UNIVERSITÉ DE RENNES 1

UFR DE MATHÉMATIQUES

Licence STS — mention mathématiques *Année 2005/2006*

A2. NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES. PERMUTATIONS

Feuille de travaux dirigés n° 4 : *Nombres premiers*

---

1. Généralités

EXERCICE 1

Ce nombre s'écrit avec 8 chiffres en base 2 et 6 chiffres en base 3. Quel est-il ? Ah, j'oubliais, c'est un nombre premier.

EXERCICE 2

1 Si tous les facteurs premiers p d'un entier n vérifient $p \equiv 1 \pmod 4$, montrer que l'on a $n \equiv 1 \pmod 4$.

2 Si $n \geqslant 4$, en déduire qu'au moins un facteur premier de $n! - 1$ est congru à -1 modulo 4, puis qu'il existe une infinité de nombres premiers de la forme $4n+3$.

3 Montrer de même qu'il existe une infinité de nombres premiers de la forme $6n+5$.

EXERCICE 3

1 Montrer qu'aucun des entiers $n!+2, \ldots, n!+n$ n'est un nombre premier.

2 En s'inspirant de la question précédente, montrer qu'il existe des suites d'entiers consécutifs arbitrairement longues telles qu'aucun d'entre eux ne soit la puissance d'un nombre premier (*Olympiades internationales de mathématiques, 1989*).

EXERCICE 4

1 Soit p un nombre premier et soit x un entier tel que $x^2 \equiv 1 \pmod p$. Montrer que l'on a $x \equiv 1 \pmod p$ ou $x \equiv -1 \pmod p$.

2 Calculer $2^{140} \pmod{561}$. En déduire que 561 n'est pas un nombre premier.

EXERCICE 5

On définit une suite (u_n) par $u_0 = 0$ et $u_{n+1} = (u_n)^2 - 3/2$. Montrer que l'on a $u_n \neq u_m$ pour $n \neq m$. (Montrer par récurrence que pour tout $n \geqslant 1$, $2^{2n-1} u_n$ est un nombre entier impair.)

EXERCICE 6

1 Montrer que pour tout entier $n \geqslant 1$, il existe un unique entier t tel que $2^t \leqslant n < 2^{t+1}$. On le note t_n.

2 Si $n \geqslant 1$, on pose

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Montrer par récurrence sur $n \geqslant 2$ qu'il existe des entiers impairs a_n et b_n tels que $H_n = a_n / 2^{t_n} b_n$. En déduire que pour $n \geqslant 2$, H_n n'est pas un nombre entier.

EXERCICE 7

Soit n un entier strictement positif ; on note $n = \prod_{i=1}^{r} p_i^{n_i}$ sa décomposition en facteurs premiers, les p_i sont des nombres premiers deux à deux distincts, les n_i des entiers $\geqslant 1$.

1 Montrer qu'un entier $d > 0$ divise n si et seulement si il existe des entiers m_i, $0 \leqslant m_i \leqslant n_i$ tel que $d = \prod_{i=1}^{r} p_i^{m_i}$.

2 Montrer que le nombre de diviseurs strictement positifs de n est égal à $\prod_{i=1}^{r} (1 + n_i)$.

3 Calculer en fonction des p_i et des n_i la somme des diviseurs positifs de n.

EXERCICE 8

1 Décomposer en facteurs premiers les entiers $a = 46848$, $b = 2379$, $c = 8633$, $d = 4183$.

2 En déduire $\mathrm{pgcd}(a,b)$ et $\mathrm{pgcd}(c,d)$. Calculer $\mathrm{ppcm}(a,b)$ et $\mathrm{ppcm}(c,d)$.

3 Comparer avec l'algorithme d'Euclide.

EXERCICE 9

1 Décomposer 51 et 216 en facteurs premiers ; calculer $\mathrm{pgcd}(51,216)$. Déterminer toutes les expressions de 216 comme le produit de deux entiers naturels premiers entre eux.

2 Soit a et b des entiers > 0 tels que $a + b = 51$, $a < b$ et $\mathrm{ppcm}(a,b) = 216$. Montrer que $d = \mathrm{pgcd}(a,b)$ divise $\mathrm{pgcd}(51,216)$.

3 Montrer que $a' = a/d$ et $b' = b/d$ sont premiers entre eux. Que vaut $\mathrm{ppcm}(a',b')$? En déduire la liste des couples (a,b) possibles.

EXERCICE 10

1 Soit p un nombre premier. Combien y a-t-il d'entiers $m \in \{1,\dots,n\}$ multiples de p ? de p^k pour $k \geqslant 1$? En déduire que

$$\mathrm{ord}_p(n!) = \sum_{k \geqslant 1} \lfloor n/p^k \rfloor.$$

(La somme est finie car les termes pour $p^k > n$ sont nuls.)

2 Combien y a-t-il de 0 à la fin du développement décimal de 1000! ? Vérifier avec MAPLE.

2. Nombres premiers de Fermat, de Mersenne

EXERCICE 1

Soit n un nombre entier et posons $M_n = 2^n - 1$ (*nombre de Mersenne*).

1 Si M_n est un nombre premier, montrer que n est premier.

2 Trouver le plus petit nombre premier n tel que M_n ne soit pas premier.

EXERCICE 2

Pour $n \geqslant 0$, on pose $F_n = 2^{2^n} + 1$ (*nombre de Fermat*).

1 Montrer que $F_0, F_1, \ldots, F_4$ sont des nombres premiers.

2 Si k n'est pas une puissance de 2, $2^k + 1$ n'est pas un nombre premier. (Si $k = ab$, avec a impair, montrer que $2^b + 1$ divise $2^k + 1$.)

3 Montrer que F_5 n'est pas un nombre premier (Euler), contrairement à une affirmation de Fermat que tous les F_n sont des nombres premiers. Précisément, montrer que 641 divise F_5. (Écrire $2^{32} + 1 = 16(2^7)^4 + 1$ et remarquer que $16 = 641 - 625$.)

4 Démontrer que $\prod_{k=0}^{n-1} F_k = F_n - 2$. Si $m \neq n$, en déduire que F_n et F_m sont premiers entre eux.

EXERCICE 3

1 Si p est un nombre premier impair, $2^{p-1} - 1$ est multiple de p.

2 Montrer que pour tout entier $n \geqslant 0$, $2^{F_n - 1} - 1$ est multiple de F_n, où $F_n = 2^{2^n} + 1$ désigne le n-ième nombre de Fermat.

3 Cela entraîne-t-il que F_n est un nombre premier ?

EXERCICE 4

Soit p un nombre premier et soit a un entier premier à p.

1 Montrer qu'il existe $b \in \{1, \ldots, p-1\}$ tel que $ab \equiv 1 \pmod{p}$.

2 Soit k le plus petit entier > 0 tel que $a^k \equiv 1 \pmod{p}$. On va montrer que k divise $p - 1$.
Soit $d = \operatorname{pgcd}(k, p-1)$ et soit u, v des entiers relatifs tels que $d = uk + v(p-1)$. Si $u \geqslant 0$ et $v \leqslant 0$, calculer $a^{uk} b^{-v(p-1)} \pmod{p}$. En déduire que $a^d \equiv 1 \pmod{p}$, puis que $d = k$.

3 Traiter les autres cas de manière analogue.

EXERCICE 5

On rappelle que $F_n = 2^{2^n} + 1$ désigne le n-ième nombre de Fermat.

1 Soit p un facteur premier de F_n. Montrer que $2^{2^n} \equiv -1 \pmod{p}$, puis que 2^{n+1} est le plus petit entier $d > 0$ tel que $2^d \equiv 1 \pmod{p}$. À l'aide de l'exercice **??**, montrer que $p \equiv 1 \pmod{2^{n+1}}$.

2 On suppose que $3^{2^{2^n - 1}} \equiv -1 \pmod{F_n}$. Soit p un facteur premier de F_n. Montrer que le plus petit entier d tel que $3^d \equiv 1 \pmod{p}$ est égal à 2^{2^n}.

3 Déduire de l'exercice **??** que 2^{2^n} divise $p - 1$, puis que $p \equiv 1 \pmod{2^{2^n}}$. Montrer enfin que $p = F_n$, autrement dit que F_n est premier (*critère de Pépin*).

3. Nombres premiers et congruences

EXERCICE 1

Soit n un nombre entier qui n'est multiple ni de 2, ni de 3, ni de 5. Montrer que $n^4 \equiv 1 \pmod{240}$.

EXERCICE 2

1 Soit a et b des entiers > 1 et soit $n = ab$. Si $n \geqslant 5$, démontrer que ab divise $(n-1)!$. (C'est facile si $a \neq b$; si $a = b$, montrer que $2a^2$ divise $(n-1)!$.)

2 Inversement, si n est un nombre premier, alors n ne divise pas $(n-1)!$.

EXERCICE 3

Soit a et b deux entiers tels que $a^2 + b^2$ soit multiple de 7. Montrer que a et b sont multiples de 7.

EXERCICE 4

Pour quelles valeurs de l'entier n,

1 le nombre $4^n + 2^n + 1$ est-il divisible par 7 ?

2 le nombre $9^n + 3^n + 1$ est-il divisible par 13 ?

3 le nombre $25^n + 5^n + 1$ est-il divisible par 31 ?

EXERCICE 5

1 Calculer les restes modulo 13 des entiers 5^{206}, 5^{381}, 5^{883}, puis 5^n pour tout entier $n \in \mathbf{N}$.

2 Calculer les restes modulo 13 des entiers 1617^{206}, 1617^{381}, 1617^{883}, 1617^n, pour $n \in \mathbf{N}$.

EXERCICE 6

Soit a et b des entiers ; on pose $A = 11a + 2b$ et $B = 18a + 5b$.

1 Montrer que si 19 divise l'un des deux entiers A ou B, il divise l'autre.

2 On suppose que a et b sont premiers entre eux. Montrer que A et B ne peuvent avoir d'autre diviseur commun que 1 et 19.

EXERCICE 7

Trois entiers a, b, c vérifient $a^2 = b^2 + c^2$.

1 Montrer que l'un au moins de b et c est multiple de 3.

2 Montrer que l'un au moins de a, b, c est multiple de 5.

3 Montrer que l'un au moins de b et c est multiple de 4.

EXERCICE 8

Soit x, y, z des entiers > 0, premiers entre eux dans leur ensemble, tels que $x^2 + y^2 = z^2$ (*triplet pythagoricien*).

1 Soit $d = \text{pgcd}(x, y)$. Montrer que d divise z. En déduire que x, y, z sont premiers entre eux deux à deux.

2 Montrer que de x et y, l'un des deux est pair et l'autre est impair. On supposera dans la suite que x est pair.

3 Montrer que $\text{pgcd}(z - y, z + y) = 2$. En utilisant que $x^2 = z^2 - y^2 = (z - y)(z + y)$, montrer qu'il existe des entiers u et v tels que $x = 2uv$, $z + y = 2u^2$ et $z - y = 2v^2$.

4 Inversement, si u et v sont premiers entre eux, le triplet $(x, y, z) = (2uv, u^2 - v^2, u^2 + v^2)$ est un triplet pythagoricien.

EXERCICE 9

Soit p un nombre premier > 2.

1 Soit a un entier tel que $a^2 \equiv -1 \pmod{p}$. Déduire du petit théorème de Fermat que $(p-1)/2$ est pair, donc que $p \equiv 1 \pmod{4}$.

2 Soit $x \in \{1, \ldots, p-1\}$; montrer qu'il existe un unique entier $y \in \{1, \ldots, p-1\}$ tel que $xy \equiv 1 \pmod{p}$. Montrer que $y \neq x$, sauf si $x = 1$ ou $x = p - 1$.

3 En regroupant les entiers compris entre 1 et $p - 1$ deux par deux, comme dans la question précédente, montrer que $(p-1)! \equiv -1 \pmod{p}$. (*théorème de Wilson*).

4 On suppose que $p \equiv 1 \pmod{4}$ et on pose $a = \left(\frac{p-1}{2}\right)!$. Montrer $a^2 \equiv -1 \pmod{p}$. (Dans $(p-1)!$, regrouper i et $p - i$.)

EXERCICE 10

1 Soit p un nombre premier ; pour tout entier $k \geqslant 0$, on pose $S_k = 1^k + 2^k + \cdots + (p-1)^k$. Calculer S_0, S_1, S_{p-1}, S_p modulo p. Montrer que $S_k \equiv S_m \pmod{p}$ si $k \equiv m \pmod{p-1}$.

2 Si $k \in \mathbf{N}$, on pose $b_k(x) = x(x-1)\ldots(x-k+1)$; c'est un polynôme de degré k, à coefficients entiers et de coefficient dominant 1. (On a $b_0 = 1$, $b_1 = x$, $b_2 = x(x-1)$, etc.)
Pour tout couple (k, n) d'entiers, calculer $\sum_{i=1}^{n} b_k(x)$.

3 Si p est un nombre premier et k un entier, en déduire la valeur de

$$b_0(1) + \cdots + b_0(p-1) \pmod{p}.$$

4 Montrer par récurrence sur n que pour tout polynôme P à coefficients entier, de degré n, il existe des entiers $a_0, \ldots, a_n$ tels que

$$P(x) = a_0 b_0(x) + a_1 b_1(x) + \cdots + a_n b_n(x).$$

5 Calculer $S_k \pmod{p}$ en fonction de k.

EXERCICE 11

Soit p un nombre premier et soit $P(x)$ le polynôme $P(x) = x^p - x$. D'après l'exercice **??**, il existe des entiers $a_0, \ldots, a_p$ tels que $P(x) = a_0 b_0(x) + a_1 b_1(x) + \cdots + a_p b_p(x)$.

1 Montrer que par récurrence sur n que a_n est multiple de p si $0 \leqslant n < p$. (Calculer $P(0) \pmod{p}$, puis $P(1) \pmod{p}$,...)

2 Montrer que

$$x(x-1)\ldots(x-p+1) \equiv x^p - x \pmod{p}.$$

4. Théorème de Tchebychev et postulat de Bertrand

EXERCICE 1

Démontrer l'équivalent $\mathrm{li}(x) \sim x/\log(x)$.

Les trois exercices ci-dessous fournissent des renseignements sur la répartition des nombres premiers. Le premier montre que la somme des inverses de tous les nombres premiers est $+\infty$. Le second démontre le résultat de Tchebychev : $\pi(x)$ est compris entre deux multiples de $x/\log(x)$. Le dernier démontre le « postulat de Bertrand » : pour tout entier n, il existe un nombre premier p tel que $n < p < 2n$.

EXERCICE 2

Soit $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. la suite des nombres entiers, en ordre croissant. On va montrer que les sommes $(1/p_1) + (1/p_2) + \cdots + (1/p_n)$ sont arbitrairement grandes. Supposons par l'absurde que ce ne soit pas vrai et qu'il existe un réel A tel que

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} \leqslant A$$

pour tout entier $n \geqslant 1$.

1 Montrer qu'il existe un entier i tel que

$$\frac{1}{p_{i+1}} + \frac{1}{p_2} + \cdots + \frac{1}{p_{i+n}} \leqslant \frac{1}{2}$$

pour tout entier $n \geqslant 0$.

2 Soit $N(x)$ le nombre d'entiers $n \leqslant x$ qui ne sont divisibles que par $p_1, \ldots, p_i$. On écrit $n = km^2$ où k est sans facteur carré. Montrer qu'il n'y a que 2^i choix pour k et au plus $\sqrt{x}$ pour m. En déduire que $N(x) \leqslant 2^i \sqrt{x}$.

3 Si x est entier, le nombre d'entiers positifs $\leqslant x$ et divisibles par un nombre premier autre que les i premiers est donc égal à $x - N(x)$. Si p_{i+n} est le premier nombre premier $> x$, montrer que

$$x - N(x) \leqslant \frac{x}{p_{i+1}} + \frac{x}{p_{i+2}} + \cdots + \frac{x}{p_{i+n}},$$

d'où $x - N(x) \leqslant \frac{1}{2}x$.

4 En déduire une contradiction.

EXERCICE 3

L'exercice qui vient démontre une forme faible du théorème des nombres premiers, due à Tchebychev (1852).

1 Posons $N = \mathrm{C}_{2n}^{n}$. Démontrer que l'on a

$$2^n \leqslant \frac{1}{2n}4^n \leqslant N \leqslant 4^n.$$

2 Soit p un nombre premier tel que $n < p \leqslant 2n$. Montrer que p divise N.

3 Montrer que $(\pi(2n) - \pi(n))\log n \leqslant 2n\log 2$.

4 Soit p un nombre premier. Montrer que $\mathrm{ord}_p(N) \leqslant \log(2n)/\log p$.

5 Montrer que $\pi(2n)\log(2n) \geqslant n\log 2$.

6 Montrer que pour tout entier k,

$$k\pi(2^k) \leqslant 3 \cdot 2^k.$$

7 Montrer que pour tout entier $x \geqslant 1$, on a l'inégalité

$$\frac{\log 2}{4}\frac{x}{\log x} \leqslant \pi(x) \leqslant 6\log 2\frac{x}{\log x}.$$

EXERCICE 4

En 1845, J. Bertrand avait postulé l'existence, pour tout entier $n \geqslant 2$, d'un nombre premier entre n et $2n$. L'exercice suivant est consacré à une démonstration (due à P. Erdös, 1932) de ce fait.

1 Soit n un entier ; on pose $N = \mathrm{C}_{2n+1}^{n}$. Montrer que $N \leqslant 4^n$.

2 Montrer que le produit des nombres premiers p tels que $n+1 < p \leqslant 2n+1$ divise N.

3 Montrer par récurrence sur n que pour tout entier n, on a

$$\prod_{p \leqslant n} p \leqslant 4^n.$$

4 Soit p un facteur premier de N tel que $p \leqslant n$. Montrer que $p < 2n/3$.

5 Montrer qu'un nombre premier p tel que $p^2 | N$ vérifie $p \leqslant \sqrt{2n}$. En déduire qu'il y a au plus $\sqrt{2n}$ tels entiers.

6 Supposons par l'absurde qu'il n'existe pas de nombre premier p tel que $n < p < 2n$. Montrer que $N \leqslant 2^{4n/3}(2n)^{\sqrt{2n}}$.

7 (*suite*) En déduire que $\log(x)/x \geqslant 1/6$, où $x = \sqrt{2n}$, puis que $x \leqslant 18$. En déduire que $n \leqslant 162$.

8 Montrer (à la main) que pour tout entier $n \leqslant 1000$, il existe un nombre premier p vérifiant $n < p < 2n$.