Arithmétique des entiers

Alix Deleporte

6 septembre 2015

Dans ce cours, on étudie plus en détail les propriétés des ensembles $\mathbb{Z}/n\mathbb{Z}$.

1 Puissances d'un entier

Proposition 1. Soit p un nombre premier et $a \in \mathbb{N}$. On a alors

$$a^p \equiv a \mod p.$$

De plus, si a n'est pas un multiple de p, alors

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

Démonstration. On démontre la première formule par récurrence sur a, en utilisant la formule de Newton. En effet, on sait que le résultat est vrai pour $a = 1$. Supposons le résultat vrai pour a. Alors on a

$$(a+1)^p = 1 + a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

Or on sait, d'une part, que $a^p \equiv a \mod p$, et d'autre part, que pour tout $1 \leq k \leq p-1$, on a $p | \binom{p}{k}$ (cf TD précédent).

On peut donc conclure, et $(a+1)^p \equiv a+1 \mod p$.

On démontre la seconde propriété à partir de la première et du théorème de Gauß. Si a n'est pas un multiple de p, alors $a \wedge p = 1$ car p est premier. Or on vient de démontrer $p | a(a^{p-1} - 1)$, et on en déduit $p | a^{p-1} - 1$. □

Exercice 1. Démontrer le second résultat à partir du premier, en utilisant le théorème de Bézout.

Démonstration. Comme $a \wedge n = 1$, il existe q et r tels que $qa = 1 + pr$, donc $qa \equiv 1 \mod p$. En multipliant l'équation $a^p \equiv a \mod p$ par q, on obtient le résultat demandé. On peut toujours « diviser »par un nombre premier avec n dans $\mathbb{Z}/n/\mathrm{Z}$. □

Le petit théorème de Fermat se généralise, et permet d'introduire une fonction très importante en arithmétique :

> **Proposition 2.** Si $n \neq 0$ et a sont deux entiers naturels premiers entre eux, alors
> $$a^{\varphi(n)} \equiv a \mod n$$
> Ici $\varphi(n)$ désigne le nombre d'entiers naturels plus petits que n et premiers avec n.

Démonstration. On considère l'ensemble $\mathrm{B} = (b_1, \ldots, b_{\varphi(n)}$ des entiers naturels plus petits que n et premiers avec n, et $\overline{\mathrm{B}} = (\overline{b_1}, \ldots, \overline{b_{\varphi(n)}})$ l'ensemble des classes associées dans $\mathbb{Z}/n\mathbb{Z}$.

L'ensemble $\overline{\mathrm{B}}$ est stable par multiplication par a. En effet, si $b \wedge n = 1$, alors $ab \wedge n = 1$ (exercice). L'application de multiplication par a est *injective* : si $ab = ab' \mod n$, alors $n|a(b-b')$ donc $n|b-b'$ par le théorème de Gauß. Cette application est donc une permutation de $\overline{\mathrm{B}}$. En particulier, on a : $(a\overline{b_1}) \cdot \ldots \cdot (\overline{ab_{\varphi(n)}}) \equiv \overline{b_1} \ldots \overline{b_{\varphi(n)}} \mod n$, et on peut diviser par chacun des b_j (car ils sont premiers avec n), donc $a^{\varphi(n)} = 1$. □

Exercice 2. Si $a \wedge n = 1$ et $b \wedge n = 1$, montrer que $ab \wedge n = 1$.

Solution de l'exercice 1. Soit p un nombre premier tel que $p|n$. Alors a n'est pas un multiple de p, ni b, donc ab n'est pas un multiple de p (par Gauß). Ainsi, le pgcd de n et ab est un diviseur de n, mais n'est un multiple d'aucun des nombres premiers p tels que $p|n$. Donc le pgcd vaut 1. □

Exercice 3. Soit n un entier impair.
Montrer que $n|2^{n!} - 1$.

Solution de l'exercice 2. On sait que $2 \wedge n = 1$, donc $2^{\varphi(n)} \equiv 1 \mod n$. Or $1 \leq \varphi(n) < n$, donc $\varphi(n)|n!$. Si $n! = k\varphi(n)$, alors $2^{n!} = (2^{\varphi(n)})^k \equiv 1^k \mod n$, ce qui conclut la preuve. □

Exercice 4. Quels sont les 5 derniers chiffres de $5^{5^{5^5}}$?

Solution de l'exercice 3. On s'intéresse à la division euclidienne de ce nombre par $10^5 = 2^5 \times 5^5$. Pour avoir des nombres premiers entre eux, on divise tout par 5^5, et

on se ramène au reste de la division euclidienne de $5^{5^{5^5}-5}$ par 2^5. On peut alors appliquer le théorème d'Euler, puisque 5 est premier avec $2^5 = 32$.

Commençons par calculer $\varphi(32)$. C'est le nombre d'entiers naturels impairs entre 1 et 32, il y en a 16. Donc pour tout entier k, on a $5^{16k} \equiv 1 \mod 32$. On se ramène donc au reste de $5^{5^{5^5}}$ modulo 16 (auquel on n'oubliera pas d'enlever 5). De même, $\varphi(16) = 8$, donc il suffit de calculer le reste de 5^{5^5} modulo 8. Avec $\varphi(8) = 4$, on recommence, et on étudie le reste de $5^5 = 25$ modulo 4. Celui-ci vaut 1. Donc $5^{5^5} \equiv 1 \times 5^1 \equiv 5 \mod 8$.

En redescendant, $5^{5^{5^5}} \equiv 5^5 \mod 16$, or $5^5 = 25 \times 25 \times 5 \sim 9 \times 9 \times 5 \sim 81 \times 5 \equiv 5 \mod 16$. Ainsi, $16 | 5^{5^{5^5}} - 5$, donc $5^{5^{5^5}-5} \equiv 1 \mod 2^5$.

En remultipliant par $5^5 = 3125$, on trouve que les quatre derniers chiffres sont 3125. □

Terminons cette section par quelques précisions sur la suite $a^k \mod n$, pour tout entier a premier avec n.

> **Proposition 3.** Soient $a \wedge n = 1$ deux nombres. Alors il existe un plus petit entier non nul k tel que $a^k \equiv 1 \mod n$. Tout autre entier vérifiant cette propriété est un multiple de k, en particulier, $k | \varphi(n)$.

Démonstration. On applique un argument de minimum. L'ensemble des k vérifiant cette propriété est une partie de $\mathbb{N}$, non vide (elle contient $\varphi(n)$), donc elle admet un plus petit élément k.

Soit k' vérifiant également cette propriété, et $k' = qk + r$ sa division euclidienne. Alors $(a^k)^q \times a^r \equiv 1 \mod n$, et donc $a^r \equiv 1 \mod n$, or $r < k$, donc $r = 0$ par définition. □

Exercice 5. Déterminer tous les entiers impairs n tels que $n | 3^n + 1$.

Solution de l'exercice 4. $n = 1$ est évidemment une solution. Soit $n > 1$ impair vérifiant cette propriété. Comme 3 ne divise pas $3^n + 1$, on a que 3 ne divise pas n. Si p est le plus petit nombre premier qui divise n, on a donc $p \geq 5$.

Soit k le plus petit entier tel que $3^k \equiv 1 \mod p$. On sait que $k | p - 1$, et par ailleurs, $p | 3^n + 1$ donc $3^n \equiv -1 \mod p$, autrement dit $k | 2n$.

Ou bien k est impair, auquel cas $k | n$, et $k \leq p - 1$, donc $k = 1$, ce qui est impossible car $3 \equiv 1 \mod p$ est équivalent à $p = 2$.

Ou bien k est pair, avec $k = 2k'$ on a de même $k' = 1$, donc $k = 2$, absurde car $9 \equiv 1 \mod p$ est équivalent à $p = 2$.

En conclusion, seul 1 vérifie cette propriété. □

2 Le théorème chinois

Proposition 4. Soient $m_1, \ldots, m_n$ des entiers naturels deux à deux premiers entre eux, et $b_1, \ldots, b_n$ des entiers. Alors le système d'équations

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \ldots \\ x \equiv b_n \mod m_n \end{cases}$$

admet une unique solution modulo $\mathrm{M} = m_1 \ldots m_n$.

Démonstration. Commençons par l'unicité, qui est la partie la plus facile. Si x et y sont deux solutions, alors pour tout i on a $m_i | (x - y)$, donc par le théorème de Gauß, $\mathrm{M} | x - y$.

Passons à l'existence. On va construire à la main une telle solution. Avec $u_i = \frac{\mathrm{M}}{m_i}$, on a $u_i \wedge m_i = 1$, et $m_j | u_i$ pour $i \neq j$. Soit v_i un inverse de u_i modulo m_i, posons $x = \sum_{i=1}^{n} u_i v_i b_i$. Alors x est une solution de l'équation. □

TD

Exercice 1. Trouver tous les entiers n tels que $\varphi(n)$ est impair.

Exercice 2. Trouver tous les entiers n tels que $2^n + 1$ est un carré parfait.

Exercice 3. Calculer le pgcd de tous les nombres de la forme $n^{13} - n$, pour $n \in \mathbb{N}$.

Exercice 4. (Olympiades des Etats-Unis - 1991) Montrer que pour tout entier $n \geq 1$, la suite $2, 2^2, 2^{2^2}, \ldots$ est constante à partir d'un certain rang, modulo n.

Exercice 5. (IMO 1978) Soient m et n deux entiers, avec $n > m \geq 1$. On suppose que les trois derniers chiffres de la représentation décimale de 1978^m sont égaux aux trois derniers chiffres de la représentation décimale de 1978^n. Déterminer m et n tels que $m + n$ soit minimal.

Exercice 6. On considère la suite définie par récurrence : $u_0 = 2015^{2015}$, et $u_{n+1} = u_n + 7$ si u_n est impair, $u_{n+1} = \frac{u_n}{2}$ si u_n est pair.

Quel est le plus petit entier que la suite u_n atteindra ?