Cours d'introduction à l'arithmétique

Razvan Barbulescu
⟨prénom⟩.⟨nom⟩@inria.fr

ENS, 8 mars 2014

1 Introduction

1.1 Définitions

Exemple 1. *Il est* $19h43$. *Combien de temps il reste jusqu'à* $20h22$ *? Si aujourd'hui on est samedi, quel jour de la semaine serons nous dans* 13 *jours ? Pour les minutes on fait des calculs modulo* 60 *et pour les jours de la semaine modulo* 7.

Définition 1. *Soient* N, a *et* b *trois entiers, avec* N *non nul. On dit que* a *est congruent à* b *modulo* N *s'il a le même reste que* b *à la division par* N. *Dans ce cas on note*

$$a \equiv b \pmod{N}.$$

Théorème 1. *Si* N, a, b, c, d *sont cinq entiers tels que*

$$a \equiv b \pmod{N} \quad et \quad c \equiv d \pmod{N}.$$

Alors on a $a + c \equiv b + d \pmod{N}$ *et* $ac \equiv bd \pmod{N}$.

Démonstration. On écrit $a = Nu + b$ et $c = Nv + d$ pour deux entiers u et v. Alors on a $a + c = N(u + v) + (b + d)$, donc $(a + c) \equiv (b + d) \pmod{N}$. De même, on a $ac = N(Nuv + vb + ud) + bd$, donc $ac \equiv bd \pmod{N}$. □

Exercice 1. *Montrer qu'il existe une infinité de nombres premiers congruents à* 3 *modulo* 4.

Démonstration. On suppose par l'absurde que l'ensemble des premiers congruents à 3 modulo 4 est fini : $p_1, \ldots, p_n$. On pose

$$N = 4p_1 \cdot p_2 \cdots p_n + 3.$$

Comme N est impair, tous ses facteurs premiers sont impairs. Si tous ses facteurs étaient congruents à 1 modulo 4, il serait également congruent à 1 modulo 4. Donc N est divisible par p_i pour un indice $i \in [1, n]$. Mais alors p_i divise $N - 4p_1 \cdots p_n = 1$. Contradiction, donc la supposition faite est fausse. □

Exercice 2. *Donner des critères de divisibilité par* 5, 4, 3, 9 *et* 11.

Démonstration. Prenons l'exemple de la divisibilité par 11. Un nombre $\overline{a_k a_{k-1} \cdots a_0}_{10} = \sum_{i=0}^{k} 10^i a_i$ est divisible par 11 si et seulement si

$$\sum_{i=0}^{k} 10^i a_i \equiv 0 \pmod{11}.$$

Or $10^i \equiv (-1)^i \pmod{11}$. Donc on doit regarder le reste modulo 11 de

$$a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$$

. □

Par exemple, pour tester si 5181 est divisible par 11 on calcule

$$1 - 8 + 1 - 5 \equiv -11 \equiv 0 \pmod{11}.$$

1.2 Relations d'équivalence

Définition 2. *Une relation sur l'ensemble E est donnée par un sous-ensemble de $E \times E$.*

Exemple 2. *Si deux entiers ont la relation $\{(n, n+1) \mid n \in \mathbb{N}\}$ ont dit qu'il sont consécutifs ou que le premier est le prédécesseur du second. Si deux entiers ont la relation $\{(D, a) \mid \exists k \in \mathbb{Z}, Dk = a\}$ alors on dit que le premier est un diviseur du second.*

Définition 3. *Soit E un ensemble et R une relation sur E, notée $a\ R\ b$. On dit que R est une relation d'équivalence si elle a les trois propriétés suivantes :*

transitivité	$a\ R\ b$ *et* $b\ R\ c$	$\Rightarrow$	$a\ R\ c$
symétrie	$a\ R\ b$	$\Rightarrow$	$b\ R\ a$
réflexivité	$\forall a$		$a\ R\ a$.

Exemple 3. *La relation de similitude entre triangles, la relation de congruence entre entiers, la propriété de deux segments d'avoir la même longueur sont des relations d'équivalence.*

Définition 4. *Soit R une relation d'équivalence sur l'ensemble E et soit a un élément de E. On appelle classe d'équivalence de a et on note $\hat{a}$ l'ensemble d'éléments de E qui sont en relation R avec a. L'ensemble des classes d'équivalences $\{\hat{a} \mid a \in E\}$ s'appelle l'ensemble quotient de E par R. On appelle ensemble de représentants de l'ensemble quotient tout sous-ensemble E' de E qui a un et un seul élément dans chaque classe d'équivalence.*

Exemple 4. *On prend $E = \mathbb{Z}$ et R la relation de congruence modulo 4. Alors les classes d'équivalence sont*

$$\begin{aligned}\hat{0} &= \{4k \mid k \in \mathbb{Z}\}\\ \hat{1} &= \{4k+1 \mid k \in \mathbb{Z}\}\\ \hat{2} &= \{4k+2 \mid k \in \mathbb{Z}\}\\ \hat{3} &= \{4k+3 \mid k \in \mathbb{Z}\}.\end{aligned}$$

Grâce au Théorème **??** *on peut écrire $\hat{3} + \hat{3} = \hat{2}$. L'ensemble $E' = \{0, 1, 2, 3\} \subset E$ est un système de représentants, mais d'autre systèmes de représentants existent, par exemple $\{0, 1, 2, -1\}$.*

Exercice 3. *On se donne un repère cartésien xOy dans le plan. On dit que deux points sont en relation R si on peut aller du premier au second en se déplaçant un nombre entier de centimètres en direction horizontale, puis un nombre entier de centimètres en direction verticale. Donner trois systèmes de représentants différents.*

Exercice 4. *On note $\mathbb{Z}/N\mathbb{Z}$ l'ensemble des classes de conjugaison (classes d'équivalence pour la congruence) modulo N. Donner deux systèmes de représentants pour $\mathbb{Z}/N\mathbb{Z}$ et dites comment on fait explicitement les calculs $\hat{a}+\hat{b}$ et $\hat{a}\cdot\hat{b}$. Montrer qu'il est plus simple de faire des additions quand on utilise un système de représentants qui contient des entiers négatifs.*

2 Propriétés générales

Théorème 2 (Bezout)**.** *Pour toute paire a et b d'entiers, il existe des coefficients entiers u et v tels que*

$$ua + vb = pgcd(a, b).$$

Démonstration. Soit $d = u_0a + v_0b$ le plus petit élément positif de l'ensemble

$$F = \{ua + vb \mid u, v \in \mathbb{Z}\}.$$

Montrons que, si $f = u_1a + v_1b$ est un élément positif de F, alors d divise f. Supposons par l'absurde que f s'écrit comme $f = dq+r$ avec $q \in \mathbb{N}$ et $0 \leq r < d$. Alors $r = f - dq = (u_1a + v_1b) - q(u_0a + v_0b) = (u_1 - qu_0)a + (v_1 - qv_0)b$ et appartient donc à F. Or, r est plus petit que d, le plus petit élément positif de F, ce qui contredit la supposition faite.

Comme d divise tous les éléments de F, il divise en particulier $a = 1 \cdot a + 0 \cdot b$ et $b = 0 \cdot a + 1 \cdot b$. Ainsi, d divise $\text{pgcd}(a, b)$.

Réciproquement, $\text{pgcd}(a, b)$ divise tout élément $ua + vb$ avec $u, v \in \mathbb{Z}$ et, en particulier, $\text{pgcd}(a, b)$ divise d. D'où $d = \text{pgcd}(a, b)$, ce qui finit la preuve. □

Exercice 5. *On dispose d'un récipient de 8 litres et d'un de 18 litres. Montrer qu'on peut remplir un bassin avec exactement 62 littres d'eau, en utilisant les deux récipients pour verser de l'eau dans le bassin ou pour en retirer.*

2.1 Inverse d'un élément

Proposition 1. *Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ non divisible par p, il existe un unique entier $u \in [1, p-1]$ tel que*

$$a \cdot u \equiv 1 \pmod{p}.$$

Démonstration. Comme a n'est pas divisible par p, on a $\text{pgcd}(a, p) = 1$. D'après le Théorème de Bezout, il existe deux entiers u et v tels que

$$au + pv = 1.$$

On a donc $au \equiv 1 - pv \equiv 1 \pmod{p}$.

Pour montrer l'unicité, considéront deux entiers u et u' dans l'intervalle $[1, p-1]$ tels que $au \equiv au' \equiv 1 \pmod{p}$. Alors on a $a(u - u') \equiv 0 \pmod{p}$, donc p divise $a(u - u')$. Comme p et premier et ne divise pas a, p divise $u - u'$. Comme $|u - u'| \leq p - 1$, on a $u = u'$. □

Définition 5. *L'entier u est appelé inverse de a modulo p et on note*

$$\hat{u} = \hat{a}^{-1}.$$

Exemple 5. *Pour $p = 7$, 2 est inverse de 4, 3 est inverse de 5 et 6 est son propre inverse. En effet, $2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$; $3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$ et $6 \cdot 6 \equiv 36 \equiv 1 \pmod{7}$.*

Proposition 2. *L'inverse de l'inverse d'un élément a de l'ensemble $\{1, 2, \ldots, p-1\}$ est a.*

Démonstration. Soit u l'inverse de a et a' l'inverse de u. Alors on a $au \equiv 1 \pmod{p}$ et $ua' \equiv p \pmod{p}$. Mais alors on a également $ua \equiv 1 \pmod{p}$. Par l'unicité de l'inverse de u on a $a' = a$. □

Théorème 3 (Théorème de Wilson)**.** *Pour tout nombre premier p, on a*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Démonstration. Comme l'inverse de l'inverse d'un élément a de $[1, p-1]$ est a lui même, on peut partitionner les éléments de $\{1, 2, \ldots, p-1\}$ en ensembles $\{a, u\}$ avec $\hat{a}^{-1} = \hat{u}$. Pour qu'un tel ensemble $\{a, u\}$ n'ait qu'un élément, il faut avoir

$$a^2 \equiv 1 \pmod{p}.$$

Or cela est équivalent à $(a^2 - 1) \equiv 0 \pmod{p}$ ou encore p divise $a^2 - 1 = (a-1)(a+1)$. Donc p divise $a-1$ ou $a+1$. Comme $a \in [1, p-1]$, cela se produit uniquement pour $a = 1$ et $a = p - 1$.

Par conséquent, pour multiplier les éléments de $\{2, 3, \ldots, p-2\}$, on peut les grouper par paires (a, u) telles que $au \equiv 1 \pmod{p}$. On a donc

$$\prod_{a=2}^{p-2} a \equiv 1 \pmod{p}.$$

En multipliant encore par $a = 1$ et $a = -1$ on trouve $(p-1)! \equiv -1 \pmod{p}$. □

2.2 Puissances modulaires

Proposition 3. *Soient a et N deux entiers avec $pgcd(a, N) = 1$. Alors la suite $\hat{a}, \hat{a}^2, \hat{a}^3, \ldots$ est périodique.*

Démonstration. Comme la suite ci-dessus est infinie, elle contient deux éléments a^i et a^j tels que $a^i \equiv a^j \pmod{N}$. Sans restreindre la généralité, on peut supposer que i est plus petit que j. On a alors $a^i(a^{j-i} - 1) \equiv 0 \pmod{N}$ ou, de manière équivalente, N divise $a^i(a^{j-i} - 1)$. Comme a et N sont premiers entre eux, N divise $a^{j-i} - 1$. De manière équivalente, on a $a^{j-i} \equiv 1 \pmod{N}$. On pose $k = j - i$ et on remarque que pour tous u et $n \in \mathbb{N}$ on a

$$a^{n+ku} \equiv a^n \pmod{N}.$$

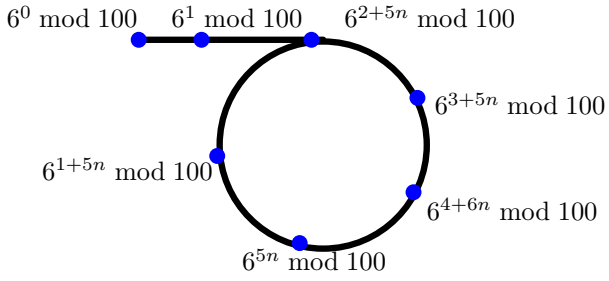
□

Définition 6. *Pour tout entier N et tout entier a premier avec N, on appelle ordre de a modulo N et on note $ord_N(a)$ la période de la suite $\hat{a}, \hat{a}^2, \ldots$.*

Exercice 6. *Calculer $ord_{10}(3)$ et $ord_{10}(7)$. Comment se comporte la suite des restes des puissances de 5 modulo 1000 ? Mais les suites des restes des puissances de 6 modulo 100 ? Représenter la situation par un dessin.*

Démonstration. On a $3^4 \equiv 81 \equiv 1 \pmod{1)0}$, alors que 3, 3^2 et 3^3 ne sont pas congruents à 1 modulo 10. Donc $\text{ord}_{10}(3) = 4$. De manière analogue, on a $\text{ord}_{10}(7) = 4$.

Pour les puissances de 5, on a les restes modulo 1000 suivants $5, 25, 125, 625, 625, 625, \ldots$. Pour les puissances de 6 on a $6^0 = 1, 6^1 = 1, 36, 16, 96, 76, 56, 36, 16, \ldots$.



□

Exercice 7. *Trouver le dernier chiffre de*

$$3^{7^{2014}}.$$

Démonstration. Comme $\mathrm{ord}_{10}(3) = 4$, il suffit de trouver le reste de 7^{2014} modulo 4. On a

$$\begin{aligned} 7^{2014} &\equiv (-1)^{2014} && \pmod 4 \\ &\equiv ((-1)^2)^{1007} && \pmod 4 \\ &\equiv 1 && \pmod 4. \end{aligned}$$

Donc le dernier chiffre de $3^{7^{2014}}$ est le dernier chiffre de $3^1 = 3$, donc 3. □

Théorème 4 (Petit théorème de Fermat)**.** *Si p est un premier, alors pour tout entier a non divisible par p a un ordre modulo p qui divise $p-1$. Par conséquent, pour tout a entier, on a*

$$a^p \equiv a \pmod p.$$

Dans ce cours, on utilise le théorème sans preuve car celle-ci requiert d'utilisez soit le binôme de Newton, soit la théorie de groupes.

Exercice 8. *Montrer que l'équation $x^3 + y^3 = x + y + 3xy^2 + 1$ n'a pas de solutions entières.*

3 Restes quadratiques

Définition 7. *On appelle reste quadratique modulo un entier N tout entier $a \in [0, N-1]$ tel que l'équation suivante a une solution*

$$a \equiv x^2 \pmod N.$$

Exercice 9. *Trouver les restes quadratiques modulo 3, 4 et 8.*

Démonstration. Le carré d'un nombre impair $2k+1$ est

$$(2k+1)^2 = 4(k^2+k) + 1.$$

Or $k^2 + k$ est pair indépendamment de la parité de k. Donc un carré est soit divisible par 4, soit congruent à 1 modulo 8. Ainsi les restes quadratiques modulo 4 sont 0 et 1 et modulo 8 ils sont $0, 1, 4$.

Une manière plus élégante de calculer les restes quadratiques et de faire la table des carrés modulo 8 :

x	0	1	2	3	4	5	6	7
x^2	0	1	4	9	16	25	36	49
$x^2 \bmod 8$	0	1	4	1	0	1	4	1

.

De manière analogue, les rested quadratiques modulo 3 sont 0 et 1. □

Exercice 10. *Montrer que le nombre de restes quadratiques modulo un premier p impair est $(p+1)/2$.*

Démonstration. On considère la fonction $f : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$, $x \mapsto$ le reste de x^2 à la division par 8. Montrons que $f(x) = f(y)$ si et seulement si $x \equiv \pm y \pmod{p}$. On a

$$\begin{array}{rrcll} & f(x) & = & f(y) & \\ \Leftrightarrow & x^2 & \equiv & y^2 & \pmod{p} \\ \Leftrightarrow & x^2 - y^2 & \equiv & 0 & \pmod{p} \\ \Leftrightarrow & (x-y)(x+y) & \equiv & 0 & \pmod{p} \\ \Leftrightarrow & p \mid (x-y)(x+1) & . & & \end{array}$$

Or, p est premier, donc p divise soit $(x - y)$, soit $x + y$. Dans le premier cas on trouve $x = y$, dans le deuxième $y = p - x$.

Comme f prend chaque valeur non nulle exactement 2 fois, elle prend $(p - 1)/2$ valeurs sur l'ensemble $\{1, 2, \ldots, p-1\}$. Si on rajoute une valeur pour $x = 0$, on a $(p - 1)/2 + 1 = (p + 1)/2$ restes quadratiques. □

Définition 8. *Soit p un nombre premier et a un entier. On définit le symbôle de Legendre par*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a, \\ 1 & \text{si } a \text{ est un reste quadratique non nul,} \\ -1 & \text{sinon.} \end{cases}$$

Proposition 4. *Si p est un nombre premier et a et b sont deux entiers, alors on a*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Démonstration. On étudie les différents cas.

Cas où $\left(\frac{a}{p}\right)$ ou $\left(\frac{b}{p}\right)$ est nul Alors p divise a ou b, donc il divise ab et $\left(\frac{ab}{p}\right) = 0$.

Cas où $\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right)$ Si a et b sont restes quadratiques, on écrit $a \equiv \alpha^2 \pmod{p}$ et $b \equiv \beta^2 \pmod{p}$. Alors on a $ab \equiv (\alpha\beta)^2 \pmod{p}$.

Cas où $\left(\frac{a}{p}\right) = 1$ et $\left(\frac{b}{p}\right) = -1$ On suppose par l'absurde que ab est reste quadratique. On a donc $a \equiv \alpha^2 \pmod{p}$ et $ab \equiv \gamma^2 \pmod{p}$ pour des entiers α et γ. Soit u un entier tel que $\alpha u \equiv 1 \pmod{p}$. Alors, on a

$$\begin{array}{rcll} \gamma^2 u^2 & \equiv & (ab)u^2 & \pmod{p} \\ & \equiv & b(au^2) & \pmod{p} \\ & \equiv & b(\alpha^2 u^2) & \pmod{p} \\ & \equiv & b(\alpha u)(\alpha u) & \pmod{p} \\ & \equiv & b & \pmod{p} \end{array} .$$

Donc, b est un reste quadratique, ce qui contredit la supposition faite sur b.

Cas où $\left(\frac{a}{p}\right) = 1$ et $\left(\frac{b}{p}\right) = -1$ Soit λ dans l'ensemble $[1, p - 1]$ qui n'est pas

reste quadratique. Alors les ensembles $\{\hat{u}^2 \mid \hat{u} \in \mathbb{Z}/p\mathbb{Z}\}$ et $\{\hat{n}\hat{u}^2 \mid \hat{u} \in \mathbb{Z}/p\mathbb{Z}\}$ sont disjointes. Comme la somme des cardinaux des deux ensembles est égale au nombre de classes différentes de $\hat{0}$, tout reste non quadratique est dans le deuxième ensemble. On peut donc écrire $a \equiv \lambda\alpha^2 \pmod{p}$ et $b \equiv \lambda\beta^2 \pmod{p}$. Mais alors $ab \equiv (\lambda\alpha\beta)^2 \pmod{p}$. □

Exercice 11. *Montrer que pour tout premier p on a*

$$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$$

Démonstration. Cas où $p \equiv 1 \pmod{4}$. D'après le Théorème de Wilson on a : $-1 \equiv (p-1)! \pmod{p}$. Pour calculer $(p-1)! \pmod{p}$, on groupe les couples $(a, p-a)$ pour tout a de l'ensemble $\{1, 2, \ldots, (p-1)/2\}$. Ainsi, on a

$$(p-1)! \equiv \prod_{a=1}^{(p-1)/2} a(-a) \equiv \left(\prod_{a=1}^{(p-1)/2} a\right)^2 (-1)^{(p-1)/2} \equiv \left(\prod_{a=1}^{(p-1)/2} a\right)^2 \pmod{p}.$$

Cas où $p \equiv 3 \pmod{4}$. Supposons par l'absurde que $-1 \equiv \alpha^2 \pmod{p}$ pour un entier α. D'après le Petit Théorème de Fermat, on a $\alpha^{p-1} \equiv 1 \pmod{p}$ et donc $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. Comme $p \equiv 3 \pmod{4}$, $(p-1)/2$ est impair, donc on a : $-1 \equiv 1 \pmod{p}$. Cela est impossible car p ne divise pas 2. □

Exercice 12. *Montrer que si un premier $p \equiv 3 \pmod{4}$ divise $a^2 + b^2$, alors il divise les deux nombres a et b.*

4 Équation diophantines

Définition 9. *On appelle équations diophantines (du nom du mathématicien grec qui les a étudiées pour la première fois) les équations dont on demande des solutions entières. Un exemple important est l'équation du grand théorème de Fermat :*

$$a^n + b^n = c^n$$

avec $n > 2$.

Remarque 1. *Si une equation diophantine a des solutions, elle doit en avoir aussi modulo N pour tout entier N. Pour prouver qu'une équation n'a pas de solutions il suffit donc de choisir un entier N et de montrer que la réduction modulo N de l'équation n'a pas de solutions.*

Exercice 13. *Montrer que l'équation suivante n'a pas de solutions entières :*

$$x^2 = 8y^3 + 3.$$

Démonstration. On réduit l'équation modulo 8 et on trouve

$$x^2 \equiv 3 \pmod 8. \tag{1}$$

D'après l'Exercice 9, 3 n'est pas reste quadratique modulo 8, donc l'équation n'a pas de solutions entières. □

Exercice 14. *Montrer que l'équation $x^2 = 3y^3 + 8$ n'a pas de solutions entières.*

Démonstration. L'équation n'a pas de solutions modulo 3 car 2 n'est pas reste quadratique. □

Remarque 2. *Il existe des équations diophantines avec des solutions modulo tout nombre premier, mais qui n'ont pas de solution. Comme exemple on a $xy = 1$, $x^2 + y^2 + z^2 + t^2 = 0$.*

Exercice 15. *Trouver tous les entiers x tels que*

$$8^x + 9^x = 11^x.$$

Démonstration. On réduit l'équation modulo 4 et on obtient

$$0^x + 1^x \equiv (-1)^x.$$

Donc x et pair et on l'écrit $x = 2k$ avec k entier. Alors on a $a^2 + b^2 = 11^{2k}$ avec $a = 8^k$ et $b = 9^k$. Comme 11 divise $a^2 + b^2$ et $11 \equiv 3 \pmod 4$, 11 divise $a = 8^k$. Cela est impossible, donc l'équation n'a pas de solutions. □

Exercice 16. *Trouver les entiers x tels que*

$$3^x = (2^x + 1)(2^x + 9).$$

Démonstration. On traite apart les cas $x = 0$ et $x = 1$ et on obtient qu'ils ne donnent pas de solutions. Supposons maintenant par l'absurde que l'équation a une solution entière $x \geq 2$. On réduit l'équation modulo 4 et on obtient

$$(-1)^x \equiv (0 + 1)(0 + 1) \pmod 4.$$

Donc x est pair.

En réduisant l'équation modulo 3 on obtient

$$0 \equiv ((-1)^x + 1)((-1)^x + 0) \pmod 3.$$

Comme x est pair on trouve $0 \equiv 2 \pmod 3$, donc l'équation n'a pas de solutions dans $\mathbb{Z}$. □