc 1 est racine de P. La division de P par $x - 1$ donne $P(x) = (x - 1)(x^2 + 2x + 5)$. Le discriminant réduit du polynôme de degré 2, $x^2 + 2x + 5$, est égal à $1 - 5 = -4$, donc n'est pas le carré d'un nombre réel. Par conséquent, ce polynôme n'a pas de racine. Cela démontre que 1 est la seule racine réelle de P.

2 Comme 7 est un nombre premier, $P(x) \equiv 0 \pmod 7$ équivaut à $x - 1 \equiv 0 \pmod 7$ ou $x^2 + 2x + 5 \equiv 0 \pmod 7$. Le premier cas donne $x \equiv 1 \pmod 7$. Pour le second, on écrit $x^2 + 2x + 5 = (x+1)^2 + 4$. Si $x^2 + 2x + 5 \equiv 0 \pmod 7$, $(x+1)^2 \equiv -4 \pmod 7$. Or, les carrés modulo 7 sont 0, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$ et $(\pm 3)^2 = 9 \equiv 2$. Donc -4 n'est pas un carré modulo 7.
Les solutions de l'équation $P(x) \equiv 0 \pmod 7$ sont donc les entiers congrus à 1 modulo 7.

3 On commence par résoudre modulo 3. Comme 3 est un nombre premier, on trouve de même $x \equiv 1 \pmod 3$ ou $(x+1)^2 \equiv -4 \equiv 2 \pmod 3$. Les carrés modulo 3 sont 0 et $(\pm 1)^2 = 1$. Donc 2 n'est pas un carré modulo 3. Donc $x \equiv 1 \pmod 3$. On écrit $x = 1 + 3y$, avec $y \in \mathbf{Z}$. On trouve alors

$$P(x) = x^3+x^2+3x-5 = (1+9y+27y^2+27y^3)+(1+6y+9y^2)+3(1+3y)-5 = 21y+36y^2+27y^3 = 9(2y+4y^2+3y^3)+3y.$$

Par suite, $P(x) \equiv 0 \pmod 9$ équivaut à $3y \equiv 0 \pmod 9$, c'est-à-dire $y \equiv 0 \pmod 3$. On écrit ainsi $y = 3z$ et les solutions de l'équation $P(x) \equiv 0 \pmod 9$ sont les entiers $x = 1 + 9z$, avec $z \in \mathbf{Z}$.
Les solutions de l'équation $P(x) \equiv 0 \pmod 9$ sont donc les entiers congrus à 1 modulo 9.

4 On a $P(0) = -5 \equiv 3 \pmod 4$, $P(1) = 0$, $P(2) = 16 + 8 + 6 - 5 \equiv 1 \pmod 4$ et $P(3) = 81 + 27 + 9 - 5 \equiv 0 \pmod 4$. Si r est le reste de la division euclidienne de x par 4, et q le quotient, on a $x \equiv r \pmod 4$ donc $P(x) \equiv P(r) \pmod 4$.
Les solutions de l'équation $P(x) \equiv 0 \pmod 4$ sont ainsi les entiers de la forme $1 + 4k$ ou $3 + 4k$, avec $k \in \mathbf{Z}$, c'est-à-dire les entiers impairs.

5 On a $168 = 2 \times 84 = 8 \times 3 \times 7$. D'après le théorème d'Euclide, $P(x) \equiv 0 \pmod{168}$ si et seulement si $P(x)$ est multiple de 8, 3 et 7.
Étudions la première. Pour que $P(x) \equiv 0 \pmod 4$, il faut et il suffit que x soit impair. Écrivons $x = 2n+1$ et calculons

$$P(x) = (2n+1)^3 + (2n+1)^2 + 3(2n+1) - 5 = 8n^3 + 16n^2 + 16n = 8(n^3 + 2n^2 + 2n).$$

Par suite, $P(x)$ est toujours multiple de 8. La première condition équivaut ainsi à ce que x soit impair, c'est-à-dire $x-1$ multiple de 2.
D'après les questions précédentes, les deux dernières conditions équivalent à ce que $x-1$ soit multiple de 3 et de 7.
Finalement, $P(x)$ est multiple de $8 \times 3 \times 7 = 168$ si et seulement si $x-1$ est multiple de $2 \times 3 \times 7 = 42$.
Autrement dit, $P(x) \equiv 0 \pmod{168}$ si et seulement si $x \equiv 1 \pmod{42}$.