Università degli Studi Roma Tre
Corso di Studi in Matematica
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 ρ 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. Usando il metodo delle basi di fattorizzazione, fattorizzare $n_1 = 540\,143$.
5. Fattorizzare:

$$8\,926\,861; \quad 24\,458\,477$$
$$1\,313\,303; \quad 6\,791\,173;$$
$$157\,954\,399; \quad 298\,217\,461.$$

Comandi utili in Mathematica

- `GCD[a,b]`
- `Mod[a,N]`
- `PowerMod[a,k,N]` calcola $a^k \pmod n$
- `Sqrt[x]` $= \sqrt{x}$
- `NestList[Mod[(#^2 + 1), n]&, x, B]`
  calcola la funzione $x^2 + 1 \pmod n$ per B iterazioni con x come valore inizale.
- `Table[expr,{i,i_min,i_max}]` calcola `expr` per i che va da i_{min} a i_{max}

  ex: `Table[i^2, {i,1,10}]`

  out `{1, 4, 9, 16, 25, 36, 49, 64, 81, 100}`