UNIVERSITÉ DE RENNES 1

ARA: Algèbre et Arithmétique

ARA-Partie 4 : Nombres premiers

1 Définition, premières propriétés

1.1 Définition

On appelle nombre premier tout entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

Un nombre non premier est dit composé.

En particulier, 1 n'est pas premier.

1.2 Exercice Donner la liste des 10 premiers nombres premiers.

1.3 Proposition

Soit p un nombre premier et n un entier. Alors

$$p \wedge n = 1 \Leftrightarrow p \not| n.$$

En particulier, $\forall 1 \leq k \leq p-1,\ k \wedge p = 1$.

Démonstration: Soit n un entier non multiple de p. Si d est un diviseur commun à p et à n, alors
. d divise p,
. d est différent de p, puisque p ne divise pas n,
donc $d = 1$. Donc $n \wedge p = 1$. ■

La démonstration de la seconde partie de la proposition est laissée en exercice.

1.5 Exemple. Deux nombres premiers distincts sont premiers entre eux.

Le théorème de Gauss prend une forme spéciale pour les nombres premiers :

1.6 Proposition (Lemme d'Euclide)

Un nombre premier divise un produit si et seulement si il divise l'un de ses facteurs.

Démonstration: Exercice. ■

Les nombres premiers jouent un rôle capital dans plusieurs domaines des mathématiques. Le *crible d'Eratosthène* est un algorithme qui permet de liste tous les nombres premiers inférieurs à une borne choisie. Il repose sur le lemme suivant :

1.8 Lemme

Soit $n \geq 2$ un entier. S'il n'est pas premier, il admet un diviseur $p \leq \sqrt{n}$ qui est premier.

Démonstration: La preuve la plus simple se fait à partir du théorème de factorisation énoncé dans la section suivante.

On peut toutefois s'en passer et démontrer ce lemme par récurrence sur n.

Le lemme est vrai pour $n = 2$ et 3 qui sont premiers, et pour $n = 4$ qui ne l'est pas.

Supposons qu'il soit vrai pour tout entier strictement inférieur àn.

Si n est premier, le résultat est vrai.

On se donne donc une décomposition $n = k_1 k_2$. Quitte à renuméroter, on peut supposer $k_1 \leq k_2$. On a donc

$k_1^2 \leq k_1 k_2 = n$, *donc* $k_1 \leq \sqrt{n}$.

Si k_1 est premier, alors on a démontré le résultat voulu. Sinon, par hypothèse de récurrence, on dispose d'un nombre premier $p \leq k_1 \leq \sqrt{n}$. Comme $p|k_1$, en particulier $p|n$. ∎

Imaginons que l'on veuille tous les nombres premiers inférieurs à 30. On commence à faire la liste de tous les entiers de 2 à 30 :

2, 3, 4, 5, 6, . . . , 26, 27, 28, 29, 30.

Le premier de la liste est premier : on le garde et on raye tous ses multiples :

2, 3, 5, . . . , 27, 29.

Le suivant non rayé, 3 n'est multiple d'aucun entier plus petit que lui : il est donc premier. On le garde et on raye ses multiples :

2, 3, 5, 7, 11, . . . , 25, 29. On continue avec 5 :

2, , 3, 5, 7, 11, . . . , 29.

Le suivant dans la liste est 7 qui est plus grand que $\sqrt{30}$. Grâce au lemme, on sait que les entiers non rayés forment la liste des premiers inférieurs à 30 :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

1.10 Exercice — Expliquer pourquoi le lemme nous permet de conclure cet algorithme.

— Comparer la liste obtenue avec Eratosthène et celle qui vous avez obtenu dans le premier exercice. Quelle méthode est la plus rapide ?

— Une autre conséquence du lemme est qu'il existe une infinité de nombres premiers. Démontrer le.

Indication : *Par l'absurde, supposer qu'on ait un nombre fini de nombres premiers* $\{p_1, \ldots, p_k\}$. *Utiliser le lemme pour* $n = (\prod_i p_i) + 1$.

2 Factorisation

2.1 Théorème

Soit $n \geq 2$ *un entier.*

Il existe un entier r, *des nombres premiers deux à deux distincts* $p_1, \ldots, p_r$ *et des entiers non nuls* $a_1, \ldots, a_r$ *tels que*

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}.$$

Cette décomposition s'appelle décomposition en facteurs premiers. Elle est unique à l'ordre des facteurs près.

Démonstration: **Existence.** On démontre d'abord Existence de la décomposition par récurrence. La propriété est vraie pour $n = 2$ puisque 2 est premier.

Soit $n \geq 2$, supposons que tous les entiers de 2 à $n-1$ admettent une décomposition en facteurs premiers. Si n est premier, n admet bien une telle décomposition, et la propriété est démontrée.

On suppose donc qu'on ait $n = pq$, avec p un nombre premier. Comme $2 \leq q \leq n-1$, par hypothèse de récurrence, on a $q = \prod_i p_i^{\alpha_i}$, et on a donc bien une décomposition

$$n = p \prod_i p_i^{\alpha_i}.$$

Unicité. Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ une décomposition en facteurs premiers de n. Pour tout $1 \leq k \leq r,\ p_k | n$. Réciproquement, si $p|n$, alors par le lemme d'Euclide il divise l'un des $p_i^{\alpha_i}$, c'est-à-dire qu'il est égal à p_i. Ainsi, la liste des facteurs premiers intervenant dans une telle décomposition est unique : c'est exactement la liste des diviseurs premiers de n.

Soient alors deux décomposition de n, que l'on peut écrire :

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r} = p_1^{\beta_1} \dots p_r^{\beta_r}.$$

Par l'absurde, on suppose qu'il y ait un indice i tel que $\alpha_i \neq \beta_i$. Alors

$$\prod_{j \neq i} p_j^{\alpha_j} = p_i^{\beta_i - \alpha_i} \prod_{j \neq i} p_j^{\beta_j}.$$

Comme $\beta_i - \alpha_i \neq 0$, on a

$$p_i | \prod_{j \neq i} p_j^{\alpha_j},$$

$$\forall j \neq i,\ p_i \wedge p_j = 1.$$

Contradiction. ∎

2.3 Exercice $7007 = 7^2 \times 11 \times 13$.

2.4 REMARQUE

Si $\{p_1, \dots, p_r\}$ est un ensemble de nombres premiers contenant tous les facteurs premiers de n, on peut encore écrire

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

avec $\alpha_i = 0$ si p_i n'est pas un diviseur de n.

Avec cette convention, 1 peut aussi s'écrire sous cette forme, en prenant tous les α_i nuls.

Etant donnés deux entiers naturels a et b non nuls, on peut écrire

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r},\ b = p_1^{\beta_1} \dots p_r^{\beta_r}$$

en utilisant les mêmes nombres premiers. Il suffit pour cela de prendre tous les facteurs premiers du produit ab.

2.5 PROPOSITION
Soient a et b deux entiers naturels non nuls. Si : $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, et $b = p_1^{\beta_1} \dots p_r^{\beta_r}$ avec les p_i des entiers deux à deux distincts, alors on a
$a|b \Leftrightarrow \forall 1 \leq i \leq k,\ \alpha_i \leq \beta_i$;
$a \wedge b = \prod_i p_i^{\min(\alpha_i,\beta_i)}$ *et* $a \vee b = \prod_i p_i^{\max(\alpha_i,\beta_i)}$.

Démonstration: Exercice. ∎

2.7 Exercice Etant donnés deux entier non nuls a et b, retrouver la formule

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

Indication : montrer que $max(\alpha,\ \beta) + \min(\alpha,\ \beta) = \alpha + \beta$
Soit n un entier naturel non nul dont la décomposition en facteurs premiers est

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

déterminer tous les diviseurs de n. En déduire le nombre de ces diviseurs.

3 Le petit théorème de Fermat

3.1 LEMME
Pour tout $1 \leq k \leq p-1,\ p \Big| \begin{pmatrix} p \\ k \end{pmatrix}$.

Démonstration: On a $k \begin{pmatrix} p \\ k \end{pmatrix} = p \begin{pmatrix} p-1 \\ k-1 \end{pmatrix}$ et $p \wedge k = 1$, donc le lemme d'Euclide permet de conclure.

3.3 THÉORÈME
Soit p un nombre premier. Pour tout entier $n \in \mathbb{Z}$, on a $n^p \equiv n \pmod p$. Si de plus $n \wedge p = 1$, alors $n^{p-1} \equiv 1 \pmod p$.

Démonstration: On montre la première assertion par récurrence sur n.
Elle est vraie pour $n = 0$.
Si elle est vraie pour un entier n, alors

$$(1+n)^p = 1 + \sum_{k=1}^{p-1} \begin{pmatrix} p \\ k \end{pmatrix} n^k + n^p \equiv 1 + n \pmod p.$$

Donc par récurrence, la propriété est vraie pour tous les entiers positifs. Pour les entiers négatifs, il suffit de remarquer que $(-n)^p \equiv -n^p \pmod p$.
On passe maintenant à la seconde assertion.
On a vu que pour tout entier n, $p|(n^p - n)$ et $n^p - n = n(n^{p-1} - 1)$.
Si de plus $n \wedge p = 1$, alors par le lemme d'Euclide $p|(n^{p-1} - 1)$.

On peut reformuler la seconde partie du théorème en un critère de non primalité :

Test de Fermat :
Soit p un entier naturel.
On choisit au hasard un entier n, $1 \leq n \leq p-1$.
Si $n^{p-1} \not\equiv 1 (\text{mod } p)$, alors p n'est pas un nombre premier.

3.5 EXEMPLE. Si $n = 2$ et $p = 9$, on a modulo 9 :

$$n^{p-1} \equiv 2^8 \equiv 4^4 \equiv 16^2 \equiv 7^2 \equiv 49 \equiv 4 \text{ (mod } p)$$

donc 9 n'est pas premier.

3.6 Exercice Reprendre l'exemple avec $n = 2$ et $p = 221$.

3.7 REMARQUE
Ce critère de non primalité ne se transforme pas en critère de primalité :

3.8 PROPOSITION
Il existe des entiers composés m tels que pour tout entier $1 \leq n \leq m-1$, $n^{m-1} \equiv 1 (\text{mod } m)$. Un tel entier m est appelé nombre de Carmichael.

3.9 REMARQUE
Le plus petit nombre de Carmichael est $561 = 3 \cdot 11 \cdot 17$.

4 Test de primalité de Miller-Rabin

4.1 PROPOSITION
Soit p un nombre premier différent de 2. L'équation $x^2 \equiv 1 (\text{mod } p)$ admet exactement deux solutions : $x \equiv 1 (\text{mod } p)$ et $x \equiv -1 (\text{mod } p)$.

Démonstration:

$$x^2 \equiv 1 \text{ (mod } p) \Leftrightarrow (x-1)(x+1) \equiv 0$$
$$\Leftrightarrow p | (x-1)(x+1).$$

$\Leftrightarrow p|x-1$ *ou* $p|x+1$,
cette dernière ligne étant vraie grâce au lemme d'Euclide. ∎

4.3 Exercice Dans le cas où on travaille modulo n avec n composé, à quel endroit la démonstration devient-elle fausse ?
Montrer que l'équation $x^2 \equiv 1 (\text{mod } 15)$ admet 4 solutions distinctes.

4.4 PROPOSITION
Soit $n \leq 3$ un entier naturel impair. On écrit $n - 1 = 2^t m$ t avec m impair.
Soit $2 \leq a \leq n-1$. Si $a^{n-1} = a^{2^t m} \neq 1$ alors n n'est pas premier.
Sinon, soit k le plus petit entier naturel tel que $a^{2^k m} = 1$. Si $a^{2^{k-1} m} \neq -1$ alors n n'est pas premier.

Démonstration: Le premier critère est le critère de Fermat.
Le second met en évidence une racine carrée de 1 différente de ± 1.

On obtient ainsi le test de Miller-Rabin :
Etape 1 : Ecrire $n-1=2^t m$, avec m impair.
Etape 2 : Tirer au hasard $2 \leq a \leq n-1$.
Etape 3 : $b \leftarrow a^m \pmod{n}$
Etape 4 : If $b=1$ Then
Return : "n est probablement premier".
End If
Etape 5 : $c \leftarrow b$
Etape 6 : For $i=1$ to t do
6.a $c' \leftarrow c^2$
6.b If $c'=1$ Then
If $c=-1$ Then
Return : "n est probablement premier".
Else Return : "n n'est pas premier".
End If
End If
6.c $c \leftarrow c'$
End For
Etape 7 Return : "n n'est pas premier ".
END.

4.6 REMARQUE
comme pour le test de Fermat, quand le test de Miller-Rabin répond que nn 'est pas premier, c'est une réponse définitive. Par contre, un entier probablement premier n'est pas forcément premier.

L'intérêt de ce test sur celui de Fermat réside dans la proposition (admise) suivante :

4.7 PROPOSITION
Soit $n \geq 3$ un entier impair non premier. Pour au moins la moitié des a compris entre 1 et $n-1$, le test de Miller-Rabin détecte la non primalité de n.

4.8 Exercice Soit n un entier impair non premier. On choisit aléatoirement d nombres entiers distincts $a_1, \ldots, a_d$ compris entre 2 et $n-1$. Quelle est la probabilité que pour chacun des a_i le test de Miller Rabin retourne "n est probablement premier" ?