

Sì, è vero. Se p è un numero primo, non soltanto ogni divisore primo di 2^p-1 è maggiore di p , ma si può dire di più: se p è un primo dispari (cioè se è diverso da 2), allora ogni divisore positivo di 2^p-1 è della forma $2kp+1$, per qualche numero intero positivo k .

La dimostrazione si basa su un famoso risultato di Fermat, noto come **Piccolo teorema di Fermat**. Questo teorema afferma che, se p è un numero primo e a è un numero intero non multiplo di p , allora $a^{p-1}-1$ è divisibile per p . Si scrive anche: " $a^{p-1} \equiv 1 \pmod{p}$ " che si legge " a^{p-1} è congruo a 1 modulo p ". In particolare, allora, se p è un primo dispari, applicando il teorema nel caso $a=2$ si ottiene che $2^{p-1}-1$ è divisibile per p .

Supponiamo ora che q sia un numero primo divisore di 2^p-1 , con p dispari. Dimosteremo nel prossimo paragrafo che, di conseguenza, p è un divisore di $q-1$. Poiché q è un divisore di 2^p-1 , q dev'essere dispari, quindi $q-1$ è pari e perciò anche 2 è divisore di $q-1$; ma allora $2p$ divide $q-1$, ossia esiste un intero k tale che $q-1=2kp$, come richiesto.

Concludiamo ora la dimostrazione mostrando che p divide $q-1$. Se per assurdo p non fosse divisore di $q-1$, p e $q-1$ sarebbero numeri primi fra loro, e di conseguenza si potrebbero trovare due interi m, n tali che: $mp+n(q-1)=1$. Necessariamente m o n dev'essere negativo, supponiamo che lo sia m (se lo è n il ragionamento è simile). Allora $-m$ è positivo. Dall'ipotesi $2^p \equiv 1 \pmod{q}$, elevando alla $-m$ si ottiene: $2^{-mp} \equiv 1^{-m} \pmod{q}$; ma $1^{-m}=1$ e perciò $2^{-mp} \equiv 1 \pmod{q}$. Per il Piccolo teorema di Fermat si ha anche $2^{q-1} \equiv 1 \pmod{q}$, e quindi $2^{n(q-1)} \equiv 1^n = 1 \pmod{q}$. D'altra parte $2^{mp+n(q-1)} = 2^1=2$; quindi, moltiplicando per 2^{-mp} , si ottiene anche $2^{mp-mp+n(q-1)} \equiv 2 \pmod{q}$: contraddizione, perchè per transitività si avrebbe $1 \equiv 2 \pmod{q}$.

Abbiamo sfruttato ripetutamente la proprietà delle congruenze che, se l è un intero positivo e $a \equiv b \pmod{q}$, allora $a^l \equiv b^l \pmod{q}$. Abbiamo anche usato la proprietà che due numeri interi a, b sono primi tra loro se e solo se esistono due interi x, y tali che $1=ax + by$.

Per maggiori dettagli e applicazioni, per esempio ai test di primalità, si veda per esempio il bel libro di Donald M. Davis "*The nature and power of mathematics*", Princeton University Press.