Dokaz da je $x^2 \equiv y^2 \pmod n$ sa predavanja 9.5.2019.

Navedeno:

$f(r) = r^2 \pmod n$.

Izabrani brojevi $r_1, \dots, r_s$ toko do su brojevi $f(r_i)$ glatki u odnosu na bazu $\{p_1, \dots, p_k\}$ i do je $f(r_1) \cdots f(r_s) = p_1^{\beta_1} \cdots p_k^{\beta_k}$, gdje su β_i -parni brojevi.

$x = r_1 \cdots r_s$, $y = p_1^{\beta_1/2} \cdots p_k^{\beta_k/2}$

Dokaz:

$x^2 \equiv r_1^2 \cdots r_s^2 \pmod n \equiv f(r_1) \cdots f(r_s) \pmod n \equiv p_1^{\beta_1} \cdots p_k^{\beta_k} \pmod n \equiv$

$\equiv y^2 \pmod n$

Napomena: Isti dokaz vrijedi ako je $f(r) = r^2 - n$