Mathématiques Discrètes

Chapitre 6
Arithmétique

Leo Donati   Noëlle Stolfi

Université de Nice Sophia Antipolis
IUT Nice Côte d'Azur
DUT Informatique

2015-2016

Chapitre 6 : Arithmétique

1. Ensemble $\mathbb{N}$
   - Propriétés
   - Les nombres premiers
   - PGCD et PPCM
   - Théorème de Bezout
   - Equations diophantiennes
2. Congruences
   - Relation de congruence
   - Propriétés
   - Critères de divisibilité
   - Équations aux congruences
3. $\mathbb{Z}/n\mathbb{Z}$
   - Définition
   - Propriétés
   - Théorème d'Euler

ENSEMBLE $\mathbb{N}$

PROPRIÉTÉS

L'ensemble des entiers naturels, noté $\mathbb{N}$, est muni de deux lois de composition internes : l'addition et la multiplication. Ces lois sont :

- commutatives et associatives
- possèdent des éléments neutres 0 et 1
- la multiplication est distributive par rapport à l'addition

De plus $\mathbb{N}$ est totalement ordonné par par $\leq$ défini par :

$$a \leq b \Longleftrightarrow \exists c \epsilon \mathbb{N}, \text{tel que } a + c = b$$

et il existe une relation de divisibilité définie par

$$a | b \Longleftrightarrow \exists c \epsilon \mathbb{N}, \text{tel que } a \times c = b$$

Division euclidienne

Définition

Quels que soient les nombres entiers relatifs a et b, avec $b \neq 0$ on peut faire la division euclidienne de a par b et obtenir une unique paire d'entiers (q, r) appelés quotient et reste avec $0 \leq r < |b|$, tels que :

$$a = b \times q + r$$

Exemples

$$\begin{aligned} 47 &= 9 \times 5 && + 2 \\ -47 &= 9 \times -6 && + 7 \\ 47 &= -9 \times -5 && + 2 \\ -47 &= -9 \times 6 && + 7 \end{aligned}$$

Vocabulaire

Vocabulaire

Lorsque $a = b \times q$ on dit que :

- a est divisible par b (car le reste est nul) ;
- a est un multiple de b ;
- b divise a ;
- b est un diviseur de a ;
- b est un facteur de a ;

et on note $b|a$.

Exemple

Les diviseurs de 12 sont $1, 2, 3, 4, 6, 12$.
Les multiples de 12 sont $0, 12, 24, 36, \ldots 12 \times i$.

Les nombres premiers

Définition

Un nombre $p \in \mathbb{N}$ est premier s'il admet exactement deux diviseurs 1 et lui-même.

Exemple

L'entier 6 n'est pas premier. L'entier 5 est premier.

Questions

On va voir que les nombres premiers sont les briques de base avec lesquelles on obtient tous les nombres. Mais :

1. Comment savoir si un nombre est premier ou pas ?
2. Comment trouver les nombres premiers ?
3. Combien y a-t-il de nombres premiers ?

Test de primalité

Principe

Pour savoir si N est premier on vérifie qu'il n'a pas de diviseur d avec $1 < d < N$.

Idées d'algorithme

- Algorithme 1 : on fait varier d de 2 à $N-1$ et on divise N par d. Si aucune division ne tombe juste, alors on peut affirmer que N est premier. Long : $N-3$ divisions dans le pire des cas
- Algorithme 2 : on remarque que si $N = d_1 \times d_2$ alors l'un des diviseurs est forcément $\leq \sqrt{N}$. Donc il suffit de faire varier d de 2 à $\sqrt{N}$. Donc $\sqrt{N}$ test dans le pire des cas.
- Algortihme 3 : si N n'est pas divisible par 2 alors ça ne sert à rien de tester sa divisibilité par 4, 6, 8.... On teste seulement la divisibilité par 2 et puis par les impairs ...

Le Crible d'Eratosthène

~~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	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156

Crible de 2

~~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~~	101	~~102~~	103	~~104~~	105	~~106~~	107	~~108~~
109	~~110~~	111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119	~~120~~
121	~~122~~	123	~~124~~	125	~~126~~	127	~~128~~	129	~~130~~	131	~~132~~
133	~~134~~	135	~~136~~	137	~~138~~	139	~~140~~	141	~~142~~	143	~~144~~
145	~~146~~	147	~~148~~	149	~~150~~	151	~~152~~	153	~~154~~	155	~~156~~

Crible de 3

~~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~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	115	~~116~~	~~117~~	~~118~~	119	~~120~~
121	~~122~~	~~123~~	~~124~~	125	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~
133	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~	~~141~~	~~142~~	143	~~144~~
145	~~146~~	~~147~~	~~148~~	149	~~150~~	151	~~152~~	~~153~~	~~154~~	155	~~156~~

CRIBLE DE 5

~~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~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	119	~~120~~
121	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~
133	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~	~~141~~	~~142~~	143	~~144~~
~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~	151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~

CRIBLE DE 7

~~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~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
121	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~
~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~	~~141~~	~~142~~	143	~~144~~
~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~	151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~

Crible de 11

~~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~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~
~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~	~~141~~	~~142~~	~~143~~	~~144~~
~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~	151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~

Crible de 13

~~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~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~
~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~	~~141~~	~~142~~	~~143~~	~~144~~
~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~	151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~

Facteurs premiers

Théorème

Tout nombre entier $N \geq 2$ admet au moins un diviseur premier.

Démonstration par récurrence sur N

Si $N = 2$ alors N admet 2 comme diviseur.
Sinon supposons que l'énoncé soit vrai pour tous les entiers inférieurs à N et prouvons-le pour N :

- si N est premier, comme il se divise soi-même alors il n'y a rien à démontrer.
- sinon, comme N n'est pas premier et il admet un diviseur d avec $1 < d < N$. En appliquant l'énoncé à d je sais que d a un diviseur premier p. Mais si $p|d$ et $d|N$ alors $p|N$.

Infinité des nombres premiers

Théorème (Euclide)

L'ensemble des nombres premiers est infini.

Démonstration par l'absurde

Supposons que l'ensemble des nombres premiers soit fini.
Alors il est composé de n premiers $p_1, \ldots, p_n$. Je pose

$$N = p_1 \ldots p_n + 1$$

Alors N admet un facteur premier, or N n'est divisible par aucun des premiers p_i (reste égal à 1). Absurde.

Décomposition en facteurs premiers

Théorème

Tout nombre premier peut être décomposé en un produit de facteurs premiers.

Ecriture

Cette écriture :

$$n = p_1^{a_1} \dots p_r^{a_r}$$

avec $p_1 < \dots < p_r$ et p_i premier $\forall i = 1, \dots, r$ est unique.

Exemple

$68 = 2^2 \times 17.$

PGCD,PPCM

Définition

Soient $a, b \in \mathbb{N}$.

- Le pgcd de a et b est le plus grand des diviseurs communs de a et b.
- le ppcm de a et b est le plus petit des multiples communs de a et de b.

Exemple

$pgcd(114, 30) = 6$ car $114 = 2.3.19$ et $30 = 2.3.5$.
$ppcm(114, 30) = 2.3.5.19 = 570$

Lien entre PGCD et PPCM

Théorème

Soient $a, b \in \mathbb{N}$ on a :

$$ppcm(a, b) = \frac{a \times b}{pgcd(a, b)}$$

Définition

Si $pgcd(a, b) = 1$ on dit que a et b sont premiers entre eux.
Dans ce cas, ils n'ont aucun facteur commun et

$$ppcm(a, b) = a \times b$$

Algorithme d'Euclide

Proposition

Soit la division euclidienne de a par b

$$a = b \times q + r$$

alors $pgcd(a,b) = pgcd(b,r)$

Algorithme d'Euclide

L'algorithme d'Euclide consiste à faire la division euclidienne de a par b, puis celle de b par le reste r ainsi de suite jusqu'à obtenir un reste nul.
Alors le dernier reste non nul est le pgcd de a et de b.

Exemple de calcul

Calculons le $pgcd(585, 247)$

$$\begin{array}{rcrcr}
585 & = & 247 \times 2 & + & 91 \\
247 & = & 91 \times 2 & + & 65 \\
91 & = & 65 \times 1 & + & 26 \\
65 & = & 26 \times 2 & + & 13 \\
26 & = & 13 \times 2 & + & 0
\end{array}$$

Donc $pgcd(585, 247) = 13$.

Théorème de Bezout

Théorème

Soient $a, b \in \mathbb{N}^*$. Il existe des entiers relatifs u et v tels que

$$pgcd(a, b) = a \times u + b \times v$$

Cette équation s'appelle identité de Bezout et u et v sont les coefficients de Bezout.

Exemple

Si $a = 585$ et $b = 247$ alors on a vu que $pgcd(585, 247) = 13$ et l'identité de Bezout est

$$585 \times (-8) + 247 \times 19 = 13$$

Conséquences

Théorème

Soient $a, b \in \mathbb{N}^*$. Alors a et b sont premiers entre eux si et seulement si $\exists u, v \in \mathbb{Z}$ t.q. $au + bv = 1$.

Démonstration

Le théorème de Bezout donne déjà la preuve de l'implication directe.
Pour la réciproque, soit d le pgcd de a et b ; alors $d|a$ donc $d|ua$; de même $d|b$ donc $d|bv$.
Il en résulte que $d|(au + bv) \Rightarrow d|1$ donc $d = 1$.

Lemme de Gauss

Lemme de Gauss

Soient $a, b, c \in \mathbb{N}^*$. Si a divise bc et si a et b sont premiers entre eux alors a divise c.

Démonstration

Si a et b sont premiers entre eux alors il existe u et v tels que $au + bv = 1$.
En multipliant par c on obtient $ac \cdot u + bc \cdot v = c$.
Or comme a divise ac et a divise bc alors a divise c

Le lemme de Gauss est une généralisation du lemme d'Euclide :

Lemme d'Euclide

Si un nombre premier p divise le produit ab alors $p|a$ ou $p|b$.

Algorithme d'Euclide étendu

Algorithme

C'est une version de l'algorithme d'Euclide, qui permet aussi de trouver les coefficients de Bezout, facilement programmable.
A partir de deux entiers a et b, l'algorithme calcule $pgcd(a,b)$ ainsi que deux entiers relatifs x et y tels que $ax+by=pgcd(a,b)$.
Algorithme :

- Entrée : a, b
- Début : $(a,1,0,b,0,1)$
- Boucle : (d,x,y,d',x',y') donne $(d',x',y',r,x-qx',y-qy')$ avec $d=qd'+r$
- Fin : $(d,x,y,0,x',y')$

Alors $d=pgcd(a,b)$ et $d=ax+by$ et $0=ax'+by'$.

Exemple d'application

Exemple

Appliquons cet algorithme à $a = 47$ et $b = 35$.

- $(47, 1, 0, 35, 0, 1)$ et $47 = 35 \times 1 + 12$
- $(35, 0, 1, 12, 1, -1)$ et $35 = 12 \times 2 + 11$
- $(12, 1, -1, 11, -2, 3)$ et $12 = 11 \times 1 + 1$
- $(11, -2, 3, 1, 3, -4)$ et $11 = 1 \times 11 + 0$
- $(1, 3, -4, 0, -35, 47)$

Donc $pgcd(47, 35) = 1$
Identité de Bezout : $47 \times 3 + 35 \times (-4) = 1$.
Les deux derniers entiers nous donnent l'égalité du ppcm :
$47 \times (-35) + 35 \times 47 = 0$.

Equation diophantienne

Définition

Les équations diophantiennes sont des équations dont les inconnues sont des nombres entiers.
Par exemple, résoudre pour $x, y \in \mathbb{Z}$

$$47x + 35y = 8$$

Résolution

Résolution à l'aide de l'identité de Bezout

L'application de l'algorithme d'Euclide étendu avec $a = 47$ et $b = 35$ a produit deux identités

$$\begin{aligned} 47 \times 3 + 35 \times (-4) &= 1 \\ 47 \times (-35) + 35 \times 47 &= 0 \end{aligned}$$

Alors

- en multipliant la première équation par 8 on obtient une solution $x = 24$ et $y = -32$
- en ajoutant k fois la seconde équation, on obtient toutes les solutions $x = 24 - 35k$ et $y = -32 + 47k$ $\forall k \in \mathbb{Z}$.

Chapitre 6 : Arithmétique

Congruence modulo n

Définition

Soit n un entier supérieur ou égal à 2.
On définit la relation de congruence modulo n sur $\mathbb{Z}$ de la façon suivante :

$$a \equiv b \mod (n)$$

si et seulement si n divise la différence $b - a$ (ou $a - b$).

Exemples

- $5 \equiv 3 \mod (2)$
- $17 \equiv 2 \mod (3)$
- si a est pair $a \equiv 0 \mod (2)$ et si a est impair $a \equiv 1 \mod (n)$.
- $49 \equiv 4 \mod (5)$
- $27 \equiv 3 \mod (4)$

Propriétés

Propriétés de la congruence modulo n

1. $a \equiv b \mod (n) \Leftrightarrow \exists k \in \mathbb{Z} \quad a = b + k \times n$;
2. La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$
3. compatible avec l'addition : si $a \equiv b \mod (n)$ et si $c \equiv d \mod (n)$ alors
$$a + c \equiv b + d \mod (n)$$
4. compatible avec la multiplication : si $a \equiv b \mod (n)$ et si $c \equiv d \mod (n)$ alors
$$ac \equiv bd \mod (n)$$
5. a est divisible par $b \Leftrightarrow a \equiv 0 \mod b$.

Critères de divisibilité

Principe

En base 10 on trouve des critères de divisibilité par n, à partir du calcul
$$10^k \mod n \quad \forall k \in \mathbb{N}$$

Divisibilité par 2 et par 5

Comme
$$10^k \equiv 0 \mod 2 \text{ et } 10^k \equiv 0 \mod 5 \quad \forall k \geq 1$$
alors un nombre N est divisible par 2 ou par 5 si et seulement si son chiffre des unités est divisible par 2 ou par 5.

Divisibilité par 3

Théorème

Un nombre N est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Démonstration

Comme

$$10^k \equiv 1 \mod 3 \quad \forall k \geq 0$$

alors

$$c_k 10^k + c_{k-1} 10^{k-1} + \cdots + c_1 10 + c_0 \equiv c_k + c_{k-1} + \cdots + c_1 + c_0 \mod 3$$

Divisibilité par 11

Théorème

Un nombre N est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

Démonstration

Comme

$$10^k \equiv (-1)^k \mod 11 \quad \forall k \geq 0$$

alors

$$c_k 10^k + c_{k-1} 10^{k-1} + \cdots + c_2 10^2 + c_1 10 + c_0 \equiv$$
$$(-1)^k c_k + (-1)^{k-1} c_{k-1} + \cdots + c_2 - c_1 + c_0 \mod 11$$

Équations aux congruences

Équation type à résoudre

Soit $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$. Trouver $x \in \mathbb{Z}$ tel que

$$ax \equiv b \mod n$$

Méthode

Cette équation se ramène à une équation diophantienne de la forme :

$$ax - nk = b$$

donc

1. si $pgcd(a, n)$ ne divise pas b, alors il n'y a pas de solution.
2. sinon il y a une infinité de solution que l'on trouve avec l'algorithme d'Euclide étendu.

Cas particulier

Théorème

$$ax \equiv ac \mod n \Rightarrow x \equiv c \mod \frac{n}{pgcd(a,n)}$$

Exemple

Résoudre

$$\begin{aligned} 6x &\equiv 18 \mod (15) \\ \Rightarrow x &\equiv 3 \mod (5) \end{aligned}$$

Donc $S = \{3 + 5k, \quad k \in \mathbb{Z}\}$

Chapitre 6 : Arithmétique

$\mathbb{Z}/n\mathbb{Z}$

Définition

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence de la relation de congruence modulo n, avec les opérations de somme et produit héritées de $\mathbb{Z}$.

$$[a]_n \in \mathbb{Z}/n\mathbb{Z} = \{b \in \mathbb{Z} \quad a \equiv b \mod n\}$$

Dans $\mathbb{Z}/2\mathbb{Z}$, il y a deux classes

$[0]_2 = \{0; 2; -2; 4; -4; \ldots\}$ et $[1]_2 = \{1; -1; 3; -3; \ldots\}$ et

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\times$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

Exemple

Exemples dans $\mathbb{Z}/10\mathbb{Z}$

C'est un ensemble de nombre "circulaire" car $9+1=0$.
Donc $9=-1$.
Mais le plus déroutant est la multiplication :

- $3\times 7=1$ car dans $\mathbb{N}$ on a $3\times 7=21\equiv 1 \mod 10$
- $3\times 5=5$
- $6\times 5=0$

Comme $3\times 7=1$ on dit que

- 7 est l'inverse de 3, et on peut noter $7=3^{-1}$

Éléments inversibles

Théorème

Un élément $a \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si

$$pgcd(a, n) = 1.$$

Notation

L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$

Conséquence

Si p est premier alors tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles.
On dit alors que $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif.

Indicatrice d'Euler

Indicatrice d'Euler

Si n est un entier, on note $\phi(n)$ le nombre d'éléments inférieurs à n premiers avec n.
La fonction ϕ s'appelle l'indicatrice d'Euler.
D'après ce qu'on a vu $\phi(n) = card((\mathbb{Z}/n\mathbb{Z})^*)$.

ϕ est, en général, difficile à calculer mais on sait :

- si p est premier, $\phi(p) = p - 1$ et $\phi(p^n) = p^n - p^{n-1}$;
- si a et b sont premiers entre eux, $\phi(a \times b) = \phi(a) \times \phi(b)$

Théorème d'Euler

Théorème d'Euler

Si $pgcd(a,n) = 1$, alors

$$a^{\phi(n)} \equiv 1 \mod n.$$

En fait le théorème d'Euler (1761) généralise le petit théorème de Fermat (1640)

(petit) Théorème de Fermat

Si a n'est pas divisible par un nombre premier p alors

$$a^{p-1} \equiv 1 \mod p.$$