Petit théorème de Fermat (1640)

Le petit théorème de Fermat énonce une propriété de a^{p-1} pour certains a et p.

I) $p = 3$

1. Soit a un entier non divisible par 3.
   On appelle r_1, r_2 les restes des divisions de a et $2a$ par 3.
   Démontrer par l'absurde que ces restes sont non nuls.
   Démontrer par l'absurde que $r_1 \neq r_2$
2. En déduire que $r_1 \times r_2 = 2$
3. En déduire que $2a^2 \equiv 2$ [3]
4. En déduire que $a^2 \equiv 1$ [3] (*Attention, ce n'est pas une simple division par 2*).
5. En déduire que, pour tout x entier, $x^3 \equiv x$ [3] (*étudier 2 cas*).

II) $p = 5$

1. Soit a un entier non divisible par 5.
   On appelle r_1, r_2, r_3, r_4 les restes des divisions de $a, 2a, 3a, 4a$ par 5.
   Démontrer par l'absurde que r_1, r_2, r_3, r_4 sont tous distincts et non nuls.
2. En déduire que $r_1 \times r_2 \times r_3 \times r_4 \equiv 4!$ [5]
3. En déduire que $a^4 \times 4! \equiv 4!$ [5]
4. En déduire que $a^4 \equiv 1$ [5]
5. En déduire que, pour tout x entier, $x^5 \equiv x$ [5]

III) Cas général

Soit p un nombre premier.
Si a n'est pas divisible par p, on a : ...?
Pour tout x entier, on a : ...?

IV) Exemples d'applications

1. Soient x et y deux entiers non multiples de 29.
   Démontrer l'équivalence : $x^3 \equiv y$ [29] $\Leftrightarrow x \equiv y^{19}$ [29]
   Il s'agit en quelque sorte d'une formule pour calculer la « racine cubique » modulo 29
   On procède en deux implications réciproques
   – Si $x^3 \equiv y$ [29], alors en élevant à puissance 19, $x^{57} \equiv y^{19}$ [29]
     Il suffirait alors de montrer que $x^{57} \equiv x$ [29].
     Comme 29 est premier, cela fait penser au théorème de Fermat, qui dit que $x^{28} \equiv 1$ [29] si x n'est pas multiple de 29.
     Or $57 = (2 \times 28) + 1$, donc $x^{57} \equiv \left(x^{28}\right)^2 x \equiv 1^2 x \equiv x$ [29]
   – Réciproquement, si $x \equiv y^{19}$ [29], alors en élevant à la puissance 3 : $x^3 = y^{57}$ [29].
     D'après ce qui précède, $y^{57} \equiv y$ [29], donc on a bien $x^3 \equiv y$ [29]
2. Démontrer que $x^{24} \equiv 1$ [35] pour tout x premier avec 35.
   Pour cela, appliquer le théorème de Fermat avec 5 et avec 7.
   x étant premier avec 35, il n'est divisible ni par 5 ni par 7.
   Donc on peut appliquer le théorème de Fermat avec 5 et avec 7 :
   $x^4 \equiv 1$ [5], donc $x^{24} \equiv 1^6 \equiv 1$ [5]
   $x^6 \equiv 1$ [7], donc $x^{24} \equiv 1^4 \equiv 1$ [7]
   Donc $x^{24} - 1$ est divisible par 5 et par 7.
   Or 5 et 7 sont des nombres *premiers*, donc $x^{24} - 1$ est divisible par 5×7.
   Donc $x^{24} \equiv 1$ [35]
3. Soit (u, v) vérifiant $5u - 24v = 1$.
   Démontrer que, si x et y sont premiers avec 35, et si $x^5 \equiv y$ [35], alors $x \equiv y^u$ [35].
   Appliquer ce résultat avec une valeur particulière de u
   $5u = 24v + 1$, donc
   $y^u \equiv x^{5u} \equiv x^{24v} x \equiv \left(x^{24}\right)^v x \equiv 1^v x \equiv x$ [35] (on applique le résultat de l'exercice précédent : $x^{24} \equiv 1$ [35]).
   Par exemple, une solution (u, v) est $(5, 1)$ car $5 \times 5 - 24 = 1$.
   Donc, si x et y sont pemiers avec 35, alors si $x^5 \equiv y$ [35], on a $x \equiv y^5$ [35]