Problem Set 3

PAWS 2025

Nathaniel Hurst

1

Let $a, b \in K$ and consider the (affine plane) curve C (not elliptic curve since $4a^3 + 27b^2$ is not necessarily 0 in this exercise), defined by $y^2 = x^3 + ax + b$.

(a) Show that $4a^3 + 27b^2 = 0$ if and only if the polynomial $f = x^3 + ax + b$ has a repeated root.

(b) A point P on an affine plane curve is a singularity if and only if both partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish at P; otherwise P is called a smooth point. Use this definition and part (a) to show that all points P on C are smooth if and only if $4a^3 + 27b^2 \neq 0$.

(a) First suppose that $4a^3 + 27b^2 = 0$, or $a^3 = \frac{-27b^2}{4}$. Then observe that for x_0 such that $a = -3x_0^2$ (note we can find one by taking the cube root of $\frac{-27b^2}{4}$ and some arithmetic) that

$$(-3x_0^2)^3 = \tfrac{-27b^2}{4} \implies b^2 = 4x_0^6 \implies b = 2x_0^3$$

But then observe that

$$f(x_0) = x_0^3 + ax_0 + b = x_0^3 + (-3x_0^2)x_0 + 2x_0^3 = 0$$

and

$$f'(x_0) = 3x_0^2 + a = 3x_0^2 - 3x_0^2 = 0$$

and so x_0 is a repeated root.

Now suppose that f has a repeated root, i.e f and f' share a root. Let x_0 be such a root. Then $x_0^3 + ax_0 + b = 0$ and $3x_0^2 + a = 0$, i.e. $-\frac{a}{3} = x_0^2$. Substituting this back into our first relation we get

$$0 = \left(-\tfrac{a}{3}\right)x_0 + ax_0 + = \left(\tfrac{2a}{3}\right)x_0 + b \implies x_0 = \tfrac{-3b}{2a}$$

i.e. $x_0^2 = \frac{9b^2}{4a^2}$. But we also found $x_0^2 = -\frac{a}{3}$. Thus we have

$$0 = \tfrac{9b^2}{4a^2} + \tfrac{a}{3} = 27b^2 + 4a^3$$

(b) Observe that if we write $f = x^3 + ax + b - y^2$ we have that $f_x = 3x^2 + a$ and $f_y = -2y$. Suppose that both partial derivatives vanish at some $P = (x, y)$, then using that in our system above we get that $x^2 = -\frac{a}{3}$ and $y = 0$. Plugging this back into $y^2 = x^3 + ax + b$ we get

$$0 = \left(-\tfrac{a}{3}\right)x + ax + b = \left(\tfrac{2a}{3}\right)x + b \implies x = \tfrac{-3b}{2a}$$

Thus we have $x^2 = \frac{9b^2}{4a^2}$. But we also found that $x^2 = -\frac{a}{3}$. Thus we have that

$$0 = \tfrac{9b^2}{4a^2} + \tfrac{a}{3} = 27b^2 + 4a^3$$

Thus if the partial derivatives vanish at any point we must have $27b^2 + 4a^3 = 0$. Now observe that if $4a^3 + 27b^2 = 0$ then by part (a) we have that $x^3 + ax + b$ has a repeated root, and so it must

share a root with its derivative $3x^2 + a$, i.e. the system $0 = 3x^2 + a = f_x$ and $0 = -2y = f_y$ has a solution, or there is some P such that the partials vanish, and so C is not smooth.

2 Consider the elliptic curve $E : y^2 = x^3 - 3x + 1$ defined over $\mathbb{F}_{13}$ and let

$$P_1 = (0, 1) \in E(\mathbb{F}_{13})$$

(a) Compute $[2] \cdot P_1$. Is there any relation to the point P_2 of Example 3.8 in the lecture notes?

(b) Compute $[12] \cdot P_1$. Try to use as few elliptic curve additions as possible.

(a) We compute $[2] \cdot P_1 = P_1 + P_1$ using the group law. Then we have

$$[2] \cdot P_1 = \left(\left(\tfrac{3(x_1)^2 + a}{2y_1} \right)^2 - 2x_1, \tfrac{3(x_1)^2 + a}{2y_1}(x_1 - x_3) - y_1 \right) =$$

$$= \left((-3 \cdot 2^{-1})^2, (-3 \cdot 2^{-1})^2 \left(1 - (-3 \cdot 2^{-1})^2 \right) - 1 \right) = (12, 5(0 - 12) - 1) = (12, 4)$$

(b) Observe that

$$[12] \cdot P_1 = [3]([2]([2] \cdot P_1))$$

Now observe that when we do $[2] \cdot ([2] \cdot P_1) = [2] \cdot (12, 4)$ we have that $m = \frac{3x_1^2 + a}{2y_1} = \frac{3-3}{2y_1} = 0$. Thus

$$[2] \cdot ([2] \cdot P_1) = [2] \cdot (12, 4) = (2, 9)$$

and finally we can compute

$$[3] \cdot (2, 9) = (2, 9) + [(2, 9) + (2, 9)] = (2, 9) + (6, 2) = (1, 1)$$

giving us our answer $[12] \cdot P_1 = (1, 1)$

3 Given an elliptic curve E over K, a point $P \in E(K)$ and an integer N. Show that Algorithm 4 computes $[N] \cdot P$ using at most $2 \log_2(N)$ elliptic curve additions (a doubling $[2] \cdot P$ is counted as one addition $P + P$).

It is clear that when $N = (e_0 e_1 e_2 ... e_n)_2$ algorithm 4 terminates in n steps, and does at most 2 additions per step (once with $R \leftarrow R + Q$ and another with $Q \leftarrow [2]Q$). Thus the maximum number of elliptic curve additions is $2N = 2\lceil \log_2(N) \rceil$. To see that algorithm 4 actually outputs $[N] \cdot P$ observe first that if $N = (e_1 e_0 e_2 ... e_n)$ then

$$[N] \cdot P = [e_0 + 2e_1 + 2^2 e_2 + ... + 2^n e_n] =$$

$$[e_0] \cdot P + [2e_1] \cdot P + [2e_2]([2] \cdot P) + ... + [2e_n]([2^{n-1}] \cdot P_n)$$

Then observe that the double-and-add algorithm starts by computing $R \leftarrow [e_0]P$ and then doubling Q to get $[2] \cdot Q = [2] \cdot P$, allowing us to compute $[e_1](Q) = [e_1]([2] \cdot P) = [2e_1] \cdot P$ and then add it

to R in the next step (note if $e_1 = 0$ then $[e_1]Q = \infty$, and so R is unchanged). Continuing in this way we add $[2^k e_k] \cdot P$ to the total R all the way up to n, giving us $[N] \cdot P$.

4

Consider $E : y^2 = x^3 - 2x + 5$ over $\mathbb{F}_{19}$. Let $P = (2, 3)$ and $Q = (10, 4)$. (Note: See the SageMath documentation for how to construct elliptic curves and points on elliptic curves.)

(a) Check that P and Q are points on E.

(b) Calculate $P + Q$, without using SageMath.

(c) Calculate $[5] \cdot P$ using the double-and-add algorithm (Algorithm 4 of the lecture notes).

(d) Calculate $[7] \cdot Q$. What does this tell you about the order of Q?

(a) To verify that P and Q are points on E, we can plug them into the elliptic curve equation and see if it is true. For $P = (2, 3)$ we have

$$9 = 8 - 4 + 5$$

which is true. For $Q = (10, 4)$ we have

$$16 = 1000 - 20 + 5$$

which is true modulo 19. Thus P and Q are points on E.

(b) To calculate $P + Q$ we use the group law. Then

$$P + Q = (2, 3) + (10, 4) = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1) = (18, 14)$$

where $m = \frac{y_2 - y_1}{x_2 - x_1}$.

(c) First we let $Q \leftarrow P = (2, 3)$ and $R \leftarrow \infty$ and observe that $5 = (e_0 e_1 e_2)_2 = (101)_2$. Then since $e_0 = 1$ we do $R \leftarrow R + Q = \infty + P = (2, 3)$ and then $Q \leftarrow [2]Q = (3, 8)$.

Then since $e_1 = 0$ we do $Q \leftarrow [2]Q = (17, 1)$.

Then finally we get our answer by doing $[5] \cdot P = R + Q = (2, 3) + (9, 14) = (5, 5)$.

(d) We will again use the double and add algorithm: first we let $K \leftarrow Q = (10, 4)$ and $R \leftarrow \infty$. The observe that $7 = (e_0 e_1 e_2)_2 = (111)_2$.

Then since $e_0 = 1$ we do $R \leftarrow R + K = (10, 4)$ and $K \leftarrow [2]K = (15, 14)$.

Then since $e_1 = 1$ we do $R \leftarrow R + K = (10, 4) + (15, 14) = (17, 1)$ and $K \leftarrow [2]K = (17, 18)$

Finally our answer is $[7] \cdot Q = R + K = (17, 1) + (17, 18) = \infty$. Thus the order of Q is seven (we know that the order divides seven, but seven is prime).

5

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a field of characteristic $\neq 2, 3$. In this exercise, you are asked to show that $\#E[3] = 9$ by describing how to compute the points.

(a) Use the description of the group law (in Theorem 3.7 of the lecture notes) to construct a polynomial φ such that $\varphi(x) = 0$ if and only if $[3] \cdot P = \infty$, where $P = (x, y)$ is a point on the (affine) curve.

(b) Show that φ has no repeated roots. (Hint: Show that φ and its derivative cannot share any roots.)

(a) Observe that for $P = (x, y)$, where $y \neq 0$ (since if $y = 0$ we would already have by the group law that $[2] \cdot P = \infty$) we must have that if $[3] \cdot P = \infty$ then $(x, y_1) + (x, y_1) = (x, y_2)$, for then $P + (P + P) = (x, y_1) + (x, y_2) = \infty$. Using the description of the group law we find that this is exactly when $x = m^2 - 2x$ where $m = \frac{3x^2+a}{2y_1}$, or

$$3x = \frac{9x^4+6x^2a+a^2}{4y_1^2}$$

Now using the fact that $y_1 = x^3 + ax + b$ we can simplify this relation to

$$3x^4 + 6x^2a + 12xb + a^2 = 0$$

Thus we have that for $\varphi(x) = 3x^4 + 6x^2a + 12xb + a^2$ that is $\varphi(x) = 0$ then $[3] \cdot P = \infty$. Observe that we need not check the condition on y_1 and y_2 ($y_1 = y_2 = 0$ or $y_1 \neq y_2$) in the group law for $(x, y_1) + (x, y_2) = \infty$) as if $y_1 = y_2$ then $(x, y_1) + (x, y_1) = (x, y_2) = (x, y_1)$ would imply that $P + P = P$, or $P = \infty$.

(b) Observe that $\varphi'(x) = 12x^3 + 12xa + 12b$, and so if $\varphi'(x) = 0$ that would imply that $x^3 + ax + b = 0$, and so any point (x, y) which satisfied this would have to have $y = 0$, and by the group law we know that $[2] \cdot (x, 0) = \infty$, so x cannot be a root of φ, for $[3] \cdot P = \infty + P = (x, 0) \neq \infty$. Thus φ and φ' share no roots, or φ has no repeated roots.

6

For each of the following elliptic curves and finite fields $\mathbb{F}_p$, list the points in $E(\mathbb{F}_p)$ and check that the number of points is within the Hasse bound:

(a) $E : y^2 = x^3 + 7x - 3$ over $\mathbb{F}_{13}$.

(b) $E : y^2 = x^3 + 11x + 2$ over $\mathbb{F}_{17}$.

(a) By plugging in every value $0 \leq x_0 \leq 12$ into the elliptic curve function we get an equation

$$y^2 = x_0^3 + 7x_0 - 3$$

Then if $x_0^3 + 7x - 3$ is a quadratic residue there is a solution $y_0^2 = x_0^3 + 7x_0 - 3$, giving points on the elliptic curve (x_0, y_0) and $(x_0, -y_0)$ and if not then no point on E has x coordinate x_0. Proceeding in this fashion and using an implementation of the Tonelli-Shanks algorithm (which can be found in the file Toneli-Shanks.ipynb) we find the following points on E:

$$(0,7), \quad (0,-7), \quad (5,1), \quad (5,-1), \quad (7,8), \quad (7,-8), \quad (9,3), \quad (9,-3), \quad (10,1), \quad (10,-1)$$
$$(11,1), \quad (11,-1), \quad \infty$$

Then $\#E(\mathbb{F}_p) = 13$, and the Hasse bound is satified as

$$p + 1 - 2\sqrt{p} \approx 6.8 \leq 13 \leq 21.2 \approx p + 1 + 2\sqrt{p}$$

(b) We employ a similar method as part (a), finding the points on E:

$$(0,6), \quad (0,-6), \quad (2,7), \quad (2,-7), \quad (4,12), \quad (4,-12), \quad (11,14), \quad (11,-14), \quad (21,14), \quad (12,-14)$$
$$(13,8), \quad (13,-8), \quad \infty$$

Then $\#E(\mathbb{F}_p) = 13$, and the Hasse bound is satified as

$$p + 1 - 2\sqrt{p} \approx 9.5 \leq 13 \leq 26.5 \approx p + 1 + 2\sqrt{p}$$

7

Let $p > 3$ be a prime, and consider two elliptic curves:

$$E : y^2 = x^3 + ax + b \quad \text{and} \quad \overline{E} : y^2 = x^3 + ax - b$$

defined over $\mathbb{F}_p$.

(a) Assume that $p \equiv 1 \pmod 4$. Show that

$$\#E(\mathbb{F}_p) = \#\overline{E}(\mathbb{F}_p)$$

(b) Assume that $p \equiv 3 \pmod 4$. Show that

$$\#E(\mathbb{F}_p) + \#\overline{E}(\mathbb{F}_p) = 2p + 2.$$

Some hints: **1)** Check if -1 is a square in $\mathbb{F}_p$. **2)** Let $p = (x_0, y_0) \in E(\mathbb{F}_p)$. Is there a point $\overline{P} = (x_0, \star) \in \overline{E}(\mathbb{F}_p)$? What about $\overline{P} = (-x_0, \star) \in \overline{E}(\mathbb{F}_p)$?

(a) Observe that by problem #8 below we have that

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\tfrac{x^3+Ax+B}{p}\right)$$

and since $p \equiv 1 \pmod 4$ we have that $\left(\tfrac{-1}{p}\right) = 1$, and so

$$\sum_{x \in \mathbb{F}_p} \left(\tfrac{x^3+Ax+B}{p}\right) = \left(\tfrac{-1}{p}\right) \sum_{x \in \mathbb{F}_p} \left(\tfrac{x^3+Ax+B}{p}\right) = \sum_{x \in \mathbb{F}_p} \left(\tfrac{(-1)(x^3+Ax+B)}{p}\right) =$$
$$= \sum_{x \in \mathbb{F}_p} \left(\tfrac{(-x)^3+A(-x)-B}{p}\right) = \sum_{(-x) \in \mathbb{F}_p} \left(\tfrac{x^3+Ax-B}{p}\right)$$

and since summing over all x is the same as summing over all $-x$ in $\mathbb{F}_p$ we have that

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\tfrac{x^3+Ax+B}{p}\right) = p + 1 + \sum_{(-x) \in \mathbb{F}_p} \left(\tfrac{x^3+Ax-B}{p}\right) = |\overline{E}(\mathbb{F}_P)|$$

(b) Similarly since $p \equiv 3 \pmod 4$ we have that $\left(\frac{-1}{p}\right) = -1$ and so by a similar reasoning as in part (a) we have

$$\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right) = -\left(\frac{-1}{p}\right)\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right) = -\sum_{x\in\mathbb{F}_p}\left(\frac{(-1)(x^3+Ax+B)}{p}\right) =$$
$$= -\sum_{x\in\mathbb{F}_p}\left(\frac{(-x)^3+A(-x)-B}{p}\right) = -\sum_{(-x)\in\mathbb{F}_p}\left(\frac{x^3+Ax-B}{p}\right)$$

and so

$$|E(\mathbb{F}_p)| + |\overline{E}(\mathbb{F}_p)| = \left(p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right)\right) + \left(p+1+\sum_{(-x)\in\mathbb{F}_p}\left(\frac{x^3+Ax-B}{p}\right)\right) =$$
$$= 2p+2+\left(\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right) - \sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right)\right) = 2p+2$$

8

Let $p > 2$ be a prime number and let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$, and denote with $E(\mathbb{F}_p)$ all points of E with coordinates in $\mathbb{F}_p$. Further, let $\left(\frac{a}{b}\right)$ be the Legendre symbol.

(a) Show that

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right).$$

(b) Let $d \in \mathbb{F}_p$ be such that $\left(\frac{d}{p}\right) = -1$ and $E' : dy^2 = x^3 + Ax + B$. Show that

$$|E(\mathbb{F}_p)| + |E'(\mathbb{F}_p)| = 2p + 2.$$

(c) Let p be a prime such that $p \equiv 3 \pmod 4$ and $E : y^2 = x^3 + Ax$. Show that $|E(\mathbb{F}_p)| = p + 1$.

(a) We can determine the number of points on an elliptic curve $E(\mathbb{F}_p)$ by taking every point $x \in \mathbb{F}_p$ and seeing if $x^3 + Ax + B$ is a quadratic residue modulo p, for if it is then there exists $y \in \mathbb{F}_p$ such that $y^2 = x^3 + Ax + B$, giving the two points on the elliptic curve $(x, y), (x, -y) \in E(\mathbb{F}_P)$. If $x^3 + Ax + B$ is not a quadratic residue then the equation $y^2 = x^3 + Ax + B$ has no solutions for y, and so no point with first coordinate x is on the elliptic curve.

In order to determine the number of points which satisfy the equation $y^2 = x^3 + ax + b$ we proceed by the following algorithm:

Let count = p. For $x \in \{0, \ldots, p-1\}$, if $\left(\frac{x^3+Ax+B}{p}\right) = 1$ we increase count by 1 (this corresponds to finding two points (x, y) and $(x, -y)$). If $\left(\frac{x^3+Ax+B}{p}\right) = -1$ we subtract one from count (this corresponds to finding no points for that x value). If $\left(\frac{x^3+Ax+B}{p}\right) = 0$ we leave count unchanged, as in this case the only solution to $y^2 = x^3 + ax + b$ is $(x, 0)$ and we already accounted for this point by letting count be p at the start. Finally we add the point at infinity to count, increasing it by one. This search exhausts all values $x \in \mathbb{F}_p$, and since square roots of quadratic residues are unique up to sign we see that this algorithm actually gives the number of points on the curve. Notice that in the way the algorithm was described, it will always yield exactly

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right)$$

(b) Observe that since $\left(\frac{d}{p}\right) = -1$ we also have that $\left(\frac{d^{-1}}{p}\right) = -1$ (for if there was a such that $a^2 = d^{-1}$ then $(a^{-1})^2 = (a^2)^{-1} = (d^{-1})^{-1} = d$, and so no such a can exist). Then if $(x, y) \in E(\mathbb{F}_p)$ we have that

$$\left(\frac{x^3+Ax+B}{p}\right) = 1$$

and so

$$\left(\frac{d^{-1}(x^3+Ax+B)}{p}\right) = \left(\frac{d^{-1}}{p}\right)\left(\frac{x^3+Ax+B}{p}\right) = -1 \cdot 1 = -1$$

(using properties of the Legendre symobl) and hence the equation $y^2 = d^{-1}(x^3 + Ax + B)$ has no solutions for y. Then we observe that

$$\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right) = -\sum_{x\in\mathbb{F}_p}\left(\frac{d^{-1}(x^3+Ax+B)}{p}\right)$$

or

$$|E(\mathbb{F}_p)| + |E'(\mathbb{F}_p)| = \left(p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right)\right) + \left(p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{d^{-1}(x^3+Ax+B)}{p}\right)\right)$$
$$= \left(p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right)\right) + \left(p+1-\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right)\right) = p+1+p+1 = 2p+2$$

(c) Since $p \equiv 3 \pmod 4$ we have that $\left(\frac{-1}{p}\right) = -1$, and so a is a quadratic residue if and only if $-a$ is not. Thus we can conlude that

$$\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax}{p}\right) = 0$$

(since for every x such that the Legendre symbol of $x^3 + Ax$ is one there is another of $(-x)^3 + (-x)A = (-1)(x^3 + Ax)$ which is negative one). Hence

$$|E(\mathbb{F}_p)| = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax}{p}\right) = p+1$$

9

Compute the group structure of $E(\mathbb{F}_p)$ for the given elliptic curves E and primes p. (Can you also find generators?)

(a) $E : y^2 = x^3 + 1$ for $p = 5$

(b) $E : y^2 = x^3 + x$ for $p = 7$

(c) $E : y^2 = x^3 - 1$ for $p = 7$

(d) $E : y^2 = x^3 + 3x + 1$ for $p = 11$

(e) For $p = 13$, compute the group structures of $E(\mathbb{F}_p)$ for all elliptic curves over $\mathbb{F}_p$. (You can use the command .abelian_group() for this.)

(a) We will employ the following process in this problem: we will find a point $P_1 \in E(\mathbb{F}_p)$, compute its order (and thus the subgroup generated by it), and then check if the number of elements (the order of all subgroups that are not the same found by the previous method) is enough such that adding any more subgroups would violate the Hasse bound.

Then observe that $(0,1) \in E(\mathbb{F}_5)$. Some computation yields that $\text{ord}((0,1)) = 3$. Then we find another point $P_2 = (2,3) \in E(\mathbb{F}_5)$ such that $(2,3) \notin \langle (0,1) \rangle$. Then again we see that $\text{ord}((2,3)) = 6$, but also through this computation we see that $(0,1) \in \langle (2,3) \rangle$ and so $\langle (0,1) \rangle \subset \langle (2,3) \rangle$.

Now observe that the Hasse Bound for this elliptic curve is

$$2 \leq \#E\big(\mathbb{F}_p\big) \leq 11$$

and since we know that $E\big(\mathbb{F}_p\big)$ contains a subgroup of order 6 we know that $6 \mid \#E\big(\mathbb{F}_p\big)$, and the only possible number of elements within the Hasse bound is 6. Thus we can conclude that

$$\langle (2,3) \rangle = E\big(\mathbb{F}_p\big) \cong \mathbb{Z}/6\mathbb{Z}$$

(b) We begin by finding $(1,4) \in E\big(\mathbb{F}_p\big)$ and computing $\text{ord}((1,4)) = 4$. Then we find $(3,4) \in E\big(\mathbb{F}_p\big)$ such that $(3,4) \notin \langle (1,4) \rangle$. Then we compute $\text{ord}((3,4)) = 8$, and in doing so see that $(1,4) \in \langle (3,4) \rangle$.

Now observe that the Hasse Bound for this elliptic curve is

$$3 \leq \#E\big(\mathbb{F}_p\big) \leq 13$$

and since we know that $E\big(\mathbb{F}_p\big)$ contains a subgroup of order 8 generated by $(3,4)$ we can conclude that $8 \mid \#E\big(\mathbb{F}_p\big)$. Now since the only possible option for the number of elements of $E\big(\mathbb{F}_p\big)$ within the Hasse bound but still divisible by 8 is 8 we can conclude that

$$\langle (3,4) \rangle = \#E\big(\mathbb{F}_p\big) \cong \mathbb{Z}/8\mathbb{Z}$$

(c) First we find $(1,0) \in E\big(\mathbb{F}_p\big)$ and compute $\text{ord}(1,0) = 2$. Then we find $(2,0) \in E\big(\mathbb{F}_p\big)$ such that and compute $\text{ord}(2,0) = 2$. Thus we have two subgroups of order 2 in $E\big(\mathbb{F}_p\big)$, or one subgroup of order 4. Thus we know that $4 \mid \#E\big(\mathbb{F}_p\big)$.

Note however that the Hasse Bound for this elliptic curve is

$$3 \leq \#E\big(\mathbb{F}_p\big) \leq 13$$

and so we can only conclude that $\#E\big(\mathbb{F}_p\big) \in \{4, 8, 12\}$. However a manual search shows that the equation $y^2 = x^3 - 1$ has no solutions moduluo 7 when $x \neq 1, 0$. Thus we can conclude that

$$\langle (1,0) \rangle \times \langle (2,0) \rangle = E(\mathbb{F}_P) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

(d) First we find $(0,1) \in E\big(\mathbb{F}_p\big)$ and compute $\text{ord}((0,1)) = 6$. Then we find $(1,4) \in E\big(\mathbb{F}_p\big)$ such that $(1,4) \notin \langle (0,1) \rangle$. Then we find that $\text{ord}(1,4) = 18$ and $(0,1) \in \langle (1,4) \rangle$. Thus $E\big(\mathbb{F}_p\big)$ contains a subgroup of order 18 and since the Hasse Bound for this elliptic curve is

$$6 \leq \#E\big(\mathbb{F}_p\big) \leq 18$$

we can conlude that $\#E\big(\mathbb{F}_p\big) = 18$, and so

$$\langle (1,4) \rangle = E\big(\mathbb{F}_p\big) \cong \mathbb{Z}/18\mathbb{Z}$$

(e) There are 22 possible group structures for an elliptic curve of the form $y^2 = x^3 + ax + b$ over $\mathbb{F}_{13}$. (computed with SageMath) They are:

$$\mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z}$$

with

$$(N_1, N_2) \in \{(2,8), (7,0), (3,3), (10,0), (16,), (3,6), (13,0), (19,0), (2,4),$$
$$(2,10), (9,0), (4,4), (12,0), (18,0), (15,0), (21,0), (2,6)\}$$

Note that problem 10 is ommitted, see Silverman's The Arithmetic of Elliptic Curves page 138 for a proof of the Hasse bound.