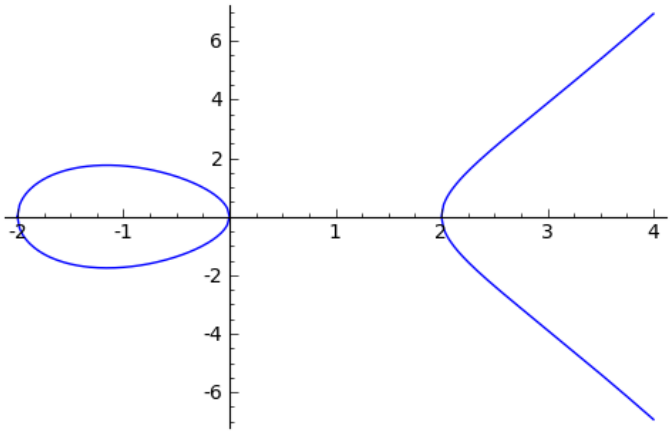
CS 259C/Math 250: Elliptic Curves in Cryptography
Homework 1 Solutions

1.

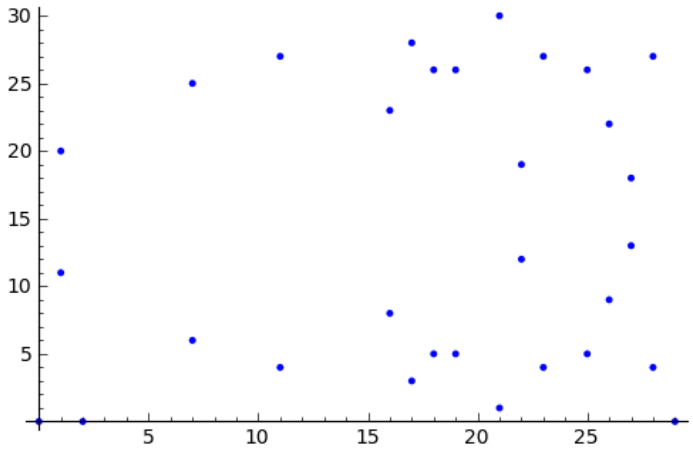
2.

3. (a)

```
ER=EllipticCurve([-4,0])
plot(ER)
```




```
EF=EllipticCurve(GF(31),[-4,0])
plot(EF)
```



(b)

```
EF.points()
```

```
[(0 : 0 : 1), (0 : 1 : 0), (1 : 11 : 1), (1 : 20 : 1), (2 : 0 : 1), (7 :
6 : 1), (7 : 25 : 1), (11 : 4 : 1), (11 : 27 : 1), (16 : 8 : 1), (16 :
23 : 1), (17 : 3 : 1), (17 : 28 : 1), (18 : 5 : 1), (18 : 26 : 1), (19 :
5 : 1), (19 : 26 : 1), (21 : 1 : 1), (21 : 30 : 1), (22 : 12 : 1), (22 :
19 : 1), (23 : 4 : 1), (23 : 27 : 1), (25 : 5 : 1), (25 : 26 : 1), (26 :
9 : 1), (26 : 22 : 1), (27 : 13 : 1), (27 : 18 : 1), (28 : 4 : 1), (28 :
27 : 1), (29 : 0 : 1)]
```

(c)

```
EF.abelian_group()
```

```
Additive abelian group isomorphic to Z/2 + Z/16 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 27*x over
Finite Field of size 31
```

Alternatively, we could compute the orders of the points in the group:

```
[P.order() for P in EF.points()]
```

```
[2, 1, 16, 16, 2, 8, 8, 16, 16, 8, 8, 4, 4, 4, 4, 16, 16, 16, 16, 16,
16, 8, 8, 16, 16, 8, 8, 16, 16, 16, 16, 2]
```

The group has 32 elements (`EF.order()` or `EF.count_points()`), there are elements with order 16, but no elements of order 32, the group structure must be $\mathbb{Z}_{16} \times \mathbb{Z}_2$

(d)

```
P=EF(1,11)
Q=EF(25,5)
P.discrete_log(Q)
```

```
9
```

Alternatively, we can compute

```
linear_relation(P,Q,'+')
```

```
(9, 1)
```

This means $9P = 1Q$. Lastly, we could have written a procedure:

```
for i in range(P.order()):
    if Q == i*P:
           print i
```

```
9
```

(e)

```
p=next_prime(2^259)
ord=EllipticCurve(GF(p),[-4,0]).order()
print(p)
print(ord)
print(ord-p)
```

```
9263367138985295633885678800695032628261598773251245123156606720633050375\
119923
9263367138985295633885678800695032628261598773251245123156606720633050375\
119924
1
```

4. (a) The easiest way to solve this part is to recall that $-(x, y) = (x, -y)$. Hence, if

$P = (x, 0)$, $-P = (x, 0) = P$, so $2P = \infty$.

When $K = \mathbb{R}$, we can interpret this geometrically. We can perform implicit differentiation on the equation for the elliptic curve (differentiating with respect to y_1, not x_1):

$$2y_1 = 3x_1^2 x_1' + Ax_1' = (3x_1^2 + A)x_1'$$

Since $y_1 = 0$, we have either $3x_1^2 + A = 0$ or $x_1' = 0$. Suppose the former was true. We have:

$$\begin{aligned} 0 &= y_1^2 = x_1^3 + Ax_1 + B, \text{ since } (x_1, 0) \text{ is on the elliptic curve} && (1)\\ A &= -3xy_1^2, \text{ by assumption} && (2)\\ 0 &= -2xy_1^3 + B \text{or } B = 2x_1^3, \text{ by 1 and 2} && (3)\\ 4A^3 + 27B^2 &= -108xy_1^6 + 108xy_1^6 = 0, \text{ by 2 and 3} && (4) \end{aligned}$$

Thus, the curve is singular, a contradiction. Hence, $x_1' = 0$. This means the tangent line through P is vertical, so $2P = \infty$.

(b) Now we are dealing with the curve $y^2 = x^3 + B$, the special case of the Weierstrass equation where $A = 0$. If $P = (0, y_1)$ is a point on this curve, then $y_1 \neq 0$, as $y_1 = 0$ would imply $B_1 = 0$, making this curve singular. Thus, the group law tells us how to compute $2P = (x_2, y_2)$:

$$\begin{aligned} m &= \frac{3x^2 + A}{2y_1} = \frac{3 \times 0 + 0}{2y_1} = 0\\ x_2 &= m^2 - 2x_1 = 0\\ y_2 &= m(x_1 - x_2) - y_1 = -y_1 \end{aligned}$$

Thus, $2P = (0, -y_1) = -P$, meaning $3P = \infty$.

When $K = \mathbb{R}$, there is also a geometric interpretation. We can perform implicit differentiation on the equation for the elliptic curve (differentiating with respect to x_1):

$$2y_1 y_1' = 3x_1^2 = 0$$

Since $y_1 \neq 0$, $y_1' = 0$. Thus, the line passing through the curve is $y = y_1$. Since $y_1^2 = B$, the only solution to $y^2 = x^3 + B$ with $y = y_1$ is $x = 0$. So $(0, y_1)$ is the only, and hence third, intersection of the curve and this line. Thus $2P = (0, -y_1) = -P$, and hence $3P = \infty$.

For the general Weierstrass equation, the points of order three are the points where the tangent line intersects the curve with order three. These turn out to be the inflection points or "flex points" of the curve.

5. (a) Suppose there was a point P that had order more than 2. Then $P \boxplus P$ is the third intersection of the elliptic curve and the tangent line passing through P. Now we compute $P \boxplus P \boxplus P = P \boxplus (P \boxplus P)$: draw the line between P and $P \boxplus P$, and $P \boxplus P \boxplus P$ is the third intersection of that line and the curve. However, this line is the same line used to compute $P \boxplus P$, so the line and the curve only intersect

at P (where the line is tangent) and $P \boxplus P$. Thus $P \boxplus P \boxplus P = P$. Assuming $\boxplus$ is a group law, we subtract out a P giving $P \boxplus P$ is equal to the identity. Thus, every point has order at most 2.

(b) Let E be an elliptic curve, and let P_1 and P_2 be points on it such that $Q_i = P_i \boxplus P_i$ is finite, and $Q_1 \neq Q_2$. It is not hard to think of such examples, especially over the real numbers (pick a P_1, and then let P_2 be a tiny displacement of P_1. Then Q_2 will be a tiny displacement of Q_1). In this case, according to part (a), Q_1 and Q_2 are both identities. Thus, there is no unique identity.

(c) Observe that $P \boxplus P = -(P + P)$ where $+$ is the usual group operation. We now can test associativity:

$$\begin{aligned}(P \boxplus Q) \boxplus R &= -((P \boxplus Q) + R) = -(-(P + Q) + R) = P + Q - R \\ P \boxplus (Q \boxplus R) &= -(P + (Q \boxplus R)) = -(P - (Q + R)) = -P + Q + R\end{aligned}$$

Subtracting these tells us that are only equal if and only if $2(P-R) = 0$. As long as the elliptic curve has some element P^* with order more than 2, $(P^* \boxplus \infty) \boxplus \infty = P^*$ while $P^* \boxplus (\infty \boxplus \infty) = -P^* \neq P^*$. Hence, in this case, $\boxplus$ will not be associative.

(d) In any elliptic curve where all points have order 2 or less, $P \boxplus Q = -(P + Q) = P + Q$, so $\boxplus$ is associative. A trivial example is when the elliptic curve has no finite solutions, as in $y^2 + y = x^3 + x + 1$ over $\mathbb{F}_2$. A more interesting example is $y^2 = x^3 - x$ over $\mathbb{F}_3$. Here, the only finite solutions are $(x, 0)$ for $x = -1, 0, 1$. $(x, 0)$ has order 2 (Problem 4a), so $\boxplus$ defines a group law.

6. We could solve this problem by showing that, if (x_1, y_1) satisfies the equation for an elliptic curve, then so does $(x_1, -a_1x_1 - a_3 - y_1)$. However, this would result in messy algebra. A simpler way is to observe that we are trying to compute an intersection (x_2, y_2) of the vertical line through (x_1, y_1) (that is, the line $x = x_1$) and the curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Clearly, $x_2 = x_1$. Now, combine the equations for the line and the curve to eliminate x, giving:

$$0 = y^2 + (a_1x + a_3)y - (x_1^3 + a_2x_1^2 + a_4x_1 + a_6) \tag{5}$$

We already have one solution, namely y_1. Thus, this expressions factors as

$$0 = (y - y_1)(y - y_2)$$

Where y_2 is the second solution and the one we are interested in. Expanding this factorization gives

$$0 = y^2 - (y_1 + y_2)y + y_1y_2$$

Compairing the linear terms of this and 5 tells us $a_1x + a_3 = -(y_1 + y_2)$, which gives $y_2 = -a_1x - a_3 - y_1$. Hence $(x_2, y_2) = (x_1, -a_1x_1 - a_3 - y_1)$ is the other point on the elliptic curve with x coordinate x_1, so it is the inverse of (x_1, y_1).

7. We will adapt section 2.5.2 or Washington to our needs. Since $x^3 + y^3 = d \neq 0$, and $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$, $x + y \neq 0$. Hence, we can write

$$\begin{aligned} x &= u + v \\ y &= u - v \end{aligned}$$

This gives us:

$$d = x^3 + y^3 = 2u^3 + 6uv^2$$

Dividing by $6^3d^2/u^3$ (which is possible since $u = (x + y)/2 \neq 0$) gives:

$$\frac{(6d)^3}{u^3} = 2 \times 6^3 d^2 + (6^2 dv/u)^2$$

Now we can write $x_1 = \frac{6d}{u}$ and $y_1 = \frac{36dv}{u}$ to get

$$y_1^2 = x_1^3 - 432d^2$$

8. (a) If (x, y) satisfies $y^2 = x^3 + Ax + B$, then $(-y)^2 = y^2 = x^3 + Ax + B$, so $(x, -y)$ satisfies the equation as well. The map $(x, y) \to (x, -y)$ is thus a linear map from the curve to itself, and it is invertible (since it is its own inverse). Therefore, it is an automorphism.

   (b) If (x, y) satisfies $y^2 = x^3 + B$, then $(-y)^2 = y^2 = x^3 + B = \zeta^3 x^3 + B = (\zeta x)^3 + B$, so $(\zeta x, -y)$ satisfies the equation as well. Composing the map $(x, y) \to (\zeta x, -y)$ with itself 6 times yields the identity transformation, so this map is invertible. It is also linear, meaning it is an automorphism on the elliptic curve.

   (c) If (x, y) satisfies $y^2 = x^3 + Ax$, then $(iy)^2 = -y^2 = -x^3 - Ax = (-x)^3 + A(-x)$, so $(-x, iy)$ satisfies the euqation as well. Composing the map $(x, y) \to (-x, iy)$ with itself 4 times yields the identity transformation, so this map is invertible. It is also linear, meaning it is an automorphism on the elliptic curve.

9.

```
K=GF(2)
E1=EllipticCurve(K,[0,0,1,0,0])
E2=EllipticCurve(K,[0,0,1,0,1])
E3=EllipticCurve(K,[0,0,1,1,0])
isomorphisms=sage.schemes.elliptic_curves.weierstrass_morphism.isomorphisms
isomorphisms(E2,E1); isomorphisms(E3,E1)
```

```
[(1, 1, 1, 0), (1, 1, 1, 1)]
[]
```

This means that, for E_1 and E_2, we have the following isomorphisms over $\mathbb{F}_2$:

$$(x, y) \to (u^2 x + r, u^3 y + su^2 x + t)$$

Where (u, r, s, t) is either $(1, 1, 1, 0)$ or $(1, 1, 1, 1)$. Note that a more verbose version of this Sage output can also be obtained by the command `E2.isomorphisms(E1)`. This gives us two isomorphisms:

$$\phi_1(x, y) = (x + 1, y + x)$$

$$\phi_2(x, y) = (x + 1, y + x + 1)$$

Since we are in characteristic 2, it turns out that the inverse of ϕ_1 is given by the same equations as ϕ_2, and vice versa. Therefore, ϕ_i are invertible. You can also check that they are indeed maps between E_1 and E_2. Therefore, these are isomorphisms.

The case for E_1 to E_3 yeilds no results. This is because there are no isomorphisms within $\mathbb{F}_2$, so we will need an extension field. If we change to the following commands:

```
K=GF(2^8,'a')
E1=EllipticCurve(K,[0,0,1,0,0])
E2=EllipticCurve(K,[0,0,1,0,1])
E3=EllipticCurve(K,[0,0,1,1,0])
isomorphisms=sage.schemes.elliptic_curves.weierstrass_morphism.isomorphisms
isomorphisms(E2,E1); isomorphisms(E3,E1)
```

We will get, in addition to many more isomorphisms for E_1 to E_2, several isomorphisms for E_1 to E_3. One of them is:

$$(u, r, s, t, u) = (1, a^6 + a^3 + a^2 + a, a^7 + a^4 + a^3, a^7 + a^6 + a^2)$$

Where a is a generator for $\mathbb{F}_{2^8}$. This corresponds to the transformation

$$(x, y) \to (x + a^6 + a^3 + a^2 + a, y + (a^7 + a^4 + a^3)x + a^7 + a^6 + a^2)$$

This begs the question: why do we need $\mathbb{F}_{2^8}$? To understand why, we will start with the general form for an isomorphism, and derive what the coefficients need to be:

$$\phi(x, y) = (ax + b, cy + dx + e)$$

With $a, c \neq 0$. For this to satisfy the equation for E_3, we must have:

$$(cy + dx + e)^2 + (cy + dx + e) = (ax + b)^3 + (ax + b)$$

Now we will expand the left side and replace y^2 with $x^3 - y$ (since (x, y) is a point on E_1):

$$c^2(x^3 - y) + d^2x^2 + e^2 + cy + dx + e = (ax + b)^3 + (ax + b)$$

This equation must hold for all x and y in the $\overline{\mathbb{F}_2}$, Thus, the coefficients of each term must be identical. This yields the following equations:

$$\begin{aligned}
x^3 : \quad & c^2 && = a^3 && (6)\\
x^2 : \quad & d^2 && = a^2 b && (7)\\
x : \quad & d && = ab^2 + a && (8)\\
y : \quad & c^2 + c && = 0 && (9)\\
1 : \quad & e^2 + e && = b^3 + b && (10)
\end{aligned}$$

Equation 9 tells us $c = 1$ (since $c \neq 0$). Eliminating d from 7 and 8 gives us:

$$a^2 b = a^2(b^4 + 1)$$

Since $a \neq 0$, this gives us $b^4 + b + 1 = 0$. 10 lets us determine e from b. Thus, the general form of an isomorphism from E_1 to E_3 is:

$$\phi(x, y) = (ax + b, y + a(b^2 + 1)x + e)$$

Where $a^3 = 1$, $b^4 + b + 1 = 0$, and $e^2 + e = b^3 + b$. If we pick $a = 1$, all we need is an extension field containing b and e. b will lie in $\mathbb{F}_{2^4}$ since it is a solution to a quartic equation with coefficients in $\mathbb{F}_2$. e will then lie in $\mathbb{F}_{2^8} = \mathbb{F}_{(2^4)^2}$ since it is a solution to a quadratic equation with coefficients in $\mathbb{F}_{2^4}$.

10. (a) It is not hard to see that this map is invertible: the inverse map is given by

$$(x, y) \to \left(\frac{x + s^2}{u^2}, y + sx + s^3 + t\right)$$

All that remains to check is that it takes an element in E to another element in E. We will do this as part of part (b).

(b) We will follow a procedure similar to that of question 9, and start with a general automorphism:

$$\phi(x, y) = (ax + b, cy + dx + e)$$

This is invertible as long as $a, c \neq 0$. Now we use the fact that the automorphism maps points on the curve to points on the curve to derive constraints on our variables: if $y^2 + y = x^3$, then

$$(cy + dx + e)^2 + (cy + dx + e) = (ax + b)^3$$

Now we expand the left side and use the fact that $y^2 = x^3 - y$ to simplify:

$$c^2(x^3 - y) + d^2x^2 + e^2 + cy + dx + e = (ax + b)^3$$

This map takes points on the curve to points on the curve if and only if all the coefficients are equal. Thus we get:

$$x^3 : \quad c^2 = a^3 \tag{11}$$
$$x^2 : \quad d^2 = a^2b \tag{12}$$
$$x : \quad d = ab^2 \tag{13}$$
$$y : \quad c^2 + c = 0 \tag{14}$$
$$1 : \quad e^2 + e = b^3 \tag{15}$$

Since $c \neq 0$, 14 tells us $c = 1$. Thus $a^3 = 1$ according to 11. Let us rewrite $u = a^2$. Then $u^2 = a^4 = a$ and $u^3 = a^6 = 1$. Combining 12 and 13 gives us $a^2b = a^2b^4$, which is equivalent to $b^4 + b = 0$. Let us define $s = b^2$. Then $s^2 = b^4 = b$, and $s^4 + s = b^8 + b^2 = b^2 + b^2 = 0$. Observe that $d = ab^2 = u^2s$. Lastly, 15 tells us that $e^2 + e = b^3 = s^6$. rewriting $t = e$ gives us:

$$\phi(x, y) = (u^2x + s^2, y + u^2sx + t)$$

Where $u^3 = 1$, $s^4 + s = 0$, and $t^2 + t = s^6$, as desired. We have also shown that, if the map satisfies this form, it will take points on the curve to points on the curve, meaning it is an automorphism.

We can now count the number of automorphisms. There are 3 different values for u (since it satisfies a cubic equation with distinct roots), each giving a different automorphism (since a will be different). There are also 4 different values for s (since it satisfies a quartic equation with distinct roots), each giving a different automorphism (since for fixed a, different s will give different d). Lastly, for fixed s, there are two values for t, since it satisfies a quadratic equation with distinct roots (check that the discriminant of $t^2 + t = s^6$ is non-zero). Thus each root gives a different automorphism. Since all automorphisms arise in this way, we have $3 \times 4 \times 2 = 24$ automorphisms.

(c) First, look at the general form of ϕ^2:

$$\phi^2(x, y) = (ux + (u^2 + 1)s^2, y + (u + 1)usx + s^3u^2)$$

If $u = 1$, this simplifies to

$$\phi^2(x, y) = (x, y + s^3)$$

If $s = 0$, then this is the identity. Otherwise, $s^3 = 1$, so this is the map taking a point to its inverse. If $u \neq 1$, let's look at ϕ^3:

$$\phi^3(x, y) = (x + (u^2 + u + 1)s^2, y + (u^2 + u + 1)sx + s^3u + t)$$

Since $u \neq 1$, $u^2 + u + 1 = 0$, giving:

$$\phi^3(x, y) = (x, y + s^3u + t)$$

Since we know this map outputs points on the curve, and the point shares an x coordinate with the original point, this output must be either the original point or its inverse. Hence $s^3u + t = 0, 1$, and thus ϕ^3 is ± 1.

(d) To show that this group is non-abelian, we just need to find an example of two automorphisms that do not commute. There are plenty of examples. For one, let $u_1 = u_2 = 1$, and let s_1 and s_2 be two distinct non-zero roots of $s^4 + s = 0$. Then if $\phi_i(x, y) = (x + s_i^2, y + s_ix + t_i)$, we have

$$\begin{aligned} \phi_1\phi_2(x, y) &= (x + s_1^2 + s_2^2, y + s_2x + t_2 + s_1(x + s_2^2) + t_1) \\ \phi_2\phi_1(x, y) &= (x + s_2^2 + s_1^2, y + s_1x + t_1 + s_2(x + s_1^2) + t_2) \end{aligned}$$

These are the same if and only if $s_2s_1^2 = s_1s_2^2$. Since s_1, s_2 were assumed to be non-zero, this is equivalent to $s_1 = s_2$, which we assumed false. Hence these two automorphisms do not commute.

Another way to show that this group is non-abelian is a proof by contradiction, using the fact that, as shown in part (c), there is an element of order 4 (the one

whose square is -1), but none of order higher than 6. If the group were abelian, by the fundamental theorem of abelian groups, we could decompose it as

$$\mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_\ell}$$

Where $r_i | r_{i+1} \forall i$. There are only 3 possibilities:

$$\begin{aligned} G_1 &= \mathbb{Z}_{24} \\ G_2 &= \mathbb{Z}_2 \times \mathbb{Z}_{12} \\ G_3 &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \end{aligned}$$

G_1 and G_2 have elements of order larger than 6, so they are not right. In G_3, all elements have order at most 6, but there are no elements of order 4. Hence none of the possible abelian groups of order 24 match the automorphism group, so the automorphism group is non-abelian.