1.4.15 *Demostrar que existen infinitos primos de la forma 4n+3 y de la forma 6n+5.*

a) Demostrar que existen infinitos primos de la forma 4n+3.

Supongamos que existe un número finito de primos congruentes con -1 (mód 4): C=$\{p_1, p_2, \ldots, p_n\}$

Vamos a probar que, si $n \equiv -1$ (mód 4) $\implies$ hay al menos un número primo p que lo divide, de tal forma que $p \equiv -1$ (mód 4). Para demostrar esta proposición, basta con estudiar la tabla de multiplicación de las clases de restos módulo 4:

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Definamos $N = 4p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} - 1$, con $\alpha_i > 1 \implies N \equiv -1$ (mód 4). Por la observación anterior, existe un $p_i \in C$ tal que $p_i \mid N$. Además, resulta evidente que $p_i \mid 4p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} \implies p_i \mid 4p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} - N \implies p_i \mid 1$. *¡Contradicción!*

b) Demostrar que existen infinitos primos de la forma 6n+5.

Supongamos que existe un número finito de primos congruentes con -1 (mód 6): C=$\{p_1, p_2, \ldots, p_n\}$

Vamos a probar que, si $n \equiv -1$ (mód 6) $\implies$ hay al menos un número primo p que lo divide, de tal forma que $p \equiv -1$ (mód 6). Para demostrar esta proposición, basta con estudiar la tabla de multiplicación de las clases de restos módulo 6:

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Definamos $N = 6p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} - 1$, con $\alpha_i > 1 \implies N \equiv -1$ (mód 6). Por la observación anterior, existe un $p_i \in C$ tal que $p_i \mid N$. Además, resulta evidente que $p_i \mid 6p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} \implies p_i \mid 6p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} - N \implies p_i \mid 1$. *¡Contradicción!*

Problema escrito por Jesús de los Nietos Valle.