L'anneau Z

I.1 Montrer que $\forall\, n \geq 0$, $(2^n + 3^n)$ et $(2^{n+1} + 3^{n+1})$ sont premiers entre eux.

I.2 Trouver les sous-groupes de $\mathbf{Z}$ contenant $48\mathbf{Z}$ et donner leurs relations d'inclusion.

I.3 Soient $a, b, c \in \mathbf{N}$. Montrer que si $a \wedge b = 1$ alors :

(a) $(ac) \wedge b = c \wedge b$

(b) $(ab) \wedge c = (a \wedge c)(b \wedge c)$.

Dans le cas ou l'on ne suppose plus $a \wedge b = 1$, donner des contre-exemples aux égalités précédentes.

I.4

(a) Déterminer $(n^2 + 2n - 2) \wedge 6$ en fonction de n.
(Appliquer le (b) de l'exercice précédent **??** et montrer que

$$n^2 + 2n - 2 \equiv 0 \bmod 3 \Longleftrightarrow n \equiv 2 \bmod 3).$$

(b) Déterminer $(n^3 + n^2 + 1) \wedge (n^2 + 2n - 1)$ en fonction de n.
(En remarquant que les coefficients dominants sont inversibles dans $\mathbf{Z}$, utiliser des divisions euclidiennes successives afin de faire descendre les degrés.)

I.5 Soient a et b des entiers premiers entre eux tels que leur produit soit une puissance k-ième d'un entier pour $k \geq 2$ entier. Montrer alors que a et b sont eux-mêmes des puissances k-ièmes d'entiers.

I.6 Variations sur le théorème de Bézout :

(a) En utilisant l'algorithme d'Euclide, trouver toutes les relations de Bézout $650u + 66v = 650 \wedge 66$ (cf. (**??**)).

(b) On suppose que dans un pays, n'existent que deux sortes de pièces de monnaie, de valeurs a et b entières (positives) avec $a \wedge b = 1$.

(i) Quelles sont les sommes qui peuvent être payées si on dispose d'un stock infini de pièces et qu'on autorise le rendu de monnaie ?

(ii) Montrer que si on interdit de rendre la monnaie, toute somme strictement supérieure à $ab - a - b$ peut être payée.
(Si $x > ab - a - b$, écrire $x = au + bv$ avec $0 \leq u \leq b - 1$).

(iii) Etudier le cas de 3 pièces de valeur 15, 20 et 48, et montrer que toute somme > 217 peut être payée sans rendu de monnaie.
(Se ramener au cas précédent en écrivant :

$$48x + 20y + 15z = 3(16x + 5z) + 20y.)$$

L'anneau $\mathbf{Z}/n\mathbf{Z}$, congruences

I.7 Montrer que pour tout entier $n \geq 1$,

$$4^{2^n} + 2^{2^n} + 1 \equiv 0 \bmod 7.$$

I.8 Donner les sous-groupes de $\mathbf{Z}/24\mathbf{Z}$ ainsi que leurs relations d'inclusion (cf. (**??**)).
Quels sont les sous-groupes engendrés par la classe de 18 (resp. 16) ?

I.9 Calculer $2005^{2005} \bmod 14$.

I.10 Calculer 10^{100} modulo $247 = 13 \times 19$.

I.11 Donner la congruence modulo 17 de $(1035125)^{5642}$.

I.12 Donner la congruence de 1823^{242} modulo 18 puis celle de 2222^{321} modulo 20.

I.13 Montrer que pour $n \geq 1$, on a $n^7 \equiv n \mod 42$.

I.14 Montrer que 429 est inversible dans $\mathbf{Z}/700\mathbf{Z}$ et donner son inverse.

I.15 Résoudre dans $\mathbf{Z}$ les congruences suivantes :

(i) $3x \equiv 4 \mod 7$;

(ii) $9x \equiv 12 \mod 21$;

(iii) $103x \equiv 612 \mod 676$.

I.16 Soient a et b deux entiers premiers entre eux, $n = a^4 + b^4$, p un diviseur premier de n, $p \neq 2$.

(a) Montrer que $n \equiv 1$ ou $2 \bmod 16$.

(b) Montrer que les classes $\bar{a}$ et $\bar{b}$ de a et $b \bmod p$ sont dans $(\mathbf{Z}/p\mathbf{Z})^*$.

(c) Calculer l'ordre de $\bar{a}/\bar{b}$ dans $(\mathbf{Z}/p\mathbf{Z})^*$.

(d) En déduire que $p \equiv 1 \bmod 8$.

I.17 "Un test de primalité" . Soient a et p deux entiers tels que $a \wedge p = 1$. Montrer que les conditions suivantes sont équivalentes :

(i) l'entier p est premier ;

(ii) on a $(X - a)^p \equiv X^p - a \bmod p$ dans l'anneau $\mathbf{Z}[X]$.

I.18 Soient $p \neq 2$ un nombre premier impair, $a, b \in \mathbf{N}$ non divisibles par p. Montrer que si p divise $a^2 + b^2$, alors $p \equiv 1 \mod 4$.

I.19 Soient p et q des nombres premiers distincts.

(a) Quel est le cardinal de $(\mathbf{Z}/pq\mathbf{Z})^*$? Combien y a-t-il d'éléments de $(\mathbf{Z}/pq\mathbf{Z})^*$ égaux à leur inverse ?

(b) Montrer la congruence :

$$\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}} \equiv 1 \bmod pq$$

(même méthode que pour le théorème de Wilson).

Morphismes

I.20

(a) Montrer que tout homomorphisme de groupes

$$\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$$

est déterminé par $\phi(1)$ et que $\phi(1)$ est un élément dont l'ordre divise a.
Réciproquement, montrer que si l'ordre de $x \in \mathbf{Z}/b\mathbf{Z}$ divise a, il existe un morphisme ϕ tel que $\phi(1) = a$.

(b) Montrer que les conditions suivantes sont équivalentes :

(i) $a \wedge b = 1$

(ii) tout homomorphisme $\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ est l'homomorphisme nul.

I.21 Déterminer les morphismes de groupes $\mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$ puis ceux de $\mathbf{Z}/12\mathbf{Z} \to \mathbf{Z}/15\mathbf{Z}$.

I.22 On fixe un nombre premier p. Soit a un entier > 0.

(a) Trouver la condition nécessaire et suffisante que doit satisfaire n pour qu'il existe un morphisme de groupes non nul :

$$\mathbf{Z}/p^a\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}.$$

(b) On suppose maintenant $n = p^b$, b étant un nombre entier > 0. Caractériser les éléments $x \in \mathbf{Z}/p^b\mathbf{Z}$ tels qu'il existe un morphisme

$$\phi : \mathbf{Z}/p^a\mathbf{Z} \longrightarrow \mathbf{Z}/p^b\mathbf{Z}$$

avec $\phi(1) = x$.

(c) Calculer le nombre de morphismes distincts : $\mathbf{Z}/p^a\mathbf{Z} \longrightarrow \mathbf{Z}/p^b\mathbf{Z}$ (on pourra supposer $a \leq b$).

I.23 Soit $\pi : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ le morphisme qui à $k \in \mathbf{Z}$ associe ses classes modulo n et m (cf. (**??**)). Montrer que le noyau de π est le PPCM de m et n et que l'image de π est $\{(\bar{a}, \bar{b})$ tels que $n \wedge m | (b - a)\}$.
Application : que peut-on dire de la congruence de k modulo 10 sachant que $k \equiv 3 \bmod 6$?

Problèmes

Problème I.1 *"Un autre test de primalité".*
Soient n un entier > 1, p un nombre premier tels que $n-1 = p^r m$, avec $r \geq 1$, $m \geq 1$.

(a) On suppose qu'il existe un entier a tel que $a^{n-1} \equiv 1 \bmod n$ et $(a^{\frac{n-1}{p}} - 1) \wedge n = 1$. Soit q un diviseur premier de n. Montrer que $(a^m - 1) \wedge q = 1$.

(b) Soit $b \in \mathbf{Z}/q\mathbf{Z}$ la classe de a^m. Montrer que $b \in (\mathbf{Z}/q\mathbf{Z})^*$ et calculer son ordre (multiplicatif).

(c) Montrer que $q \equiv 1 \bmod p^r$.

(d) On écrit maintenant $n-1 = uv$ (sans hypothèse particulière sur u, v). On suppose que pour tout facteur premier p de u, il existe un entier a_p tel que $a_p^{n-1} \equiv 1 \bmod n$ et $(a_p^{\frac{n-1}{p}} - 1) \wedge n = 1$. Montrer que tout facteur premier q de n vérifie $q \equiv 1 \bmod u$.

(e) On suppose en plus des hypothèses de (d) que $v \leq u+1$. Montrer que n est premier.

Problème I.2

1. Soit n un entier ≥ 2. On considère les conditions suivantes :

   (i) n est sans facteurs carrés et $p|n \Rightarrow p-1|n-1$ (p est un nombre premier) ;

   (ii) $\forall a \in \mathbf{Z}, a^n \equiv a \bmod n$;

   (iii) $\forall a \in \mathbf{Z}$ tel que $(a,n) = (1)$, $a^{n-1} \equiv 1 \bmod n$.

   a) Montrer que (i) $\Leftrightarrow$ (ii) ;

   b) montrer que (ii) $\Leftrightarrow$ (iii).

2. On considère les conditions suivantes (pour n impair) :

   (i) n est sans facteurs carrés et $p|n \Rightarrow p-1|(n-1)/2$;

   (ii) $\forall a \in \mathbf{Z}$, $(a,n) = (1)$, $a^{(n-1)/2} \equiv 1 \bmod n$.

   Montrer que (i) $\Leftrightarrow$ (ii).

3. Soit m un entier > 0. On suppose ques les nombres $6m+1$, $12m+1$, $18m+1$ sont premiers. Montrer que $n = (6m+1)(12m+1)(18m+1)$ vérifie les propriétés de 1.

   Montrer que si m est impair, alors n vérifie les propriétés de 2.

Problème I.3 *Etude des premiers nombres de Fermat.*
On pose pour tout $n \in \mathbf{N}$, $F_n = 2^{2^n} + 1$; F_n est par définition le n-ième nombre de Fermat.

(a) Soit $m \in \mathbf{N}\backslash\{0\}$. Prouver que si $2^m + 1$ est premier alors m est une puissance de 2.

(b) Calculer F_n pour $n \leq 4$ et vérifier qu'ils sont tous premiers.

(c) Montrer qu'à priori, un diviseur premier potentiel de F_5 est de la forme $64k + 1$.

(d) Montrer que F_5 est divisible par $641 = 1 + 5.2^7 = 5^4 + 2^4$.

(e) Montrer que pour $n \neq m$, F_n et F_m sont premiers entre eux et en déduire l'existence d'une infinité de nombres premiers.

Problème I.4 *Utilisation des entiers de Gauss.*
On note $A = \mathbf{Z}[i] = \{a + ib \,|\, (a, b) \in \mathbf{Z}^2\}$ l'anneau des entiers de Gauss . Pour $z = a + ib \in A$, on pose $N(a + ib) = a^2 + b^2$.

(i) Montrer que N est multiplicative,*i.e.* $N(zz') = N(z)N(z')$; en déduire que $A^* = \{\pm 1, \pm i\}$ ainsi que l'identité de Lagrange :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

(ii) En remarquant que tout nombre complexe peut s'écrire comme la somme d'un élément de $\mathbf{Z}[i]$ et d'un nombre complexe de module strictement plus petit que 1, en déduire que A est euclidien mais que la division euclidienne n'est pas unique.

(iii) Soit S l'ensemble des entiers > 0 somme de deux carrés. Montrer que S est stable par multiplications.

(iv) Soit p un nombre premier. Montrer l'équivalence des points suivants :

- p est irréductible dans A ;
- $p \equiv 3 \bmod (4)$;
- $p \notin S$.

(v) En déduire que les éléments irréductibles de A modulo les éléments inversibles sont les p premiers congrus à 3 modulo 4 et les $a + ib$ tels que $a^2 + b^2$ est premier.

(vi) Montrer que si $n \geq 2$, alors $n \in S$ si et seulement si la multiplicité $v_p(n)$ de p dans n est paire pour tout $p \equiv 3 \bmod 4$ ("théorème des deux carrés") .

Problème I.5 Soit $A := \mathbf{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \ / \ (a, b) \in \mathbf{Z}^2\}$. On introduit l'application "norme" $N : a + ib\sqrt{5} \in A \mapsto a^2 + 5b^2 \in \mathbf{N}$. On rappelle (**??**) qu'un élément $z \in A$ est dit irréductible si et seulement si il vérifie la propriété suivante :

$$z = z_1 z_2 \text{ et } z_1 \notin A^* \Longrightarrow z_2 \in A^*$$

(i) Montrer que $z \in A^*$ si et seulement si $N(z) = 1$ puis que si $N(z)$ est un nombre premier alors z est irréductible.

(ii) Montrer que tout élément $z \in A$ tel que $N(z) = 9$ est irréductible. En étudiant alors l'égalité :

$$3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

montrer que $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel (cf. (**??**)).

(iii) Etudiez de même l'égalité $2.3 = a.b$ avec $a = 1 + i\sqrt{5}$ et $b = 1 - i\sqrt{5}$; montrer avec cet exemple que le lemme de Gauss n'est pas vérifié et que $2a$ et ab n'ont pas de pgcd.