# Makeup Exam

Jacob Doskocil

October 29th, 2018

2. **[30points] Elliptic Curves and ECC:** Solve problems 10-12, 10-13, 10-14, 10-15 from the text book.

10-12 Consider the elliptic curve $E_7(2,1)$; that is, the curve is defined by $y^2 = x^3 + 2x + 1$ with a modulus of $p = 7$. Determine all of the points in $E_7(2,1)$. Hint: Start by calculating the right-hand side of the equation for all values of $x$.
The process can be begun by calculating the values of $y^2 \mod 7$ for each of the values of $y$ from 0 to 6.

| $y$ | y$^2$ | y$^2$ mod 7 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 1 |
| 2 | 4 | 4 |
| 3 | 9 | 2 |
| 4 | 16 | 2 |
| 5 | 25 | 4 |
| 6 | 36 | 1 |

The next step is calculating the values for $x^3 + 2x + 1$ and $y^2 = x^3 + 2x + 1 \mod 7$ for each of the possible values of $x$ from 0 to 6.

| $x$ | x$^3 + 2x + 1$ | y$^2$ | y |
|---|---|---|---|
| 0 | 1 | 1 | 1,6 |
| 1 | 4 | 4 | 2,5 |
| 2 | 13 | 6 | — |
| 3 | 34 | 6 | — |
| 4 | 73 | 3 | — |
| 5 | 136 | 3 | — |
| 6 | 229 | 5 | — |

This gives the points on the curve $E_7(2,1)$ to be $(0,1)$, $(0,6)$, $(1,2)$, $(1,5)$, and $(\infty, \infty)$.

10-13 What are the negatives of the following elliptic curve points over $Z_7$? $P = (3,5)$; $Q = (2,5)$; $R = (5,0)$.
$-P = (3,2)$
$-Q = (2,2)$
$-R = (5,0)$

10-14 For $E_{11}(1,7)$, consider the point $G = (3,2)$. Compute the multiple of $G$ from $2G$ through $13G$.
This problem is solved using the EC point multiplication function in the file `problem2.cpp`.

| | |
|---|---|
| $2G$ | $(10,4)$ |
| $3G$ | $(1,8)$ |
| $4G$ | $(5,4)$ |
| $5G$ | $(4,8)$ |
| $6G$ | $(7,7)$ |
| $7G$ | $(6,8)$ |
| $8G$ | $(6,3)$ |
| $9G$ | $(7,4)$ |
| $10G$ | $(4,3)$ |
| $12G$ | $(1,3)$ |
| $13G$ | $(10,7)$ |

10-15 This problem performs elliptic curve encryption/decryption using the scheme outlined in Section 10.4. The cryptosystem parameters are $E_{11}(1,7)$ and $G = (3,2)$. B's private key is $n_B = 7$.
Each of these parts are solved using the point addition and multiplication functions in the file `problem2.cpp`.

(a) Find B's public key $P_B$.
$P_B = n_b \times G = 7G = (6,8)$

(b) A wishes to encrypt the message $P_m = (10,7)$ and chooses the random value $k = 5$. Determine the ciphertext $C_m$.
$C_m = \{kG, P_m + kP_B\}$
$kG = 5G = (4,8)$ $kP_B = 5P_B = (4,8)$
$P_m + kP_B = (10,7) + (4,8) = (1,8)$
$C_m = \{(4,8),(1,8)\}$

(c) Show the calculation by which B recovers $P_m$ from $C_m$.
$P_m = C_{m2} - n_B \times C_{m1}$
$P_m = (1,8) - 7 \times (4,8) = (1,8) - (4,8) = (1,8) + (4,3)$
$P_m = (10,7)$

3. [**40points**] **Primality and Factorization:** Consider the following integers: 31531; 520482; 485827; 15485863.

(a) Implement and check with Miller-Rabin algorithm if they are prime or not

(b) Implement Pollard-Rho method and factor them if they are not prime

The implementation of this problem is done in the file `problem3.cpp` which takes a number, and an accuracy value, and outputs whether or not the number is prime. It is important to note that the Miller-Rabin test cannot prove a number to be prime, only prove that one is not prime. So the test is run a number of times, provided as the accuracy value. As the number of times the test is run increases, the probability that there was an error decreases, allowing the test to get fairly accurate. If the program determines that the number is not prime, it factors it using Pollard's Rho Algorithm. This algorithm only finds a single non-trivial factor, so, this factor may need to be factored, and the remainder from dividing the original number from the found factor needs to be factored as well. The output from the program is found below, using an accuracy of 99.

```
$./problem3 31531 99
31531 is probably prime

$./problem3 520482 99
520482 not prime
Factors:  2 3 223 389

$./problem3 485827 99
485827 is probably prime

$./problem3 15485863 99
15485863 is probably prime
```