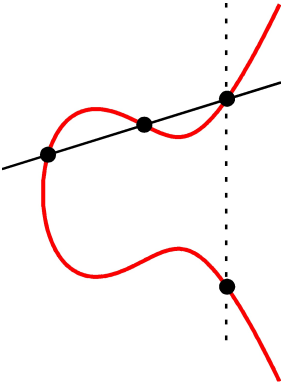
Elliptic Curve Cryptography Fundamentals



Elliptic Curves

- An elliptic curve is the solution set of a nonsingular cubic polynomial equation in two unknowns over a field $\mathcal{F}$

$$\mathcal{E} = \{(x, y) \in \mathcal{F} \times \mathcal{F} \mid f(x, y) = 0\}$$

- The general equation of a cubic in two variables is given by

$$ax^3 + by^3 + cx^2y + dxy^2 + ex^2 + fy^2 + gxy + hx + iy + j = 0$$

- When $\text{char}(\mathcal{F}) \neq \{2, 3\}$, the **short Weierstrass** form is useful in cryptography

$$y^2 = x^3 + ax + b$$

- Also, the **Edwards** curves and **Montgomery** curves are useful in cryptography

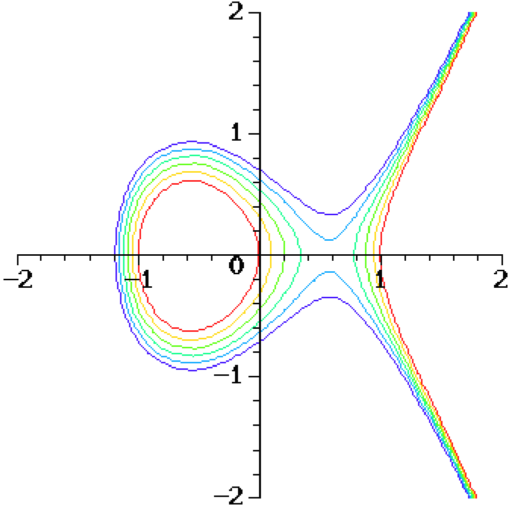
Elliptic Curves over $\mathcal{R}$

- The field in which this equation solved can be an infinite field, such as $\mathcal{C}$ (complex numbers), $\mathcal{R}$ (real numbers), or $\mathcal{Q}$ (rational numbers)
- Since

$$\lim_{x \to \infty} y = \infty$$

  The **point at infinity** written as $\mathcal{O} = (\infty, \infty)$ is also considered as one of the solutions of the equation
- The elliptic curves over $\mathcal{R}$ for different values of a and b make continuous curves on the plane, which have either one or two parts

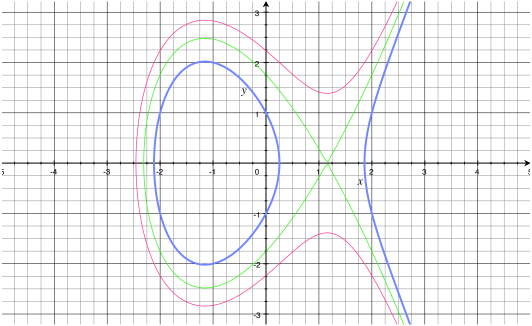
Elliptic Curves over $\mathcal{R}$



Elliptic Curves over $\mathcal{R}$

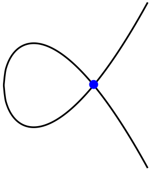
- When the discriminant $\Delta = 4a^3 + 27b^2 = 0$, the curve is **singular**

- $\Delta = 419 > 0$ for $a = -4$ and $b = 5$ (red, smooth)
- $\Delta = -229 < 0$ for $a = -4$ and $b = 1$ (blue, smooth)
- $\Delta = 0$ for $a = -4$ and $\sqrt{256/27} = 3.079201$ (green, singular)

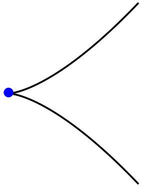


Singular vs Smooth Curves over $\mathcal{R}$

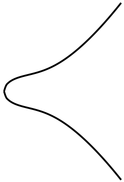
$\Delta = 4a^3 + 27b^2 = 0$ for singular curves



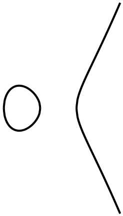
Singular curve
$y^2 = x^3 - 3x + 2$
over $\mathcal{R}$
$\Delta = 0$



Singular curve
$y^2 = x^3$
over $\mathcal{R}$
$\Delta = 0$

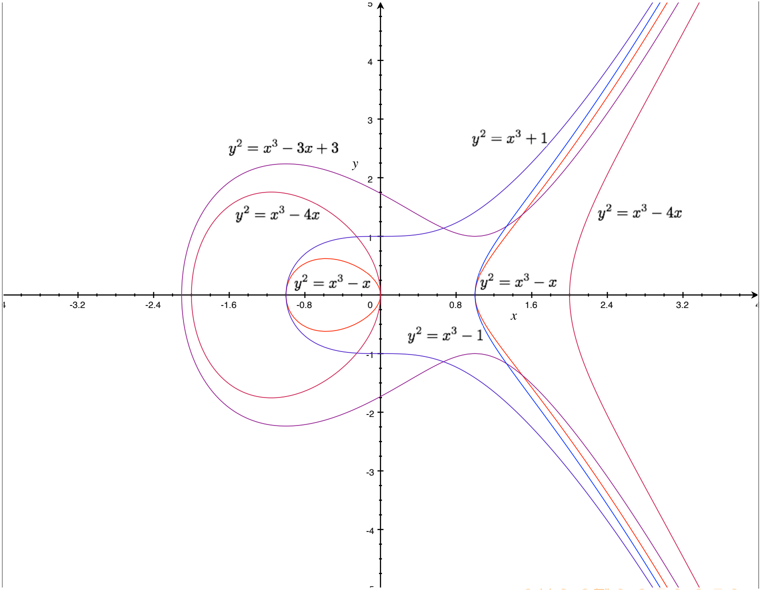


Smooth curve
$y^2 = x^3 + x + 1$
over $\mathcal{R}$
$\Delta = 31$



Smooth curve
$y^2 = x^3 - x$
over $\mathcal{R}$
$\Delta = -4$

Elliptic Curves over $\mathcal{R}$



Bezout Theorem

Theorem

A line that intersects an elliptic curve at 2 points crosses at a third point.

- Consider the elliptic curve and the linear equation together:

$$\begin{aligned} y^2 &= x^3 + ax + b \\ y &= cx + d \end{aligned}$$

- Substituting y from the second equation to the first one, we obtain a cubic equation in x

$$x^3 + ax + b = (cx + d)^2$$

Elliptic Curve Chord

- This is simplified as

$$x^3 - c^2x^2 + (a - 2cd)x + (b - d^2) = 0$$

- This is a cubic equation in x with real coefficients
- A cubic equation with real coefficients has either:
  - 1 real and 2 complex (conjugate) roots, or
  - 3 real roots
- Since we already have 2 real points on the curve (2 real roots), the third point must be real too

Elliptic Curve Chord with Line $y = x$

- For example, by solving $y^2 = x^3 - 4x$ with the linear equation $y = x$ together, we find $x^3 - 4x = x^2$, and thus

$$x(x^2 - x - 4) = 0$$

- This equation has 3 solutions: $x = 0$, $x = \frac{1-\sqrt{17}}{2}$, and $x = \frac{1+\sqrt{17}}{2}$
- By evaluating the elliptic curve equation $y^2 = x^3 - 4x$ at these x values, we find the solution points as

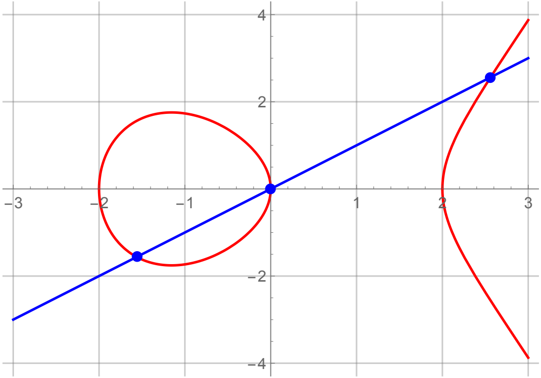
$$\left(\tfrac{1}{2}(1-\sqrt{17}),\ \sqrt{\tfrac{1}{2}(9-\sqrt{17})}\right),\ \ (0,\ 0),\ \ \left(\tfrac{1}{2}(1+\sqrt{17}),\ \sqrt{\tfrac{1}{2}(9+\sqrt{17})}\right)$$

- Approximate values of the points are

$$(-1.56155, -1.56155), \quad (0, 0), \quad (2.56155, 2.56155)$$

Elliptic Curve Chord with Line $y = x$

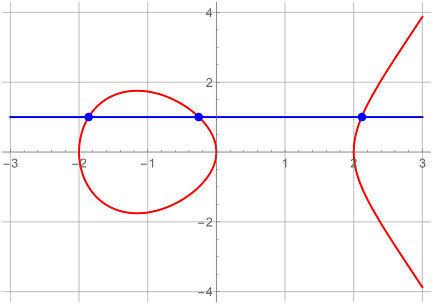
- This graph shows the elliptic curve equation $y^2 = x^4 - 4x$, the line $y = x$, and their 3 intersections



Elliptic Curve Chord with Line $y = 1$

- By solving $y^2 = x^3 - 4x$ with the linear equation $y = 1$ together, we find $x^3 - 4x = 1$, and thus $x^3 - 4x - 1 = 0$
- This equation in x has 3 solutions and their approximate values are $x = -1.86081$, $x = -0.254102$, and $x = 2.11491$
- Approximate values of the points are

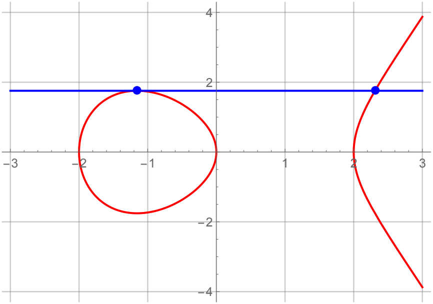
$$(-1.86081,\ 1),\ \ (-0.254102,\ 1),\ \ (2.11491,\ 1)$$



Elliptic Curve Chord with Line $y = 4/(27)^{1/4} = 1.75477$

- By solving $y^2 = x^3 - 4x$ with the linear equation $y = 4/(27)^{1/4}$ together, we obtain $x^3 - 4x - 16/\sqrt{27} = 0$
- This equation in x has 2 repeated solutions and 1 other solution as $-2/\sqrt{3}$, $-2/\sqrt{3}$, and $4/\sqrt{3}$
- Their approximate values of the points are

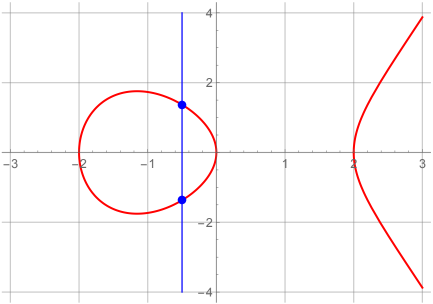
$$(-1.1547,\ 1.75477),\ \ (-1.1547,\ 1.75477),\ \ (2.3094,\ 1.75477)$$



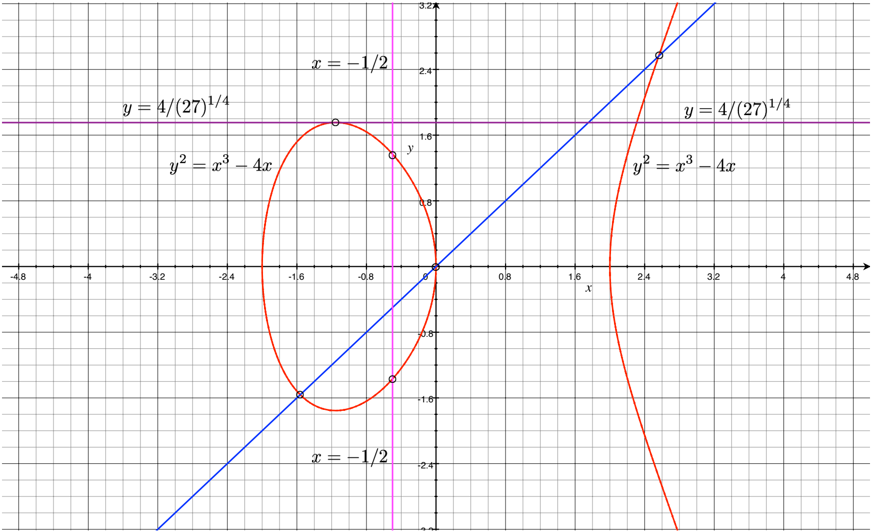
Elliptic Curve Chord with Line $x = -1/2$

- By solving $y^2 = x^3 - 4x$ with the linear equation $x = -1/2$ together, we obtain $y^2 = -1/8 + 2 = 15/8$
- Solving for y, we find the two points

$$(-1/2, -\sqrt{15/8}), \quad (-1/2, \sqrt{15/8})$$



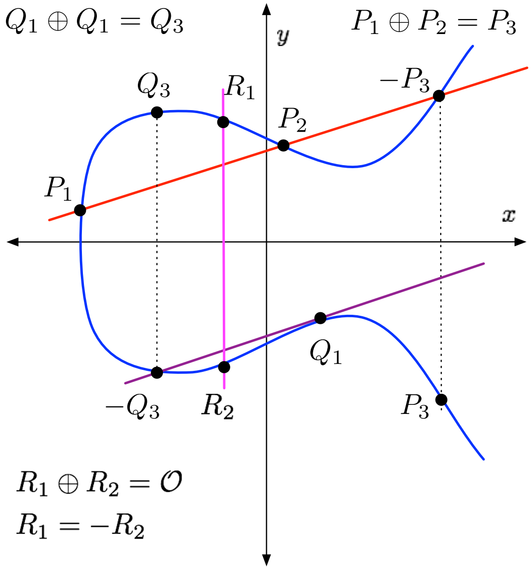
Elliptic Curve Chord and Tangent



Weierstrass Curve Chord-and-Tangent Rule

- The Weierstrass curves has a chord-and-tangent rule for adding two points on the curve to get a third point
- Together with this addition rule, the set of points on the curve forms an Abelian additive group in which the point at infinity is the zero element of the group
- The point at infinity, denoted as $\mathcal{O}$ is also a solution of the Weierstrass equation $y^2 = x^3 + ax + b$
- The best way to explain the addition rule is to use geometry over $\mathcal{R}$

Weierstrass Curve Point Addition



Weierstrass Curve Point Addition

- The "point addition" is a geometric operation: a linear line that connects P_1 and P_2 also crosses the elliptic curve at a third point, which we will name as $-P_3$
- The new "sum" point $P_3 = P_1 \oplus P_2$ is the mirror image of $-P_3$ with respect to the x axis:

$$\text{if} \quad P_3 = (x_3, y_3) \quad \text{then} \quad -P_3 = (x_3, -y_3)$$

- The point at infinity $\mathcal{O}$ acts as the neutral (zero) element

$$\begin{aligned} P \oplus \mathcal{O} &= \mathcal{O} \oplus P = P \\ P \oplus (-P) &= (-P) \oplus P = \mathcal{O} \end{aligned}$$

Weierstrass Curve Point Addition

- The addition rule for $P_3 = P_1 \oplus P_2$ can be algebraically obtained by first computing the slope m of the straight line that connects $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ using

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

- In the case of doubling $Q_3 = Q_1 \oplus Q_1 = (x_1, y_1) \oplus (x_1, y_1)$, the slope m of the linear line is equal to the derivative of the elliptic curve equation $y^2 = x^3 + ax + b$ evaluated at point x_1 as

$$2yy' = 3x^2 + a \quad \rightarrow \quad y' = \frac{3x^2 + a}{2y} \quad = \quad m$$

Weierstrass Curve Point Addition

- Once the slope m is obtained, the linear equation can be written, and solved together with the elliptic curve equation to find x_3 and y_3
- Since the slope is m, and the linear line goes through (x_1, y_1), its equation would be of the form

$$y - y_1 = m(x - x_1)$$

- Therefore, the new coordinates of new point (x_3, y_3) can be obtained by solving these two equations together

$$\begin{aligned} y^2 &= x^3 + ax + b \\ y &= m(x - x_1) + y_1 \end{aligned}$$

Weierstrass Curve Point $P_3 = P_1 \oplus P_2$

- If $P_1 = \mathcal{O}$, then $P_3 = \mathcal{O} \oplus P_2 = P_2$
- If $P_2 = \mathcal{O}$, then $P_3 = P_1 \oplus \mathcal{O} = P_1$
- If $P_2 = -P_1$, then $P_3 = P_1 \oplus (-P_1) = \mathcal{O}$
- Otherwise, first compute the slope using

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{for } \; x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{for } \; x_1 = x_2 \text{ and } y_1 = y_2 \end{cases}$$

- Then, (x_3, y_3) is computed using

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m\,(x_1 - x_3) - y_1 \end{aligned}$$

Elliptic Curves over Finite Fields

- The field in which the Weierstrass equation solved can also be a finite field, which is of interest in cryptography
- Most common cases of finite fields are:
  - Characteristic p: GF(p), where p is a large prime
  - Characteristic 2: GF(2^k), where k is a small prime
  - Characteristic p: GF(p^k), where p and k are small primes

Elliptic Curves over GF(p)

- In GF(p) for a prime $p \neq 2, 3$, we can use the Weierstrass equation

$$y^2 = x^3 + ax + b$$

  with the understanding that the solution of this equation and all field operations are performed in the finite field GF(p)
- We will denote this group by $\mathcal{E}(a, b, p)$

An Elliptic Curve over GF(23)

- Consider the elliptic curve group $\mathcal{E}(1, 1, 23)$: The solutions of the equation with $a = 1$ and $b = 1$

$$y^2 = x^3 + x + 1$$

  over the finite field GF(23)
- We will obtain the elements of the group by solving this equation in GF(23) for all values of $x \in \mathcal{Z}_{23}^*$

An Elliptic Curve over GF(23)

- As we give a particular value for x, we obtain a quadratic equation in y modulo 23, whose solution will depend on whether the right hand side is a QR mod 23
- If (x, y) is a solution, so is $(x, -y)$ because $y^2 = (-y)^2$, i.e., the elliptic curve is symmetric with respect to the x axis

An Elliptic Curve over GF(23)

- Starting with $x = 0$, we get $y^2 = 1 \pmod{23}$ which immediately gives two solutions as $(0, 1)$ and $(0, -1) = (0, 22)$

An Elliptic Curve over GF(23)

- Similarly, for $x = 1$, we obtain $y^2 = 3 \pmod{23}$
- This is a quadratic equation, the solution will depend on whether 3 is a quadratic residue (QR)
- Euler's test shows that 3 is a QR

$$3^{(p-1)/2} = 3^{11} = 1 \pmod{23}$$

- When $p = 3 \pmod 4$, the solution for y can be found using

$$y = 3^{(p+1)/4} = 3^6 = 16 \pmod{23}$$

- For $x = 1$, we find a pair of solutions: $(1, 16)$, $(1, -16) = (1, 7)$

An Elliptic Curve over GF(23)

- For $x = 2$, we have $y^2 = 2^3 + 2 + 1 = 11 \pmod{23}$
- However, 11 is a quadratic non-residue (QNR) since

$$11^{(p-1)/2} = 11^{11} = -1 \pmod{23}$$

- There is no solution for $y^2 = 11 \pmod{23}$
- This elliptic curve does not have a point whose x coordinate is 2

An Elliptic Curve over GF(23)

- For $x = 3$, we have $y^2 = 3^3 + 3 + 1 = 31 = 8 \pmod{23}$
- 8 is a QR since

$$8^{(p-1)/2} = 8^{11} = 1 \pmod{23}$$

- We solve for $y^2 = 8 \pmod{23}$ using

$$y = 8^{(p+1)/4} = 8^6 = 13 \pmod{23}$$

- We obtain the pair of coordinates: $(3, 13)$, $(3, -13) = (3, 10)$

An Elliptic Curve over GF(23)

- Proceeding for the other values of $x \in \mathcal{Z}_{23}^*$, we find 27 solutions:

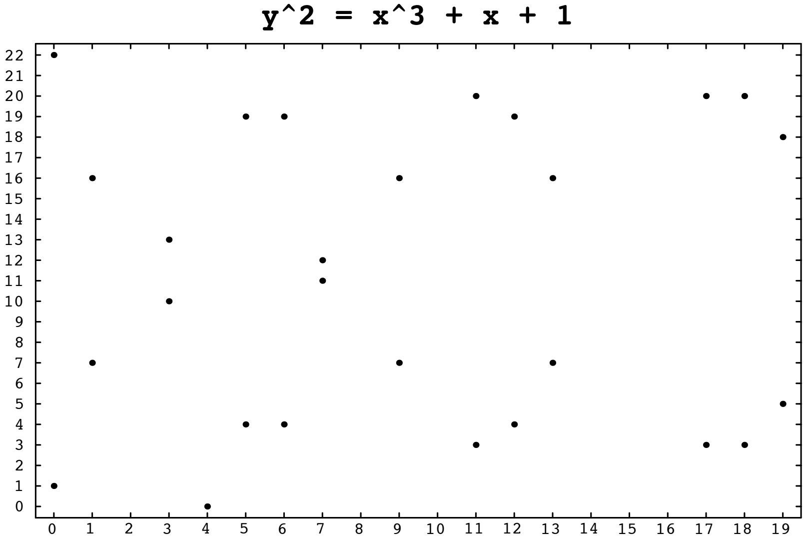
$$
\begin{array}{ccccccc}
(0,1) & (0,22) & (1,7) & (1,16) & (3,10) & (3,13) & (4,0) \\
(5,4) & (5,19) & (6,4) & (6,19) & (7,11) & (7,12) & \\
(9,7) & (9,16) & (11,3) & (11,20) & (12,4) & (12,19) & \\
(13,7) & (13,16) & (17,3) & (17,20) & (18,3) & (18,20) & \\
(19,5) & (19,18) & & & & &
\end{array}
$$

- The solutions come in pairs (x, y) and $(x, -y)$
- Except one of them is alone: $(4, 0)$
- For $x = 4$, we have

$$y^2 = 4^3 + 4 + 1 = 69 = 0 \pmod{23}$$

which has only one solution $y = 0$ and thus one point $(4, 0)$

An Elliptic Curve over GF(23)



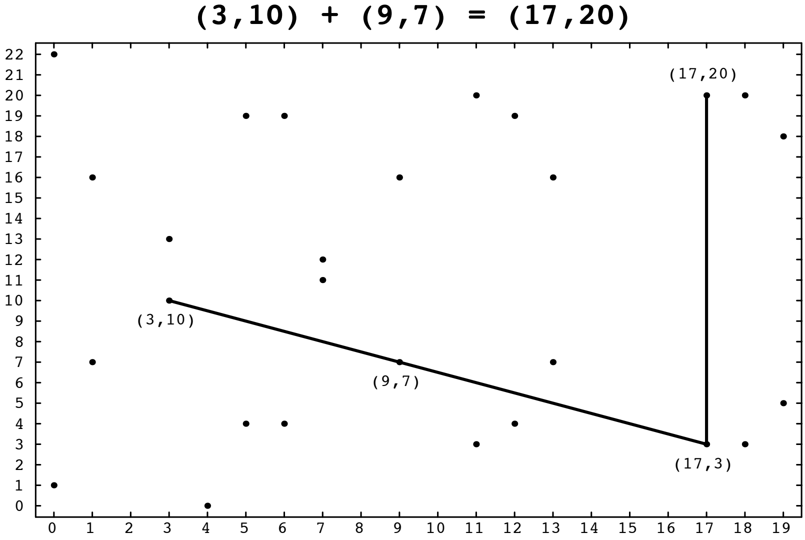
Elliptic Curve Point Addition over GF(23)

- Given $P_1 = (3, 10)$ and $P_2 = (9, 7)$, compute $P_3 = P_1 \oplus P_2$
- Since $x_1 \neq x_2$, we have

$$
\begin{aligned}
m &= (y_2 - y_1) \cdot (x_2 - x_1)^{-1} \pmod{23} \\
&= (7 - 10) \cdot (9 - 3)^{-1} = (-3) \cdot 6^{-1} = 11 \pmod{23} \\
x_3 &= m^2 - x_1 - x_2 \pmod{23} \\
&= 11^2 - 3 - 9 \;=\; 17 \pmod{23} \\
y_3 &= m\,(x_1 - x_3) - y_1 \pmod{23} \\
&= 11 \cdot (3 - 17) - 10 \;=\; 20 \pmod{23}
\end{aligned}
$$

- Thus, we have $(x_3, y_3) = (3, 10) \oplus (9, 7) = (17, 20)$
- Question: Is the geometry of point addition still valid?

Elliptic Curve Point Addition over GF(23)



Elliptic Curve Point Doubling over GF(23)

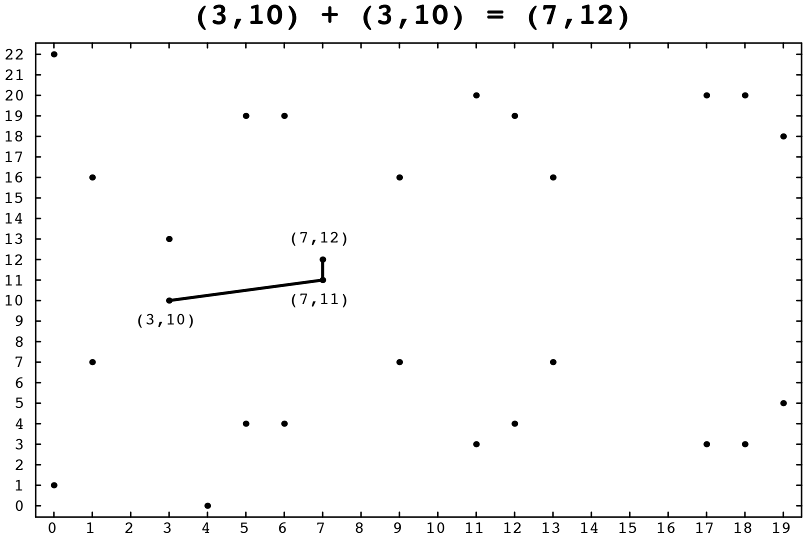
- Given $P_1 = (3, 10)$, compute $P_3 = P_1 \oplus P_1$
- Since $x_1 = x_2$ and $y_1 = y_2$, we have

$$
\begin{aligned}
m &= (3x_1^2 + a) \cdot (2y_1)^{-1} \pmod{23} \\
&= (3 \cdot 3^2 + 1) \cdot (20)^{-1} \pmod{23} \\
&= 6 \\
x_3 &= m^2 - x_1 - x_2 \pmod{23} \\
&= 6^2 - 3 - 3 \pmod{23} \\
&= 7 \\
y_3 &= m\,(x_1 - x_3) - y_1 \pmod{23} \\
&= 6 \cdot (3 - 7) - 10 \pmod{23} \\
&= 12
\end{aligned}
$$

Elliptic Curve Point Doubling over GF(23)

- Thus, we have $(x_3, y_3) = (3, 10) \oplus (3, 10) = (7, 12)$
- Question: Is the geometry of point doubling still valid?

Elliptic Curve Point Doubling over GF(23)



Elliptic Curve Point Multiplication

- The elliptic curve point multiplication operation takes an integer k and a point on the curve P, and computes

$$[k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ terms}}$$

- This can be accomplished with the binary method, using the binary expansion of the integer $k = (k_{m-1} \cdots k_1 k_0)_2$
- For example $[17]P$ is computed using the addition chain

$$P \xrightarrow{d} [2]P \xrightarrow{d} [4]P \xrightarrow{d} [8]P \xrightarrow{d} [16]P \xrightarrow{a} [17]P$$

- The symbol $\xrightarrow{d}$ stands for doubling, such as $[2]P \oplus [2]P = [4]P$
- The symbol $\xrightarrow{a}$ stands for addition, such as $P \oplus [16]P = [17]P$

Number of Points on an Elliptic Curve

- The elliptic curve group $\mathcal{E}(1,1,23)$ had the following elements:

$$\begin{array}{ccccccc}
(0,1) & (0,22) & (1,7) & (1,16) & (3,10) & (3,13) & (4,0) \\
(5,4) & (5,19) & (6,4) & (6,19) & (7,11) & (7,12) & \\
(9,7) & (9,16) & (11,3) & (11,20) & (12,4) & (12,19) & \\
(13,7) & (13,16) & (17,3) & (17,20) & (18,3) & (18,20) & \\
(19,5) & (19,18) & & & & &
\end{array}$$

- There are 27 points in the above list
- Including the point at infinity $\mathcal{O}$, the elliptic curve group $\mathcal{E}(1,1,23)$ has $27+1=28$ elements
- The order of the group $\mathcal{E}(1,1,23)$ is 28

Order of Elliptic Curve Groups

- In order to use an elliptic curve group $\mathcal{E}$ in cryptography, we need to know the order of the group, denoted as order($\mathcal{E}$)
- The order of $\mathcal{E}(a, b, p)$ is always less than $2p + 1$
- The finite field has p elements, and we solve the equation

$$y^2 = x^3 + ax + b$$

  for values of $x = 0, 1, \ldots, p - 1$, and obtain a pair of solutions (x, y) and $(x, -y)$ for every x, we can have no more than $2p$ points
- Including the point at infinity, the order is bounded as

$$\text{order}(\mathcal{E}(a, b, p)) \leq 2p + 1$$

- The order of $\mathcal{E}(1, 1, 23)$ is 28 which is less than $2 \cdot 23 + 1 = 47$

Order of Elliptic Curve Groups

- However, this bound is not very precise
- As we discovered in finding the elements of $\mathcal{E}(1, 1, 23)$, not every x value yields a solution of the quadratic equation $y^2 = x^3 + x + 1$
- For a solution to exists, $u = x^3 + ax + b$ needs to be a QR mod p
- Only half of the elements in GF(p) are QRs
- As x takes values in GF(p), depending on whether

$$u = x^3 + ax + b$$

  is a QR or QNR, we will have a solution for $y^2 = u \pmod{p}$ or not, respectively
- Therefore, the number of solutions will be less than $2p$

Order of Elliptic Curve Groups

- If we define $\chi(u)$ as

$$\chi(u) = \begin{cases} +1 & \text{if } u \text{ is QR} \\ -1 & \text{if } u \text{ is QNR} \end{cases}$$

  we can write the number of solutions to $y^2 = u \pmod{p}$ as $1 + \chi(u)$

- Therefore, we find the size of the group including $\mathcal{O}$ as

$$\begin{aligned} \text{order}(\mathcal{E}) &= 1 + \sum_{x \in \mathrm{GF}(p)} (1 + \chi(x^3 + ax + b)) \\ &= p + 1 + \sum_{x \in \mathrm{GF}(p)} \chi(x^3 + ax + b) \end{aligned}$$

  which is a function of $\chi(x^3 + ax + b)$ as x takes values in $\mathrm{GF}(p)$

Hasse Theorem

- As x takes values in GF(p), the value of $\chi(x^3 + ax + b)$ will be equally likely as $+1$ and -1
- This is a random walk where we toss a coin p times, and take either a forward and backward step
- According to the probability theory, the sum $\sum \chi(x^3 + ax + b)$ is of order $\sqrt{p}$
- More precisely, this sum is bounded by $2\sqrt{p}$
- Thus, we have a bound on the order of $\mathcal{E}(a, b, p)$, due to Hasse:

Theorem

The order of an elliptic curve group over GF(p) is bounded by

$$p + 1 - 2\sqrt{p} \leq order(\mathcal{E}) \leq p + 1 + 2\sqrt{p}$$

Order of Elements

- The order of an element P is the smallest integer k such that

$$[k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ terms}} = \mathcal{O}$$

- According to the Lagrange Theorem, the order of any point divides the order of the group
- The primitive element is defined as the element $P \in \mathcal{E}$ whose order $n = \text{order}(P)$ is equal to the group order

$$n = \text{order}(P) = \text{order}(\mathcal{E})$$

- According to the Hasse Theorem, we have

$$p + 1 - 2\sqrt{p} \leq \text{order}(\mathcal{E}(a, b, p)) \leq p + 1 + 2\sqrt{p}$$

Order of Elements

- For the group $\mathcal{E}(1,1,23)$, we have $\lceil\sqrt{23}\rceil = 5$, and the bounds are

$$14 \leq \text{order}(\mathcal{E}(1,1,23)) \leq 34$$

  Indeed, we found it as $\text{order}(\mathcal{E}(1,1,23)) = 28$
- According to the Lagrange Theorem, the element orders in $\mathcal{E}(1,1,23)$ can only be the divisors of 28 which are $1, 2, 4, 7, 14, 28$
- The order of a primitive element is 28
- The order of $\mathcal{O}$ is 1 since $[1]\mathcal{O} = \mathcal{O}$
- The order $(4,0)$ is 2 since $[2](4,0) = (4,0) \oplus (4,0) = \mathcal{O}$

Order of Elements

- Compute the order of the point $P = (11,3)$ in $\mathcal{E}(1,1,23)$

$$\begin{array}{rcccl} [2]P & = & (11,3) \oplus (11,3) & = & (4,0) \\ [3]P & = & (11,3) \oplus (4,0) & = & (11,20) \quad \leftarrow \end{array}$$

- Note that

$$[3]P = (11,20) = (11,-3) = -P$$

- This gives

$$[4]P = [3]P \oplus P = (-P) \oplus P = \mathcal{O}$$

- Therefore, the order of $(11,3)$ is 4

Order of Elements

- Compute the order of the point $P = (1,7)$ in $\mathcal{E}(1,1,23)$

$$\begin{array}{rclcll}
[2]P & = & (1,7) \oplus (1,7) & = & (7,11) & \\
[3]P & = & (1,7) \oplus (7,11) & = & (18,20) & \\
[4]P & = & (7,11) \oplus (7,11) & = & (17,20) & \\
[7]P & = & (18,20) \oplus (17,20) & = & (11,3) & \leftarrow \\
[14]P & = & (11,3) \oplus (11,3) & = & (4,0) & \\
[21]P & = & (11,3) \oplus (4,0) & = & (11,20) & \leftarrow
\end{array}$$

- Since the order of $(1,7)$ is not 2, or 7, or 14, it must be 28
- Indeed $(11,20)$ and $(11,3)$ are negatives of one another

$$[28]P = [7]P \oplus [21]P = (11,3) \oplus (11,-3) = \mathcal{O}$$

- Therefore, the order of $P = (1,7)$ is 28 and $(1,7)$ is primitive

Elliptic Curve Group Order

- One remarkable property of the elliptic curve groups is that the order n can be a prime number, while the multiplicative group $\mathcal{Z}_p^*$ order is always even: $p-1$
- When the group order is a prime, all elements of the group are primitive elements (except the neutral element $\mathcal{O}$ whose order is 1)
- As a small example, consider $\mathcal{E}(2,1,5)$: The equation

$$y^2 = x^3 + 2x + 1 \pmod{5}$$

has 6 finite solutions $(0,1)$, $(0,4)$, $(1,2)$, $(1,3)$, $(3,2)$, and $(3,3)$

- Including $\mathcal{O}$, this group has 7 elements, and thus, its order is a prime number and all elements (except $\mathcal{O}$) are primitive

Elliptic Curve Point Multiplication

- The elliptic curve point multiplication operation is the computation of the point $Q = [k]P$ given an integer k and a point on the curve P

$$Q = [k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ terms}}$$

- If the order of the point P is n, we have $[n]P = \mathcal{O}$
- Thus, the computation of $[k]P$ effectively gives

$$[k]P = [k \bmod n]P$$

- Similarly, we have

$$\begin{aligned} [a]P \oplus [b]P &= [a + b \bmod n]P \\ [a][b]P &= [a \cdot b \bmod n]P \end{aligned}$$

Elliptic Curve DLP

- Once we have a primitive element $P \in \mathcal{E}$ whose order n equal to the group order, we can execute the steps of the Diffie-Hellman key exchange algorithm using the elliptic curve group $\mathcal{E}$
- Diffie-Hellman works over any group as long as the DLP in that group is a difficult problem
- The Elliptic Curve DLP is defined as the computation of the integer k given P and Q such that

$$Q = [k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ terms}}$$

- The ECDLP requires an exhaustive search on the integer k
- No subexponential algorithm for the ECDLP exists as of yet

Elliptic Curve Diffie-Hellman

- A and B agree on the elliptic curve group $\mathcal{E}$ of order n and a primitive element $P \in \mathcal{E}$ (whose order is also n)
- This is done in public: $\mathcal{E}$, n, and P are known to the adversary
- A selects integer $a \in [2, n-1]$, computes $Q = [a]P$, and sends Q to B
- B selects integer $b \in [2, n-1]$, computes $R = [b]P$, and sends R to A
- A receives R, and computes $S = [a]R$
- B receives Q, and computes $S = [b]Q$

$$S = [a]R = [a][b]P = [a \cdot b \bmod n]P$$
$$S = [b]Q = [b][a]P = [b \cdot a \bmod n]P$$

Elliptic Curve Diffie-Hellman