Arithmétique

O. Simon, Université de Rennes I

6 décembre 2005

Sur ce chapître, il est conseillé
- de faire les sujets de la deuxième épreuve de 2001, 2002, 2003.
- consulter les bulletins APMEP n^0 432, 433, 434 de janvier à juin 2001.

1 Divisibilité - PGCD - Congruences

Exercice 1. [Terracher]
Soit n un entier naturel non nul et d un diviseur de n. Montrer que, pour tout entier $a \geq 1$, $a^n - 1$ est divisible par $a^d - 1$.
En déduire que $2^{1998} - 1$ est divisible par 3, 7, 9 et 511.

Exercice 2. [Terracher]
Soient a et b deux entiers naturels. Montrer que $a^n - b^n$ est divisible par $a - b$.
En déduire que, pour tout n, $1998^n - 1789^n$ est divisible par 11 et 19.

Exercice 3.
- On a $3^{20} = 3486784401$, les derniers chiffres de 3^{100} sont donc :
  A - 205 B - 001 C - 005 D - 221 E - 841
- Quel est le dernier chiffre dans l'écriture décimale de 2^{46} ? le chiffre des unités de $7^{(7^7)}$?

Exercice 4. [Bordas-S]
Utiliser l'algorithme d'Euclide pour déterminer le PGCD des nombres :

a) 360 et 756
b) 322 et 1078
c) 2200 et 5733
d) 6600 et 30576

Trouver pour chaque couple une identité de Bézout.

Exercice 5. [Bordas-S]
Soient a, b deux entiers naturels non nuls, A, B les nombres tels que : $A = 3a + 4b$ et $B = 4a + 5b$

1. Montrer que $D(a, b) \subset D(A, B)$.
2. Exprimer a et b en fonction de A et B ; en déduire que

$$PGCD(a, b) = PGCD(A, B)$$

Exercice 6. [Sierpinski]
Trouver tous les entiers $n > 0$ tels que chacun des nombres $n + 1, n + 3, n + 7, n + 9, n + 13, n + 15$ soit un nombre premier.

Exercice 7. On dit que le couple (p, q) est un couple de nombres premiers jumeaux si p et q sont premiers et $q = p + 2$. Montrer qu'il existe une infinité de couples de nombres premiers consécutifs qui ne sont pas jumeaux. (On ne sait pas s'il existe une infinité de couples de nombres premiers jumeaux)

Exercice 8. On appelle, nombres de Fermat, les nombres de la forme
$F_n = 2^{2^n} + 1$. Calculer F_0, F_1, F_2, F_3, F_4. Montrer que, pour $n \neq m$, F_n et F_m sont premiers entre eux.
On constate que F_0, F_1, F_2, F_3, F_4 sont des nombres premiers. On démontre que F_5 est divisible par 641, et il est conjecturé, que pour $n \geq 5$, F_n est un nombre composé.

Exercice 9. Montrer que l'ensemble des nombres premiers de la forme $4n+3$ (ou $4n-1$) sont en nombre infini.

Exercice 10. On appelle nombre de Mersenne (1588 - 1648) tout nombre de la forme $M_n = 2^n - 1$. Calculer M_n pour quelques valeurs de n. Montrer que si M_p est un nombre premier alors p est un nombre premier.
La recherche des nombres premiers de Mersenne se poursuit encore aujourd'hui, grâce aux ordinateurs. En 1998, on a trouvé M_{859433} qui n'a pas moins de 258716 chiffres.

Exercice 11. [TangArith]
On prend un nombre premier p différent de 2 et 3. On l'élève au carré et on lui ajoute 11. Quel est le reste de la division du nombre obtenu par 24 ?

Exercice 12. [Terracher] **Nombre de diviseurs**

a) Soit $n \geq 2$, admettant la décomposition en facteurs premiers $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, où $p_1, \dots p_r$ sont des nombres premiers distincts et $\alpha_i > 0$ pour $1 \leq i \leq r$.
Montrer que le nombre de diviseurs de n est :

$$d(n) = (\alpha_1 + 1) \dots (\alpha_r + 1).$$

b) Déterminer le nombre de diviseurs des entiers suivants :

1000 ; 1515 ; 1850 ; 100^{100}

p^n, avec p premier ; $2^n.p^m$, avec p premier impair.

Exercice 13. (Dossier "zéro" du CNED)

1. Que peut-on dire des nombres : 16, 1156, 111556, 11115556, ... ?(On peut s'aider d'une calculatrice)
2. En considérant x_n le nombre entier écrit avec n chiffres 1 (ainsi $x_4 = 1111$), on note A_n le nombre entier écrit avec $n+1$ chiffres 1, suivis de n chiffres 5, suivis d'un chiffre 6,(ainsi $A_3 = 11115556$)
   (a) Formuler une conjecture pour les nombres A_n.
   (b) Montrer que $A_n - 1 = x_{n+1} \times 10^{n+1} + 5 \times x_{n+1}$
   (c) Montrer que, pour tout $n \in \mathbb{N}$, on a : $x_n = \dfrac{10^n - 1}{9}$.
   (d) Conclure.

Exercice 14. [Terracher]

1. Déterminer les restes des divisions de :
   – 1024 par 11 et par 31
   – 4×1024 par 21
   – 1024^2 par 41
2. En déduire que le nombre $2^{60} - 1$ est divisible par $11 \times 21 \times 31 \times 41$.

Exercice 15. [Terracher] Rallye mathématique d'Alsace.

1. Montrer que $2^{21} - 1$ est divisible par 49.
2. Montrer que pour tout entier x, $(1 + x)^7 - (1 + 7x)$ est divisible par x^2.
3. En déduire que $2^{147} - 1$ est divisible par 343.

Exercice 16. (Dossier "zéro" de Versailles)
Soit a un entier, avec $1 \leq a \leq 20$. On considère l'équation $3x^2 - 35y^2 = a$ et on veut préciser, selon les valeurs de a, si cette équation a des solutions dans $\mathbb{Z}$.

1. Montrer que si l'on a une solutions entière x, y de l'équation $3x^2 - 35y^2 = a$, elle vérifie $3x^2 = a$ modulo 5. Dresser la table des congruences possibles de $3x^2$ modulo 5. En déduire que l'équation n'a pas de solution lorsque a est congru à ± 1 modulo 5. Quelles valeurs de a peut-on éliminer ainsi ?
2. En utilisant la même méthode, montrer que l'équation n'a pas de solution si a est congru à 1, 2,-3 modulo 7. Quelles valeurs de a peut-on éliminer ainsi ?
3. Appliquer la même méthode en calculant modulo 3. Quelles valeurs de a peut-on éliminer ainsi ?

4. Montrer que si l'on a une solution x, y de l'équation $3x^2 - 35y^2 = a$, elle vérifie $-x^2 + y^2 = a$ modulo 4. Dresser la table des congruences possibles de $y^2 - x^2$ modulo 4. En déduire que l'équation n'a pas de solution lorsque a est congru à 2 modulo 4. Quelles valeurs de a peut-on éliminer ainsi ?
5. Montrer qu'il reste une incertitude seulement pour quatre valeurs de a. Montrer que dans ces quatre cas l'équation admet des solutions (on pourra utiliser une calculatrice).
6. Comment tester si l'équation $3x^2 - 35y^2 = 97$ a des solutions x, y avec $0 \leq x, y \leq 50$?

2 Etude des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème 2.1 *Dans un groupe fini commutatif, l'ordre de tout élément divise l'ordre du groupe.*

Si un groupe commutatif G a n éléments, si $x \in G$ est d'ordre d alors d divise n.

Exercice 17. (**Théorème chinois**). Soient m, n deux entiers premiers entre eux, montrer qu'il existe un isomorphisme d'anneaux de $\mathbb{Z}/nm\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

On note, pour $n \in \mathbb{N}^*$, $U(n)$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On appelle indicateur d'Euler la fonction $\phi(n)$ définie comme le nombre d'éléments de $U(n)$. (1760)
Par convention, on pose $\phi(0) = 0,\ \phi(1) = 1$.

Exercice 18.

1. Montrer que $U(n)$ est un groupe multiplicatif.
2. Montrer que $\phi(n)$ est le nombre d'éléments de $\{1, \ldots, n\}$ premiers avec n.
3. Montrer que $U(n)$ est l'ensemble des générateurs du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$
4. Montrer que si p est premier, $k \in \mathbb{N}^*$, alors
$$\phi(p^k) = p^{k-1}(p-1)$$
5. Montrer que si m, n sont premiers entre eux, alors
$$\phi(mn) = \phi(m)\phi(n)$$
6. En déduire que si $n = \prod_{i=1}^{r} p^{k_i}$ est la décomposition en facteurs premiers de n, alors
$$\phi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$
7. (Théorème de Gauss). Montrer que pour tout $n \in \mathbb{N}^*$,
$$\sum_{d|n} \phi(d) = n$$

Définition 2.2 *[Sierpinski] On appelle racine primitive de n, tout élément de $U(n)$, générateur de $U(n)$.*

Si g est une racine primitive de n, on a alors
$$U(n) = \{g^0 = 1, g, \ldots, g^{\phi(n)-1}\}$$
Ainsi g est un élément d'ordre $\phi(n)$.

Définition 2.3 *(Sierpinski) Si g est une racine primitive de n, pour un élément x de $U(n)$, on appelle indice de x relativement à g ou logarithme discret de base g de x, le nombre $y, 0 \leq y < \phi(n)$, tel que $x = g^y$. On note*
$$y = ind_g(x) = log_g(x)$$
S'il n'y a pas de confusion, on peut noter ind, log.

Si $f(x)$ est l'indice de x relativement à g, alors $f(x)$ est défini modulo $\phi(n)$ et
$$f(x_1 x_2) = f(x_1) + f(x_2)\ modulo(\phi(n))$$

Exercice 19.

1. Montrer que $U(17)$ est un groupe cyclique engendré par 3.
2. Etudier l'ordre des éléments de $U(15)$. Ce groupe est-il cyclique ?
3. Même question pour $U(10)$

voir la deuxième épreuve du CAPES 2003

Exercice 20.
- En utilisant un générateur de $U(7)$, résoudre dans $\mathbb{Z}/7\mathbb{Z}$, l'équation

$$6x^2 = 5$$

- En utilisant un générateur de $U(17)$, résoudre dans $\mathbb{Z}/17\mathbb{Z}$, l'équation

$$6x^{10} = 4$$

Théorème 2.4 *Soit K un corps fini. Alors le groupe multiplicatif K^* est un groupe cyclique.*

Si K a q éléments, K^* a $q-1$ éléments et il existe un élément g de K^* tel que

$$K^* = \{g^0 = 1, g, \ldots, g^{q-2}\}$$

Démonstration : [Schwartz]

3 Autour du petit théorème de Fermat.

Théorème 3.1 Petit théorème de Fermat *: Soit p un nombre premier :*
pour tout $x \in \mathbb{Z} - 0, x^{p-1} = 1 mod(p)$, c'est-à-dire, p divise $x^{p-1} - 1$.
pour tout $x \in \mathbb{Z}, x^p = x \ mod(p)$, c'est-à-dire, p divise $x^p - x$.

Exercice 21. Montrer que ce théorème donne un test de non primalité, (un critère pour affirmer qu'un nombre n n'est pas premier).
La réciproque de ce théorème est-elle vraie ?

Définition 3.2 *: On dit qu'un nombre non premier, n, est pseudo-premier de base b entier naturel non nul, si $b^{n-1} = 1 mod(n)$.*

Exercice 22. : Montrer que $n = 341$ est pseudo-premier de base 2.

Définition 3.3 *: Un entier non nul n est dit un nombre de Carmichaël, s'il est pseudo-premier de base b, pour chaque b premier avec n, sans être premier.*

voir la deuxième épreuve du CAPES 2003
Exemple : $n = 561$ se factorise $561 = 3 * 11 * 17$ et pour tout b premier avec 561, on a $b^{560} = 1 mod(561)$.
Il existe une infinité de nombres de Carmichaël, ceci a été démontré en

Conséquences pratiques du petit théorème de Fermat
Soit p un nombre premier et $a \in \mathbb{Z}$, non multiple de p.
Ceci est utile pour calculer de grandes puissances.
Exercice 23. : Soient r et s tels que $r = s \ mod(p-1)$, alors $a^r = a^s \ mod(p)$.

Exercice 24. : Soient p et q deux nombres premiers distincts et a non multiple de p et non multiple de q. Soient r et s tels que $r = s \ mod((p-1)(q-1))$, montrer que $a^r = a^s \ mod(pq)$.

Exercice 25. :
- Si p est un nombre premier et a un un entier non multiple de p, donner deux méthodes pour calculer l'inverse de a modulo p.
- Si a et n sont premiers entre eux, donner une méthode pour calculer l'inverse de a modulo n.

3.1 Cryptographie : code R.S.A. Algorithme à clé publique

Pour éviter le problème de transmission de la clé secrète au correspondant, le principe de l'algorithme à clé publique a été proposé par Diffie et Hellman en 1976 :
- On pourrait établir un annuaire de clés, porté à la connaissance de tous.
- Toute personne peut envoyer un message à celles figurant dans l'annuaire.
- Mais, ce message ne pourrait être décoder que par le destinataire qui, seul, possède la clé de décodage.

Cet algorithme a été réalisé par Rivest, Shamir, Adleman en 1977, sous le nom de système RSA.
Soient p et q deux nombres premiers assez grands tels que $n = p \times q$ ne puisse pas être factorisé. Dans $\mathbb{Z}/n\mathbb{Z}$, on a, pour tout x, si

$$k = 1 \ mod((p-1) \times (q-1)), \ x^k = x.$$

Donc, si c et d sont inverses l'un de l'autre modulo $((p-1) \times (q-1))$, alors $f(x) = x^c$ et $g(x) = x^d$ sont des applications réciproques l'une de l'autre dans $\mathbb{Z}/n\mathbb{Z}$. Comme on ne peut pas factoriser n, on ne peut pas obtenir $(p-1) \times (q-1)$ et donc, d, l'inverse de c est inconnu du public. D'où, l'algorithme de codage, avec la clé publique (n, c) :

1. on découpe le message en blocs de longueur l selon la longueur du nombre n,
2. on élève chacun des blocs à la puissance c, $modulo(n)$
3. seul, le destinataire qui connaît p et q , connaît d et peut décoder le message reçu.

Voir description dans [Schwartz]

Exercice 26. : Alice détermine sa clé : $p = 17, q = 31, n = 527$, montrer qu'elle peut choisir $c = 7$. Dans l'annuaire, on trouve la clé publique $(527, 7)$.
Claire veut envoyer à Alice le message 472. Donner le message codé qu'enverra Claire, et expliquer comment Alice retrouve le message de départ.

Utilisation du système RSA, selon la priorité :

a. le contenu du message doit rester secret

b. la provenance doit être authentifiée, et le contenu peut être déchiffré

c. le contenu doit rester secret et la signature être authentifiée

Un groupe de personnes s'échange des messages, elles possèdent un annuaire public et chaque personne a son code secret qui est privé :

	annuaire public		privé :
Alice :	n	c	d
Claire :	m	e	f
Romain :	r	g	h

On a les algorithmes de codage Cc, Ce, Cg , qui peuvent être effectués par n'importe qui et de décodage Dd, Df, Dh qui sont privés.
On a vu le fonctionnement de (a).
Pour (b), Alice veut faire reconnaître sa carte bancaire par un distributeur pour retirer 160 euros. Alice introduit sa carte, le distributeur dispose d'un message M, le numéro de la carte (?), grâce à M, il reconnaît la carte d'Alice, et peut utiliser les données de l'annuaire, donc calculer M^c. Elle compose son code d, ce qui renvoie $(M^c)^d$. Si $(M^c)^d = M$, alors c'est Alice (ou une personne connaissant le code) qui est en possession de la carte.
Pour (c), Claire veut envoyer un message signé à Romain : soit M le message elle fait $(M^f)^g = M'$, Romain le reçoit, il fait $(M'^h)^e$, il retrouve M.

4 Résidus quadratiques

Si p est un nombre premier, dans $\mathbb{Z}/p\mathbb{Z}$, résoudre $ax^2 + bx + c = 0$, revient à résoudre $(x - r)^2 = q$, car $a \neq 0$ est inversible. D'où, l'intérêt des carrés.
On notera $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{F}_p^* = \mathbb{Z}/p\mathbb{Z} - \{0\}$

Définition 4.1 *On dit que $a \in \mathbb{Z}$ est un résidu quadratique modulo n, si a est un carré dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire qu'il existe $x \in \mathbb{Z}$ tel que $a = x^2 \ mod(n)$.*

Exercice 27.

1. Ecrire les carrés dans $\mathbb{Z}/n\mathbb{Z}$, pour les valeurs de n suivantes : $n = 7$, $n = 8$, $n = 15$.
2. Montrer que si $a = b \ mod(n)$ dans $\mathbb{Z}$, alors a est un résidu quadratique modulo n si et seulement si b est un résidu quadratique modulo n.

Définition 4.2 *On appelle symbole de Legendre, ou caractère quadratique, pour $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, la fonction notée $(\frac{a}{n})$, définie par*

- $(\frac{a}{n}) = 1$ *si a est un carré modulo n*
- $(\frac{a}{n}) = -1$ *sinon*

Exercice 28. Soient m, n deux entiers premiers entre eux et $a \in \mathbb{Z}$. Montrer que a est résidu quadratique modulo mn si et seulement si il est résidu quadratique modulo m et modulo n. (Théorème chinois)
Constater sur un exemple, $(n = 3,\ m = 5,\ a = 2)$ que $(\frac{a}{nm}) \neq (\frac{a}{n}) \times (\frac{a}{m})$

Exercice 29. Si p est premier, impair, dans $\mathbb{F}_p^*$, il y a exactement $\frac{p-1}{2}$ résidus quadratiques.

Exercice 30. Critère d'Euler : Première expression du symbole de Legendre
Soit p est premier, impair. Montrer que, dans $\mathbb{F}_p^*$, les résidus sont les racines de $x^{\frac{p-1}{2}} - 1 = 0$ et que pour tout $a \neq 0$,

$$(\frac{a}{p}) = a^{\frac{p-1}{2}}$$

En déduire que le symbole de Legendre est un homomorphisme de groupe multiplicatif de $\mathbb{Z}/p\mathbb{Z} - \{0\}$ dans $\{-1, 1\}$. Pour $a, b \in \mathbb{Z}/p\mathbb{Z} - \{0\}$, on a

$$(\frac{a \times b}{p}) = (\frac{a}{p}) \times (\frac{b}{p}).$$

Exercice 31. Montrer que -1 est un carré modulo p, premier impair si et seulement si $p = 1\ mod(4)$.
En déduire qu'il existe une infinité de nombres premiers de la forme $4k + 1$.

Exercice 32. Une deuxième expression du symbole de Legendre
Soit p un nombre premier impair. Si g est un générateur de $\mathbb{Z}/p\mathbb{Z} - \{0\}$, montrer que, pour tout a, si $a = g^{ind(a)}$, on a

$$(\frac{a}{p}) = (-1)^{ind(a)}.$$

En déduire qu'un générateur de $\mathbb{Z}/p\mathbb{Z} - \{0\}$ n'est pas un résidu quadratique modulo p.

Exercice 33. [Itard] Une troisième expression du symbole de Legendre
Soit p un nombre premier impair. Pour $a \in \{1, \ldots, p-1\}$ et $k \in \{1, \ldots, \frac{p-1}{2}\}$, si $ka = q \times p + r_k$ est la division euclidienne de ka par p, on définit le reste minimal de ka, ρ_k par

- $\rho_k = r_k$, si $1 \leq r_k \leq \frac{p-1}{2}$
- $\rho_k = r_k - p$, si $\frac{p-1}{2} < r_k \leq p - 1$

1. Pour $a \in \{1, \ldots, p-1\}$, montrer que les restes minimaux de $\{ka \mid k = 1, \ldots, \frac{p-1}{2}\}$ ont pour valeurs absolues $\{1, \ldots, \frac{p-1}{2}\}$.
2. (Lemme de Gauss) Montrer que le nombre λ des restes minimaux négatifs de $\{ka \mid k = 1, \ldots, \frac{p-1}{2}\}$ est
   - pair si $(\frac{a}{p}) = 1$
   - impair si $(\frac{a}{p}) = -1$

   De façon équivalente, $(\frac{a}{p}) = (-1)^{\lambda}$

Exercice 34. Une quatrième expression du symbole de Legendre
Soit p un nombre premier impair. Pour tout $a \in \{1, \ldots, p-1\}$, si on écrit le nombre de restes minimaux négatifs :

$$\lambda = \lambda_1 + \ldots + \lambda_{\frac{p-1}{2}}$$

où $\lambda_k = 0$ ou 1, selon que le reste minimal, ρ_k, est positif ou négatif.

1. Montrer que $(-1)^{\lambda_k} = (-1)^{[\frac{2ka}{p}]}$ où $[x]$ =partie entière de x.
2. En déduire $(\frac{a}{p}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{2ka}{p}]}$

Exercice 35. Soit p un nombre premier impair. Montrer que $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Autrement dit, $(\frac{2}{p}) = 1 \iff p = \pm 1 \ mod\ 8$

Exercice 36. (Difficile) Loi de réciprocité quadratique
Soient p et q deux nombres premiers impairs distincts positifs,

1. Si $E = \{(kq, lp) \mid k = 1, \ldots, \frac{p-1}{2},\ l = 1, \ldots, \frac{q-1}{2}\}$, montrer que

$$Card(E) = \frac{p-1}{2} \times \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] + \sum_{l=1}^{\frac{q-1}{2}}[\frac{lp}{q}]$$

2. En utilisant les différentes expressions du symbole de Legendre, montrer que (loi de réciprocité quadratique) :

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Voir une autre démonstration dans [Franchini]

Exercice 37. [Naudin] Applications de la loi de réciprocité quadratique :

1. En déduire que $(\frac{p}{q}) \neq (\frac{q}{p})$ si et seulement si p et q sont tous les deux de la forme $4k-1$
2. Le nombre 323 est-il un carré modulo 479 ?
   (On pourra vérifier que 479 est premier et $323 = 17 \times 19$)

5 Anneaux et arithmétique

Exercice 38. (**Anneau des entiers de Gauss**) Voir deuxième épreuve 1981, II.
Soit $A = \mathbb{Z}[i]$.
Montrer que l'ensemble des éléments inversibles de A est isomorphe à $\mathbb{Z}/4\mathbb{Z}$

Exercice 39. Calculer le PGCD de $P_1 = 2X^4 - 3X^2 + 1$ et de $P_2 = X^3 + X^2 - X - 1$ dans $\mathbb{Q}[X]$ ainsi que $S,\ T \in \mathbb{Q}[X]$ tel que $PGCD(P_1, P_2) = P_1.S + P_2.T$

Exercice 40.

1. Décomposer $X^n - 1$ en produit de facteurs irréductibles pour $n \leq 8$ dans $\mathbb{Z}[X],\ \mathbb{Q}[X],\ \mathbb{R}[X]$.
2. Montrer que le polynôme $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$ mais que le polynôme $X^4 + 4$ est réductible dans $\mathbb{Q}[X]$.

Exercice 41.
Soit $P = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ avec $n \geq 1$ et $a_n \neq 0$. Montrer que si $r = \frac{c}{d} \in \mathbb{Q}$, avec $pgcd(c, d) = 1$ est une racine de P alors c divise a_0 et d divise a_n.
Trouver les racines de $2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10$ dans $\mathbb{Q}$.

Exercice 42. Deuxième épreuve 2002, A,III 2 ii).

Exercice 43. Soit p un nombre premier et $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ un polynôme de degré $n \geq 1$ à coefficients entiers tel que a_n n'est pas divisible par p, montrer que parmi les nombres $\{0, 1, 2, \ldots, p-1\}$, il n'existe pas plus de n nombres x pour lesquels $P(x)$ soit divisible par p.
Montrer par un contre exemple, que ce résultat n'est plus vrai si p n'est pas premier.
(Pour $p = 6$, voir la deuxième épreuve du CAPES 2003)

Références

[Appert] Problèmes résolus de mathématiques. M. Appert, J. Debardieux. Dunod Université.

[Bordas-S] Maths spécialité terminale S, collection Fractale, Bordas

[De Biasi] Mathématiques pour le CAPES et l'Agrégation interne. Ellipses.

[Escofier] : Difficulté d'évaluer la difficulté en arithmétique. Bulletin de l'APMEP n^0 434 mai-juin 2001, p. 328.

[Escofier] Toute l'algèbre du 1er cycle, J.P. Escofier, Dunod 2002

[Franchini] Algèbre, Mathématiques Spéciales. Ellipses 1999

[Francinou] Algèbre 1. Exercices de mathématiques pour l'agrégation. S. Francinou et H. Gianella. Ed. Masson. 1994

[Goblot] Algèbre commutative. Cours et exercices résolus. Rémi Goblot. Ed. Masson. 1996

[Gostiaux] Cours de mathématiques spéciales, 1. Algèbre, Bernard Gostiaux. PUF 1993

[Itard] Les nombres premiers. J. Itard. Que sais-je ? P.U.F. 1976

[Monier] Nouveau cours de mathématiques, Tome 5, Algèbre 1, Chapitre 4. J.-M. Monier. Dunod 1996

[Naudin] Algorithmique Algébrique, P. Naudin - C. Quitté. Ed. Masson 1992

[Robin] Apprenons l'Arithmétique élémentaire pour comprendre la Cryptographie Moderne. G.Robin. Publication de l'IREM de Limoges, mai 1998

[Schwartz] Mathématiques pour la licence, Algèbre. Lionel Schwartz. Dunod 1998.

[Sierpinski] Theory of numbers, W. Sierpinski. Warsawa 1964 (Printed in Poland)

[Sierpinski] 250 problems in elementary number theory, W. Sierpinski. Warsawa 1970 (American Elsevier Publishing Company, INC, New York)

[TangArith] Secrets de Nombres, Tangente Hors série n^0 6 ; Editions Archimède,1998.

[Terracher] Enseignement de spécialité terminale S, collection Terracher, Hachette