# Teoria dei Numeri (Crittografia)

a.a. 2018-19

## Teoremi di cui è richiesta la dimostrazione

### Algoritmi fondamentali e loro "running-time"

- Algoritmo euclideo per il calcolo del massimo comun divisore ed identità di Bézout.
- Potenza modulare ("square and multiply")

### Teoremi fondamentali

- Ogni numero ammette una fattorizzazione prima.
- I numeri primi sono infiniti (Euclide)
- Teorema fondamentale dell'Aritmetica (la fattorizzazione prima di un numero è unica a meno dell'ordine)
- Teorema di Eulero-Fermat
- Teorema riguardante il numero delle soluzioni di una congruenza lineare

$$ax \equiv b \pmod{m}$$

- Come risolvere "velocemente" le congruenze lineari (algoritmo euclideo ed identità di Bézout)

- Teorema cinese del resto.

## Crittosistemi

- Scambio di chiavi: metodo di Diffie-Hellman
- R.S.A.
- El Gamal
- Blum-Goldwasser
- Protocollo di Massey-Omura.

## Firme digitali

- Firma R.S.A
- Firma di El Gamal

Paolo Codeca

Ferrara, 20 maggio 2019