IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises VIII.

1. Consider the following elliptic curve $E : y^2 = x^3 + 4x + 20 \pmod{29}$.
   a) Calculate the number of points of E.
   b) Show that the group generated by E is cyclic. Find all its generators.
   c) Compute in detail $7P$ where $P = (1, 5)$.
2. Show that $(p-1)! + 1$ is a multiple of p if and only if p is a prime.
3. Show that $\forall n \in \mathbb{N}$ it holds
   a) $12 \mid n^4 - n^2$
   b) $133 \mid 11^{n+2} + 12^{2n+1}$
4. a) Use the first Pollard's rho method with $f(x) = x^2 - 1$ and $x_0 = 3$ to find a factor of $n = 4559$.
   b) Find a factor of $n = 355$ using the elliptic curve $E : y^2 = x^3 - 3x + 3$ and the point $P = (1, 1)$.
5. Consider an elliptic curve version of the ElGamal digital signature scheme from the lecture. Show how one can recover the private key a if the same r is used to sign more than one message.
6. Bob uses an elliptic curve version of the ElGamal cryptosystem with public key $p = 7$, $E : x^3 + 3x + 5 \pmod{7}$, $P = (1, 3)$ and $Q = (6, 6)$.
   a) Encrypt a message $m = (1, 4)$ with $r = 3$. Show computation steps.
   b) Decrypt the ciphertext computed in a) with Bob's secret key $a = 2$. Show computation steps.
7. To which group is the elliptic curve $E : y^2 = x^3 + 2x + 1 \pmod{7}$ isomorphic to? Compute the addition table of E.