

## PUBLIC KEY CRYPTOGRAPHY

### Seminar 4

1. Use Pollard's  $\rho$  algorithm with  $f(x) = x^2 + 1$  and  $x_0 = 2$  in order to factorize  $n = 2701$ .
2. Use Pollard's  $\rho$  algorithm with  $f(x) = 2x + 5$  and  $x_0 = 2$  in order to factorize  $n = 2701$ .
3. Use Pollard's  $p - 1$  algorithm in order to factorize  $n = 2701$ .
4. Use Fermat's algorithm in order to factorize  $n = 9709$ .
5. Use Fermat's algorithm in order to factorize  $n = 10123$ .
6. Example from Moodle.