E. Dummit's Math 4527 ~ Number Theory 2, Spring 2021 ~ Homework 7, due Thu Mar 11th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. Find the rational torsion points on each elliptic curve and identify its group structure.
   (a) $E : y^2 = x^3 - 4x + 3$.
   (b) $E : y^2 = x^3 + x + 1$.
   (c) $E : y^2 = x^3 + 1$.
   (d) $E : y^2 = x^3 - 7x + 6$.
   (e) $E : y^2 = x^3 - 43x + 166$.
   (f) $E : y^2 = x^3 + x + 2$.
   (g) $E : y^2 = x^3 - 4x^2 + 16$. [All our results hold for elliptic curves in general Weierstrass form.]
   (h) $E : y^2 = x^3 - 14x^2 + 81x$.
   (i) $E : y^2 = x^3 + x^2 - 20x$.

---

2. Show that each of the following curves has infinitely many rational points, and explicitly compute at least five rational points on the curve:
   (a) $E : y^2 = x^3 - 4x + 4$.
   (b) $E : y^2 = x^3 - 2x + 5$.
   (c) $E : y^2 = x^3 + 4x + 15$. [Hint: Try seaching for $4x \in \mathbb{Z}$.]

---

3. The goal of this problem is to compute some 3-torsion and 4-torsion points on an elliptic curve $E : y^2 = x^3 + Ax + B$.
   (a) Show that $P = (x, y)$ is a 3-torsion point if and only if $12x(x^3 + Ax + B) = (3x^2 + A)^2$. Deduce that there are at most nine 3-torsion points on E. [Hint: I essentially did this in class.]
   (b) Find all nine complex 3-torsion points of the curve $y^2 = x^3 - 16$.
   (c) Show that $P = (x, y)$ is a point of order 4 if and only if $(3x^2 + A) \cdot 3x \cdot 4(x^3 + Ax + B) - (3x^2 + A)^3 - 8(x^3 + Ax + B)^2 = 0$. Deduce that there are at most sixteen 4-torsion points on E. [Hint: P is a 4-torsion point if and only if the y-coordinate of $2P$ is zero.]
   (d) Find all sixteen complex 4-torsion points of the curve $y^2 = x^3 - 52x - 272i$.

---

4. For each value of n, (i) use Tunnell's theorem to determine whether n is a congruent number, and (ii) if so, find an explicit non-torsion rational point on $y^2 = x^3 - n^2x$ and use it to write down a rational right triangle with area n.
   (a) $n = 10$.
   (b) $n = 11$.
   (c) $n = 15$.
   (d) $n = 14$.
   (e) $n = 34$.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

5. Prove that for any positive integer N, there exist integers A and B such that the elliptic curve $E : y^2 = x^3 + Ax + B$ has at least N integral points (x, y) on it. [Hint: Start with a curve that has infinitely many rational points, and then clear some denominators.]

---

6. The goal of this problem is to prove that if $p \geq 3$ is a prime, then the number of points on the elliptic curve $E : y^2 = x^3 + x$ modulo p is divisible by 4.

   (a) If $p \equiv 1 \pmod 4$, show that E has three points of order 2 modulo p, and use this to deduce that the number of points on E is divisible by 4.

   (b) If $p \equiv 3 \pmod 4$, show that there is a point of order 4 on E, and use this to deduce that the number of points on E is divisible by 4. [Hint: Try finding a point Q such that $2Q$ has order 2.]

---

7. The goal of this problem is to explain why elliptic curves are called elliptic curves.

   (a) If $E : y^2 = x^3 + Ax + B$ is an elliptic curve in reduced Weierstrass form over $\mathbb{C}$, show that there exists a linear change of variables $x = ax' + b$, $y = cy'$ such that E has an equation in Legendre form: $(y')^2 = x'(x' - 1)(x' - \lambda)$ for some $\lambda \in \mathbb{C}$. [Hint: Translate one root of the cubic to 0, and then scale so that another is 1.]

   (b) If $E : y^2 = x(x - 1)(x - \lambda)$ is an elliptic curve in Legendre form, show that there exists a rational change of variables $x = (ax' + b)/(cx' + d)$, $y = ey'/(cx' + d)^2$ such that E has an equation of the form $(y')^2 = (1 - (x')^2)(1 - k^2(x')^2)$ for some constant k. [Hint: Try $c = d = 1$ and $a = -b$.]

   If $0 < k < 1$, and $E : y^2 = (1 - x^2)(1 - k^2x^2)$, define the complete elliptic integrals for E as

$$\begin{aligned} K(k) &= \int_0^1 \frac{dx}{y} = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} \\ T(k) &= \int_0^1 \frac{y}{1-x^2}\,dx = \int_0^1 \sqrt{\frac{1-k^2x^2}{1-x^2}}\,dx \end{aligned}$$

   (c) Show that $K(k) = \displaystyle\int_0^{\pi/2} \frac{d\theta}{\sqrt{1 - k^2 \sin^2\theta}}$ and $E(k) = \displaystyle\int_0^{\pi/2} \sqrt{1 - k^2 \sin^2\theta}\,d\theta$.

   (d) If $0 < a \leq b$, show that the arclength of the ellipse $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$ is $4b \cdot T(\sqrt{1 - a^2/b^2})$.

   - Remark: The point is that computing the arclength of an ellipse, upon doing suitable changes of variable in the resulting integral, leads one to study the integrals $T(k)$ and $K(k)$, which in turn lead to studying elliptic curves in various different forms. We will also note that these elliptic integrals give a way to calculate the complex lattice corresponding to E: explicitly, by making appropriate branch cuts, one can show that the lattice Λ has periods $\omega_1 = 4K(k)$ and $\omega_2 = 2iK(\sqrt{1 - k^2})$. The point is that the poles of the differential $\dfrac{dx}{y}$ have been moved to ± 1, $\pm 1/k$, and so integrating from -1 to 1 will give the period ω_1 while integrating from $1/k$ to 1 will give the period ω_2 (after making a substitution).
