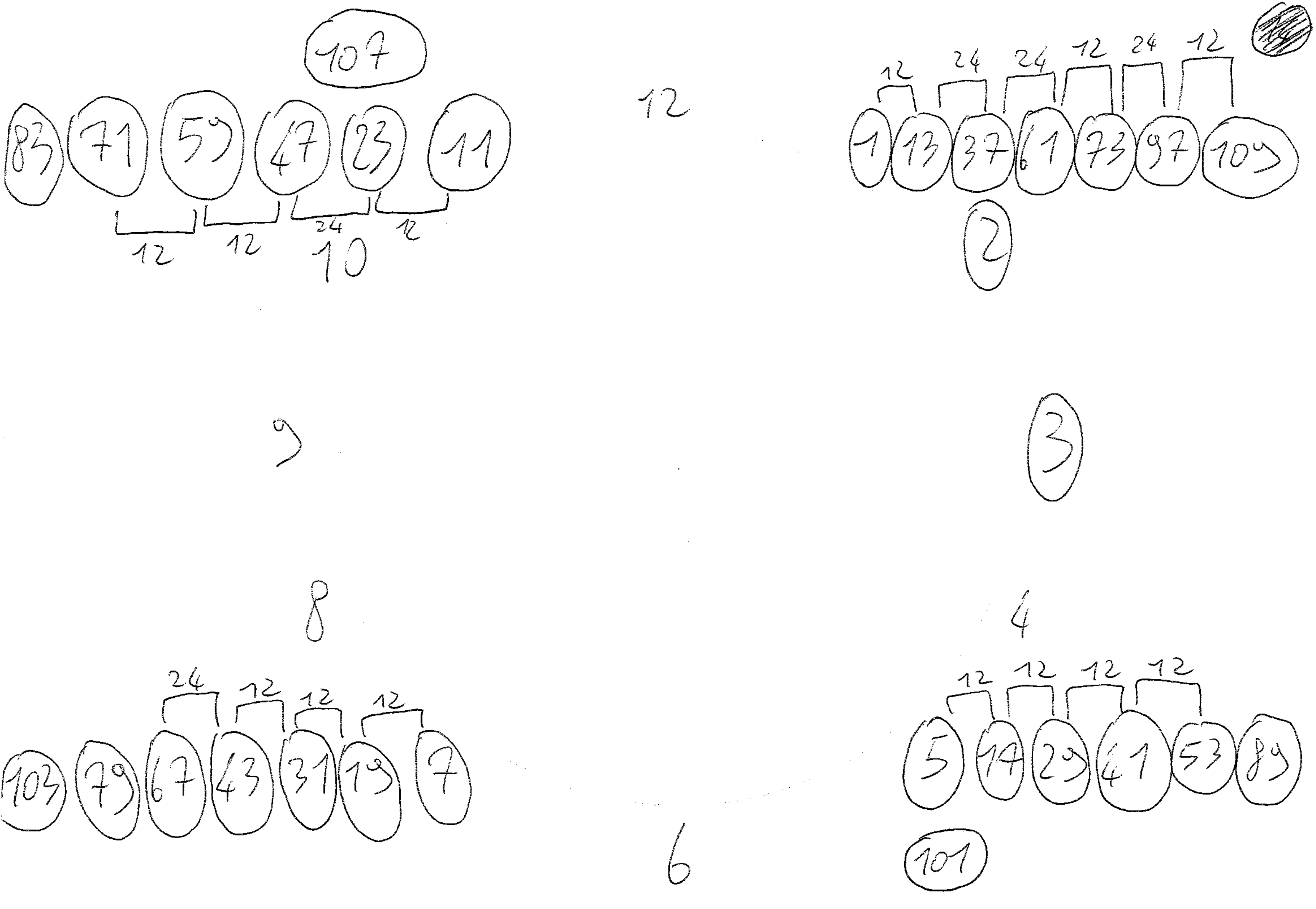
NUMERI PRIMI E PSEUDOPRIMI

Costruisco un orologio di 12ore come nella figura a pagina seguente. Dopo ~~continuo~~ scrivo la numerazione sull'orologio così ottenuto partendo dal 13 (che segue 1) e così via. I numeri che seguono 1, 5, 7, 11 ipotizzo che siano tutti primi (il 3 rimane isolato!)

Adesso tutte le serie di numeri primi che partono con 1, 5, 7, 11 sono del tipo:

$$\begin{cases} 1+12K_1 \\ 5+12K_2 \\ 7+12K_3 \\ 11+12K_4 \end{cases}$$

con K_1, K_2, K_3, K_4 opportuni per ogni serie purché restituiscano un primo!!!


107
12
83 71 59 47 23 11
12 12 24 12
10
12 24 24 12 24 12
1 13 37 61 73 97 109
2
9
3
8
4
24 12 12 12
103 79 67 43 31 19 7
12 12 12 12
5 17 29 41 53 89
101
6

Indicando k_1 con k e volendo sapere per quali valori di k $1+12k$ è primo (7)
posso usare il piccolo th. di Fermat, ma in questo modo ottengo solo alcuni valori di k per i quali $1+12k$ è primo e ottengo anche i valori di k per i quali $1+12k$ è pseudoprimo. Applicando il piccolo th di Fermat si ottiene l'eq. diofantea:

$$\frac{2^{12k}-1}{12k+1} = m, \quad \text{resto } r = 0 \text{ ossia}$$

(1) $\boxed{2^{12k}-1 = m(12k+1)}$ la (1) si può riscrivere come (2) $\boxed{(2^{6k}+1)(2^{6k}-1) = m(12k+1)}$

dovendo essere ~~supponendo~~ $12k+1$ primo per ipotesi compilo la seguente tabella:

k	$12k+1$	$2^{6k}+1$
1	13	$65 = 13 \cdot 5$
3	37	$262145 = 37 \cdot 7085$
5	61	$1073741825 =$ $= 17602325 \cdot 61$

$\longrightarrow$ ipotizzo che $\boxed{2^{6k}+1 = m(12k+1)}$ (3)

dalla (3) si ricava :

(4) $n\cancel{(12k+1)}(2^{6k}-1) = m\cancel{(12k+1)}$ ossia $\boxed{2^{6k}-1 = \frac{m}{n}}$

ripetendo lo stesso ragionamento per il fattore $(2^{6k}+1)$ si ottiene:

$$2^{(2k)^3}+1 = (2^{2k}+1)(2^{4k}-2^{2k}+1) = n(12k+1)$$

k	$12k+1$	$2^{4k}-2^{2k}+1$
1	13	$13 = 13 \cdot 1$
3	37	$4033 = 37 \cdot 109$
5	61	$1047553 = 17173 \cdot 61$

$\longrightarrow$ ipotizzo che $\boxed{2^{4k}-2^{2k}+1 = h(12k+1)}$ (5)

dalla (5) si ottiene (6) $\boxed{2^{2k}+1 = \frac{n}{h}}$

in conclusione si ottiene (7)

$$(7)\begin{cases} 2^{6k}+1 = m(12k+1) & (\mathrm{I}) \\ \boxed{2^{6k}-1 = \dfrac{m}{n}} & (\mathrm{II}) \\ 2^{4k}-2^{2k}+1 = h(12k+1) & (\mathrm{III}) \\ \boxed{2^{2k}+1 = \dfrac{m}{h}} & (\mathrm{IV}) \end{cases}$$

– le equazioni indipendenti sono soltanto la (II) e la (IV) infatti dividendo la (I) per la (III) si ottiene la (IV) ricavo k dalle (II), (IV):

$$(\text{II}) \Rightarrow k = \log_2\left(\frac{m}{n}+1\right)/6 \Rightarrow \frac{m}{n}+1 = 2^{\sigma} \Rightarrow \boxed{k = \frac{\sigma}{6}}$$

essendo 2^{σ} intero anche $\frac{m}{n}$ deve essere intero e quindi $\boxed{m = nz}$ con z intero

$$(\text{IV}) \Rightarrow k = \log_2\left(\frac{n}{h}-1\right)/2 \Rightarrow \frac{n}{h}-1 = 2^{\gamma} \Rightarrow \boxed{k = \frac{\gamma}{2}}$$

essendo 2^{γ} intero anche $\frac{n}{h}$ deve essere intero e quindi $\boxed{n = \alpha h}$ con α intero

uguagliando i 2 valori di k si ottiene:

$$\log_2\left(\frac{m}{n}+1\right) = \log_2\left(\frac{n}{h}-1\right)^3 \Rightarrow \boxed{\sigma = 3\gamma} \quad (8)$$

$$\boxed{(\alpha-1)^3 = 2^{\left(\frac{\gamma}{2}=k\right)}} \quad (9)$$

l'applicazione pratica delle (8), (9) conduce alla verifica contemporanea delle 2 condizioni:

$$\begin{cases} k = \dfrac{\gamma}{2} \\[2ex] q = \left(2^{k}\right)^{1/3} + 1 \end{cases}$$

q	γ	K	12K+1	q	γ	K	12K+1
$\nexists$	2	$\nexists$	$\nexists$	$\nexists$	10	$\nexists$	$\nexists$
$\nexists$	4	$\nexists$	$\nexists$	5	12	$\boxed{6}$	$\boxed{73}$ P
3	6	$\boxed{3}$	$\boxed{37}$ P	$\nexists$	14	$\nexists$	$\nexists$
$\nexists$	8	$\nexists$	$\nexists$	$\nexists$	16	$\nexists$	$\nexists$

d	γ	k	12k+1	d	γ	k	12k+1	12
9	18	$\boxed{9}$	$\boxed{109}$ P	65	36	$\boxed{18}$	$\boxed{217=31\cdot 7}$ P_F	
∄	~~16~~ 20	∄	∄	∄	38	∄	∄	
∄	~~18~~ 22	∄	∄	∄	40	∄	∄	
17	~~20~~ 24	$\boxed{12}$	$\boxed{145=29\cdot 5}$ P_F	129	42	$\boxed{21}$	$\boxed{253=11\cdot 23}$ P_F	
∄	~~22~~ 26	∄	∄	∄	44	∄	∄	
∄	~~24~~ 28	∄	∄	∄	46	∄	∄	
33	~~26~~ 30	$\boxed{15}$	$\boxed{181}$ P	257	48	$\boxed{24}$	$\boxed{289=17^2}$ P_F	
∄	~~28~~ 32	∄	∄	∄	50	∄	∄	
∄	~~30~~ 34	∄	∄	∄	52	∄	∄	

$P \rightarrow$ numero primo

$P_F \rightarrow$ pseudoprimo di Fermat

$$\boxed{(P_F, P) = 12k+1 = 12(3m)+1 \qquad m = 1, 2, 3, 4, 5, 6 \ldots}$$

AUTORE: DR. SIMONE MASINI

CELL: 3337335862

MAIL: SIMONMASINI10@GMAIL.COM