Fattorizzando Fermat

Per ogni $i \in \mathbb{N}$ sia $F_i = 1 + 2^{2^i}$, l'i-esimo numero di Fermat. Dunque, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 2^{16} + 1 = 65537$, $F_5 = 2^{32} + 1 = 4294967297$. Si ponga anche $2_i = [2]_{F_i}$; chiaramente questo è un elemento invertibile di $\mathbb{Z}_{F_i}$.

Sia p un primo divisore di F_i, per un fissato $i \in \mathbb{N}$. Risulta subito che p è dispari e $2^{2^i} \equiv_p -1$, quindi $[2]_p$ ha periodo 2^{i+1} (vale anche il viceversa, ovviamente: un primo p divide F_i se e solo se $2^{2^i} \equiv_p -1$). Una prima conseguenza è:

1. *Se i e j sono due numeri naturali distinti, F_i e F_j sono coprimi.*

Infatti, se il primo p divide sia F_i che F_j allora il periodo di $[2]_p$ è sia 2^{i+1} che 2^{j+1}. Inoltre, e questo ci interessa di più, se p divide F_i allora il periodo 2^{i+1} di $[2]_p$ deve anche dividere l'ordine $p-1$ di $\mathbb{Z}_p^*$; vale a dire: $p \equiv_{2^{i+1}} 1$. Si può fare di meglio, infatti si può mostrare che se $i > 1$ allora 2_i è un quadrato in $\mathbb{Z}_{F_i}$, dunque $[2]_p$ è un quadrato in $\mathbb{Z}_p^*$, una radice quadrata di $[2]_p$ sarà quindi un elemento di periodo 2^{i+2} in $\mathbb{Z}_p^*$; come sopra si ottiene dunque:

2. *Se il primo p divide il numero di Fermat F_i, per un fissato intero $i > 1$, allora $p \equiv_{2^{i+2}} 1$.*

C'è solo da spiegare perché 2_i è un quadrato (se $i > 1$). Una maniera semplicissima è questa.

$$F_{i-1}^2 \equiv_{F_i} 1 + 2^{1+2^{i-1}} - 1 = 2^{1+2^{i-1}},$$

dunque $2_i^{1+2^{i-1}}$ è un quadrato. Dal momento che 2_i ha per periodo una potenza di 2, si ha che 2_i è una potenza di $2_i^{1+2^{i-1}}$ (il fatto che $i > 1$ interviene per garantire che l'esponente che qui appare è dispari), quindi anch'esso un quadrato.

Se proprio ci si tiene, una radice quadrata di 2_i si può anche calcolare esplicitamente così: $2_i^{2^{i-2}}$ è ovviamente invertibile; se $[t]_{F_i}$ è il suo inverso allora $(tF_{i-1})^2 \equiv_{F_i} 2^{1+2^{i-1}}t^2 = 2(2^{2^{i-2}}t)^2 \equiv_{F_i} 2$. Anche t è facile da calcolare: $2_i^{2^{i-2}}$ ha periodo 8, come è chiaro, quindi $t \equiv_{F_i} 2_i^{2^{i-2}7}$.

Tornando all'argomento, le osservazioni fatte permettono di stabilire subito che (tralasciando $3 = F_0$ e $5 = F_1$) F_2, F_3 e F_4 sono primi. Ad esempio, se il primo p divide $F_3 = 257$ allora $p \equiv_{32} 1$, ma $33 > \sqrt{257}$, quindi $p = 257$. Se invece p è il minimo primo che divide F_4, si deve avere $p \equiv_{64} 1$, e, senza voler strafare con i conti, $p < 300$, perché $300^3 = 90000 > F_4$. Dunque p andrebbe cercato tra 65, 129, 193 e $257 = F_3$; esclusi i primi due (chiaramente non primi) e l'ultimo (F_3 e F_4 sono coprimi; del resto $F_3^2 > F_4$, in generale è ovvio che $F_i^2 > F_{i+1}$, quindi un fattore primo proprio di F_{i+1} va cercato al di sotto di F_i) resta da testare solo 193 (che in effetti è primo), che si verifica non dividere F_4.

Passiamo al successivo numero di Fermat. Se p è il minimo primo divisore di F_5 allora $p \equiv_{128} 1$. Esclusi 129, 385 e 513, chiaramente composti, e $257 = F_3$, coprimo con F_5, il primo candidato ad essere p è 641. Ora, alcune coincidenze possono insospettire:

$$641 = 2^4 + 5^4 \qquad \text{e} \qquad 641 = 1 + 2^7 5.$$

Queste uguaglianze portano immediatamente a

$$5^4 \equiv_{641} -2^4 \qquad \text{e} \qquad 2^7 5 \equiv_{641} -1.$$

Elevando alla quarta potenza, dalla seconda si ottiene: $2^{28}5^4 \equiv_{641} 1$; utilizzando la prima questa si trasforma in

$$2^{32} = 2^{28}2^4 \equiv_{641} -1$$

che equivale proprio a dire: 641 divide $2^{32} - 1 = F_5$. Dunque F_5 non è primo.