

## Math 497A: Elliptic Curves and Applications to Cryptography - Fall 2008

### List of theoretical questions for the final exam:

- (1) Explain how to find all rational points on a nondegenerate conic defined over  $\mathbb{Q}$ .
- (2) State the Lutz-Nagell Theorem and give an outline of its proof.
- (3) State two different methods of computing the torsion group of an elliptic curve over  $\mathbb{Q}$ , and explain how/why they work.
- (4) Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  (given by an equation with integer coefficients), and let  $p$  be a prime. Prove that the set

$$E(p^k) := \{\mathbf{O}\} \cup \{(x, y) \in E(\mathbb{Q}) : \text{ord}_p(x) \leq -2k, \text{ord}_p(y) \leq -3k\}$$

forms a subgroup of  $E(\mathbb{Q})$ .

- (5) State and prove the Descent Theorem.
- (6) State the Weak Mordell-Weil Theorem and give an outline of its proof.
- (7) Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . Explain how the index of  $2E(\mathbb{Q})$  in  $E(\mathbb{Q})$ ,  $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ , is related to the rank of the elliptic curve.
- (8) State a theorem that allows you to compute the rank of elliptic curves of the form  $y^2 = x^3 + ax^2 + bx$ . Give an outline of its proof.
- (9) State properties of the reduction map  $\rho_p : E(\mathbb{Q}) \rightarrow E(\mathbb{F}_p)$ , and prove them.
- (10) State Hasse's theorem about the number of rational points on an elliptic curve defined over a finite field and give an outline of the proof.
- (11) Define what the characteristic polynomial of the Frobenius endomorphism is and state/prove the theorem that tells you what its coefficients are.
- (12) What is the Weil pairing on an elliptic curve? What are the properties of the Weil pairing, and what theorems can you prove using the Weil pairing?

- (13) Give two different definitions of the Weil pairing. Explain which of the two definitions is more suitable for explicitly computing the pairing.
- (14) What is the Weil pairing on an elliptic curve? Give at least two applications of the Weil pairing to cryptography and explain why/how they work. What are the underlying hardness assumptions in each case?
- (15) Explain Lenstra's method for factoring integers that uses elliptic curves. (In this context, what can you say about elliptic curves modulo  $n$  when  $n$  is not necessarily prime?)
- (16) Explain how elliptic curves can be used for Primality Testing. Explain why this works. Explain a related primality test, the Pocklington-Lehmer test.
- (17) State a theorem that characterizes the  $n$ -torsion on an elliptic curve. (You should have different cases depending on the characteristic of the field over which your curve is defined.) Explain how to prove this theorem.
- (18) Define what an endomorphism of an elliptic curve is, and define the endomorphism ring of an elliptic curve. Define what the degree of an endomorphism is, and what it means for an endomorphism to be separable. Now let  $\alpha$  be a separable endomorphism of an elliptic curve  $E$  defined over a finite field  $\mathbb{F}_q$ . State/prove a theorem that lets you relate the degree of  $\alpha$  to a determinant calculation.
- (19) Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . Prove that  $E[n] \not\subseteq E(\mathbb{Q})$  for  $n \geq 3$ .
- (20) Let  $E$  be an elliptic curve defined over a finite field  $K$ . Let  $n$  be an integer that is coprime to the characteristic of  $K$ . Let  $\{T_1, T_2\}$  be a basis for the  $n$ -torsion on  $E$ . State what properties the Weil pairing  $e_n$  has and use them that  $e_n(T_1, T_2)$  is a primitive  $n$ -th root of unity.
- (21) Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and let  $P$  be a point on  $E$ . State several equivalent criteria that hold if and only if  $P$  is a point of order 3 on  $E$ . Prove your statement.