

**Università degli Studi Roma Tre**  
**Corso di Studi in Matematica, a.a. 2016/2017**  
**CR410 – Crittografia1**  
**Esercizi**  
**Foglio 4**

1. Usando l'algoritmo  $p - 1$  di Pollard, fattorizzare  $n_1 = 18\,923$  e  $n_2 = 115\,147$ .
2. Usando l'algoritmo  $\rho$  di Pollard, fattorizzare  $n_1 = 1649$ ,  $n_2 = 24\,911$ ,  $n_3 = 96\,637$ .
3. Usando il metodo di Fermat, fattorizzare  $n_1 = 18\,896\,309$  e  $n_2 = 192\,404\,497$
4. Fattorizzare:  
540 143; 8 926 861; 24 458 477  
1 313 303; 6 791 173;  
157 954 399; 298 217 461.

Comandi utili in Mathematica

- `GCD[a,b]`
- `Mod[a,N]`
- `PowerMod[a,k,N]` calcola  $a^k \pmod{n}$
- `NestList[Mod[(#^2 + 1), n]&, x, B]`  
calcola la funzione  $x^2 + 1 \pmod{n}$  per  $B$  iterazioni con  $x$  come valore iniziale.
- `Sqrt[x] =  $\sqrt{x}$`