Álgebra 1

Práctica 4: Números Primos
y
Teorema Fundamental de la Aritmética

Patricia Jancsa

Viernes 7/5/2021

Números Primos

- $p \in \mathbb{Z}$, *p es primo* $\Leftrightarrow$ *p* tiene exactamente 4 divisores
- *p es primo* $\Leftrightarrow$ los únicos divisores de p son $\pm 1, \pm p$
  - *p es primo* es equivalente a que

$$p \mid a \cdot b \Longrightarrow p \mid a \text{ ó bien } p \mid b$$

Contraejemplo si *p* no primo: $4 \mid 4 = 2 \cdot 2$ *pero* $4 \nmid 2$

Ejemplos de primos

Existen infinitos primos: probarlo...!

$$\mathcal{P}_+ = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 \dots\}$$

Criterio para determinar si p es primo

Ej 1.

Probar que n es compuesto si y sólo si existe un primo positivo $p|n$ tal que $1 < p \leq \sqrt{n}$

Dem: $\Leftarrow$ vale por la definición de primo: nada que probar

$\Longrightarrow$ Sea $n > 0$ compuesto y supongamos que existe primo $p|n$ que verifica $p > \sqrt{n}$

$$\Longrightarrow n = p \cdot d : \ d \in \mathbb{Z} \quad \Longrightarrow d \leq \sqrt{n}$$

pues si ocurriera $d > \sqrt{n}$

$$\Longrightarrow n = p \cdot d > \sqrt{n} \cdot \sqrt{n} \geq n, \ \textit{absurdo}$$

- Si d es primo, listo ✓

Tenemos $n = p \cdot d : \ d \in \mathbb{Z} \quad \Longrightarrow d \leq \sqrt{n}$

- Si d es compuesto $\Longrightarrow$ existe primo positivo $q \mid d$,

y por transitividad

$$q \mid n$$

Por lo tanto, q primo cumple todo:

$$q \leq d \leq \sqrt{n} \quad \text{y} \quad q \mid n \ \checkmark$$

Números Primos

Ej 2.

Hallar todos los primos entre 100 y 140.

- Si $2 < p$ es primo $\Longrightarrow p$ es impar
- Si $n > 5$ termina en 5 $\Longrightarrow n$ no es primo

$\Longrightarrow$ Los primos $p > 5$ son impares y no terminan en 5

- $11^2 = 121 \leq 140 < 169 = 13^2$

$\Longrightarrow$ Para determinar si n es primo ó compuesto tenemos que dividirlo a lo sumo por los primos

$$\mathcal{P}_+ = \{2, 3, 5, 7, 11\}$$

- 101 es primo pues

$$101 \equiv 2 \mod 3 \implies 3 \not| 101$$

$$101 \equiv 1 \mod 5 \implies 5 \not| 101$$

$$101 \equiv 3 \mod 7 \implies 7 \not| 101 \checkmark$$

- 103 es primo pues

$$103 \equiv 1 \mod 3 \implies 3 \not| 103$$

$$101 \equiv 3 \mod 5 \implies 5 \not| 103$$

$$103 \equiv 5 \mod 7 \implies 7 \not| 103 \checkmark$$

- 107 es primo pues

$$107 \equiv 2 \mod 3 \implies 3 \not| 107$$

$$107 \equiv 2 \mod 5 \implies 5 \not| 107$$

$$107 \equiv 2 \mod 7 \implies 7 \not| 107 \checkmark$$

- 109 es primo pues

$$109 \equiv 1 \mod 3 \implies 3 \not| 109$$

$$109 \equiv 4 \mod 5 \implies 5 \not| 109$$

$$109 \equiv 4 \mod 7 \implies 7 \not| 109 \checkmark$$

- $111 \equiv 0 \mod 3 \implies$ 111 *no es primo*

- 113 es primo pues

$$113 \equiv 2 \mod 3 \implies 3 \not| 113$$

$$113 \equiv 3 \mod 5 \implies 5 \not| 113$$

$$113 \equiv 1 \mod 7 \implies 7 \not| 113 \checkmark$$

- $117 \equiv 0 \mod 3 \implies$ 117 *no es primo*
- $119 = 70 + 49 \equiv 0 \mod 7 \implies$ 119 *no es primo*
- $121 \equiv 0 \mod 11 \implies$ 121 *no es primo*
- $123 \equiv 0 \mod 3 \implies$ 123 *no es primo*

- 127 es primo pues

$$127 \equiv 1 \mod 3 \implies 3 \nmid 127$$

$$127 \equiv 2 \mod 5 \implies 5 \nmid 127$$

$$127 \equiv 1 \mod 7 \implies 7 \nmid 127$$

$$127 \equiv 6 \mod 11 \implies 11 \nmid 127 \checkmark$$

- $129 \equiv 0 \mod 3 \implies 129$ *no es primo*

- 131 es primo pues

$$131 \equiv 2 \mod 3 \implies 3 \not| 131$$

$$131 \equiv 1 \mod 5 \implies 5 \not| 131$$

$$131 \equiv 5 \mod 7 \implies 7 \not| 131$$

$$131 \equiv 10 \mod 11 \implies 11 \not| 131 \checkmark$$

- $133 = 70 + 63 \equiv 0 \mod 7 \implies$ 133 *no es primo* ✓

- 137 es primo pues

$$137 \equiv 2 \mod 3 \implies 3 \not| 137$$

$$137 \equiv 2 \mod 5 \implies 5 \not| 137$$

$$137 \equiv 4 \mod 7 \implies 7 \not| 137$$

$$137 \equiv 5 \mod 11 \implies 11 \not| 137 \checkmark$$

- 139 es primo pues

$$139 \equiv 1 \mod 3 \implies 3 \not| 139$$
$$139 \equiv 4 \mod 5 \implies 5 \not| 139$$
$$139 \equiv 6 \mod 7 \implies 7 \not| 139$$
$$139 \equiv 7 \mod 11 \implies 11 \not| 139 \checkmark$$

Primos entre 100 y 140

$$\Longrightarrow \mathcal{P} = \{101, 103, 107, 109, 113, 127, 131, 137, 139\}$$

Primos entre 100 y 200

100	101	102	103	104	105	106	107	108	109
110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129
130	131	132	133	134	135	136	137	138	139
140	141	142	143	144	145	146	147	148	149
150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169
170	171	172	173	174	175	176	177	178	179
180	181	182	183	184	185	186	187	188	189
190	191	192	193	194	195	196	197	198	199

Teorema Fundamental de la Aritmética

Dado $n \in \mathbb{Z},\ n \neq 0, \pm 1$, existen únicos primos distintos

$$p_1 < p_2 < \cdots < p_r \in \mathbb{N}$$

y $m_1, \ldots, m_r \in \mathbb{N}$ tales que

$$n = \pm p_1^{m_1} \cdot p_2^{m_2} \cdot \cdots \cdot p_r^{m_r}$$

Teorema Fundamental de la Aritmética

Ej 3.

Hallar la factorización prima de 20111

Solución: Usando la lista de la introducción tenemos que ver qué primos lo dividen y a qué potencias:

$$\mathcal{P}_+ = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \dots\}$$

- $20111 \equiv 1 \mod 2 \implies 2 \not| 20111$
- $20111 \equiv 2 \mod 3 \implies 3 \not| 20111$
- $20111 \equiv 1 \mod 5 \implies 5 \not| 20111$

Teorema Fundamental de la Aritmética

- $20111 = 14000 + 6111 \equiv 6111 \ mod\ 7$
  $\equiv 4900 + 1211 \equiv 1211 \ mod\ 7$
  $\equiv 700 + 511 \equiv 511 \equiv 490 + 21 \equiv 0 \ mod\ 7$
  $\Longrightarrow 20111 = 7 \cdot 2873$
- $2873 = 2800 + 70 + 3 \equiv 3 \ mod\ 7 \Rightarrow 7^2 \not| 20111$
- $2873 = 2200 + 660 + 13 \equiv 2 \ mod\ 11 \Rightarrow 11 \not| 20111$
- $2873 = 2600 + 260 + 13 \equiv 0 \ mod\ 13 \Rightarrow 2873 = 13 \cdot 221$
- $221 = 130 + 52 + 39 \equiv 0 \ mod\ 13 \Rightarrow 13^2 | 20111$

$\Rightarrow 20111 = 7 \cdot 13^2 \cdot 17$ ✓

Ej 4.

a) Probar que el exponente de todo primo en la factorización prima de n^3 es un múltiplo de 3.
b) Probar que $\sqrt[3]{4}$ no es racional

Solución: Dado $n \in \mathbb{Z},\ n \neq 0, \pm 1$, existen únicos primos distintos

$$p_1 < p_2 < \cdots < p_r \in \mathbb{N}$$

y $m_1, \ldots, m_r \in \mathbb{N}$ tales que

$$n = \pm p_1^{m_1} \cdot p_2^{m_2} \cdot \cdots \cdot p_r^{m_r}$$

$$\Longrightarrow n^3 = \pm p_1^{3m_1} \cdot p_2^{3m_2} \cdot \cdots \cdot p_r^{3m_r}$$

b) Recordemos que $q \in \mathbb{Q}$ si y sólo si $q =$ cociente de enteros

$$\mathbb{Q} = \left\{ \frac{n}{m} : n, m \in \mathbb{Z},\ m \neq 0 \right\}$$

Dem por el absurdo: Supongamos que $\sqrt[3]{4}$ es racional $\Longrightarrow$ existen $n, m \in \mathbb{Z},\ m \neq 0$ tales que

$$\sqrt[3]{4} = \frac{n}{m} \Longrightarrow \sqrt[3]{4} \cdot m = n$$

$$\Longrightarrow 4 \cdot m^3 = n^3 \in \mathbb{Z}$$

$$\Longrightarrow 2^2 \cdot m^3 = n^3 \in \mathbb{Z}$$

$$\Longrightarrow 2 \text{ aparece en la factorización prima de } n^3 \Longrightarrow 2 \Big| n$$

$$2|n^3 \Longrightarrow 2|n$$

Dem por el absurdo: Supongamos que $2 \nmid n$

$\Longrightarrow$ n es un entero impar $n = 2k + 1$

$$\Longrightarrow n^3 = (2k+1)^3 = \binom{3}{0}2^3k^3 + \binom{3}{1}2^2k^2 + \binom{3}{2}2^1k^1 + \binom{3}{3}2^0k^0$$

$$\underbrace{= 8k^3 + 12k^2 + 6k}_{2\cdot q} + 1 \Longrightarrow n^3 \text{ es impar, absurdo}$$

$\Longrightarrow$ Concluímos que $2|n$

Pero entonces $\Longrightarrow 4 \cdot m^3 = n^3$

$$\Longrightarrow 2^2 \cdot q^{3j_s} \cdot \ldots \cdot q_r^{3j_s} = 2^{3m_1} \cdot p_2^{3m_2} \cdot \ldots \cdot p_r^{3m_r}$$

$$\Longrightarrow 2^2 \cdot 2^{3\ell} \cdot \tilde{k} = 2^{3m_1} \cdot k$$

donde $2 \not| \tilde{k},\ k \in \mathbb{Z}$

$\Longrightarrow$ absurdo pues del lado izquierdo el exponente de $p = 2$ es

$$2 + 3\ell \Longrightarrow \text{no es múltiplo de 3}$$

$\Longrightarrow$ queda probado que $\sqrt[3]{4}$ no es racional ✓

T. F. Aritmética

Corolario:

El exponente de todo primo en la factorización prima de n^2 es par.
El exponente de todo primo en la factorización prima de n^3 es múltiplo de 3.
El exponente de todo primo en la factorización prima de n^4 es múltiplo de 4.
Etc.

$$n^2 = p_1^{2m_1} \cdot p_2^{2m_2} \cdot \dots \cdot p_r^{2m_r}$$

$$n^3 = p_1^{3m_1} \cdot p_2^{3m_2} \cdot \dots \cdot p_r^{3m_r}$$

$$n^4 = p_1^{4m_1} \cdot p_2^{4m_2} \cdot \dots \cdot p_r^{4m_r}$$

Ej. 5.

Decidir si existen $m, n \in \mathbb{Z}$ tales que

a) $3m^2 = 17n^3$, b) $5m^2 = 7n^4$

Solución: $3m^2 = 3 \cdot 3^2 \cdot 17^4 = 17 \cdot 17^3 \cdot 3^3 = 17n^3$

$\Longrightarrow$ verdadero eligiendo $m = 3 \cdot 17^2,\ n = 3 \cdot 17$

b) $5m^2 = 7n^4 \Longrightarrow$ falso! pues

$5|$ lado izquierdo $\Longrightarrow 5|$ lado derecho

$$7n^4 = 7 \cdot 5^{4\ell} \cdot p_2^{4\ell_2} \cdots p_r^{4\ell_r}$$

Pero del lado izquierdo

$5m^2 = 5^{2k+1} \cdot q_2^{2j_2} \cdots q_s^{2j_s}$ *absurdo*! pues $2k+1$ no es par

Cómo calcular el mcd y no morir en el intento

Ej. 6.

a) Calcular los posibles valores de

$$d(n) = mcd(7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1})$$

b) Encontrar n tales que $d(n)$ tome 3 valores distintos.

Solución: a) Usemos propiedades

- $d = (a : b) = (a - bc : b)$
- p, q primos distintos, $p^\ell | d,\ q | d \Longrightarrow p^\ell \cdot q | d$
- m coprimo con d entonces $d = (a : mb) = (a : b)$
- $$\left.\begin{array}{l} p \text{ primo} \quad p \nmid d \\ d | p \cdot k \end{array}\right\} \Longrightarrow d | k$$

$$
\begin{aligned}
d &= (7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1}) \\
&= (7^{n-1} + 5^{n+2} + 5 \cdot [5 \cdot 7^n - 5^{n+1}] : 5 \cdot 7^n - 5^{n+1})
\end{aligned}
$$

$$
\begin{aligned}
d &= (7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1}) \\
&= (\underbrace{7^{n-1} + 5^{n+2} + 5 \cdot [5 \cdot 7^n - 5^{n+1}]}_{=7^{n-1}(1+5^2 \cdot 7)} : 5 \cdot 7^n - 5^{n+1}) \\
&= (7^{n-1}(1 + 5^2 \cdot 7) : 5 \cdot 7^n - 5^{n+1}) \\
&= (7^{n-1} \cdot 176 : 5 \cdot 7^n - 5^{n+1}) = (176 : 7^n - 5^n)
\end{aligned}
$$

Pero $7 \not| d$ pues si $7|d \Longrightarrow 7|ambos \Longrightarrow 7|5^{n+1}$ lo cual es imposible pues

$$(7 : 5^{n+1}) = 1 \text{ dado que 5 y 7 son primos distintos}$$

$$\Longrightarrow d \Big| 176 \Longrightarrow d \in \{1, 2, 4, 8, 11, 16, 22, 44, 88, 176\}$$

pues $176 = 2^4 \cdot 11$

b) • Módulo 2:

$$7^n - 5^n \equiv 1^n - 1^n \equiv 0 \ mod\ 2 \ \Big\} \Longrightarrow 2|d$$

• Módulo 8, con n par =2k:

$$\left.\begin{array}{l} 7^n - 5^n \equiv (-1)^{2k} - 5^{2k} \\ \equiv 1 - (25)^k \equiv 1 - 1^k \equiv 0 \ mod\ 8 \end{array}\right\} \Longrightarrow 8|d,\ n\ par$$

• Módulo 4, n impar =2k+1:

$$\begin{array}{l} 7^n - 5^n \equiv (-1)^{2k+1} - 1^{2k+1} \\ \equiv (-1)^{2k}(-1) - (-1)^{2k} \cdot 1 \equiv -1 - 1 \\ \equiv 2 \ mod\ 4 \\ \Longrightarrow 4 \not| d \end{array}$$

$$\Longrightarrow d \in \{\cancel{1}, 2, \cancel{4}, 8, \cancel{11}, 16, 22, \cancel{44}, 88, 176\}$$

b) Haciendo la cuenta con los originales da lo mismo:

- Módulo 2:

$$\left.\begin{array}{ll} 7^{n-1}+5^{n+2} \equiv 1^{n-1}+1^{n+2} & \equiv 0 \ mod\ 2 \\ 5\cdot 7^{n}-5^{n+1} \equiv 1\cdot 1^{n}-1^{n-1} & \equiv 0 \ mod\ 2 \end{array}\right\} \Longrightarrow 2|d$$

- Módulo 8, con n par =2k:

$$\left.\begin{array}{ll} 7^{n-1}+5^{n+2} & \equiv (-1)^{2k-1}+5^{2k+2} \\ & \equiv -1+(5^2)^{k+1} \equiv -1+1 \equiv 0 \ mod\ 8 \\ 5\cdot 7^{n}-5^{n+1} & \equiv 5\cdot(-1)^{2k}-5^{2k+1} \\ & \equiv 5-(25)^{k}\cdot 5 \equiv 5-5 \equiv 0 \ mod\ 8 \end{array}\right\} \Longrightarrow 8|d,\ n\ par$$

- Módulo 4, n impar =2k+1:

$$\left.\begin{array}{ll} 7^{n-1}+5^{n+2} & \equiv (-1)^{2k+1-1}+1^{2k+2} \\ & \equiv (-1)^{2k}+1 \equiv 1+1 \equiv 2 \ mod\ 4 \end{array}\right\} \Longrightarrow 4 \not| d$$

$$\Longrightarrow d \in \{\cancel{1}, 2, \cancel{4}, 8, \cancel{11}, 16, 22, \cancel{44}, 88, 176\}$$

Ejemplos de valores distintos:

- $n = 1 \Longrightarrow d = (7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1})$

$$= (126 : 10) = 2$$

- $n = 2 \Longrightarrow d = (7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1})$

$$= (632 : 120) = 8$$

- $n = 4 \Longrightarrow d = (176 : 7^4 - 5^4)$

$$= (176 : 1776) = 16$$

- $n = 10 \Longrightarrow d = (176 : 7^{10} - 5^{10})$

$$= (176 : 2^3 \cdot 3 \cdot 11) = 88$$

- $n = 20 \Longrightarrow d = (176 : 7^{20} - 5^{20})$

$$= (176 : 2^4 \cdot 3 \cdot 11) = 176$$

Adicional

c) Construir una tabla de restos módulo 11 para $7^n - 5^n$ y probar que si

$$n \text{ impar} \implies 11 \not| 7^n - 5^n$$

Concluir entonces que

- d no puede ser 22
- Si n impar $\implies d = 2$

Por lo tanto, los valores alcanzados por d son

$$\implies d \in \{\cancel{1}, 2, \cancel{4}, 8, \cancel{11}, 16, \cancel{22}, \cancel{44}, 88, 176\} \checkmark$$

Restos módulo 11

$\Longrightarrow$ Cálculos de restos mod (11) para 7^n

n impar	7^n	$\equiv$	$\equiv$	7^n *mod* 11
1	7	7	7	7
3	7^3	$7^2 \cdot 7$	$5 \cdot 7$	2
5	7^5	$7^2 \cdot 2$	$5 \cdot 2$	10
7	7^7	$7^2 \cdot 10$	$5 \cdot 10$	6
9	7^9	$7^2 \cdot 6$	$5 \cdot 6$	8
11	7^{11}	$7^2 \cdot 8$	$5 \cdot 8$	7
13	7^{13}	$7^2 \cdot 7$	$5 \cdot 7$	2
15	7^{15}	$7^2 \cdot 2$	$5 \cdot 2$	10
17	7^{17}	$7^2 \cdot 10$	$5 \cdot 10$	6
19	7^{19}	$7^2 \cdot 6$	$5 \cdot 6$	8
21	7^{21}	$7^2 \cdot 8$	$5 \cdot 8$	7
23	7^{23}	$7^2 \cdot 7$	$5 \cdot 7$	2

Restos módulo 11

$\Longrightarrow$ Cálculos de restos mod (11) para 5^n

n impar	5^n	$\equiv$	$\equiv$	5^n *mod* 11
1	5	5	5	5
3	5^3	$5^2 \cdot 5$	$3 \cdot 5$	4
5	5^5	$5^2 \cdot 4$	$3 \cdot 4$	1
7	5^7	$7^2 \cdot 1$	$3 \cdot 1$	3
9	5^9	$5^2 \cdot 6$	$3 \cdot 3$	9
11	5^{11}	$5^2 \cdot 9$	$3 \cdot 9$	5
13	5^{13}	$5^2 \cdot 5$	$3 \cdot 5$	4
15	5^{15}	$5^2 \cdot 2$	$3 \cdot 4$	1
15	5^{15}	$5^2 \cdot 1$	$3 \cdot 1$	3
19	5^{19}	$5^2 \cdot 3$	$3 \cdot 3$	9
21	5^{21}	$5^2 \cdot 9$	$3 \cdot 9$	5
23	5^{23}	$5^2 \cdot 5$	$3 \cdot 5$	4

Restos módulo 11

$\Longrightarrow$ Tabla de restos mod (11) para $7^n - 5^n$

n impar	7^n	5^n	$7^n - 5^n$	$7^n - 5^n$ *mod* 11
1	7	5	$7 - 5$	2
3	7^3	5^3	$2 - 4$	9
5	7^5	5^5	$10 - 1$	9
7	7^7	5^7	$6 - 3$	3
9	7^9	5^9	$8 - 9$	10
11	7^{11}	5^{11}	$7 - 5$	2
13	7^{13}	5^{13}	$2 - 4$	9
15	7^{15}	5^{15}	$10 - 1$	9
17	7^{17}	5^{17}	$6 - 3$	3
19	7^{19}	5^{19}	$8 - 9$	10
21	7^{21}	5^{21}	$7 - 5$	2
23	7^{23}	5^{23}	$2 - 4$	9

Cálculos Auxiliares: n *impar* $\Longrightarrow 11 \not| 7^n - 5^n$

$$
\begin{array}{lll}
7^5 & \equiv (-4)^5 & \textit{mod } 11 \\
& \equiv (-4)(-4)^4 & \textit{mod } 11 \\
& \equiv -4 \cdot 16^2 & \textit{mod } 11 \\
& \equiv -4 \cdot 5^2 & \textit{mod } 11 \\
& \equiv -4 \cdot 3 & \textit{mod } 11 \\
& \equiv -12 & \textit{mod } 11 \\
& \equiv -1 & \textit{mod } 11 \\
\Longrightarrow 7^{10} & \equiv +1 & \textit{mod } 11
\end{array}
\qquad
\begin{array}{lll}
5^5 & \equiv 5 \cdot 5^4 & \textit{mod } 11 \\
& \equiv 5 \cdot 25^2 & \textit{mod } 11 \\
& \equiv 5 \cdot 3^2 & \textit{mod } 11 \\
& \equiv 5 \cdot 9 & \textit{mod } 11 \\
& \equiv 45 & \textit{mod } 11 \\
& \equiv 44 + 1 & \textit{mod } 11 \\
& \equiv 1 & \textit{mod } 11 \\
\Longrightarrow 5^{10} & \equiv 1 & \textit{mod } 11
\end{array}
$$

Escribamos cada exponente $n = 10q + r$ con r impar,
$r = 1, 3, 5, 7, 9$, entonces a partir de la tabla de restos

$$
\begin{aligned}
7^n - 5^n = 7^{10q+r} - 5^{10q+r} &= (7^{10})^q 7^r - (5^{10})^q 5^r \\
&\equiv 1 \cdot 7^r - 1 \cdot 5^r \equiv 7^r - 5^r \neq 0 \ \textit{mod } 11 \ \checkmark
\end{aligned}
$$

Primos congruentes a 5 módulo 6

Ej. 7.

a) Probar que para todo $n \in \mathbb{N}, n \equiv 5 \bmod 6$ existe un primo positivo $p|n$ tal que $p \equiv 5 \bmod 6$.
b) Probar que existen infinitos primos congruentes a 5 módulo 6.

Dem: a) Teorema Fundamental de la Aritmética para $n > 1$

$\Longrightarrow$ existen únicos primos $1 < p_1 < p_2 < \cdots < p_\ell$ y $m_k \in \mathbb{N}$ tales que

$$n = \prod_{k=1}^{\ell} p_k^{m_k}$$

Veamos que entonces

$$\Longrightarrow p_k \equiv 1 \text{ ó bien } p_k \equiv 5 \ mod\ 6 \ \forall\ k$$

Descartemos los otros resultados mod 6

Sea p alguno de los primos $p_k|n$, entonces

- Si $p \equiv r = 0, 2, 4 \ mod\ 6 \Longrightarrow r = 2\tilde{r}$

$$\Longrightarrow p = 6q + r = 2(3q + \tilde{r}) \equiv 0 \ mod\ 2$$

Pero p es primo $\Longrightarrow p = 2$, absurdo pues

$$n \equiv 5 \ mod\ 6 \Longrightarrow n = 6q + 5 \equiv 1 \ mod\ 2 \Longrightarrow 2 \not| n$$

- Si algún $p \equiv r = 3 \ mod\ 6 \Longrightarrow p = 6q + 3$

$$p = 3(2q + 1) \equiv 0 \ mod\ 3$$

Pero p es primo $\Longrightarrow p = 3 \Longrightarrow 3|n$, imposible pues

$$n \equiv 5 \ mod\ 6 \Longrightarrow n = 6q + 5 \equiv 2 \ mod\ 3$$

$\Longrightarrow$ Todo $p_k \equiv 1$ ó bien $p_k \equiv 5 \ mod\ 6$ ✓

Algún primo $p \equiv 5 \bmod 6$

$$n = \prod_{k=1}^{\ell} p_k^{m_k} \Longrightarrow p_k \equiv 1 \text{ ó bien } p_k \equiv 5 \ mod\ 6 \ \forall \ k$$

¿Podrían ser todos los $p_k \equiv 1 \ mod\ 6$?

$$Si\ todos\ p_k \equiv 1\ mod\ 6 \Longrightarrow n = \prod_{k=1}^{\ell} p_k^{m_k} \equiv \prod_{k=1}^{\ell} 1^{m_k} \equiv 1 \not\equiv 5\ mod\ 6$$

$\Longrightarrow$ Algún $p_k \equiv 5 \ mod\ 6$ ✓

Probemos $\exists$ infinitos primos $p \equiv 5 \bmod 6$

Supongamos que existen sólo finitos $p_1, \ldots, p_\ell \equiv 5 \ mod\ 6$

$$\Longrightarrow p_k \equiv 5 \equiv -1 \ mod\ 6$$

$$\prod_{k=1}^{\ell} p_k \equiv (-1)^\ell \equiv \begin{cases} 1 & si\ \ell\ par \\ -1 & si\ \ell\ impar \end{cases}$$

- *Si* ℓ *par* $\Longrightarrow N = \prod_{k=1}^{\ell} p_k + 4 \equiv 1 + 4 \equiv 5 \ mod\ 6$

$\Longrightarrow$ algún $p_k | N \Longrightarrow p_k | 4 \Longrightarrow p_k = 2 \not\equiv 5 \ mod\ 6$ *absurdo*

- *Si* ℓ *impar* $\Longrightarrow M = \prod_{k=1}^{\ell} p_k + 6 \equiv -1 + 6 \equiv 5 \ mod\ 6$

entonces algún $p_k | M \Longrightarrow p_k | 6 \Longrightarrow p_k = 2$ ó bien $p_k = 3$
absurdo pues $2, 3 \not\equiv 5 \bmod 6$

Por lo tanto, queda probado que

existen infinitos primos $p \equiv 5 \bmod 6$ ✓