

Relazione N3

(a) Per prima cosa, si dimostra che esistono infiniti primi p tali che -1 è residuo quadratico modulo p . Questo si può fare coi generatori (si prende un generatore g , e poiché $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, basta che $\frac{p-1}{2}$ sia pari...), elevando alla $\frac{p-1}{2}$ (come prima, per il teorema di Fermat, vale che $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ sse a è un residuo quadratico), oppure imitando la dimostrazione dell'infinità dei primi (si prende un divisore di $k^2 + 1$, si ipotizza che i primi p_i di questa forma siano finiti e si prende un divisore di $(\prod p_i)^2 + 1$). A questo punto, basta prendere per ogni p il suo residuo α tale che $\alpha^2 \equiv -1$. Inoltre, per garantirsi che gli α siano distinti, basta prendere i primi abbastanza distanti...

(b) Bisogna fare in modo che, dati degli interi a_i tali che $\prod a_i = n^2 + 1$. Per farlo, ci sono vari modi:

- Prendere gli interi della forma $n = 4k^2 + 2k + 1$, varrà infatti $n^2 + 1 = 2(4k^2 + 1)(2k^2 + 2k + 1)$
- Prendere gli interi della forma $n = 2k^2$, varrà $n^2 + 1 = (2k^2 + 2k + 1)(2k^2 - 2k + 1)$, a questo punto basta un'ipotesi aggiuntiva su k (ad esempio $k \equiv 1 \pmod{5}$) perché $2k^2 + 2k + 1$ sia scomponibile in due fattori minori di n
- Considerare un primo p dello stesso tipo del punto (a) e prendere il residuo $n > p^{a-1}$ tale che $n^2 + 1 \equiv 0 \pmod{p^a}$. E' facile dimostrare che ci sono abbastanza fattori p in $n!$ e che $\frac{n^2+1}{p^a}$ è minore di n
- Invece che con p^a , fare la stessa cosa con pq , dove p e q sono due primi distinti.
- Casi particolari degli ultimi due modi, come $p = 5$ o $a = 2$