UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 1

Feuille n°4 : Nombres premiers

1 Exercices à savoir faire

Exercice 1

Effectuer sans calculatrice la division euclidienne de 66227 par 13.

Exercice 2

1 Écrire la liste des nombres premiers inférieurs à 100.
2 161 est-il premier ?
3 On appelle nombres premiers jumeaux, deux nombres premiers qui comme 11 et 13, diffèrent de 2. A l'aide du crible d'Erathosthène, déterminer deux nombres premiers jumeaux, compris entre 200 et 250.

Exercice 3

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 4

1 Rappeler le critère de divisibilité par 3.
2 Déterminer un critère de divisibilité par 11.
3 Déterminer le $pgcd(41, 11111)$.
4 Les nombres $111, 1111, 11111, 111111$ sont-ils premiers ?

Exercice 5

1 Décomposer en facteurs premiers les entiers $a = 46\,848$, $b = 2379$, $c = 8\,633$, $d = 4\,183$.
2 En déduire $\text{pgcd}(a, b)$ et $\text{pgcd}(c, d)$. Calculer $\text{ppcm}(a, b)$ et $\text{ppcm}(c, d)$.
3 Comparer avec l'algorithme d'Euclide.
4 Calculer le pgcd(46 848,2379).

Exercice 6

Calculer le pgcd de $(36, 100, 45)$ et donner un triplet de Bezout pour $(36, 100, 45)$.

Exercice 7

1. Déterminez le pgcd de 2873 et 1001, ainsi que deux entiers relatifs u et v tels que $2873\,u + 1001\,v = \mathrm{pgcd}(2873, 1001)$.
2. Décomposez 2873 et 1001 en facteurs premiers.
3. Existe-t-il des entiers relatifs u et v vérifiant

$$2873\,u + 1001\,v = 15 \quad ?$$

Exercice 8

Déterminer les couples d'entiers naturels de pgcd 18 et de somme 360. De même avec pgcd 18 et produit 6480.

Exercice 9

1 Calculer toutes les puissances de 3 modulo 7, c'est à dire $3^0 \pmod 7, 3^1 \pmod 7, 3^2 \pmod 7, \cdots$.
2 Calculer toutes les puissances de 38 modulo 7.

Exercice 10

On remarque que $7 \equiv -1 \pmod 8$. Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est impair ; dans le cas n pair, donner le reste de sa division par 8.

Exercice 11

Montrer que $2^{70} + 3^{70}$ est divisible par 13.

Exercice 12

1 Calculer les restes modulo 13 des entiers 5^{206}, 5^{381}, 5^{883}, puis 5^n pour tout entier naturel n.
2 Calculer les restes modulo 13 des entiers 1617^{206}, 1617^{381}, 1617^{883}, 1617^n, pour $n \in \mathbf{N}$.

Exercice 13

1 Soit $n = \overline{14555957}^{12}$. Déterminer le reste des divisions euclidiennes de n par $12, 3, 9, 48, 27$.

Exercice 14

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 15

1 Résoudre dans $\mathbf{N}$, l'équation $6a + 11b = 1$.
2 Trouver une solution dans $\mathbf{N}$ de l'équation $6a + 11b = 6$, puis résoudre dans $\mathbf{N}$, l'équation $6a + 11b = 6$.
3 Résoudre dans $\mathbf{N}$, l'équation $6a + 12b = 5$.

Exercice 16

1 Que peut-on dire d'un entier nul modulo 3, 5, et 16 ?
2 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 17

1 Soit a et b deux entiers relatifs premiers entre eux. Montrer que a et $a + b$ sont premiers entre eux.
2 Montrer que si a est premier avec b et c, il est premier avec leur produit bc.
3 Soit a et b deux entiers relatifs premiers entre eux. Montrer que pour tout $(k, l) \in \mathbf{N}^2$, a^k et b^l sont premiers entre eux.

2 Exercices à chercher

Exercice 18

Démontrer que, si a et b sont des entiers premiers entre eux, il en est de même des entiers $a + b$ et ab. (On pourra raisonner par l'absurde en supposant l'existence d'un diviseur *premier* commun à $a + b$ et ab.)

Exercice 19

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 20

1 Décomposer 51 et 216 en facteurs premiers ; calculer $\text{pgcd}(51, 216)$. Déterminer toutes les expressions de 216 comme le produit de deux entiers naturels premiers entre eux.
2 Soit a et b des entiers strictement positifs tels que $a + b = 51$, $a < b$ et $\text{ppcm}(a, b) = 216$. Montrer que $d = \text{pgcd}(a, b)$ divise $\text{pgcd}(51, 216)$.

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

Exercice 21

1 Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair est 1.
2 Montrer de même que tout nombre pair vérifie $x^2 \equiv 0 \pmod 8$ ou $x^2 \equiv 4 \pmod 8$.
3 Quelles sont les valeurs possibles de $2x^2 \pmod 8$?
4 Soient a, b, c trois entiers impairs. Déterminer le reste modulo 8 de $a^2 + b^2 + c^2$ et celui de $2(ab + bc + ca)$.
5 En déduire que ces deux nombres ne sont pas des carrés puis que $ab + bc + ca$ non plus. (Quelle est la parité de $ab + bc + ca$?)

Exercice 22

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. On pourra utiliser la contraposé.
2 Trouver le plus petit nombre premier n tel que M_n ne soit pas premier.

Exercice 23

Pour $n \geq 0$, 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 Montrer que si $2^k + 1$ est un nombre premier, k est une puissance de 2. (Si $k = ab$, avec a impair, montrer que $2^b + 1$ divise $2^k + 1$.) (Si $k = ab$, avec a premier impair, montrer en utilisant une factorisation de $x^a + 1$ 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 24

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 25

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 ≥ 1.

1 Montrer qu'un entier $d > 0$ divise n si et seulement si il existe des entiers m_i, $0 \leq m_i \leq n_i$ 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 26

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 $n \geq 4$, 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 $6n + 5$.

3 Exercices pour aller plus loin

Exercice 27

1 Soit $\overline{c_n \dots c_1 c_0}^{(10)}$ un nombre écrit en base dix. Montrer qu'il est multiple de 7 si et seulement si $\overline{c_n \dots c_1}^{(10)} - 2c_0$ l'est.
2 Montrer qu'il est multiple de 13 si et seulement si $\overline{c_n \dots c_1}^{(10)} + 4c_0$ l'est.
3 Généraliser à tout nombre premier autre que 2 et 5, et donner explicitement un test de divisibilité par 17.
4 Montrer que $\overline{c_{3n-1} \dots c_0}^{(10)}$ est multiple de 7 si et seulement si $\sum_{i=0}^{n-1} (-1)^i \overline{c_{3i+2} c_{3i+1} c_{3i}}^{(10)}$ l'est.
5 Donner un test de divisibilité par 13 analogue.
6 Soit p un nombre premier autre que 2 et 5. Montrer que la suite des restes modulo p des 10^m pour $m \in \mathbb{N}$ est périodique.
7 En déduire qu'il existe une puissance de 10 qui est congrue à 1 modulo p.
8 Pour $p = 7$, montrer qu'il existe une puissance de 10 qui est congrue à -1 modulo p.
9 S'il existe une puissance de 10 qui est congrue à -1 modulo p, construire un test de divisibilité analogue au précédent.
10 Comment faire si l'on connaît seulement une puissance de 10 qui est congrue à 1 modulo p ? (On pourra réfléchir au cas $p = 3$).
11 Pourquoi a-t-on distingué la cas où il existe une puissance de 10 qui est congrue à -1 modulo p ?

Exercice 28

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 29

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 ≥ 1.

1 Montrer qu'un entier $d > 0$ divise n si et seulement si il existe des entiers m_i, $0 \leq m_i \leq n_i$ 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.