Freshman Seminar 21n: Elliptic Curves

William Stein

February 18, 2003

1 Remarks

Your reading for this coming week is about points of finite order and how to work modulo p. The first section of chapter 2 characterizes the points of order 2 or 3 on an elliptic curve, and the second sectoin discusses the analytic way of viewing an elliptic curve as a complex torus. This analytic point of view makes it easy to see that the group of points of order dividing m on an elliptic curve is isomorphic to $\mathbb{Z}/m \times \mathbb{Z}/m$. Section 3 contains some remarks about discriminants of cubics that are useful in the theorem that bounds torsion points, which you will read about next week. The reading from the appendix is concerned with how to define a reduction map from $\mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$. If E is an elliptic curve with discriminant not divisible by p, this map induces a group homomorphism $E(\mathbb{Q}) \to E(\mathbb{F}_p)$.

You should also read a proof that every finitely generated abelian group can be written as a product of cyclic groups.

2 New reading and problems

Reading Assignment: *Read pages* **251–254** *of Appendix A and pages* **38–48** *of Chapter II, both in [Silverman-Tate]. Also, read a proof of the fundamental theorem of abelian groups in an algebra book (part of the assignment is to find one).*

2.1 Problems for next time.

1. (Jenna) Let P, P_1, P_2, P_3 be points in $\mathbb{P}^2$ and let L be a line in $\mathbb{P}^2$.

   (a) If P_1, P_2, and P_3 do not lie on a line, prove that there is a projective transformation of $\mathbb{P}^2$ so that
   $$P_1 \mapsto (0:0:1), \qquad P_2 \mapsto (0:1:0), \qquad P_3 \mapsto (1:0:0).$$

   (b) If no three of P_1, P_2, P_3 and P lie on a line, prove that there is a unique projective transformation as in (a) which also sends P to $(1:1:1)$.

   (c) Prove that if P does not lie on L, then there is a projective transformation of $\mathbb{P}^2$ so that L is sent to the line $Z = 0$ and P is sent to the point $(0:0:1)$.

2. (Jennifer) Let C be the cubic curve $y^2 = x^3 + 1$.

   (a) For each prime $5 \le p < 30$, describe the group $C(\mathbb{F}_p)$ of points on this curve having coordinates in the finite field of order p. (Use a computer.)

   (b) For each prime in (a), let N_p be the number of points in $C(\mathbb{F}_p)$. (Don't forget the point at infinity.) For the set of primes satisfying $p \equiv 2 \pmod 3$, can you see a pattern for the values of N_p? Make a general conjecture about the value of N_p when $p \equiv 2 \pmod 3$ and prove that your conjecture is correct.

   (c) Find a conjectural pattern for the values of N_p for the set of primes $p \equiv 1 \pmod 3$, and give evidence for your conjecture. Feel free to try to find the answer to this question by looking in other books or asking around the department, since this problem is double starred in Silverman-Tate.

3. (Mauro) Let C be a nonsingular cubic curve given by a Weierstrass equation
$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

   (a) Prove that
$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)}.$$
   Deduce that a point $P = (x, y) \in C$ is a point of order three if and only if $P \neq \mathcal{O}$ and P is a point of inflection on the curve C.

   (b) Suppose that $a, b, c \in \mathbb{R}$. Prove that $\psi_3(x)$ has exactly two real roots, say α_1, α_2 with $\alpha_1 < \alpha_2$. Prove that $f(\alpha_1) < 0$ and $f(\alpha_2) > 0$. Deduce that the points in $C(\mathbb{R})$ of order dividing 3 form a cyclic group of order 3.

4. (Alex) Let A be an abelian group, and for every integer $m \ge 1$, let $A[m]$ be the set of elements $P \in A$ satisfying $mP = \mathcal{O}$. (Note that $A[m]$ is denoted A_m in [Silverman-Tate].)

   (a) Prove that $A[m]$ is a subgroup of A.

   (b) Suppose that A has order M^2 and that for every integer m dividing M, the subgroup $A[m]$ has order m^2. Prove that A is the direct product of two cyclic groups of order M.

   (c) Find an example of a non-abelian group G and an integer $m \ge 1$ so that the set $G[m] = \{g \in G : g^m = 1\}$ is not a subgroup of G.

5. (Jeff)

   (a) Let $f(x) = x^2 + ax + b = (x - \alpha_1)(x - \alpha_2)$ be a quadratic polynomial with the indicated factorization. Prove that
$$(\alpha_1 - \alpha_2)^2 = a^2 - 4b.$$

   (b) Let $f(x) = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ be a cubic polynomial with the indicated factorization. Prove that
$$(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$