# 3.3 Wilson's theorem

June 16, 2015

## 1

$\diamond$ $p$ **est le plus petit nombre premier divisant** $(p-1)!+1$.

On a que si $a$ divise $b$ et $b-1$, alors $a=1$, car alors $a$ divise $b-(b-1)=1$.

Soit alors $p^* < p$ un premier divisant $(p-1)!+1$. Puisque $p^*$ divise $(p^*-1)!+1$ par Wilson, on a que $p^*$ divise également $(p-1)!+1-((p^*-1)!+1) = (p-1)!-(p^*-1)! = (p^*-1)!((p-1)\cdots(p^*)-1)$.

Or, $p^*$ ne peut pas diviser $(p^*-1)!$ puisqu'il divise $(p^*-1)!+1$, et s'il le fesait il serait alors égal à 1.

Il doit donc diviser $((p-1)\cdots(p^*)-1)$ (**justification**). Mais $p^*$ divise $(p-1)\cdots(p^*)$. Alors divisant $(p-1)\cdots(p^*)-1$, il doit être égal à 1, ce qui est absurde.

Alors $p$ est le plus petit premier divisant $(p-1)!+1$.

## 2

$\diamond$ $10 \not| [(n-1)!+1]$ pour tout $n$.

Car SLC. Alors $10k=(n-1)!+1$ pour un certain $n>4$. Alors $(n-1)!+1$ est pair, car divisble par 2.

Or, $(n-1)!$ est pair pour tout $n>1$. Donc $(n-1)!+1$ est impair.