E. Dummit's Math 4527 ~ Number Theory 2, Spring 2021 ~ Homework 5, due Thu Mar 25th.

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. Consider the elliptic curve $E : y^2 = x^3 - 4x + 1$ over the real numbers, with the points $P_1 = (3, 4)$, $P_2 = (0, 1)$, and $P_3 = (-1, -2)$.

   (a) Find the sum $P_1 + P_2$ by explicitly computing the equation of the line through them and finding its third intersection point with $E$.

   (b) Find the sum $P_2 + P_3$ by explicitly computing the equation of the line through them and finding its third intersection point with $E$.

   (c) Verify the associative law $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for these points by explicitly calculating both sums.

   (d) Find the double $2P_2$ by explicitly computing the equation of the tangent line to $E$ at $P_2$ and finding its third intersection point with $E$.

   (e) Find $3P_2 = 2P_2 + P_2$ and then verify that $3P_2 + P_2 = 2P_2 + 2P_2$ by explicitly computing both sums.

---

2. Consider the elliptic curve $E : y^2 = x^3 + 1$ modulo 5.

   (a) Identify all the points on $E$ and verify that the Hasse bound holds.

   (b) Construct an addition table for the points on $E$.

   (c) Find the order of each point on $E$, and verify that each point's order divides the total number of points on $E$.

   (d) Describe the group structure of the group of points on $E$.

---

3. For each elliptic curve $E$ modulo each prime $p$, (i) verify that $E$ is nonsingular modulo $p$, (ii) identify all points on $E$ modulo $p$, (iii) find the order of each point on $E$, and (iv) describe the group structure of the points on $E$.

   (a) $y^2 = x^3 + 4x + 1$, $p = 13$.

   (b) $y^2 = x^3 + x + 2$, $p = 11$.

---

4. Suppose $p$ is a prime and $E$ is a nonsingular elliptic curve that has exactly 2021 points modulo $p$.

   (a) Use the Hasse bound to determine a range of possible values for $p$.

   (b) [Optional] Find an explicit example $(E, p)$ where $E$ has 2021 points modulo $p$.

---

5. Consider the elliptic curve $E : y^2 = x^3 + x + 3$ modulo the prime $p = 15107$.

   (a) Show that the point $P = (13, 2838)$ lies on $E$ and that it has order exactly 1071.

   (b) What range of values for the number $N$ of points on $E$ does the Hasse bound give?

   (c) Determine the exact number of points on $E$.

---

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

6. Consider the elliptic curve $E : y^2 = x^3 + x$ over the complex numbers. We define a "multiplication by $i$" map as the one sending $P = (x, y)$ to the point $iP = (-x, iy)$.

   (a) Show that if $P$ lies on $E$, then so does $iP$.

   (b) Show that $i(iP) = -P$ for any $P$ lying on $E$, where $-P$ denotes the inverse of $P$ under the addition law.

   (c) Show that $i(2P) = 2(iP)$ for any $P$ lying on $E$. [Hint: If the slope of the tangent at $P$ is $m$, show the slope of the tangent at $iP$ is $-im$.]

   (d) Show that $i(P+Q) = iP + iQ$ for any two distinct points $P$ and $Q$ lying on $E$. [Hint: If the line joining $P$ and $Q$ has slope $m$, show that the line joining $iP$ and $iQ$ has slope $-im$.]

   (e) Now define $(a + bi)P = aP + b(iP)$ for any integers $a$ and $b$. Show that for any two complex numbers $z = a + bi$ and $w = c + di$ with $a, b, c, d$ integers, it is true that $(zw)P = z(wP)$. [Hint: Use (b)-(d) to expand out both sides in terms of $P$ and $iP$.]

   - Remark: Part (e) says that we can extend the multiplication operation on this curve to include a "complex multiplication".

---

7. For a nonsingular elliptic curve $E : y^2 = x^3 + Ax + B$, the j-invariant is defined to be the quantity $j = -1728 \cdot \dfrac{(4A)^3}{\Delta} = 1728 \cdot \dfrac{4A^3}{4A^3 + 27B^2}$. Note that if $A$ and $B$ are rational numbers, then so is $j$.

   (a) Find the $j$-invariants of the elliptic curves $E_1 : y^2 = x^3 + x$, $E_2 : y^2 = x^3 + 1$, $E_3 : y^2 = x^3 - 21x + 14$.

   (b) Suppose we make the change of variables $x = u^2x'$ and $y = u^3y'$ in the equation for $E$ to obtain a new curve $E' : (y')^2 = (x')^3 + A'(x') + B'$ for new coefficients of $A'$ and $B'$. Show that the $j$-invariant of the new curve $E'$ is the same as the original curve $E$.

   (c) Find the $j$-invariant of the elliptic curve $E : y^2 = x^3 - \left(\dfrac{r}{48(r - 1728)}\right) x + \left(\dfrac{r}{864(r - 1728)}\right)$ for $r \neq 0, 1728$. Use the result to show that there exists a nonsingular elliptic curve with rational coefficients having any rational-valued $j$-invariant.

   - Remark: In fact, the value of the $j$-invariant uniquely characterizes an elliptic curve up to isomorphism over an algebraically closed field (such as $\mathbb{C}$).

---

8. Observe that, for fixed values of $x$, $A$, and $B$, the number of values of $y$ modulo $p$ with $y^2 \equiv x^3 + Ax + B \pmod{p}$ is equal to $1 + \left(\dfrac{x^3 + Ax + B}{p}\right)_L$, where $\left(\dfrac{z}{p}\right)_L$ represents the Legendre (or Jacobi) symbol. Thus, the number of points on the elliptic curve $E_p : y^2 = x^3 + Ax + B \pmod{p}$ is given by $p + 1 + \displaystyle\sum_{x=0}^{p-1} \left(\dfrac{x^3 + Ax + B}{p}\right)_L$.

   (a) Find the number of points on the elliptic curve $y^2 = x^3 + 5x + 13$ modulo $p = 11027$.

   (b) Find the number of points on the elliptic curve $y^2 = x^3 + 1$ modulo $p = 14939$.

   (c) Find the number of points on the elliptic curve $y^2 = x^3 + 1$ modulo $p = 34361$.

   (d) Suppose that $p \equiv 5 \pmod{6}$, so that 3 is relatively prime to $\varphi(p)$, and let $k = 3^{-1} \pmod{\varphi(p)}$. Show that the statements $x^3 \equiv a \pmod{p}$ and $x \equiv a^k \pmod{p}$ are equivalent, and conclude that for a given $b$, there is a unique solution to $x^3 \equiv b \pmod{p}$.

   (e) Suppose $p \equiv 5 \pmod{6}$. Show that the elliptic curve $y^2 = x^3 + 1$ has exactly $p + 1$ points modulo $p$, and use this to explain the results of parts (b) and (c).

---