Exercici 18.

Siguin $K \in \mathbb{N}$ i $N := 4K + 3$. Demostreu que, si N no és primer, llavors existeix un divisor primer p de N de la forma $p = 4k+3$, per a algun $k \in \mathbb{N}$. Adapteu la demostració del teorema d'Euclides feta a classe per a demostrar que el conjunt dels nombres naturals primers de la forma $4K + 3$, $K \in \mathbb{N}$, conte una infinitat de nombres primers

Solució 18.

$K \in \mathbb{N}$ i $N := 4K + 3$ i N no primer $\Rightarrow \exists p = 4k + 3$ primer on $k \in \mathbb{N}$ i $p|N$

Sigui N un nombre no primer de forma $4K + 3$ s'observa clarament que aquest nombre és senar al ser la suma d'un nombre parell (4k) i senar (3). Per tant, aplicant la T$^{\underline{a}}$ fundamental de la Aritmètica, com el nombre no és primer es podrà descompondre en producte de nombres primers. Com és un nombre senar, tots els seus factors primers seràn senars.

> LEMA: Tots els nombres primers senars tenen forma de $4z + 1$ o $4z + 3$ per a un z arbitrari natural.
>
> Tots els nombres naturals es pot escriure de forma $4z + r$ on $z \in \mathbb{N}$ i $0 \leq r \leq 3$, és a dir, els poden escriure de forma $4z$, $4z+1$, $4z+2$, o $4z+3$. S'observa que $4z$ i $2(2z+1)$ són nombres parells, per tant, tots els nombres primers senars es pot escriure com $4z + 1$ o $4z + 3$

Aplicant el lema anterior podem afirmar què la descomposició en factors primers de N estarà format per nombres primers de forma $4z + 1$ o $4z + 3$. Hem de demostrar que a la descomposició hi existirà almenys un primer de forma $4z + 3$

Ho demostrarem per reducció a l'absurd:
Suposem que tots els factors primers de la descomposició té forma de $4z + 1$, per tant,

$$N = (4t_1 + 1)(4t_2 + 1)\cdots\cdots(4t_n + 1) \text{ on } t_i \in \mathbb{N}\ \forall i, 1 \leq i \leq n \Rightarrow$$

$$N = (4(4t_1t_2 + t_1 + t_2) + 1)\cdots\cdots(4t_n + 1) \text{ Observem què } 4t_1t_2 + t_1 + t_2 \in \mathbb{N}$$
ja què els naturals està tancat per la suma i el producte.

Si continuem multiplicant tenim què: $N = 4T + 1$ on $T \in \mathbb{N}$

Per tant hem arribat a una contradicció, ja què si tots els primers són de la forma $4z+1 \Rightarrow N$ serà de la forma $4T + 1$ i no de la forma $4K + 3$. Per tant almenys un factor de N serà de la forma $4z + 3$ $\square$

Demostrar que hi ha infinits nombres escrits de la forma $4K+3$ on $K \in N$

Ho demostrarem per reducció a l'absurd:
Suposem que hi exiteix un nombre finit de nombres primers escrit de la forma $4k+3$ per a algun $k \in \mathbb{N}$
Per tant, tots els nombres primers escrits de la forma $4k+3$ són:

$$p_0 = 3, p_1 = 7, p_3, ..., p_{q-1}, p_q \text{ per a un } q \in \mathbb{N}$$

Per tant, si definim que $X = 4(p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q) + 3$. Aplicant la demostració anterior X tindrà un factor primer de la forma $4k+3$ per a algun $k \in \mathbb{N}$, ja què $p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q \in \mathbb{N}$
Aplicant la suposició inicial tots els nombres primers de forma $4k+3$ són $p_0 = 3, p_1 = 7, p_3 .... p_{q-1}, p_q$. Per tant, X tindrà com a factor un d'aquest nombres.

Podem trobar dos casos:

(1) Si $p = p_0 = 3$
$p|X \Leftrightarrow 3|4(p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q) + 3$ Com 3 divideix a 3 $\Rightarrow$
$3|4(p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q) \Rightarrow 3|4$ o $3|p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q$ Hem arribat a una contradicció.
Ja què $3 \nmid 4$ i $3 \nmid p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q$ sabent què $p_i \neq 3 \ \forall i, 1 \leq i \leq q$

(2) Si $p = p_i$ per a algún i on $1 \leq i \leq q$
Si $p|X \Leftrightarrow p_i|4(p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q) + 3 \Rightarrow$
$p_i|3$ i $p_i|4(p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q)$ Hem arribat a una contradicció.
Ja què $p_i|4(p_1 p_3 \cdot\cdots\cdot p_{q-1} p_q)$ però $p_i \nmid 3$ sabent què $p_i \neq 3 \ \forall i, 1 \leq i \leq q$. A més $3 < p_i$

Per tant, com hem arribat a contradiccions a tots els casos al suposar que els nombres primers de la forma $4K+3$ són finits, aplicant la llei de la reducció a l'absurd, els nombres primers escrits d'aquesta forma són infinits $\square$