The Arithmetic of Elliptic Curves: Final Exam

Wenhan Dai

To Thank Dr. Dao Van Thinh
for His Hard Work Throughout the Semester.

---

1. **Division Polynomials and the Multiplication Degrees.**

   Comment and Errata. Silverman's definition of ψ_2 and ω_m are not compatible with the results in (a) and (b), for an obvious example, $(2y)^{-1}\psi_2$ does not lie in the given polynomial ring. Some original statements have been revised in the following, and those correct descriptions are labeled by red color.

   This exercise includes a very horrible computation in (c) and (d), because we are working over a general field whose characteristic may be 2 and 3. Unfortunately, **neither the reduced Weierstrass form for elliptic curves nor complex analysis can be applied in our solution**. Not all of those details for calculations are given in the solution as follows. Some inspection is done by `SageMath`, which we choose to discard.

   This exercise gives an elementary, highly computational, proof that the multiplication-by-m map has degree m^2. Let E be given by the Weierstrass equation

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

   and let b_2, b_4, b_6, b_8 be the usual quantities. (If you're content to work with char $(K) \neq 2, 3$, you may find it easier to use the short Weierstrass form $E : y^2 = x^3 + Ax + B$.) We define division polynomials $\psi_m \in \mathbb{Z}[a_1, \dots, a_6, x, y]$ using initial values

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = 2y + a_1x + a_3,\\
&\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
&\psi_4 = \psi_2 \cdot (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),
\end{aligned}$$

   and then inductively by the formulas

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 && \text{for } m \geq 2,\\
\psi_2\psi_{2m} &= \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2 && \text{for } m \geq 3.
\end{aligned}$$

   Verify that ψ_m is a polynomial for all $m \geq 1$, and then define further polynomials ϕ_m and ω_m by

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
2\psi_2\omega_m &= \psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

   (a) Prove that if m is odd, then ψ_m, ϕ_m, and $\psi_2^{-1}\omega_m$ are polynomials in

$$\mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2],$$

   and similarly for $\psi_2^{-1}\psi_m$, ϕ_m, and ω_m if m is even. So replacing $(2y + a_1x + a_3)^2$ by $4x^3 + b_2x^2 + 2b_4x + b_6$, we may treat each of these quantities as a polynomial in $\mathbb{Z}[a_1, \dots, a_6, x]$.

Solution. By definition, it is true for $m \le 4$ that

$$\begin{aligned}\psi_1, \psi_3 &\in \mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2] = R,\\ \psi_2, \psi_4 &\in \psi_2\mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2] = \psi_2 R.\end{aligned}$$

We make inductive hypothesis that ψ_m lies in the first polynomial ring for odd $4 < m < 2n + 1$, and in the second for even $4 < m < 2n$. Under this assumption, note that $\psi_2^2 \in R$ and either $\psi_{n+2}\psi_n^3 \in \psi_2^4 R \subseteq R$ or $\psi_{n-1}\psi_{n+1}^3 \in \psi_2^4 R \subseteq R$, depending on the parity of n. For induction, let $m = 2n + 1 > 4$ be odd, then $2n + 1 > n + 2$ and $n \ge 2$, so

$$\psi_m = \psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \in R$$

since all ψ_k for $k \le n + 2$ satisfy the inductive hypothesis. On the other hand, let $m = 2n > 4$ be even, then $2n > n + 2$ and $n \ge 3$, hence

$$\psi_2^{-1}\psi_m = \psi_2^{-1}\psi_{2n} = \psi_2^{-2}(\psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2).$$

Now, if n is even then $\psi_{n-2}, \psi_n, \psi_{n+2} \in \psi_2 R$ whereas $\psi_{n-1} \in R$. Hence,

$$\psi_2^{-1}\psi_m \in \psi_2^{-2}\psi_2^2 R = \mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2].$$

Again, if n is odd, then $\psi_{n-1}^2, \psi_{n+1}^2 \in \psi_2^2\mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2]$. We get the same result as above.

Consider $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$. Similarly, either ψ_m^2 or $\psi_{m+1}\psi_{m-1}$ lies in $\psi_2^2 R$. So $\phi_m \in \mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2]$ for all m. As for ω_m, our claim is that there are two integers, say $r, s \in \mathbb{Z}$ such that

$$\begin{aligned}\psi_{2n+1} &\equiv (x^2 + rx + s)^{n^2+n} \quad \bmod 2,\\ \psi_{2n} &\equiv n\psi_2(x^2 + rx + s)^{n^2-1} \quad \bmod 2,\end{aligned}$$

which can be easily checked by induction on n. Thus,

$$\psi_{2n-1}^2\psi_{2n+2} - \psi_{2n-2}\psi_{2n+1}^2 \equiv 0 \bmod 2\psi_2.$$

This gives the result $\psi_2^{-1}\omega_m \in \mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2]$ for $m = 2n + 1$ and $\omega_m \in \mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2]$ for $m = 2n$.

(b) As polynomials in x, show that

$$\begin{aligned}\phi_m(x) &= x^{m^2} + (\text{lower order terms})\\ \psi_m(x)^2 &= m^2x^{m^2-1} + (\text{lower order terms})\end{aligned}$$

Solution. Let $T^0(f)$ denote the leading term of f as a polynomial to x.

Claim. For all m,

$$\begin{aligned}&T^0(\phi_m) = x^{m^2};\\ &T^0(\psi_{2n+1}) = (2n + 1)x^{2n^2+2n} \quad \text{if } m = 2n + 1,\\ &T^0(\psi_{2n}) = n\psi_2x^{2n^2-2} \quad \text{if } m = 2n.\end{aligned}$$

To prove this claim, the strategy is induction again, after checking the result is valid for $m \le 4$. Let the inductive hypothesis be true for odd $4 < m < 2n + 1$ and for even $4 < m < 2n$. Note that $T^0(\psi_2^2) = T^0(4y^2 + 4y(a_1x + a_3)) = 4x^3$, this will be used many times. Let's consider ϕ_m first.

(i) When $m = 2n$, we obtain

$$\begin{aligned} T^0(\phi_{2n}) &= T^0(x\psi_{2n}^2 - \psi_{2n+1}\psi_{2n-1}) \\ &= T^0(xn^2\psi_2^2 x^{4n^2-4} - (2n+1)x^{2n^2+2n}(2n-1)x^{2(n-1)^2+2(n-1)}) \\ &= T^0(n^2\psi_2^2 x^{4n^2-3} - (4n^2-1)x^{4n^2}) \\ &= 4n^2x^{4n^2} - (4n^2-1)x^{4n^2} = x^{4n^2}. \end{aligned}$$

(ii) When $m = 2n+1$, similarly,

$$\begin{aligned} T^0(\phi_{2n+1}) &= T^0(x\psi_{2n+1}^2 - \psi_{2n+2}\psi_{2n}) \\ &= T^0(x(2n+1)^2x^{4n^2+4n} - (n+1)\psi_2 x^{2(n+1)^2-2} n\psi_2 x^{2n^2-2}) \\ &= T^0((2n+1)^2x^{(2n+1)^2} - n(n+1)\psi_2^2 x^{4n^2+4n-2}) \\ &= (2n+1)^2x^{(2n+1)^2} - ((2n+1)^2-1)x^{(2n+1)^2} = x^{(2n+1)^2}. \end{aligned}$$

These deduce the claim for ψ_m. Under the inductive hypothesis, we then compute $T^0(\psi_m)$ in the following.

(i) Let $m \equiv 1 \bmod 4$, that is, $m = 2n+1$ for some even n. Thus,

$$\begin{aligned} T^0(\psi_{2n+1}) &= T^0(\psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3) \\ &= T^0((n+2)\psi_2 x^{(n^2+4n)/2} n^3 \psi_2^3 x^{(3n^2-12)/2} \\ &\quad - (n-1)x^{(n^2-2n)/2}(n+1)^3 x^{(3n^2+6n)/2}) \\ &= (n+2)n^3x^{2n^2+2n} - (n-1)(n+1)^3x^{2n^2+2n} = (2n+1)x^{2n^2+2n}. \end{aligned}$$

(ii) Let $m \equiv 2 \bmod 4$, that is, $m = 2n$ for some odd n. Therefore,

$$\begin{aligned} T^0(\psi_{2n}) &= T^0(\psi_2^{-1}(\psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2)) \\ &= (\psi_2)^{-1} n x^{(n^2-1)/2} (\frac{(n-1)^2\psi_2^2}{4} x^{(n-1)^2-4}(n+2)x^{(n^2+4n+3)/2} \\ &\quad - (n-2)x^{(n^2-4n+3)/2}\frac{(n+1)^2\psi_2^2}{4}x^{(n+1)^2-4}) \\ &= \frac{n\psi_2}{4}((n+2)(n-1)^2x^{2n^2-2} - (n-2)(n+1)^2x^{2n^2-2}) \\ &= \frac{n\psi_2}{4}((n+2)(n-1)^2 - (n-2)(n+1)^2)x^{2n^2-2} \\ &= n\psi_2 x^{2n^2-2}. \end{aligned}$$

(iii) Let $m \equiv 3 \bmod 4$, that is, $m = 2n+1$ with n odd. We have

$$\begin{aligned} T^0(\psi_{2n+1}) &= T^0(\psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3) \\ &= T^0((n+2)x^{(n^2+4n+3)/2} n^3 x^{(3n^2-3)/2} \\ &\quad - \psi_2(n-1)x^{(n^2-2n-3)/2}\psi_2^3(n+1)^3x^{(3(n+1)^2-12)/2}) \\ &= (n+2)n^3x^{2n^2+2n} - (n-1)(n+1)^3x^{2n^2+2n-6}(4x^3)^2 \\ &= (2n+1)x^{2n^2+2n}. \end{aligned}$$

(iv) Let $4 \mid m$, i.e. $m = 2n$ for some even n. This deduces

$$\begin{aligned}
T^0(\psi_{2n}) &= T^0(\psi_2^{-1}(\psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2)) \\
&= (\psi_2)^{-1}\frac{n\psi_2}{2}x^{(n^2-4)/2}((n-1)^2x^{(n-1)^2-1}\frac{(n+2)\psi_2}{2}x^{(n^2+4n)/2} \\
&\quad - \frac{(n-2)\psi_2}{2}x^{(n^2-4n)/2}(n+1)^2x^{(n+1)^2-1}) \\
&= \frac{n\psi_2}{4}((n+2)(n-1)^2 - (n-2)(n+1)^2)x^{2n^2-2} \\
&= n\psi_2x^{2n^2-2}.
\end{aligned}$$

Hence we have proved the claim. The desired result of ψ_m is given by

$$\begin{aligned}
&T^0(\psi_{2n+1}^2) = (2n+1)^2x^{4n^2+4n} = (2n+1)^2x^{(2n+1)^2-1} && \text{for } m = 2n+1; \\
&T^0(\psi_{2n}^2) = n^2\psi_2^2x^{4n^2-4} = (2n)^2x^{(2n)^2-1} && \text{for } m = 2n.
\end{aligned}$$

Hence $\psi_m(x)^2 = m^2x^{m^2-1} + (\text{lower order terms})$.

(c) If $\Delta \neq 0$, prove that $\phi_m(x)$ and $\psi_m^2(x)$ are relatively prime polynomials in $K[x]$.

Solution. Without loss of generality, we may assume K is algebraically closed. Suppose two given polynomials in x are not relatively prime so that there is some common root $x_0 \in K$ such that $\phi_m(x_0) = \psi_m^2(x_0) = 0$. Let m be the smallest index satisfying this assumption. Recall that $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$, and $\psi_{m+1}^2, \psi_{m-1}^2$ are polynomials in x by (a). Hence $\psi_{m+1}^2(x_0) = 0$ or $\psi_{m-1}^2(x_0) = 0$.

(i) (*Easy Step*) If $m = 2n+1$ is odd, then $\psi_{m-2}, \psi_m, \psi_{m+2}$ are all polynomials in x. It follows that $\psi_{m\pm2}(x_0)\psi_m(x_0) = 0$. So at least one of the following two equations is true:

$$\begin{aligned}
\phi_{m+1}(x_0) &= x\psi_{m+1}^2(x_0) - \psi_{m+2}(x_0)\psi_m(x_0) = 0, \\
\phi_{m-1}(x_0) &= x\psi_{m-1}^2(x_0) - \psi_m(x_0)\psi_{m-2}(x_0) = 0.
\end{aligned}$$

This deduces that $\phi_{m+1}(x_0) = \psi_{m+1}^2(x_0) = 0$ or $\phi_{m-1}(x_0) = \psi_{m-1}^2(x_0) = 0$. Note that the latter case for $m-1$ is not valid due to the minimality of m.

(ii) (*Tough Step*) Suppose for the sake of contradiction that $m = 2n$. Let $P = (x/z^2, y/z^3)$ be a point with Jacobian coordinates. Say $2P = (x'/z'^2, y'/z'^3)$ and the tangent line for E on $\mathbb{A}_K^2$ at P is $y = \lambda x + \nu$. From the group law,

$$x' = \lambda^2 + a_1\lambda - a_2 - 2x, \quad y' = (a_1 - \lambda)x' - \nu - a_3,$$

where

$$\lambda = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}, \quad \nu = \frac{-x^3 + a_4x + 2a_6 - a_3y}{2y + a_1x + a_3}.$$

Change this from affine coordinates into Jacobian coordinates, we get

$$\begin{aligned}
\frac{x'}{z'^2} &= \lambda(x/z^2, y/z^3)^2 - a_1\lambda(x/z^2, y/z^3) - a_2 - 2\frac{x}{z^2} \\
&= \frac{(3(x/z^2)^2 + 2a_2(x/z^2) + a_4 - a_1(y/z^3))^2}{(2(y/z^3) + a_1(x/z^2) + a_3)^2} - a_2 - 2\frac{x}{z^2} \\
&\quad - \frac{a_1(3(x/z^2)^2 + 2a_2(x/z^2) + a_4 - a_1(y/z^3))}{(2(y/z^3) + a_1(x/z^2) + a_3)} \\
&= \frac{(\cdots)}{z^2(a_3z^3 + a_1xz + 2y)^2},
\end{aligned}$$

where the numerator is given by

$$
\begin{aligned}
(\cdots) = &-a_1^3xyz^3 + a_1^2a_2x^2z^4 - a_1^2a_3yz^5 + a_1^2a_4xz^6 + a_1^2x^3z^2 \\
&-a_1^2y^2z^2 - 4a_1a_2xyz^3 + a_1a_3a_4z^8 - a_1a_3x^2z^4 - 8a_1x^2yz \\
&+ 4a_2^2x^2z^4 - a_2a_3^2z^8 - 4a_2a_3yz^5 + 4a_2a_4xz^6 + 12a_2x^3z^2 \\
&-4a_2y^2z^2 - 2a_3^2xz^6 - 8a_3xyz^3 + a_4^2z^8 + 6a_4x^2z^4 + 9x^4 - 8xy^2 \\
= &-8x(y^2 + a_1xyz + a_3yz^3) - 4a_2z^2(y^2 + a_1xyz + a_3yz^3) \\
&-a_1^2z^2(y^2 + a_1xyz + a_3yz^3) + (a_1^2a_2 - a_1a_3 + 4a_2^2 + 6a_4)x^2z^4 \\
&+ (a_1^2a_4 + 4a_2a_4 - 2a_3^2)xz^6 + (a_1^2 + 12a_2)x^3z^2 + 9x^4 \\
&+ (a_1a_3a_4 - a_2a_3^2 + a_4^2)z^8 \\
= &(-8x - 4a_2z^2 - a_1^2z^2)(x^3 + a_2x^2z^2 + a_4xz^4 + a_6z^6) + 9x^4 \\
&+ (a_1^2a_2 - a_1a_3 + 4a_2^2 + 6a_4)x^2z^4 + (a_1^2 + 12a_2)x^3z^2 \\
&+ (a_1^2a_4 + 4a_2a_4 - 2a_3^2)xz^6 + (a_1a_3a_4 - a_2a_3^2 + a_4^2)z^8 \\
= &-a_1^2a_2x^2z^4 - a_1^2x^3z^2 - a_4a_1^2xz^6 - a_6a_1^2z^8 - 4a_2^2x^2z^4 - 12a_2x^3z^2 \\
&-4a_4a_2xz^6 - 4a_6a_2z^8 - 8x^4 - 8a_4x^2z^4 - 8a_6xz^6 + 9x^4 \\
&+ (a_1^2a_2 - a_1a_3 + 4a_2^2 + 6a_4)x^2z^4 + (a_1^2 + 12a_2)x^3z^2 \\
&+ (a_1^2a_4 + 4a_2a_4 - 2a_3^2)xz^6 + (a_1a_3a_4 - a_2a_3^2 + a_4^2)z^8 \\
= &\, x^4 - (2a_3^2 - 8a_6)xz^6 - (2a_4 + a_1a_3)x^2z^4 \\
&- (a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2)z^8 \\
= &\, x^4 - b_4x^2z^4 - 2b_6xz^6 - b_8z^8.
\end{aligned}
$$

On the other hand, (a) deduces that both ψ_2^2 and ϕ_2 are polynomials in x, then by definitions,

$$
\begin{aligned}
\psi_2^2(x) &= (2y + a_1x + a_3)^2 \\
&= 4x^3 + (a_1^2 + 4a_2)x^2 + (2a_1a_3 + 4a_4)x + (a_3^2 + 4a_6) \\
&= 4x^3 + b_2x^2 + 2b_4x + b_6, \\
\phi_2(x) &= x\psi_2^2(x) - \psi_3(x)\psi_1(x) \\
&= 4x^4 + b_2x^3 + 2b_4x^2 + b_6x - (3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8) \\
&= x^4 - b_4x^2 - 2b_6x - b_8.
\end{aligned}
$$

Plugging the Jacobian coordinates into these, we obtain

$$
\begin{aligned}
\psi_2^2(x/z^2) &= 4\frac{x^3}{z^6} + b_2\frac{x^2}{z^4} + 2b_4\frac{x}{z^2} + b_6, \\
\phi_2(x/z^2) &= \frac{x^4}{z^8} - b_4\frac{x^2}{z^4} - 2b_6\frac{x}{z^2} - b_8.
\end{aligned}
$$

And therefore, by a comparison on all coefficients, the prolix calculation above has proved that

$$x' = z^8\phi_2(x/z^2), \quad z'^2 = z^8\psi_2^2(x/z^2).$$

In particular, we own the conclusion that

$$x([2](x/z^2, y/z^3)) = \frac{\phi_2(P)}{\psi_2^2(P)},$$

where $x([2](x/z^2, y/z^3))$ denotes the first coordinate for $[2]P = [2](x/z^2, y/z^3)$. Note that x is free from z in this case. If the pair (x, z^2) happens to be (ϕ_n, ψ_n^2), we actually obtain

$$\frac{\phi_{2n}}{\psi_{2n}^2} = \frac{x'}{z'^2} = \frac{\psi_n^8 \phi_2(\phi_n/\psi_n^2)}{\psi_n^8 \psi_2^2(\phi_n/\psi_n^2)} = \frac{\phi_2(\phi_n/\psi_n^2)}{\psi_2^2(\phi_n/\psi_n^2)}.$$

As an emphasis, the first equality above between two ratios is deduced from the group law together with definitions of division polynomials[1] only, which is not from any corollary of (d). We will use this to prove (d) later. Let us now apply (b) here to give a comparison for leading terms, which is

$$T^0(\psi_n^8 \phi_2(\frac{\phi_n}{\psi_n^2})) = (n^2 x^{n^2-1})^4 (\frac{x^{n^2}}{n^2 x^{n^2-1}})^4 = x^{4n^2} = T^0(\phi_{2n}),$$
$$T^0(\psi_n^8 \psi_2^2(\frac{\phi_n}{\psi_n^2})) = (n^2 x^{n^2-1})^4 \cdot 4(\frac{x^{n^2}}{n^2 x^{n^2-1}})^3 = 4n^2 x^{4n^2-1} = T^0(\psi_{2n}^2).$$

This finally shows that, qua desired result,

$$\phi_{2n} = \psi_n^8 \phi_2(\frac{\phi_n}{\psi_n^2}), \quad \psi_{2n}^2 = \psi_n^8 \psi_2^2(\frac{\phi_n}{\psi_n^2}).$$

Now, let $F(x, z^2) = z^8 \psi_2^2(x/z^2), G(x, z^2) = z^8 \phi_2(x/z^2)$. By Euclidean division algorithm, $F(x, z^2)$ and $G(x, z^2)$ are relatively prime in both x and z respectively, i.e. $F(x, 1), G(x, 1)$ have no common roots, so $F(1, z^2), G(1, z^2)$ do, with respect to z^2. Furthermore, there exist polynomials $u_1(x, z), v_1(x, z)$ and $u_2(x, z), v_2(x, z)$ such that

$$\begin{aligned} &F(x, 1)u_1(x, 1) + G(x, 1)v_1(x, 1) = 1 && \text{for } x, \\ &F(1, z^2)u_2(1, z^2) + G(1, z^2)v_2(1, z^2) = 1 && \text{for } z^2. \end{aligned}$$

Here we do not require explicit descriptions for u_1, u_2, v_1, v_2 and only focus on the degrees of x and z to get the result which read as[2]

$$\begin{aligned} F(x, z^2)u_1(x, z^2) - G(x, z^2)v_1(x, z^2) = 4\Delta \cdot z^{12}, \\ F(x, z^2)u_2(x, z^2) - G(x, z^2)v_2(x, z^2) = 4\Delta \cdot x^6, \end{aligned}$$

where $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$. Note that these equations do not rely on any relations between x and z. So it is safe to substitute the pair (x, z^2) with (ϕ_n, ψ_n^2). In the end, from the essential condition $\Delta \neq 0$, we see if $m = 2n$ and $\phi_{2n}(x_0) = \psi_{2n}^2(x_0) = 0$, then $\phi_n(x_0) = \psi_n^2(x_0) = 0$.

[1]The upshot here is the general definition of division polynomials automatically guarantees the homomorphic condition that read as

$$(\phi_m/\psi_m^2, \omega_m/\psi_m^3) + (\phi_n/\psi_n^2, \omega_n/\psi_n^3) = (\phi_{m+n}/\psi_{m+n}^2, \omega_{m+n}/\psi_{m+n}^3)$$

under the additive group law, which also implies (d). However, under Silverman's statement, we have no way but to check by computation to get this. The idea is to check it for $m, n \leq 4$, and then by induction, it suffices to consider two cases, which are $m = n$ and $m + 1 = n$. Since the initial conditions and the recurrence formulas determine our coordinates, the solution on E goes to be unique.

Unfortunately, it is computationally intensive and morally should be done with computer software instead of by hand only. This process does not relate to the main question, so we choose to omit it. I claim I had been checking this using `SageMath`.

[2]This is the same argument as in Silverman's Sublemma VIII.4.3. But it does not require any condition for the base field K.

If m is even, the result of (ii) contradicts to the minimality of m. Hence m must be odd. However, $\phi_{m+1}(x_0) = \psi_{m+1}^2(x_0) = 0$ is valid in this case by (i) with $m+1$ being even. Apply (ii) to obtain

$$\phi_{(m+1)/2}(x_0) = \psi_{(m+1)/2}^2(x_0) = 0.$$

Thus, since m is the minimal index,

$$\frac{m+1}{2} \geq m,$$

Hence, if $\phi_m(x)$ and $\psi_m^2(x)$ are not relatively prime, m is forced to be 1. But $\psi_1 = 1$, which leads to a contradiction. This completes the proof of (c).

(d) Continuing with the assumption that $\Delta \neq 0$, so E is an elliptic curve, prove that for any point $P = (x_0, y_0) \in E$ we have

$$[m]P = (\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}).$$

Solution. We check this by induction and more complicated computation under the group law. Using induction, it suffices to show that

$$(\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}) + (\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}) = (\frac{\phi_{2m}(P)}{\psi_{2m}^2(P)}, \frac{\omega_{2m}(P)}{\psi_{2m}^3(P)}),$$
$$(\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}) + (\frac{\phi_{m+1}(P)}{\psi_{m+1}^2(P)}, \frac{\omega_{m+1}(P)}{\psi_{m+1}^3(P)}) = (\frac{\phi_{2m+1}(P)}{\psi_{2m+1}^2(P)}, \frac{\omega_{2m+1}(P)}{\psi_{2m+1}^3(P)}),$$

where the addition is given by the group law. Step (ii) of (c) has set up the additive law for two coincident points. As for the case for two different points, $(x', y') = (x_1, y_1) + (x_2, y_2)$ is given by

$$x' = \lambda^2 + a_1\lambda - a_2 - (x_1 + x_2), \quad y' = (a_1 - \lambda)x' - \nu - a_3,$$

where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}.$$

(i) Let's dispose for the odd case when $[2m+1]P$. Taking $(x_1, y_1) = (\phi_m/\psi_m^2, \omega_m, \psi_m^3)$ and $(x_2, y_2) = (\phi_{m+1}/\psi_{m+1}^2, \omega_{m+1}/\psi_{m+1}^3)$. Our goal is to check that

$$(x', y') = (\frac{\phi_{2m+1}}{\psi_{2m+1}^2}, \frac{\omega_{2m+1}}{\psi_{2m+1}^3}) = (x_1, y_1) + (x_2, y_2).$$

Firstly, we obtain

$$\begin{aligned}
\lambda &= \frac{\omega_{m+1}/\psi_{m+1}^3 - \omega_m/\psi_m^3}{\phi_{m+1}/\psi_{m+1}^2 - \phi_m/\psi_m^2} \\
&= \frac{\omega_{m+1}\psi_m^3 - \omega_m\psi_{m+1}^3}{\phi_{m+1}\psi_m^3\psi_{m+1} - \phi_m\psi_{m+1}^3\psi_m} \\
&= \frac{\omega_{m+1}\psi_m^3 - \omega_m\psi_{m+1}^3}{\psi_{m+1}\psi_m(\psi_m^2(x\psi_{m+1}^2 - \psi_{m+2}\psi_m) - \psi_{m+1}^2(x\psi_m - \psi_{m+1}\psi_{m-1}))} \\
&= \frac{\omega_m\psi_{m+1}^3 - \omega_{m+1}\psi_m^3}{\psi_{m+1}\psi_m\psi_{2m+1}}.
\end{aligned}$$

Plugging this into the formula of x', we get

$$x' = \lambda^2 + a_1\lambda - a_2 - \frac{\psi_m\psi_{m+1}^2 + \phi_{m+1}\psi_m^2}{\psi_m^2\psi_{m+1}^2} = \frac{(\cdots)}{\psi_m^2\psi_{m+1}^2\psi_{2m+1}^2},$$

where the numerator is given by

$$\begin{aligned}(\cdots) = & -\phi_m^3\psi_{m+1}^6 + \phi_m^2\phi_{m+1}\psi_m^2\psi_{m+1}^4 - a_2\phi_m^2\psi_m^2\psi_{m+1}^6 + \phi_m\phi_{m+1}^2\psi_m^4\psi_{m+1}^2 \\ & + 2a_2\phi_m\phi_{m+1}\psi_m^4\psi_{m+1}^4 + a_1\phi_m\omega_m\psi_m\psi_{m+1}^6 - a_1\phi_m\omega_{m+1}\psi_m^4\psi_{m+1}^3 \\ & - a_1\phi_{m+1}\omega_m\psi_m^3\psi_{m+1}^4 - \phi_{m+1}^3\psi_m^6 - a_2\phi_{m+1}^2\psi_m^6\psi_{m+1}^2 + \omega_m^2\psi_{m+1}^6 \\ & - 2\omega_m\omega_{m+1}\psi_m^3\psi_{m+1}^3 + a_1\phi_{m+1}\omega_{m+1}\psi_m^6\psi_{m+1} + \omega_{m+1}^2\psi_m^6 \\ = & \ \psi_{m+1}^6(a_4\phi_{m+1}\psi_{m+1}^4\psi_m^6 + a_6\psi_{m+1}^6\psi_m^6 - a_3\omega_{m+1}\psi_{m+1}^3\psi_m^6) \\ & + \psi_m^6(a_4\phi_m\psi_m^4\psi_{m+1}^6 + a_6\psi_m^6\psi_{m+1}^6 - a_3\omega_m\psi_m^3\psi_{m+1}^6) \\ & + \phi_m^2\phi_{m+1}\psi_m^2\psi_{m+1}^4 + \phi_m\phi_{m+1}^2\psi_m^4\psi_{m+1}^2 + 2a_2\phi_m\phi_{m+1}\psi_m^4\psi_{m+1}^4 \\ & - a_1\phi_m\omega_{m+1}\psi_m^4\psi_{m+1}^3 - a_1\phi_{m+1}\omega_m\psi_m^3\psi_{m+1}^4 - 2\omega_m\omega_{m+1}\psi_m^3\psi_{m+1}^3.\end{aligned}$$

Using the idea given by (c), there is no need to continue reducing this formula. The upshot here is noting that every one of items in the numerator is divided by $\psi_m^2\psi_{m+1}^2$. Thus we have shown that ψ_{2m+1} is precisely the denominator of x'. Again, by a computation on leading terms which is the same as in (c), being omitted here,

$$x' = x\left(\left(\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}\right) + \left(\frac{\phi_{m+1}(P)}{\psi_{m+1}^2(P)}, \frac{\omega_{m+1}(P)}{\psi_{m+1}^3(P)}\right)\right) = \frac{\phi_{2m+1}(P)}{\psi_{2m+1}^2(P)}.$$

Let us now deal with y'. Considering the line passing through $(x_1, y_1), (x_2, y_2)$,

$$\begin{aligned}\nu &= \frac{\phi_{m+1}\omega_m/\psi_{m+1}^2\psi_m^3 - \phi_m\omega_{m+1}/\psi_m^2\psi_{m+1}^3}{\phi_{m+1}/\psi_{m+1}^2 - \phi_m/\psi_m^2} \\ &= \frac{\phi_{m+1}\omega_m\psi_{m+1} - \phi_m\omega_{m+1}\psi_m}{\phi_{m+1}\psi_m^3\psi_{m+1} - \phi_m\psi_m\psi_{m+1}^3} \\ &= \frac{\phi_m\omega_{m+1}\psi_m - \phi_{m+1}\omega_m\psi_{m+1}}{\psi_{m+1}\psi_m\psi_{2m+1}}.\end{aligned}$$

Hence by the group law,

$$y' = (a_1 - \lambda)\frac{\phi_{2m+1}}{\psi_{2m+1}^2} - \nu - a_3 = \frac{(\cdots)}{\psi_m^3\psi_{m+1}^3\psi_{2m+1}^3},$$

where the numerator is even more complicated just so we do not give it out explicitly. The way to use is not different from that before. Plugging in the elliptic curve formulas

$$y^2 + a_1xyz + a_3yz^3 = x^3 + a_2x^2z^2 + a_4xz^4 + a_6z^6$$

for $(x, y, z) = (\phi_m, \omega_m, \psi_m), (\phi_{m+1}, \omega_{m+1}, \psi_{m+1})$ into it, and then note that every one of those terms is divided by $\psi_m^3\psi_{m+1}^3$. So the denominator of y' is again ψ_{m+1}^3, as expected. Moreover, a similar comparison for leading terms should reveal that

$$y' = y\left(\left(\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}\right) + \left(\frac{\phi_{m+1}(P)}{\psi_{m+1}^2(P)}, \frac{\omega_{m+1}(P)}{\psi_{m+1}^3(P)}\right)\right) = \frac{\omega_{2m+1}(P)}{\psi_{2m+1}^3(P)}.$$

(ii) Now we consider $[2m]P$. The first coordinate is done by (c). Using the same argument, it remains to show that

$$\frac{\omega_{2m}(P)}{\psi_{2m}^3(P)} = \frac{\omega_2([m]P)}{\psi_2^3([m]P)}.$$

By definitions, we see

$$\psi_2\psi_{2m} = \psi_m(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2) = 2\psi_2\psi_m\omega_m,$$

so that $\psi_{2m} = 2\psi_m\omega_m$. Thus,

$$\begin{aligned}\frac{\omega_{2m}(P)}{\psi_{2m}^3(P)} &= \frac{2\omega_{2m}(P)\psi_{2m}(P)}{2\psi_{2m}^4(P)} = \frac{\psi_{4m}(P)}{2\psi_{2m}^4(P)},\\ \frac{\omega_2([m]P)}{\psi_2^3([m]P)} &= \frac{2\omega_2([m]P)\psi_2([m]P)}{2\psi_2^4([m]P)} = \frac{\psi_4([m]P)}{2\psi_2^4([m]P)}.\end{aligned}$$

However, by (a), when n is even, ψ_n may contain a linear factor in y rather than being a polynomial in x only. But this can be resolved by taking squares. It suffices to show that

$$\frac{\psi_{4m}^2(P)}{\psi_{2m}^8(P)} = \frac{\psi_4^2([m]P)}{\psi_2^8([m]P)}.$$

The denominators are directly given by our result of (c), read as

$$\psi_{2m}^2(P) = \psi_m^8(P)\psi_2^2([m]P).$$

Apply this once directly, and then once inversely, we get

$$\begin{aligned}\psi_{4m}^2(P) &= \psi_{2m}^8(P)\psi_2^2([2m]P)\\ &= (\psi_m^8(P)\psi_2^2([m]P))^4\psi_2^2([2][m]P)\\ &= \psi_m^{32}(P)(\psi_2^8([m]P)\psi_2^2([2][m]P))\\ &= \psi_m^{32}(P)\psi_4^2([m]P).\end{aligned}$$

Drawing together all three threads given above, we finally attain

$$y([2](\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)})) = \frac{\omega_{2m}(P)}{\psi_{2m}^3(P)}.$$

Joint with (c), this completes the proof of (ii).

To complete the induction, there is still one thing in residue, that is, to check for $2 \leq m \leq 4$. Note that $[4]P$ is given by $[2]P$, it suffices to check for $m = 2, 3$. But these can be given by easier computations, which completes the proof.

(e) Prove that the map $[m] : E \to E$ has degree m^2.

Solution. Firstly, by (a), note that solutions of $\psi_m^2(x) = 0$ as a polynomial in x correspond to solutions of $\psi_m(P) = 0$ as a map for points on E, and similarly for $\phi_m(x)$ versus $\phi_m(P)$. We know $\deg\phi_m = m^2$ and $\deg\psi_m^2 = m^2 - 1$ as polynomials in x for all m by (b). On the other hand, (c) says that ϕ_m and ψ_m^2 are relatively prime. Using (d), it follows that

$$\deg[m] = \#\ker[m] = \deg\phi_m = m^2.$$

(f) Prove that the function $\psi_n \in K(E)$ has divisor

$$\operatorname{div}(\psi_n) = \sum_{T\in E[n]} (T) - n^2(O).$$

Thus ψ_n vanishes at precisely the nontrivial n-torsion points and has a corresponding pole at O.

Solution. We first consider zeros of ψ_n. From (d) and by definition of $E[n]$ as the torsion group,

$$E[n] = \ker[n] = \{P \in E : [n]P = O\},$$

which consists of O together with affine points (x, y) such that $\psi_m^2(x) = 0$. Or equivalently, it consists of O and those P such that $\psi_m(P) = 0$. This shows that if $P \in E[n]$ then $\psi_n(P) = 0$. By (e), since $\#E[n] = n^2$, we obtain $n^2 - 1$ nontrivial zeros of ψ_n.

On the other hand, (b) reduces that there are at most $n^2 - 1$ nontrivial zeros of ψ_n^2 as a polynomial in x. Or equivalently, there are at most $n^2 - 1$ nontrivial $Q \in E$ such that $\psi_n(Q) = 0$. Combining these, $E[n] - \{O\}$ is exactly the nontrivial zero set of ψ_n, namely ψ_n vanishes at precisely the nontrivial n-torsion points.

As for poles, note that if $R \in E$ is a pole of ψ_n, then $[n]R = O$, that is, $R \in E[n]$. However, the only point left is the trivial $O \in E[n]$. This forces O to be the single pole. It similarly has degree $n^2 - 1$ by (b) again. Therefore,

$$\operatorname{div}(\psi_n) = \sum_{P\in E[n]\setminus\{O\}} (P) - (n^2 - 1)(O) = \sum_{T\in E[n]} (T) - n^2(O).$$

(g) Prove that

$$\psi_{n+m}\psi_{n-m}\psi_r^2 = \psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2 \quad \text{for all } n > m > r.$$

Solution. Given $P = (x, y) \in E$, let $x([m]P)$ denote the x-coordinate of $[m]P$. By the result of (e), for $m > r$,

$$x([m]P) - x([r]P) = \frac{\phi_m(P)}{\psi_m^2(P)} - \frac{\phi_r(P)}{\psi_r^2(P)} = \frac{\phi_m(P)\psi_r^2(P) - \phi_r(P)\psi_m^2(P)}{\psi_m^2(P)\psi_r^2(P)}.$$

Now (f) tells us zeroes of ψ_k are exactly those points of order k. If $P_0 = (x_0, y_0)$ has order $m \pm r$, then $[m](x_0) = [r](x_0)$. This shows that $\phi_m(P)\psi_r^2(P) - \phi_r(P)\psi_m^2(P)$ is divided by $\psi_{m+r}(P)\psi_{m-r}(P)$. Applying (b), since $m + r$ and $m - r$ must be in the same parity,

$$\begin{aligned}
\text{either} \quad T^0(\psi_{m+r}\psi_{m-r}) &= (m+r)x^{((m+r)^2-1)/2}(m-r)x^{((m-r)^2-1)/2} \\
&= (m^2 - r^2)x^{m^2+r^2-1}, \\
\text{or} \quad T^0(\psi_{m+r}\psi_{m-r}) &= \frac{\psi_2}{2}(m+r)x^{((m+r)^2-4)/2}\frac{\psi_2}{2}(m-r)x^{((m-r)^2-4)/2} \\
&= (m^2 - r^2)x^{m^2+r^2-1}.
\end{aligned}$$

On the other hand,

$$T^0(\phi_m\psi_r^2 - \phi_r\psi_m^2) = x^{m^2}r^2x^{r^2-1} - x^{r^2}m^2x^{m^2-1} = (r^2-m^2)x^{m^2+r^2-1}.$$

Running the same argument for $n > r$ again and combining with the computation of T^0 above, we attain

$$x([m]P)-x([r]P) = \frac{-\psi_{m+r}(P)\psi_{m-r}(P)}{\psi_m^2(P)\psi_r^2(P)}, \quad x([n]P)-x([r]P) = \frac{-\psi_{n+r}(P)\psi_{n-r}(P)}{\psi_n^2(P)\psi_r^2(P)}.$$

Consider $x([m]P) - x([r]P) = x([n]P) - x([r]P)$. This is valid when x is the first coordinate of some torsion point P of order $m \pm n$ or r, by (f) again. This kind of P satisfy

$$\begin{aligned}
0 &= \psi_{n+m}(P)\psi_{n-m}(P)\psi_r^2(P) \\
&= \frac{-\psi_{m+r}(P)\psi_{m-r}(P)}{\psi_m^2(P)\psi_r^2(P)} - \frac{-\psi_{n+r}(P)\psi_{n-r}(P)}{\psi_n^2(P)\psi_r^2(P)} \\
&= \frac{\psi_{n+r}(P)\psi_{n-r}(P)\psi_m^2(P) - \psi_{m+r}(P)\psi_{m-r}(P)\psi_n^2(P)}{\psi_m^2(P)\psi_n^2(P)\psi_r^2(P)}.
\end{aligned}$$

The last step below comes from (b) again, which is given by

$$\begin{aligned}
T^0(\psi_{n+m}\psi_{n-m}\psi_r^2) &= (n+m)(n-m)x^{m^2+n^2-1}r^2x^{r^2-1} \\
&= (n^2-m^2)r^2x^{m^2+n^2+r^2-2}.
\end{aligned}$$

And after switching positions of m, n, r, similarly,

$$\begin{aligned}
&T^0(\psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2) \\
=&(n^2-r^2)m^2x^{m^2+n^2+r^2-2} - (m^2-r^2)n^2x^{m^2+n^2+r^2-2} \\
=&(n^2-m^2)r^2x^{m^2+n^2+r^2-2}.
\end{aligned}$$

This inspection shows that for all $m > n > r$,

$$\psi_{n+m}\psi_{n-m}\psi_r^2 = \psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2$$

because both of two sides have the same zeros on E and the same leading term. We remark that it overlaps with the definition of elliptic divisible sequences (EDS) in Silverman's Exercise 3.34.

2. **Arithmetic Properties for Multiplication via Log Heights.**

Comment and Erratum. The second inequality in (c) should have coefficient 10 in the last term instead of 5, otherwise (a) and (b) lead to a contradiction when $P = Q$.

Let E/K be an elliptic curve given by a Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

(a) Prove that there are *absolute constants* c_1 and c_2 such that for all points $P \in E(\bar{K})$ we have

$$|h_x([2]P) - 4h_x(P)| \leq c_1 h([A, B, 1]) + c_2.$$

Find explicit values for c_1 and c_2.

Solution. The idea is to calculate the upper bounds of $h_x([2]P) - 4h_x(P)$ and $4h_x(P) - h_x([2]P)$ respectively. Let $t = p/q \in K$ as a fraction in lowest terms. Recall that the height of t, denoted by $H(t)$, is defined by

$$H(t) = \max\{|p|, |q|\}.$$

The logarithmic height on $E(K)$, relative to the given Weierstrass equation, is

$$h_x : E(K) \to \mathbb{R}; \quad h_x(P) = \begin{cases} \log H(x(P)) & \text{if } P \neq O, \\ 0 & \text{if } P = O. \end{cases}$$

Taking $a_1 = a_2 = a_3 = 0$ and $a_4 = A, a_6 = B$ in the previous problem, we obtain the first coordinate of $[2]P$. Say $x(P) = a/b$ in affine coordinate, according to the duplication formula,

$$x([2]P) = \frac{a^4 - 2Aa^2b^2 - 8Bab^3 + A^2b^4}{4a^3b + 4Aab^3 + 4Bb^4} = \frac{F(a, b)}{G(a, b)},$$

where the numerator and denominator above, say F and G, are two homogeneous polynomials of degree 4. Note that (as if in (c) of the previous problem)

$$\begin{aligned} F(a, 1) &= (3a^2 + A)^2 - 8a(a^3 + Aa + B), \\ G(a, 1) &= 4(a^3 + Aa + B). \end{aligned}$$

Since $a^3 + Aa + B$ and its derivative $3a^2 + A$ have no common root, neither do $F(a, 1)$ and $G(a, 1)$. For any monomial in the form $cA^iB^jx^ky^{m-k}$, we see

$$cA^iB^ja^kb^{m-k} \leq |c| \max\{|A|, |B|, 1\}^{i+j} \max\{|a|^m, |b|^m\}.$$

This shows that

$$\begin{aligned} |F(a, b)| &\leq (1 + |-2| + |-8| + 1) \max\{|A|, |B|, 1\}^2 \max\{|a|^4, |b|^4\}, \\ |G(a, b)| &\leq (4 + 4 + 4) \max\{|A|, |B|, 1\} \max\{|a|^4, |b|^4\}. \end{aligned}$$

To sum it up, that is

$$\begin{aligned} H(x([2]P)) &= \max\{|F(a, b)|, |G(a, b)|\} \\ &\leq 12 \max\{|A|, |B|, 1\}^2 \max\{|a|, |b|\}^4 \\ &= 12H([A, B, 1])^2 H(x(P))^4. \end{aligned}$$

On taking logs, we obtain the inequality

$$h_x([2]P) - 4h_x(P) \leq 2h([A,B,1]) + \log 12.$$

We then consider its opposite number. Repeating the same argument for Step (ii) of (c) in Problem 1, there are homogeneous polynomials u_1, u_2, v_1, v_2 in (x, y) of degree 3 such that

$$\begin{aligned} u_1(a,b)F(a,b) - v_1(a,b)G(a,b) &= 4\Delta \cdot b^7, \\ u_2(a,b)F(a,b) - v_2(a,b)G(a,b) &= 4\Delta \cdot a^7. \end{aligned}$$

By Silverman's Sublemma 4.3,

$$\begin{aligned} u_1(a,b) &= 12a^2b + 16Ab^3, \\ v_1(a,b) &= 3a^3 - 5Aab^2 - 27Bb^3, \\ u_2(a,b) &= 4(4A^3+27B^2)a^3 - 4A^2Ba^2b \\ &\quad + 4A(3A^3+22B^2)ab^2 + 12B(A^3+8B^2)b^3, \\ v_2(a,b) &= A^2Ba^2 + A(5A^3+32B^2)a^2b \\ &\quad + 2B(13A^3+96B^2)ab^2 - 3A^2(A^3+8B^2)b^3. \end{aligned}$$

Hence

$$\begin{aligned} |u_1(a,b)| &\leq (12+16)\max\{|A|,|B|,1\}\max\{|a|,|b|\}^3, \\ |v_1(a,b)| &\leq (3+5+27)\max\{|A|,|B|,1\}\max\{|a|,|b|\}^3, \\ |u_2(a,b)| &\leq (16+108+4+12+88+12+96)\max\{|A|,|B|,1\}^4\max\{|a|,|b|\}^3, \\ |v_2(a,b)| &\leq (1+5+32+26+192+3+24)\max\{|A|,|B|,1\}^4\max\{|a|,|b|\}^3, \end{aligned}$$

Taking the largest upper bound, we get

$$\max\{|u_1(a,b)|,|v_1(a,b)|,|u_2(a,b)|,|v_2(a,b)|\} \leq 336\max\{|A|,|B|,1\}^4\max\{|a|,|b|\}^3.$$

Therefore, the equations above of degree 7 shows that

$$4|\Delta|\max\{|a|,|b|\}^7 \leq 772\max\{|A|,|B|,1\}^4\max\{|a|,|b|\}^3\max\{|F(a,b)|,|G(a,b)|\}.$$

On taking logs, we finally get

$$\log|\Delta| + 4h_x(P) \leq 4h([A,B,1]) + h_x([2]P) + \log 168,$$

which is equivalent to

$$4h_x(P) - h_x([2]P) \leq 4h([A,B,1]) + \log\frac{168}{|4A^3+27B^2|}.$$

Hence the desired explicit values are

$$c_1 = 4, \quad c_2 = \max\{\log 12, \log\frac{168}{|4A^3+27B^2|}\}.$$

This is actually not the best bound, but it is convenient to compute. Furthermore, we see the error is not large unless $\Delta \to 0$.

(b) Find *absolute constants* c_3 and c_4 such that for all points $P \in E(\bar{K})$ we have

$$|\frac{1}{2}h_x(P) - \hat{h}(P)| \leq c_3 h([A, B, 1]) + c_4.$$

Solution. By definition, let $f \in K(E)$ be a non-constant even function, then

$$\hat{h}(P) = \frac{1}{\deg(f)} \lim_{N\to\infty} 4^{-N} h_f([2^N]P),$$

which is in fact independent of the choice of f. By (a), the map [2] is represented by homogeneous polynomials of degree 4 in the first coordinate, so we may choose f to be a 2-folding such that $\deg(f) = 2$, to get

$$\hat{h}(P) = \frac{1}{2} \lim_{N\to\infty} \frac{h_x([2^N]P)}{4^N}.$$

Since (a) is valid for all $P \in E(\bar{K})$, we are able to plug $[2^N]P$ for all $N \in \mathbb{N}$ into the inequality. Dividing by 4^{N+1}, it turns out to be

$$\left| \frac{h_x([2^{N+1}]P)}{4^{N+1}} - \frac{h_x([2^N]P)}{4^N} \right| \leq \frac{c_1}{4^{N+1}} h([A, B, 1]) + \frac{c_2}{4^{N+1}}.$$

Taking the sum for all N and applying the triangle inequality,

$$\begin{aligned}
\sum_{N=0}^{\infty} \frac{c_1 h([A, B, 1]) + c_2}{4^{N+1}} &\geq \sum_{N=0}^{\infty} \left| \frac{h_x([2^{N+1}]P)}{4^{N+1}} - \frac{h_x([2^N]P)}{4^N} \right| \\
&\geq \left| \sum_{N=0}^{\infty} \frac{h_x([2^{N+1}]P)}{4^{N+1}} - \frac{h_x([2^N]P)}{4^N} \right| \\
&= \left| \lim_{N\to\infty} \frac{h_x([2^N]P)}{4^N} - h_x(P) \right|.
\end{aligned}$$

Dividing this inequality by 2, we attain that

$$|\frac{1}{2}h_x(P) - \hat{h}(P)| \leq \frac{1}{2} \sum_{N=0}^{\infty} \frac{c_1 h([A, B, 1]) + c_2}{4^{N+1}} = \frac{c_1 h([A, B, 1]) + c_2}{6}.$$

Thus, the result follows from taking $c_3 = c_1/6$ and $c_4 = c_2/6$.

(c) Prove that for all integers $m \geq 1$ and all points $P, Q \in E(\bar{K})$ we have

$$|h_x([m]P) - m^2 h_x(P)| \leq 2(m^2 + 1)(c_3 h([A, B, 1]) + c_4)$$

and

$$h_x(P + Q) \leq 2h_x(P) + 2h_x(Q) + 10(c_3 h([A, B, 1]) + c_4).$$

Solution. The celebrated Néron-Tate Theorem is applied here (see Silverman's Theorem VIII.9.3). It says that

$$\hat{h}([m]P) = m^2 \hat{h}(P)$$

for all $P \in E(\bar{K})$, and

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

for all $P, Q \in E(\bar{K})$. From the first equality, the result of (b) becomes

$$\begin{aligned}|\frac{1}{2}h_x([m]P) - \hat{h}([m]P)| &= |\frac{1}{2}h_x([m]P) - m^2\hat{h}(P)| \\ &\leq c_3 h([A,B,1]) + c_4.\end{aligned}$$

Multiplying this by 2 and applying (b) again, we obtain

$$\begin{aligned}2(c_3h([A,B,1]) + c_4) &\geq |h_x([m]P) - 2m^2\hat{h}(P)| \\ &\geq |h_x([m]P) - m^2h_x(P)| - |m^2h_x(P) - 2m^2\hat{h}(P)| \\ &\geq |h_x([m]P) - m^2h_x(P)| - 2m^2(c_3h([A,B,1]) + c_4).\end{aligned}$$

This proves the first desired result

$$|h_x([m]P) - m^2h_x(P)| \leq 2(m^2+1)(c_3h([A,B,1]) + c_4).$$

By Néron-Tate's second equality,

$$\hat{h}(P+Q) \leq 2\hat{h}(P) + 2\hat{h}(Q).$$

Applying (b) again to $P+Q$, P and Q respectively,

$$\begin{aligned}&\frac{1}{2}h_x(P+Q) - (c_3h([A,B,1]) + c_4) \\ &\leq \hat{h}(P+Q) \leq 2\hat{h}(P) + 2\hat{h}(Q) \\ &\leq 2(\frac{1}{2}h_x(P) + (c_3h([A,B,1]) + c_4)) + 2(\frac{1}{2}h_x(Q) + (c_3h([A,B,1]) + c_4)) \\ &= h_x(P) + h_x(Q) + 4(c_3h([A,B,1]) + c_4).\end{aligned}$$

This then deduces

$$h_x(P+Q) \leq 2h_x(P) + 2h_x(Q) + 10(c_3h([A,B,1]) + c_4).$$

(d) Let $Q_1, \ldots, Q_r \in E(K)$ be a set of generators for $E(K)/2E(K)$. Find *absolute constants* c_5, c_6, and c_7 such that the set of points $P \in E(K)$ satisfying

$$h_x(P) \leq c_5 \max_{1\leq i\leq r} h_x(Q_i) + c_6h([A,B,1]) + c_7$$

contains a complete set of generators for $E(K)$.

Solution. Let $c = \max\{\hat{h}(Q_1), \ldots, \hat{h}(Q_r)\}$. Since $Q_1, \ldots, Q_r$ are representatives of $E(K)/2E(K)$, all of these points are in finite height. Accordingly, the basic property of Néron-Tate height implies that

$$\#\{P \in E : \hat{h}(P) \leq c\} < \infty,$$

i.e. there are finitely many points on E, say $R_1, \ldots, R_k$, whose Néron-Tate height cannot goes beyond the constant $c < \infty$. Let G be the subgroup of $E(K)$ that is generated by them. For the sake of contradiction, let us suppose $G \neq E(K)$. Choose an element $A \in E(K)\backslash G$. Since there are only finitely many points of Néron-Tate height less than $\hat{h}(A)$, we may change A to one of these, if necessary, and assume that

$$\hat{h}(A) = \min_{P \in E(K)\backslash G} \{\hat{h}(P)\}.$$

Consider the factorization of A. There exists some Q_i lying in the set of generators of $E(K)/2E(K)$ such that

$$A = Q_i + B, \qquad \text{for some } B \in 2E(K).$$

We can rewrite $B = 2C$ for some $C \in E(K)$. Then after applying Néron-Tate Theorem for canonical heights, we obtain

$$\hat{h}(B) = \hat{h}(A - Q_i) = 2\hat{h}(A) + 2\hat{h}(Q_i) - \hat{h}(A + Q_i) \leq 2\hat{h}(A) + 2c$$

since the height function is non-negative. Note that if $\hat{h}(A) \leq c$, then A must lie in the generator set of G, which is impossible by assumption. Consequently,

$$\hat{h}(B) \leq 2\hat{h}(A) + 2c \leq 4\hat{h}(A).$$

On the other hand, $\hat{h}(B) = \hat{h}(2C) = 4\hat{h}(C)$. This shows that

$$\hat{h}(C) \leq \hat{h}(A).$$

Since A had the smallest height for points not in G, we must have $C \in G$. Therefore, $A = Q_i + 2C \in G$, which leads to a contradiction, so $E(K) = G$. By the way, this also completes the proof of the Mordell-Weil Theorem.
Back to the condition $\hat{h}(P) \leq c$. It is from (b) that

$$\begin{aligned} \hat{h}(P) &\geq \frac{1}{2}h_x(P) - (c_3 h([A, B, 1]) + c_4), \\ \hat{h}(Q_i) &\leq \frac{1}{2}h_x(Q_i) + (c_3 h([A, B, 1]) + c_4). \end{aligned}$$

And therefore

$$\frac{1}{2}h_x(P) - (c_3 h([A, B, 1]) + c_4) \leq \frac{1}{2} \max_{1 \leq i \leq r} \{h_x(Q_i)\} + (c_3 h([A, B, 1]) + c_4),$$

or equivalently,

$$h_x(P) \leq \max_{1 \leq i \leq r} \{h_x(Q_i)\} + 4c_3 h([A, B, 1]) + 4c_4.$$

Taking $(c_5, c_6, c_7) = (1, 4c_3, 4c_4)$ gives the desired result.

3. **The L-Series Attached to an Elliptic Curve.**

Erratum. The displayed equation defining $L_E(s)$ should have p^{-s} instead of p^{-2}.

Let $E/\mathbb{Q}$ be an elliptic curve and choose a global minimal Weierstrass equation for $E/\mathbb{Q}$,

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

For each prime p, let $\widetilde{E}$ denote the reduction of the Weierstrass equation modulo p, and let

$$t_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p).$$

The L-series associated to $E/\mathbb{Q}$ is defined by the Euler product

$$L_E(s) = \prod_{p\mid\Delta(E)} (1 - t_p p^{-s})^{-1} \prod_{p\nmid\Delta(E)} (1 - t_p p^{-s} + p^{1-2s})^{-1}.$$

(a) If $L_E(s)$ is expanded as a Dirichlet series $\sum c_n n^{-s}$, show that for all primes p, its p^{th} coefficient satisfies $c_p = t_p$.

Solution. For convenience, we define the trivial character for E that read as

$$\chi_E(p) = \chi(p) = \begin{cases} 1, & p \nmid \Delta(E); \\ 0, & p \mid \Delta(E). \end{cases}$$

for all prime p. Just so

$$L_E(s) = \prod_p (1 - t_p p^{-s} + \chi(p) p^{1-2s})^{-1}.$$

It is known that the definition of coefficients t_p can be extended to t_n for all positive integers $n \geq 1$. In particular, they satisfy the recurrence formula

$$\begin{aligned} t_1 &= 1 && \text{for } e = 0, \\ t_{p^e} &= t_p t_{p^{e-1}} - \chi(p) p t_{p^{e-2}} && \text{for } e \geq 2. \end{aligned}$$

Fix a prime p. Multiply the prime power recurrence by p^{-es} and summing over $e \geq 2$ to get

$$\begin{aligned} \sum_{e\geq 2} t_{p^e} p^{-es} &= \sum_{e\geq 2} t_p t_{p^{e-1}} p^{-es} - \sum_{e\geq 2} \chi(p) p t_{p^{e-2}} p^{-es} \\ &= t_p p^{-s} \sum_{e\geq 1} t_{p^e} p^{-es} - \chi(p) p^{1-2s} \sum_{e\geq 0} t_{p^e} p^{-es} \\ &= t_p p^{-s} \sum_{e\geq 0} t_{p^e} p^{-es} - t_p p^{-s} - \chi(p) p^{1-2s} \sum_{e\geq 0} t_{p^e} p^{-es} \\ &= \sum_{e\geq 0} t_{p^e} p^{-es} - t_p p^{-s} - 1. \end{aligned}$$

The last equality above renders that

$$(1 - t_p p^{-s} + \chi(p) p^{1-2s}) \sum_{e\geq 0} t_{p^e} p^{-es} = 1.$$

Or equivalently,

$$\sum_{e\geq 0} t_{p^e}p^{-es} = (1 - t_p p^{-s} + \chi(p)p^{1-2s})^{-1}.$$

On the other hand, note that the Fundamental Theorem of Arithmetic (positive integers factor uniquely into prime powers) implies that for a function g of prime powers,

$$\prod_p \sum_{e\geq 0} g(p^e) = \sum_{n\geq 1} \prod_{p^e \| n} g(p^e).$$

The notation $p^e \| n$ means that p^e is the highest power of p that divides n, and we are assuming that g is small enough to justify formal rearrangements.

Now, we are ready to compute the Euler product:

$$\begin{aligned} L_E(s) &= \prod_p (1 - t_p p^{-s} + \chi(p)p^{1-2s})^{-1} \\ &= \prod_p \sum_{e\geq 0} t_{p^e}p^{-es} = \sum_{n\geq 1} \prod_{p^e\|n} t_{p^e}p^{-es} \\ &= \sum_{n\geq 1} (\prod_{p^e\|n} t_{p^e}) n^{-s} = \sum_{n\geq 1} t_n n^{-s}. \end{aligned}$$

Since this is the Dirichlet series $\sum c_n n^{-s}$ as well, we get $c_n = t_n$ for all n. In particular, under the original definition for primes, we have $c_p = t_p$ for all p.

(b) If E has bad reduction at p, so $p \mid \Delta(E)$, prove that t_p equals $1, -1$, or 0 according to whether the reduced curve $\widetilde{E}$ modulo p has a node with tangents whose slopes are rational over $\mathbb{F}_p$ (split multiplicative reduction), a node with tangents whose slopes are quadratic over $\mathbb{F}_p$ (nonsplit multiplicative reduction), or a cusp (additive reduction).

Solution. The description of the group of nonsingular points on E is used separately in three given cases. The result can be found in Silverman's Exercise 3.5 whose proof is given by similar argument as in his Proposition 2.5, which we choose to omit here.

(i) When $\widetilde{E}$ has split multiplicative reduction, by definition, there is 1 node as the unique singular point. And the group of nonsingular points

$$\widetilde{E}_{\text{ns}} \cong (\mathbb{F}_p^*, \times).$$

Hence we obtain $p-1$ nonsingular points, and

$$\#\widetilde{E}(\mathbb{F}_p) = 1 + (p-1) = p.$$

(ii) When $\widetilde{E}$ has nonsplit multiplicative reduction, there is 1 node as the unique singular point again. Also, the coefficients of the double line renders a quadratic extension over $\mathbb{F}_p$. Thus,

$$\widetilde{E}_{\text{ns}} \cong (\mathbb{F}_{p^2}^*/\mathbb{F}_p^*, \times).$$

This gives $p+1$ nonsingular points. So

$$\#\widetilde{E}(\mathbb{F}_p) = 1 + (p+1) = p+2.$$

(iii) When $\widetilde{E}$ has additive reduction, the cusp is the unique singular point together with

$$\widetilde{E}_{\mathrm{ns}} \cong (\mathbb{F}_p, +),$$

and then

$$\#\widetilde{E}(\mathbb{F}_p) = 1 + p.$$

To sum these up, we get

$$\begin{aligned} t_p &= p + 1 - \#\widetilde{E}(\mathbb{F}_p) \\ &= \begin{cases} 1, & \text{split multiplicative reduction;} \\ -1, & \text{nonsplit multiplicative reduction;} \\ 0, & \text{additive reduction.} \end{cases} \end{aligned}$$

(c) Prove that the Euler product for $L_E(s)$ converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 3/2$.

Solution. By the Hasse theorem, if $p \nmid \Delta(E)$ then

$$|t_p| = |p + 1 - \#\widetilde{E}(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

Combining this with (b), we see

$$\begin{aligned} L_E(s) &= \prod_{p \mid \Delta(E)} (1 - t_p p^{-s})^{-1} \prod_{p \nmid \Delta(E)} (1 - t_p p^{-s} + p^{1-2s})^{-1} \\ &\leq \prod_{p \mid \Delta(E)} (1 - p^{-s})^{-1} \prod_{p \nmid \Delta(E)} (1 - 2p^{-s+1/2} + p^{1-2s})^{-1} \end{aligned}$$

for all $s \in \mathbb{C}$. By complex analysis, this upper bound goes to be convergent when $\mathrm{Re}(-s + 1/2) < -1$, that is, $\mathrm{Re}(s) > 3/2$. More generally, an Euler product with coefficients bounded by $p^{w/2}$ is absolutely convergent for $\mathrm{Re}(s) > 1 + w/2$.