

Correction exercice

$$(x+1)^n - x^n = ny \quad (x, y) \in \mathbb{N}^2 \quad (0.1)$$

1/(a)

p divise n donc $n=kp$ avec $k \in \mathbb{N}$. D'après (0.1) $(x+1)^n = x^n + kyp$ donc :

$$(x+1)^n \equiv x^n \pmod{p}$$

1/(b)

- si p non premier avec x alors p/x car p est premier donc p/x^n donc $x^n \equiv 0 \pmod{p}$ donc $(x+1)^n \equiv 0 \pmod{p}$ soit $p/(x+1)^n$ et $p/(x+1)$ car p est premier ce qui est impossible car x et x+1 sont premiers entre eux.
- si p non premier avec x+1 alors $p/x+1$ (p premier) donc $p/(x+1)^n$ $(x+1)^n \equiv 0 \pmod{p}$ donc $x^n \equiv 0 \pmod{p}$ soit p/x^n et p/x car p est premier ce qui est impossible car x et x+1 sont premiers entre eux.

1/(c)

p premier et p premier avec x donc d'après le petit théorème de Fermat : $x^{p-1} \equiv 1 \pmod{p}$ de même : $(x+1)^{p-1} \equiv 1 \pmod{p}$ donc $(x+1)^{p-1} - x^{p-1} \equiv 0 \pmod{p}$ ou encore :

$$(x+1)^{p-1} \equiv x^{p-1} \pmod{p} \quad (0.2)$$

2/

n est pair, donc le plus petit diviseur premier de n $p=2$. Si (x,y) solution de 0.1 alors d'après 1/(c) :

$$(x+1) \equiv x \pmod{2}$$

$x+1 = x + 2k$ et $k \in \mathbb{N} \Rightarrow k = \frac{1}{2}$, ce qui est impossible.

L'équation (0.1) n'admet pas de solution si n est pair.

3/(a)

Montrons que n et $p-1$ sont premiers entre eux :

Si n et $p-1$ non premiers entre eux alors il existe q premier tel que :

$q/(p-1)$ et q/n . Impossible car $q > p$ puisque p plus petit nombre premier qui divise n .

n et $p-1$ premiers entre donc d'après le théorème de Bézout :

$$\exists (u, v) \in \mathbb{Z}^2 \text{ tels que } nu + (p-1)v = 1 \quad (0.3)$$

3/(b)

$u = (p-1)q + r$ et $r < p-1$. D'après (0.3) $n(p-1)q + (p-1)v = 1 \Rightarrow$

$$nr = 1 - (p-1)(v + nq)$$

3/(c)

$(p-1)v' = nr - 1$. D'après (0.3) n et $p-1$ premiers entre eux donc $r \geq 1$.
 $n > 1$ donc $nr - 1 \geq 0$ or $p > 1$ donc $v' \geq 0$.

3/(d)

$v' \geq 0$ et (0.2) donne $(x+1)^{(p-1)v'} \equiv x^{(p-1)v'} \pmod{p}$

$(x+1)^{nr-1} \equiv x^{nr-1} \pmod{p}$ or (1.a) donne :

$$(x+1)^{nr} \equiv x^{nr} \pmod{p}$$

$$x(x+1)^{nr-1} \equiv x^{nr} \pmod{p}$$

$$(x+1)^{nr} \equiv x(x+1)^{nr-1} \pmod{p}$$

$$(x+1)^{nr} - x(x+1)^{nr-1} \equiv 0 \pmod{p}$$

$$(x+1)^{nr-1}((x+1) - x) \equiv 0 \pmod{p} \text{ soit :}$$

$(x+1)^{nr-1} \equiv 0 \pmod{p}$ donc $p/(x+1)$ impossible car p et $x+1$ premiers entre eux.

il en résulte que (0.1) n'admet aucune solution.