MATH 195: CRYPTOGRAPHY
HOMEWORK #14

Problem 6.28. *Let* $E: y^2 = x^3 + x^2 + 1$ *over* $\mathbb{F}_3$.

(a) *Determine all points of* $E(\mathbb{F}_3)$.
(b) *Make a group table for* $E(\mathbb{F}_3)$.

Problem 6.29. *Let* E *be an elliptic curve over* $\mathbb{F}_q$, *and define* $t_0, t_1, t_2, \ldots$ *by* $t_0 = 2$, $t_1 = q + 1 - \#E(\mathbb{F}_q)$, *and*

$$t_n = t_1 \cdot t_{n-1} - qt_{n-2},$$

for $n \geq 2$. *Prove that for all* n *one has*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - t_n.$$

[Use the theorem stated in class.]

Problem 6.30. *Let* $E: y^2 = x^3 - x + 1$ *over* $\mathbb{F}_3$.

(a) *Determine* $\#E(\mathbb{F}_3)$.
(b) *Prove:* $E(\mathbb{F}_3) = E(\mathbb{F}_9)$.
(c) *Compute* $\#E(\mathbb{F}_{27})$ *and* $\#E(\mathbb{F}_{81})$.

Problem 6.31. *Alice and Bob do a Diffie-Hellman key exchange using the group* $E(\mathbb{F}_3)$, *where* $E: y^2 = x^3 - x + 1$, *with* $g = (1, 1)$. *They use secret exponents* $a = 2$ *and* $b = 3$. *What is the secret common key that they exchange?*

Date: May 7, 2002.
6.28, 6.29, 6.30, 6.31.