

Group	Elliptic	Curves in Cryptography	List No.
		Final Exam	
	: 2013 : Fall : Küçüksakallı	Name : Last Name : Signature :	
Time Duration	: 9/1/2014 : 10:40 : 110 minutes	7 QUESTIONS ON 4 PAGE 40 TOTAL POINTS	ES
1 2	3 4 5 6		

- 1. (10pts) True or False? Justify your answer.
 - There exists E/\mathbf{F}_q such that $\operatorname{End}(E) \cong \mathbf{Z}$.
 - The group $E(\mathbf{F}_q)$ is finite and cyclic.
 - If E/\mathbb{C} , then $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.
 - If $E: y^2 = x^3 x$ is defined over \mathbf{F}_q , then $\operatorname{End}(E) \cong \mathbf{Z}[i]$.
 - MOV attack for supersingular curves is more efficient than the ordinary case.

2. (5pts) Consider the elliptic curve $E: y^2 = x^3 + x + 6$ defined over \mathbf{F}_7 . Observe that P = (1,1), Q = (2,3), R = (3,1) are points on E. Show that P + (Q+R) = (P+Q) + R without using the fact that $E(\mathbf{F}_7)$ is a group.

3. (5pts) Let E be the elliptic curve defined by the equation $y^2 + y = x^3 + x$ over \mathbf{F}_2 . Show that $E(\mathbf{F}_{16}) = E[5]$. (Hint: Show that $\phi_2^4 - 1 = [-5]$.)

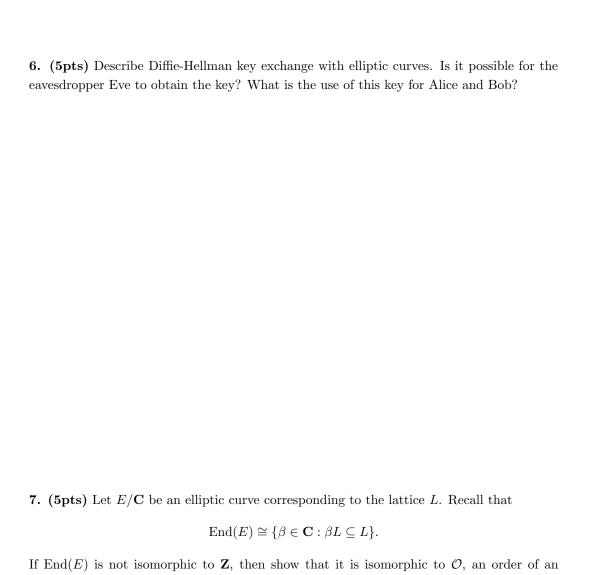
_

4. (5pts) Let E be the elliptic curve $y^2 = x^3 + x + 8$ defined over \mathbf{F}_{71} . The point P = (1,9) is of order 79 and therefore generates $E(\mathbf{F}_{71})$. Let Q = (70,19), a point on E. Let $f: E(\mathbf{F}_{71}) \to E(\mathbf{F}_{71})$ be defined by f(R) = 2R + Q. Set $P_0 = P$ and define $P_i = f(P_{i-1})$ for all $i \geq 1$ recursively. Solve the discrete logarithm problem Q = kP using the following table.

i	0	1	2	3	4	5	6
$x(P_i)$	1	32	26	1	43	60	47
$y(P_i)$	9	19	59	62	31	50	54

5. (5pts) Let \mathbf{F}_q be a finite field with $q \equiv 2 \pmod{3}$. If $E: y^2 = x^3 + B$ is an elliptic curve defined over \mathbf{F}_q then show that E is supersingular.

.



imaginary quadratic field K.