Індивідуальний проект з курсу
“Сучасні методи розробки програм”
1 семестр 2019/2020 навчального року

Для еліптичної кривої E над полем $GF(p)$, заданої рівнянням

$$y^2 = x^3 + Ax + B,$$

реалізувати

- алгоритм генерування точки на кривій E,
- алгоритм додавання точок,
- алгоритм подвоєння точки,
- алгоритм знаходження цілого кратного точки,
- алгоритм, генерування дівізора D над кривою E з носієм $supp(D)$ заданого розміру d,
- алгоритм Міллера обчислення значення функції Вейля $f_{n,P}$ від дівізора D такого, що $supp(D) \cap \{P, O\} = \emptyset$.

1. Крива `brainpoolP160r1`

   $p = E95E4A5F737059DC60DFC7AD95B3D8139515620F$

   $A = 340E7BE2A280EB74E2BE61BADA745D97E8F7C300$

   $B = 1E589A8595423412134FAA2DBDEC95C8D8675E58$

2. Крива `brainpoolP192r1`

   $p = C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297$

   $A = 6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF$

   $B = 469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9$

3. Крива `brainpoolP224r1`

   $p = D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF$

   $A = 68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43$

   $B = 2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B$

4. Крива `brainpoolP256r1`

   $p = A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377$

   $A = 7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9$

   $B = 26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6$

5. Крива `brainpoolP320r1`

   $p = D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27$

   $A = 3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4$

   $B = 520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6$

6. Крива `brainpoolP384r1`

   $p = 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53$

   $A = 7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826$

   $B = 04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11$

7. Крива `brainpoolP512r1`

   $p = AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3$

   $A = 7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA$

   $B = 3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723$

8. Крива `secp192k1`

   $p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFEE37$

   $A = 000000000000000000000000000000000000000000000000$

   $B = 000000000000000000000000000000000000000000000003$

9. Крива `secp192r1`

   $p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$

   $A = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFC$

   $B = 64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1$

10. Крива `secp224k1`

    $p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFE56D$

    $A = 00000000000000000000000000000000000000000000000000000000$

    $B = 00000000000000000000000000000000000000000000000000000005$

11. Крива `secp224r1`

    $p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF000000000000000000000001$

    $A = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFF$
    $FFFFFFFE$

    $B = B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4$

12. Крива `secp256k1`

    $p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
    $FFFFFFFEFFFFFC2F$

    $A = 0000000000000000000000000000000000000000000000000000000000000000$

    $B = 0000000000000000000000000000000000000000000000000000000000000007$

13. Крива `secp256r1`

    $p = FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF$

    $A = FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC$

    $B = 5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B$

14. Крива `secp384r1`

    $p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
    $FFFFFFFFFFFFFFFEFFFFFFFF0000000000000000FFFFFFFF$

    $A = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
    $FFFFFFFFFFFFFFFEFFFFFFFF0000000000000000FFFFFFFC$

    $B = B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F$
    $5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF$

15. Крива `secp384r1`

    $p = 01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
    $FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
    $FFFFFFFFFFFFFFFFFFFFFFFF$

    $A = 01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
    $FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
    $FFFFFFFFFFFFFFFFFFFFFFFC$

    $B = 0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3$
    $B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF88$
    $3D2C34F1EF451FD46B503F00$