**Question 1.**

---

**(a)** There are 8 points: $(0,2),(0,9),(2,0),(4,0),(5,0),(10,3),(10,8),\mathcal{O}$.

| x | $x^3+5x+4 \mod 11$ | in $QR_{11}$ | y |
|---|---|---|---|
| 0 | 4 | ✓ | (2,9) |
| 1 | 10 | × | |
| 2 | 0 | ✓ | 0 |
| 3 | 2 | × | |
| 4 | 0 | ✓ | 0 |
| 5 | 0 | ✓ | 0 |
| 6 | 8 | × | |
| 7 | 8 | × | |
| 8 | 6 | × | |
| 9 | 8 | × | |
| 10 | 10 | ✓ | (3,8) |

Table 1: 8.1.a

**(b)** What is the order of point $P=(10,3)$? Order $k$ of point $P$ is $kP=\mathcal{O}$.

- $E$ is non-singular: $-16(4a^3+27b^2)=-14912\neq 0$
- $P$ is on $E$ - see a).
- $P\cdot P=(x_3,y_3)=(5,0)$

$$\lambda=\frac{3x_1^2+a}{2y_1}\equiv 5 \mod 11$$
$$x_3=\lambda^2-x_1-x_2\equiv 5 \mod 11$$
$$y_3=\lambda(x_1-x_3)-y_1\equiv 0 \mod 11$$

- $2P+P=(x_3,y_3)=(10,8)$

$$\lambda=\frac{y_2-y_1}{x_2-x_1}\equiv 5 \mod 11$$
$$x_3=\lambda^2-x_1-x_2\equiv 10 \mod 11$$
$$y_3=\lambda(x_1-x_3)-y_1\equiv 8 \mod 11$$

- $3P+P=(x_3,y_3)=\mathcal{O}$

$$\lambda=\frac{y_2-y_1}{x_2-x_1}=\frac{3-8}{10-10}$$

Order of point $P=(10,3)$ is 4.

**(c)** $P + P = \mathcal{O}$. When $\lambda$ is undefined.

- $x_1 = x_2$ but $y_1 \neq y_2$
- $P_1 = P_2$ but $y_1 = 0$

## Question 2.

**(a)** Factorize 3551, starting with $x_0 = 2$ and using pseudo-random function $x_i + 1 = x_i^2 + 3 \mod 3551$.

- Pollard's $\rho$-method version 1. First factor is 53.

| i | j | $x_i$ | $x_j$ | $gcd(x_i - x_j, n)$ |
|---|---|---|---|---|
| 2 | 1 | 52 | 7 | 1 |
| 3 | 1 | 2707 | 7 | 1 |
| 3 | 2 | 2707 | 52 | 1 |
| 4 | 1 | 2139 | 7 | 1 |
| 4 | 2 | 2139 | 52 | 1 |
| 4 | 3 | 2139 | 2707 | 1 |
| 5 | 1 | 1636 | 7 | 1 |
| 5 | 2 | 1636 | 52 | 1 |
| 5 | 3 | 1636 | 2707 | 1 |
| 5 | 4 | 1636 | 2139 | 1 |
| 6 | 1 | 2596 | 7 | 1 |
| 6 | 2 | 2596 | 52 | 53 |

Table 2: 8.2.a Pollard's $\rho$-method version 1

- Pollard's $\rho$-method version 2. First factor is 53.

| i | x | y | $gcd(\lvert x - y\rvert, 3551)$ |
|---|---|---|---|
| 1 | 7 | 52 | 1 |
| 2 | 52 | 2139 | 1 |
| 3 | 2707 | 2596 | 1 |
| 4 | 2139 | 1450 | 53 |

Table 3: 8.2.a Pollard's $\rho$-method version 2

**(b)** Pollard's $p - 1$ method. Factorize n = 178297. B = 23, a = 2.

$$M = \prod_{\text{primes } q \leq B} q^{\lfloor \log_q B \rfloor} = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \mod 178297 = 148267$$

$$\gcd(2^M - 1, 178297) = \gcd(165942, 178297) = 7$$

First factor is 7.

## Question 3.

**(a)** Hash your UCO using a hash function $h(x) = 5^x \mod 1033$ and label the result $h$.

$$h(x) = 5^{433652} \mod 1033 = 1029 = h$$

**(b)** EC Elgamal signature scheme. $E : y^2 = x^3 + 3x + 983 \mod 997$. Public points $P = (325, 345)$, $Q = xP = (879, 211)$ and secret key $x = 140$. Random component $r = 339$. Note that order of $P$ in $E$ is 1034. Signed message $(h, R, s) = (1029, (838, 741), 511)$.

$$R = r \cdot P = (838, 741)$$

$$s = r^{-1}(h - x \cdot x_R) \mod n = 973(1029 - 140 \cdot 838) \mod 1034 = 511$$

Verification:

$$x_R Q + sR = hP$$

$$(815, 880) + (248, 445) = (569, 100)\checkmark$$

## Question 4.

Curve 1: $y^2 = x^3 + 4x$. Has points: $\infty, (0,0), (1,0), (2,1), (2,4), (3,2), (3,3), (4,0)$. The sorted sequence of point orders is $[1, 2, 2, 2, 4, 4, 4, 4]$.

Curve 2: $y^2 = x^3 + 4x + 1$. Has points: $\infty, (0,1), (0,4), (1,1), (1,4), (3,0), (4,1), (4,4)$. The sorted sequence of point orders is $[1, 2, 4, 4, 8, 8, 8, 8]$.

As the sorted sequences of point orders are different, the group structures are different.

8.5 Consider an elliptic curve $E : y^2 = x^3 + 8$ over $\mathbb{R}$. Show that $E$ does not have multiple roots. Algebraically determine the number of roots $E$ has.

Solution: $0 = x^3 + 8$ is equivalent to $0 = (x + 2)(x^2 - 2x + 4)$, therefore $-2$ is a root, but not multiple root. Now we calculate discriminant of quadratic equivalence $0 = x^2 - 2x + 4$:

$$D = (-2)^2 - 4 \cdot 1 \cdot 4 = -12.$$

We see that discriminant is $< 0$, therefore there is no more solution in $\mathbb{R}$, but $E$ has two more complex (non-real) conjugate solution (this means that it is not multiple solution). Therefore we prove that $E$ does not have multiple root and have **one** root over $\mathbb{R}$. □

## Question 6.

**(a)** 5 points: It is not possible for an elliptic curve over $\mathbb{Z}_{11}$ to have 5 points, because the lower bound according to Hesse's theorem is $N \geq p - 2\sqrt{p} + 1 \geq 11 - 6 + 1 \geq 6$

**(b)** 6 points: $y^2 = x^3 + x + 8$ mod 11 has 6 points: $\{(3, 4), (3, 7), (8, 0), (9, 3), (9, 8), \infty\}$

**(c)** 14 points: $y^2 = x^3 + x + 1$ mod 11 has 14 points: $\{(0, 1), (0, 10), (1, 5), (1, 6), (2, 0), (3, 3), (3, 8), (4, 5), (4, 6), (6, 5), (6, 6), (8, 2), (8, 9), \infty\}$

**(d)** 19 points: It is not possible for an elliptic curve over $\mathbb{Z}_{11}$ to have 19 points, because the upper bound according to Hesse's theorem is $N \leq p + 2\sqrt{p} + 1 \leq 11 + 6 + 1 \leq 18$

8.7 Show that $42 \mid n^7 - n$ for all integers $n \in \mathbb{N}$.

Solution: We know that $n^7 - n = n(n^3-1)(n^3+1) = (n-1)n(n+1)(n^2-n+1)(n^2+n+1)$. Now we prove three statements $2 \mid n^7 - n$, $3 \mid n^7 - n$ and $7 \mid n^7 - n$.

- $2 \mid n^7 - n$: We know that $\forall n : 2 \mid n(n+1)$, because $n$ and $n+1$ are consecutive numbers, therefore one of them is even. Therefore $\forall n : 2 \mid (n-1)n(n+1)(n^2-n+1)(n^2+n+1)$.
- $3 \mid n^7 - n$: We know that $\forall n : 3 \mid (n-1)n(n+1)$, because $n-1$, $n$ and $n+1$ are consecutive numbers, therefore one of them is divisible by 3. Therefore $\forall n : 3 \mid (n-1)n(n+1)(n^2-n+1)(n^2+n+1)$.
- $7 \mid n^7 - n$: From the Fermat's Little Theorem we know that $n^6 = 1 \mod 7 \Leftrightarrow n^7 = n \mod 7 \Leftrightarrow n^7 - n = 0 \mod 7$. Therefore we show that $\forall n : 7 \mid n^7 - n$.

Finally we use Chinese Remainder Theorem for these three statements therefore we prove $\forall n : 42 \mid n^7 - n$. □

8.8 Recall the definition of a Fermat number:

$$F_n = 2^{2^n} + 1$$

where $n$ is a non-negative integer. Prove the following claims:

(a) For $n \geq 1$, $F_n = F_0 \cdots F_{n-1} + 2$.

Solution: We use mathematical induction:

- *Base step*: $n = 1$ – We know that $F_0 = 3$ and $F_1 = 5$ and $5 = 3 + 2$ therefore we prove that $F_1 = F_0 + 2$.
- *Induction step*: Let $n$ be an integer $\geq 1$. The statements holds for $n$ ($F_n = F_0 \cdots F_{n-1} + 2$) and we have to prove it for $n+1$ ($F_{n+1} = F_0 \cdots F_n + 2$).

$$F_n = F_0 \cdots F_{n-1} + 2 \Longleftrightarrow F_n - 2 = F_0 \cdots F_{n-1}.$$

$$\begin{aligned} F_0 \cdots F_n + 2 &= F_0 \cdots F_{n-1} \cdot F_n + 2 \\ &= (F_n - 2)F_n + 2 \\ &= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) + 2 \\ &= \left(2^{2^n}\right)^2 - 1 + 2 \\ &= 2^{2^{n+1}} + 1 \\ &= F_{n+1} \end{aligned}$$

We prove $F_n = F_0 \cdots F_{n-1} + 2$. □

(b) For $n \geq 2$, the last digit of $F_n$ is 7.

Solution: We use mathematical induction:

- *Base step*: $n = 2$ – $F_2 = 17$ so the statement is true.
- *Induction step*: Let $n$ be an integer $\geq 2$. The statements holds for $n$ ($F_n \equiv 7 \mod 10$) and we have to prove it for $n+1$ ($F_{n+1} \equiv 7 \mod 10$).

$$F_n \equiv 7 \mod 10 \Longleftrightarrow 2^{2^n} + 1 \equiv 7 \mod 10 \Longleftrightarrow 2^{2^n} \equiv 6 \mod 10.$$

$$F_{n+1} = 2^{2^{n+1}} + 1 = \left(2^{2^n}\right)^2 + 1 \equiv 6^2 + 1 \equiv 7 \mod 10.$$

Therefore we prove $F_n \equiv 7 \mod 10$ (last digit is 7). □

(c) No Fermat number is a perfect square.

Solution: It is obvious that $F_0 = 3$ and $F_1 = 5$ are not perfect squares.
From part (b) we know that $\forall n \geq 2 : F_n \equiv 7 \mod 10$, so if any of Fermat numbers is perfect square ($k^2$) then $k^2 = F_n \equiv 7 \mod 10$. All digits (we look only on last digit of $k$) have this last digit for $k^2$: 0, 1, 4, 9, 6, 5, 6, 9, 4, 1. Therefore $\forall k : k^2 \not\equiv 7 \mod 10$ therefore we prove that no Fermat number is a perfect square. □

(d) Every Fermat number $F_n$ for $n \geq 1$ has the form $6m - 1$ for an integer $m > 0$.

Solution: The equivalent definition is $6 \mid F_n + 1$.

- $2 \mid F_n + 1$: $2 \mid 2^{2^n} + 1 + 1$, which is obviously true for all $n \geq 1$.
- $3 \mid F_n + 1$: We want to show that $\forall n \geq 1 : 2^{2^n} + 1 + 1 \equiv 0 \mod 3$ which is equivalent to $\forall n \geq 1 : 2^{2^n} \equiv 1 \mod 3$.

$$2^{2^n} = \left(2^2\right)^{2^{n-1}} = 4^{2^{n-1}} \equiv 1^{2^{n-1}} \equiv 1 \mod 3$$

Finally we use Chinese Remainder Theorem for them therefore we prove $\forall n \geq 1 : 6 \mid F_n + 1$. □

**Question 9.**

To decrypt, calculate:

$$dR = (c_1, c_2)$$
$$m_1 = y_1 c_1^{-1} \mod p$$
$$m_2 = y_2 c_2^{-1} \mod p$$

Since the encryptor used $(c_1, c_2) = kQ$, and $Q = dP, R = kP$, it holds $(c_1, c_2) = kQ = kdP = dR$. Thus the $(c_1, c_2)$ obtained during decryption is the same as in encryption, thus we simply reverse the mod-multiplication by mod-multiplying by an inverse. Inverse is calculated easily, as $p$ is a prime.