Definera $F_n = 2^{2^n} + 1$ d.v.s. $(F_0 = 3), F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, \ldots$.

Antag att p är ett primtal sådant att $p|F_N$ för något N.

Sätt $x_1 = 2^2(p)$ och definera rekursivt $x_{n+1} = x_n^2(p)$ Frågan är kan det hända att $x_n = -1(p)$ för något n. I så fall gäller att $p|F_n$.

(Vi antar att $n > 0$) Ett nödvändigt villkor är att $p = 1(4)$ ty alla x_n är kvadrater per definition.

Låt nu M vara ordningen av 2. (D.v.s. $2^M = 1(p)$). Notera att vi vet att $M|p-1$.

Vi kan nu omformulera det hela. Låt $x_n = 2^{y_n}$ vi finner då att $y_{n+1} = 2y_n(M)$. Frågan är

a) Kan -1 överhuvudtaget skrivas som en potens av 2

b) ifall a) kan denna potens uppkomma på detta sätt?

Några exempel

$p = 5$ potenserna av 2 ges av $2, 4, 3, 1$ således $M = 4$ och $2^2 = 4 = -1(5)$ d.v.s $y_1 = 2$ löser d.v.s. $5|F_1$

$p = 13$ potenserna ges av $2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$ vi har $M = 12$ och vi har $2^6 = 12 = -1(13)$ Tar vi modulo 12 erhåller vi serien $2, 4, 8, 4, 8, 4, 8 \ldots$ d.v.s. 6 förekommer aldrig. Inget Fermattal delas av 13

Fallet $p = 17$ känner vi redan till, låt oss slutligen ta $p = 29$

vi finner $2, 4, 8, 16, 3, 6, 12, 24, 19, 9, 18, 7, 14, 28, \ldots$ eftersom $2^{14} = -1(29)$ finner vi att $M = 28$. Vi får serien $2, 4, 8, 16, 4, 8, 16 \ldots$ modulo 28, och 14 förekommer inte. Alltså delar inte heller 29 något Fermattal.

Skriv ett datorprogram för att undersöka detta systematiskt!

D.v.s. för $37, 41, 53, 61, 73, \ldots$