ARITHMÉTIQUE SUR LES ENTIERS

Trois semaines

Table des matières

ECUE **3**

Motivation **3**

Attendus **3**

1 Relation de divisibilité sur les entiers et division euclidienne **4**
1.1 Résumé . . . 4
1.2 Exercices . . . 4
Exercice 1.1 . . . 4
Exercice 1.2 . . . 5
Exercice 1.3 . . . 5
Exercice 1.4 . . . 5

2 Relation de congruence **5**
2.1 Résumé . . . 5
2.2 Exercices . . . 6
Exercice 2.5 . . . 6
Exercice 2.6 . . . 6
Exercice 2.7 . . . 6
Exercice 2.8 . . . 7

3 Primalité et primalité relative **7**
3.1 Résumé . . . 7
3.2 Exercices . . . 8
Exercice 3.9 . . . 8
Exercice 3.10 . . . 8
Exercice 3.11 . . . 8
★ Exercice 3.12 . . . 8
Exercice 3.13 . . . 8
Exercice 3.14 . . . 9
Exercice 3.15 . . . 9
Exercice 3.16 . . . 9

4 Théorème de Bézout **9**
4.1 Résumé . . . 9
4.2 Exercices . . . 9
Exercice 4.17 . . . 9
Exercice 4.18 . . . 9
Exercice 4.19 . . . 9
Exercice 4.20 . . . 10
Exercice 4.21 . . . 10

5 Petit théorème de Fermat **10**
5.1 Résumé 10
5.2 Exercices 10
Exercice 5.22 10
★ Exercice 5.23 11

ECUE

Cette feuille de TD concerne l'ECUE ARITH : arithmétique sur les entiers.

Les **prérequis** sont :
— Manipuler les nombres entiers (somme, produit, quotient essentiellement).
— Connaitre ses tables de multiplications.
— Poser une division euclidienne comme en primaire.
— l'ECUE OBM

Motivation

L'arithmétique, ou théorie des nombres, traite des nombres entiers et de leurs propriétés vis-à-vis de l'addition et de la multiplication. C'est essentiellement la multiplication et son opération inverse, la division, qui nous occuperont. Il est en effet difficile, au sens de la complexité algorithmique, d'énumérer les diviseurs d'un nombre ou les diviseurs communs à deux nombres entiers.

De façon plus générale, les propriétés de divisibilité entre nombres entiers se formalisent de façon extrêmement simple, de même qu'il est simple de les comprendre et de les vérifier quand on est confronté à des petits nombres (par exemple entre 1 et 100). Pendant ce chapitre, purement mathématique, on se focalisera sur cet aspect : formaliser et démontrer les propriétés, en les illustrant par des exemples sur des petits nombres.

Il faut néanmoins avoir à l'esprit que, dans les applications informatiques, ces propriétés sont établies et manipulées avec des nombres beaucoup plus élevés, des nombres qui s'écrivent sur plus de 1000 bits. En effet, pour de tels nombres il est extrêmement coûteux, en terme de temps de calcul, d'énumérer les diviseurs, de trouver un PGCD, etc.

Les algorithmes de chiffrement/déchiffrement de messages, notamment, sont basés sur cette complexité : on considère un message à transmettre comme un grand nombre (après tout, c'est une suite de bits) auquel on fait subir des transformations arithmétiques (élévation à une puissance n, reste d'une division euclidienne par un autre nombre p par exemple), et on considère le résultat obtenu comme le message codé. Quand on ne connait pas la «clé privée», le déchiffrement du message est très long, de l'ordre de quelques siècles de calcul.

Un autre ECUE du second semestre revisitera certaines notions vues dans ce chapitre : nous parlerons d'arithmétique des ***polynômes***. En effet, comme les nombres entiers, les polynômes peuvent être multipliés entre eux ou, au contraire, factorisés. Par exemple, le polynôme $P = X^2 - 3X + 2$ peut être factorisé en $(X-1)(X-2)$, de la même façon que le nombre entier 6 peut être factorisé en 2×3. Plusieurs notions vues maintenant sur les nombres entiers seront transcrites dans l'ensemble des polynômes.

Attendus

Quand elle est utilisée dans un code informatique, l'arithmétique met en jeu des nombres très élevés dans le but d'introduire de la complexité (chiffrement/déchiffrement de messages). Cependant, dans cet ECUE qui ne fait pas intervenir de programmation, on se limitera à des calculs sur de petits nombres, mais on vous demandera déjà de réfléchir à une mise en œuvre ***efficace*** des algorithmes.

Les AAV et leurs détails sont les suivants :

1. Identifier le reste et le quotient d'une division euclidienne ainsi que les cas de divisibilité.
   (a) Formuler mathématiquement la relation de divisibilité
   (b) Identifier le reste et le quotient d'une division euclidienne et la distinguer d'une autre division

2. Manipuler et composer des relations de congruence : additions, multiplications, inversions quand c'est possible, élévation à la puissance.

   (a) Simplifier des calculs en utilisant la congruence
   (b) Composer des relations de congruence par additions, multiplications et divisions quand c'est possible
   (c) Utiliser le théorème de Bézout pour déterminer les éléments inversibles modulo n et trouver leur inverse
   (d) Calculer les puissances d'un entier modulo p en utilisant le petit théorème de Fermat

3. Mettre en œuvre des algorithmes de calculs arithmétiques (Bézout, Euclide, puissances, inverse modulaire, factorisation)
   (a) Exécuter l'algorithme d'Euclide pour déterminer le PGCD de deux nombres entiers et trouver une relation de Bézout
   (b) Déterminer la décomposition d'un nombre entier en facteurs premiers
   (c) Utiliser les décompositions en facteurs premiers de deux nombres entiers pour énumérer leurs diviseurs communs et trouver leur PGCD
   (d) Tester si un nombre est premier ou non
   (e) Résoudre une équation diophantienne en utilisant le théorème de Gauss

1 Relation de divisibilité sur les entiers et division euclidienne

1.1 Résumé

La relation de divisibilité constitue la première étape dans l'approche des ensembles d'entiers par l'opération de produit : c'est une comparaison qui détermine si un entier peut être écrit comme multiple d'un autre, c'est-à-dire si l'on peut, en ajoutant plusieurs fois un nombre donné, obtenir le nombre voulu. Néanmoins, c'est une relation partielle ; il est en effet assez peu probable [1] que parmi deux entiers pris au hasard, l'un des deux soit multiple de l'autre. Il va donc falloir compléter cette notion par des approches plus fines : ce sera l'objet des sections suivantes.

Les intérêts de cette notion en informatique sont nombreux : en effet, pouvoir décomposer un entier en produit d'entiers plus petits ouvre la porte aux stratégies de diviser pour régner. Une factorisation non triviale d'un entier scinde en effet un problème en deux sous-problèmes beaucoup plus petits ; il sera en général moins coûteux de résoudre ces problèmes simplifiés et de recoller les résultats que de travailler avec des grands nombres, le côté logarithmique de la complexité des opérations impliquées offrant un gain substantiel en temps et en espace. De plus, dans le cas où les sous-problèmes sont indépendants, on peut même paralléliser les calculs ce qui permet d'avoir un gain de temps encore plus important [2].

Si la divisibilité ne permet pas toujours de comparer deux entiers positifs a et b, on peut néanmoins toujours approcher un nombre par un multiple d'un autre, moyennant un certain reste r : l'identité $a = bq + r$ est ce que l'on appelle une division de a par b. La division euclidienne est celle dont le reste r est positif mais strictement inférieur au diviseur b.

1.2 Exercices

Exercice 1.1

1. Chercher tous les diviseurs positifs de 84 puis de 60.
2. Les diviseurs de 60 divisent-ils 120 ? divisent-ils 30 ?
3. Quels sont les diviseurs communs positifs à 84 et 60 ?

1. Une fois les nombres choisis, la probabilité est en fait égale à l'inverse du plus petit des deux nombres.
2. Un exemple d'exploitation de la factorisation d'entiers pour paralléliser des calculs est donné dans la section 5 de votre poly AFIT.

4. 12 est un diviseur commun de 84 et 60, est-ce que 12 divise $84+60$? $84-60$?

Exercice 1.2

Soient a, b et c trois entiers relatifs, tels que $c \mid a$ et $c \mid b$.

1. Montrer que $c \mid (a+b)$.
2. Montrer que pour tout $u \in \mathbb{Z}$, $c \mid au$.
3. En déduire que pour tout couple (u, v) de $\mathbb{Z}^2$, $c \mid (au+bv)$.

Exercice 1.3

1. Étudier toutes les relations de divisibilité existant sur $[\![1; 12]\!]$.
2. Montrer que la relation de divisibilité sur $[\![1; 12]\!]$ est une relation d'ordre.
   Est-elle totale ou partielle ? Peut-on étendre ce résultat sur $\mathbb{N}$? sur $\mathbb{Z}$?
3. Établir le diagramme de Hasse de cette relation sur l'ensemble $[\![1; 12]\!]$.

Exercice 1.4

1. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Rappeler l'énoncé du théorème de la division euclidienne de a par b.
2. En admettant l'existence du couple (q, r) résultat de cette division, montrer son unicité.
3. Trouver le quotient et le reste de la division euclidienne de a par b dans les cas suivants :
   (a) $a = 24$ et $b = 5$.
   (b) $a = 24$ et $b = -5$
   (c) $a = -24$ et $b = 5$
   (d) $a = -24$ et $b = -5$
   (e) $a = 5$ et $b = 24$
   (f) $a = 5$ et $b = -24$
   (g) $a = -5$ et $b = 24$
   (h) $a = -5$ et $b = -24$

2 Relation de congruence

2.1 Résumé

La notion de congruence tire son intérêt de la régularité de la répartition des multiples d'un entier donné : elle permet de matérialiser une symétrie profonde dans l'organisation des nombres par rapport aux multiples d'un nombre donné. C'est une relation d'équivalence, dont toutes les classes sont de structure identique : elle permet de classer simplement les entiers par rapport à un entier de référence donné, loin de l'apparence chaotique et du manque d'informations qui semblent se dégager de la relation de divisibilité.

Le reste de la division euclidienne de a par b donne un représentant simple (compris entre 0 et $b-1$) de la classe d'équivalence de a : $a \equiv r\ [b]$.

L'arithmétique modulaire (qui concerne les entiers vus via une relation de congruence) est d'intérêt fondamental en informatique : structurellement, car les opérations sur les entiers dans un ordinateur se font sur un intervalle limité (la capacité) et donc sont en fait des opérations de congruence relativement à l'entier maximum ; et de manière plus appliquée en cryptographie, où les propriétés des congruences permettent d'établir des méthodes de chiffrement faciles à calculer et implémenter et difficiles à casser.

Cette relation étant compatible avec les opérations d'addition et de multiplication, elle est d'utilisation très facile, et permet souvent de ne dégager de calculs lourds que la partie qui va nous intéresser au final. Mieux, une gestion intelligente des congruences dans lesdits calculs aide à faire disparaître des problèmes intermédiaires comme les dépassements de capacité et réduit en général drastiquement

le temps nécessaire aux calculs : non seulement on fait moins d'opérations, mais elles concernent des nombres plus petits et sont donc plus rapides.

Cette notion peut être étendue à d'autres objets que les entiers. On a déjà vu comment les arguments des nombres complexes sont en fait définis via une relation de congruence modulo 2π. Mais on peut même songer à des congruences de polynômes, puisque ceux-ci vérifient toutes les propriétés structurelles des entiers qui nous intéressent ici...

2.2 Exercices

Exercice 2.5

1. Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Expliquer pourquoi $\exists\, !b \in [\![0, n-1]\!]$, $a \equiv b\,[n]$.
2. Faire la division euclidienne de 158 par 6 et trouver un entier k, $0 \leqslant k < 6$, tel que : $158 \equiv k\ [6]$
3. Dans le tableau ci-dessous des entiers de 0 à 29, entourer en bleu les entiers n tels que $n \equiv 0\ [6]$. Entourer en rouge les entiers p tels que $p \equiv 2\ [6]$. Qu'observez-vous ?

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29

4. On observe que $8 \equiv 2\ [6]$, $26 \equiv 2\ [6]$ et $15 \equiv 3\ [6]$.
   (a) Quelle est la relation de congruence entre 8 et 26 ?
   (b) Que peut-on dire de $8 + 15$? 8×15 ? 2×8 ?
   (c) $20 \equiv 2\ [6]$. Que peut on en déduire pour 10 ?

Exercice 2.6

Soit $n \in \mathbb{N}^*$.

1. Montrer que la relation de congruence modulo n est une relation d'équivalence.
2. Montrer que cette relation est compatible avec l'addition et la multiplication, c'est-à-dire :

$$\text{Si } a \equiv c\ [n] \text{ et } b \equiv d\ [n] \text{ alors } a + b \equiv c + d\ [n],\ ab \equiv cd\ [n] \text{ et } \forall\, k \in \mathbb{N}^*,\ a^k \equiv c^k\ [n].$$

3. Remplir le tableau suivant, sachant que dans chaque case, votre réponse doit être un entier entre 0 et 10.

a	-2	1	28	36	35
b	3	4	14	-4	49
$a\,[11]$					
$b\,[11]$					
$a^3 - 2b\,[11]$					

4. Trouver le reste de la division euclidienne de 13^{126} par 5.

Exercice 2.7

Quelques critères de divisibilité

On note b_i les digits d'un entier n en base 10, de telle sorte que n s'écrive $n = \sum_{i \geqslant 0} b_i 10^i$ avec $0 \leqslant b_i \leqslant 9$ pour tout $i \geqslant 0$.

1. a. Montrer que $n \equiv b_0\ [2]$ et $n \equiv b_0\ [5]$.

b. En déduire un critère de divisibilité par 2 et par 5.

2. a. Montrer que $n \equiv \sum_{i \geqslant 0} b_i$ [3] et $n \equiv \sum_{i \geqslant 0} b_i$ [9].

   b. En déduire un critère de divisibilité par 3 et par 9.

3. a. Montrer que $n \equiv \sum_{i \geqslant 0} (-1)^i b_i$ [11].

   b. En déduire un critère de divisibilité par 11.

4. Tester ces critères sur 239 734.

Exercice 2.8

1. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.
2. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{n+3} - 5.4^{4n}$ est divisible par 11.
3. (**travail personnel**) Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $15^{4n+2} - 5^{2n+11}$ est divisible par 11 (sans utiliser le petit théorème de Fermat).

3 Primalité et primalité relative

3.1 Résumé

Les nombres premiers sont en quelque sorte les briques de base de l'ensemble des entiers, quand on essaie de le construire par des multiplications : ce sont les nombres qui ne peuvent pas être scindés en produit d'entiers inférieurs. Un résultat crucial de l'arithmétique des entiers est que tout entier non nul s'écrit de manière unique comme un produit de facteurs premiers, ce qui implique qu'on peut entièrement caractériser l'ensemble des entiers par celui des nombres premiers, au regard de la multiplication. Cette connaissance structurelle ouvre la porte à des approches de type "diviser pour régner" pour tout ce qui concerne des calculs ou raisonnements pour lesquels la multiplication est l'opération cruciale.

Cependant, la difficulté de cette modélisation réside dans le fait qu'il est difficile (coûteux) de déterminer si un nombre est un nombre premier, de trouver des nombres premiers, d'effectuer une décomposition en produit de nombres premiers. Si l'on connaît de plus en plus de résultats théoriques sur les nombres premiers, ceux-ci sont en général loin d'être exploitables et il n'existe à l'heure actuelle aucune méthode efficace pour générer des nombres premiers. La difficulté de ce problème est ce qui en fait un candidat idéal pour la cryptographie, où la résolution de telles questions sera une manière d'implémenter une couche de difficulté dans les questions de chiffrement et déchiffrement.

S'il est peu aisé de déterminer les facteurs d'un nombre (sauf bien sûr par force brute), on a en revanche un algorithme efficace qui permet de déterminer si deux nombres ont des facteurs en commun : l'algorithme d'Euclide. Fondé sur la division euclidienne, cet algorithme permet de déterminer facilement le PGCD de deux entiers : en effet, on peut y parvenir en itérant des divisions euclidiennes (cf. exercice 3-15).

De la simplicité de cet algorithme, on déduit qu'il est en fait plus facile de trouver des facteurs communs à deux entiers que de trouver un facteur d'un seul entier, on peut donc imaginer une recherche de décomposition comme une suite de recherches de PGCD [3]...

Ainsi, la notion de primalité relative occupe un rôle important en arithmétique modulaire, non seulement car elle permet de faciliter de nombreuses approches (diviser pour régner, parallélisation de sous-problèmes indépendants, simplifications via le lemme de Gauss), mais aussi car c'est un problème que l'on sait résoudre facilement.

3. Cette méthode est notamment utilisée pour factoriser des polynômes, étant par exemple à la base des algorithmes de Berlekamp ou de Cantor-Zassenhaus.

3.2 Exercices

Exercice 3.9

1. Reprendre le diagramme de Hasse de l'exercice 1-3
   (a) Quels sont les nombres premiers compris dans $[\![1;12]\!]$?
   (b) Comment se positionnent-ils dans ce diagramme ?
2. Reprendre les diviseurs de 84 à l'exercice 1-1 .
   (a) Remarquer que ces diviseurs vont par couples (d, d') tels que $d \leqslant d'$ et $dd' = 84$.
   (b) En déduire que, dans chacun de ces couples, $d \leqslant \sqrt{84}$.

Exercice 3.10

Soit n un entier supérieur ou égal à 2. On note d son plus petit diviseur strictement supérieur à 1 (remarque : un tel entier existe, car l'ensemble des diviseurs strictement supérieurs à 1 étant une partie non vide – elle contient n – de $\mathbb{N}$, elle admet un plus petit élément).

1. Montrer que d est un nombre premier.
2. Montrer que si n n'est pas premier alors $d \leqslant \sqrt{n}$.
3. En déduire que si aucun nombre premier inférieur ou égal à $\sqrt{n}$ ne divise n, alors n est premier.

Exercice 3.11

En utilisant le crible d'ératosthène, trouver tous les nombres premiers inférieurs à 100 dans le tableau ci-dessous.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

★ **Exercice 3.12**

Montrer que l'ensemble des nombres premiers $\mathcal{P}$ est infini.

Exercice 3.13

1. (a) Décomposer en facteurs premiers 84 et 60.
   (b) Reprendre les diviseurs de 84 et de 60 énumérés à l'exercice 1-1. Quel est leur lien avec les facteurs premiers de 84 et 60 ?
   (c) Que peut-on dire des diviseurs communs à 84 et 60 ?
2. (a) Décomposer 700 en produits de facteurs premiers.
   (b) Soit $d \in \mathbb{N}^*$ qui divise 700. Quelle est la forme générale de la décomposition en facteurs premiers de d ?
   (c) Combien 700 admet-il de diviseurs positifs distincts ?

Exercice 3.14

Décomposer en produits de facteurs premiers les nombres 9360 et 4200. En déduire leur PGCD.

Exercice 3.15

1. Soit $(a, b) \in \mathbb{Z}^2 \backslash \{(0, 0)\}$, on écrit la division $a = bq + r$.
   Montrer que $a \wedge b = b \wedge r$.
2. Expliquer pourquoi l'algorithme d'Euclide converge, et pourquoi le dernier reste non nul est le PGCD des deux entiers de départ.

Exercice 3.16

En utilisant l'algorithme d'Euclide, calculer le PGCD de 9360 et 4200.
Comparer avec la méthode utilisée dans l'exercice 3-14.

4 Théorème de Bézout

4.1 Résumé

Le théorème de Bézout est un théorème existentiel, c'est-à-dire qu'il énonce qu'il existe des solutions à un problème donné : ici écrire le PGCD de deux nombres comme une somme de multiples de ces nombres. Souvent, ce genre de résultat est difficilement utilisable de manière appliquée ; mais ce n'est pas le cas ici puisque l'on dispose d'un méthode constructive et efficace pour démontrer le théorème en en donnant une solution particulière : celle-ci utilise l'algorithme d'Euclide, et la compatibilité de la forme voulue (combinaision entière) avec les opérations de la division euclidienne (addition et multiplication).

Remarquez que si précédemment on pouvait se cantonner aux entiers positifs, ce n'est plus le cas avec le théorème de Bézout qui trouve des coefficients sous forme d'entiers relatifs.

Le théorème de Bézout trouve des applications pratiques en cryptographie : la recherche de coefficients de Bézout donne un moyen de résoudre des équations diophantiennes qui peuvent correspondre à des inversions modulaires, permettant le décodage efficace d'un message, voire le cassage d'un code.

4.2 Exercices

Exercice 4.17

1. Reprendre les diviseurs communs de 84 et 60, identifier le pgcd. Quel est le lien entre les diviseurs communs et le pgcd en termes de divisibilité ?
2. On considère deux nombres relatifs a et b tels que $(a, b) \neq (0, 0)$.
   (a) Montrer que tout diviseur commun de a et b divise aussi $a \wedge b$.
   (b) Montrer que tout nombre peut s'écrire sous la forme $au + bv$ si et seulement si c'est un multiple de $a \wedge b$.

Exercice 4.18

Soit $(a, b, c) \in \mathbb{N}^3$.

1. À l'aide du théorème de Bézout, montrer que a est premier avec b et c si et seulement si a est premier avec bc.
2. À l'aide du théorème de Bézout, montrer que a est premier avec b si et seulement si $a + b$ est premier avec ab.

Exercice 4.19

À quelle condition sur $n \in \mathbb{N}$, le nombre entier $3^{n+3} + n.4^{4n}$ est-il divisible par 11 ?

Exercice 4.20

1. À l'aide de l'algorithme d'Euclide, calculer le PGCD de 237 et 156 et donner un couple de coefficients de Bézout associés.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $237x + 156y = 3$.
3. Trouver tous les entiers $z \in \mathbb{Z}$ tels que $52z \equiv 1\ [79]$.

Exercice 4.21

(Travail Maison) Résoudre dans $\mathbb{Z}^2$ les équations ci-dessous en respectant les étapes suivantes :

a. Trouver une solution particulière.

b. Déterminer l'ensemble des solutions en citant le Lemme de Gauss au moment où vous l'utilisez.

(E1) $544x - 944y = 160$

(E2) $134x - 56y = 24$

5 Petit théorème de Fermat

5.1 Résumé

Le petit théorème de Fermat donne un résultat simple sur le calcul de puissances modulo un nombre premier. L'exponentiation modulaire est un problème crucial en cryptographie : pour les algorithmes RSA et ElGamal, c'est l'opération qui permet le chiffrement et le déchiffrement des messages. Cette opération très coûteuse [4] par la méthode naïve se retrouve extrêmement simplifiée grâce au résultat énoncé par le petit théorème de Fermat, qui réduit énormément le nombre d'opérations nécessaires tout en utilisant des nombres plus petits. C'est donc un résultat théorique structurel qui permet d'améliorer la facilité et la rapidité des calculs, ce qui est d'autant plus important que la solidité des algorithmes énoncés vient de l'utilisation de nombres extrêmement grands pour limiter les possibilités de résolution par force brute. Ainsi, on peut augmenter la complexité de cassage du problème avec des nombres gigantesques sans impact négatif sur son efficacité pour l'utilisateur.

Le théorème de Fermat peut être reformulé ainsi : (p premier) $\implies$ ($a \wedge p = 1 \implies a^{p-1} \equiv 1\ [p]$). Cette implication n'est pas une équivalence : il existe en effet des nombres [5] qui ne sont pas premiers mais vérifient la propriété de droite. Ainsi on ne peut pas utiliser cette relation pour caractériser à coup sûr un nombre premier. On peut néanmoins en déduire des tests probabilistes de primalité ; on peut également considérer que les nombres en question sont aussi utiles que les nombres premiers pour l'utilisation que l'on compte en faire. On parle alors de pseudo-primalité : un nombre n est pseudo-premier de base a si $a^{n-1} \equiv 1\ [n]$, et absolument pseudo-premier s'il vérifie la propriété pour tout a premier avec lui.

5.2 Exercices

Exercice 5.22

1. Calculer le reste dans la division euclidienne de 529^{326} par 17.
2. Calculer le reste dans la division euclidienne de 288^{288} par 29.
3. Soient $n \in \mathbb{N}$ et $A_n = 15^{4n+2} - 5^{2n+11}$. Montrer que $11 \mid A_n$.

4. voire impossible pour des raisons de capacité
5. appelés pseudo-premiers, ou nombres de Carmichael. Les plus petits sont 561, 1105 et 1729.

★ **Exercice 5.23**

Le but de cet exercice est de donner une preuve différente[6] du petit théorème de Fermat : une démonstration par récurrence qui utilise le lemme de Gauss et la formule du binôme.

Soit p un nombre premier.

1. Montrer que pour tout entier k vérifiant $0 < k < p$, alors p divise C_p^k.
   Remarque : ce résultat n'est pas vrai pour un nombre composé[7] (vous pouvez chercher des contre-exemples).
2. Montrer par récurrence sur $n \in \mathbb{N}$ que $n^p \equiv n\ [p]$.
3. On suppose maintenant que n n'est pas un multiple de p. Montrer alors que $n \wedge p = 1$, puis en déduire que $n^{p-1} \equiv 1\ [p]$.

6. Vous trouverez dans votre poly AFIT une preuve du théorème d'Euler : si $a \wedge n = 1$ alors $a^{\varphi(n)} \equiv 1\ [n]$, où φ désigne la fonction indicatrice d'Euler. Le petit théorème de Fermat en est un cas particulier.

7. c'est-à-dire un nombre qui peut s'écrire comme un produit d'au moins deux facteurs premiers (possiblement identiques), ce qui équivaut à dire qu'il admet un diviseur strictement compris entre 1 et lui-même ; il s'agit donc de tout nombre non premier supérieur ou égal à 4.