

Elliptic Curves MT25: Solutions to Sheet 3

(1) Following the hint, there exist polynomials $p(x), q(x) \in R[x]$ such that $p(x)f(x) + q(x)f'(x) = D$, and so: $p(a_0)f(a_0) + q(a_0)f'(a_0) = D$. Since $|a_0| \leq 1$, and since $p(x), q(x), f(x), f'(x) \in R[x]$, we must have $|p(a_0)|, |f(a_0)|, |q(a_0)|, |f'(a_0)| \leq 1$ and so $|D| \leq \max(|p(a_0)f(a_0)|, |q(a_0)f'(a_0)|) \leq 1$, which also implies $|D|^2 = |D|^2 \leq |D|$. Now, we are given that $|f(a_0)| < |D|^2$ and so $|p(a_0)f(a_0)| \leq |f(a_0)| < |D|^2 \leq |D|$. Hence $|D| \neq |p(a_0)f(a_0)|$, and so $|q(a_0)f'(a_0)| = |D - p(a_0)f(a_0)| = \max(|D|, |p(a_0)f(a_0)|) = |D|$ [using the fact that, if $|u| \neq |v|$ then $|u \pm v| = \max(|u|, |v|)$]. Since also $|q(a_0)| \leq 1$, this gives that $|f'(a_0)| \geq |D|$. Finally, $|f(a_0)| < |D|^2 \leq |f'(a_0)|^2$, and so $f(X)$ has a root $a \in R$ by Hensel's Lemma.

(2) In projective form, the point is: $(-64/25, 59/125, 1)$. The coordinate with largest 5-adic value is $59/125$, and on dividing all coordinates through by this, we can also represent the point as: $(-320/59, 1, 125/59)$, which is in 5-adic standard form (that is, 1 is the maximum of the 5-adic valuations of the coordinates). Reducing mod 5 gives $(0, 1, 0)$ on $\tilde{\mathcal{E}}$, which is the point at infinity.

(3) Let $\mathcal{C}$ be the curve $2Y^2 = X^4 - 17$. Over $\mathbb{R}$, the curve has the point $(4, \sqrt{239/2})$. In $\mathbb{Q}_2$, let $x = 11$. Then $11^4 - 17 = 2^5 \cdot 457$; but 457 is an integer congruent to 1 mod 8, and so, from lectures, there exists $\gamma \in \mathbb{Z}_2 \subset \mathbb{Q}_2$ such that $457 = \gamma^2$; then $(11, 4\gamma)$ is a point on the curve over $\mathbb{Q}_2$. For the next few primes, we shall repeatedly use the result from lectures that, if $p \neq 2$ and $|a|_p = 1$, then a is a square in $\mathbb{Q}_p$ iff it is a square mod p . Now, note that $-8, -34, -34, -8, 10, -8$ are quadratic residues modulo $p = 3, 5, 7, 11, 13, 17$, respectively, and so there exists $\gamma \in \mathbb{Q}_p$ such that $\gamma^2 = -8, -34, -34, -8, 10, -8$, respectively; this gives the $\mathbb{Q}_p$ -rational points on the curve: $(1, \gamma), (0, \gamma/2), (0, \gamma/2), (1, \gamma), (4, \gamma/2), (1, \gamma)$, respectively. Hence $\mathcal{C}$ has $\mathbb{Q}_p$ -rational points for all primes up to and including $p = 17$ [in fact, it was only necessary to do here $p = 2, 3, 5, 7, 11, 17$ here].

Let p be any prime $p \neq 13$ and $p \neq 17$. Our curve $\mathcal{C}$ (after multiplying both sides by 2) is birationally equivalent to $V^2 = 2X^4 - 34$, where $V = 2Y$; note that $2X^4 - 34$ has discriminant $-2^{11}17^3$. Recall Theorem 2.16 from lectures, that any curve $y^2 = Q(x)$, where $Q(x) = f_4x^4 + \dots + f_0$ has nonzero discriminant over $\mathbb{F}_p$, has at least $p - 1 - 2\sqrt{p} > 4$ affine points over $\mathbb{F}_p$, and so at least 5 affine points. At most 4 of these can have $2x^4 - 34 \equiv 0 \pmod{p}$, and so there exists $x_0 \in \mathbb{Z}$ such that $2(x_0^4 - 17)$ is a nonzero quadratic residue mod p . As above, there exists $\gamma \in \mathbb{Q}_p$ such that $\gamma^2 = 2(x_0^4 - 17)$, and so $(x_0, \gamma/2)$ is a $\mathbb{Q}_p$ -rational point on our original curve $\mathcal{C}$. Hence $\mathcal{C}$ has points in $\mathbb{R}$ and every $\mathbb{Q}_p$.

Alternative method for the above parts: Note that for $p \nmid 2\Delta$ (that is: $p \neq 2, 17$) $p \nmid 7$, we have (from a theorem from lectures) the number of affine points in $\tilde{\mathcal{C}}(\mathbb{F}_p)$ $p - 1 - 2\sqrt{p} > 0$, and so the number of affine points is > 0 ; these are non-singular, since $2\Delta \neq 0$ in $\mathbb{F}_p$. Also, by a theorem from lectures, any non-singular point on $\tilde{\mathcal{C}}(\mathbb{F}_p)$ lifts to a point on $\mathcal{C}(\mathbb{Q}_p)$; also, any affine non-singular point on $\tilde{\mathcal{C}}(\mathbb{F}_p)$ lifts to an affine point on $\mathcal{C}(\mathbb{Q}_p)$ (since the point at infinity on $\mathcal{C}(\mathbb{Q}_p)$ maps to the point at infinity on $\tilde{\mathcal{C}}(\mathbb{F}_p)$ under the reduction map mod p). This shows the existence of such $x, y \in \mathbb{Q}_p$ for all p except $p = 2, 3, 5$ and bad primes, so only still need to consider $p = 2, 3, 5, 17$. Also, note that for $p = 3$ there is the non-singular affine point $(1, 1)$ on $\tilde{\mathcal{C}}(\mathbb{F}_3)$, for $p = 5$ there is the non-singular affine point $(0, 2)$ on $\tilde{\mathcal{C}}(\mathbb{F}_5)$, and for $p = 17$ there is the non-singular affine point $(1, 3)$ on $\tilde{\mathcal{C}}(\mathbb{F}_{17})$, and as before these must lift to affine points $(x, y) \in \mathcal{C}(\mathbb{Q}_p)$. Over $\mathbb{R}$, the curve has the point $(4, \sqrt{239/2})$. In $\mathbb{Q}_2$, let $x = 11$. Then $11^4 - 17 = 2^5 \cdot 457$; but 457 is an integer congruent to 1 mod 8, and so, from lectures, there exists $\gamma \in \mathbb{Z}_2 \subset \mathbb{Q}_2$ such that $457 = \gamma^2$; then $(11, 4\gamma)$ is a point on the curve over $\mathbb{Q}_2$. This completes the alternative method of showing that $\mathcal{C}$ has points in $\mathbb{R}$ and every $\mathbb{Q}_p$.

Now, imagine that $\mathcal{C}$ had a $\mathbb{Q}$ -rational point; that is, imagine that there exist $X, Y \in \mathbb{Q}$ such that $2Y^2 = X^4 - 17$. Let $X = t/r$, where $r, t \in \mathbb{Z}$ and $\gcd(r, t) = 1$. Then $2(r^2Y)^2 = t^4 - 17r^4 \in \mathbb{Z}$. For any prime p , this gives that $|2|_p |r^2Y|_p^2 \leq 1$. When $p \neq 2$, we have $|2|_p = 1$ and so $|r^2Y|_p^2 \leq 1$ and so $|r^2Y|_p \leq 1$. When $p = 2$, we have $2^{-1}|r^2Y|_2^2 \leq 1$; but this still gives $|r^2Y|_2 \leq 1$ [since $|r^2Y|_2 > 1$ would mean $|r^2Y|_2 \geq 2^1$ and so $2^{-1}|r^2Y|_2^2 \geq 2^{-1}2^2 > 1$]. Overall, we have shown that $|r^2Y|_p \leq 1$ for all p ; since also $r^2Y \in \mathbb{Q}$, this gives that $r^2Y \in \mathbb{Z}$; let us say: $s = r^2Y \in \mathbb{Z}$. Therefore $r, s, t \in \mathbb{Z}$ satisfy $2s^2 = t^4 - 17r^4$ and $\gcd(r, t) = 1$.

Let q be any prime such that $q|s$. Note that $q \neq 17$ [since if $17|s$ then our equation $2s^2 = t^4 - 17r^4$ would force $17|t$, and so $17^2|2s^2$ and $17^2|t^4$, which would give $17^2|17r^4$, forcing $17|r$, which would contradict $\gcd(r, t) = 1$]. Note also that we must not then have $q|r$ [since if $q|s$ and $q|r$, then our equation $2s^2 = t^4 - 17r^4$ would force $q|t$, which would contradict $\gcd(r, t) = 1$]. Reducing our equation modulo q gives that $0 \equiv t^4 - 17r^4$ and so $(t^2/r^2)^2 \equiv 17 \pmod{q}$ [note that division by r^2 is allowable mod q since r is not divisible by q]. Hence 17 is a nonzero quadratic residue mod q . For $q \neq 2$, quadratic reciprocity then allows us to deduce that q is a quadratic residue mod 17 [since $17 \equiv 1 \pmod{4}$]. Furthermore, one can check directly that 2 is a quadratic residue mod 17, since $2 \equiv 6^2 \pmod{17}$. Overall, we have shown that every prime q dividing s must be a quadratic residue mod 17, and we can take $s > 0$ (if necessary, replacing s by $-s$), so that s is the product of its prime factors. It follows that s itself must be a quadratic residue mod 17, since it is a product of quadratic residues mod 17. Hence s^2 is a nonzero fourth power [also known as a *quartic residue*] mod 17. Note also that reducing our equation mod 17 gives $2s^2 \equiv t^4 \pmod{17}$, so that $2s^2$ is also a nonzero fourth power mod 17. Since $s, 2s^2$ are both nonzero fourth powers mod 17, it follows that $2 = (2s^2)/s^2$ is also a fourth power mod 17. On the other hand, one can compute directly that $0^4, 1^4, 2^4, 3^4, 4^4, 5^4, 6^4, 7^4, 8^4, 9^4, 10^4, 11^4, 12^4, 13^4, 14^4, 15^4, 16^4$ are con-

gruent mod 17 to: 0, 1, 16, 13, 1, 13, 4, 4, 16, 16, 4, 4, 13, 1, 13, 16, 1, respectively, so that in fact 2 is not a fourth power mod 17 (alternatively: if $2 \equiv w^4 \pmod{17}$ then $-1 \equiv 2^4 \equiv w^{16} \equiv 1 \pmod{17}$ by FLT, a contradiction, avoiding the need for an enumeration). This contradiction shows that our original curve $\mathcal{C}$ has no $\mathbb{Q}$ -rational points.

- (4) (a). Let $\mathcal{E} : Y^2 = X^3 + p^2$. Then the point $(0, p)$ on $\mathcal{E}$ reduces modulo p to the cusp $(0, 0)$ on $\tilde{\mathcal{E}} : Y^2 = X^3$, which is another way of saying that $(0, 0)$ on $\tilde{\mathcal{E}}$ lifts to the point $(0, p)$ in $\mathcal{E}(\mathbb{Q}_p)$.

(b). Question 3 is an example of this.

(c). Let $\mathcal{E} : Y^2 = X^3 + X^2 + p^2$. Then the point $(0, p)$ on $\mathcal{E}$ reduces modulo p to the node $(0, 0)$ on $\tilde{\mathcal{E}} : Y^2 = X^3 + X^2$, which is another way of saying that $(0, 0)$ on $\tilde{\mathcal{E}}$ lifts to the point $(0, p)$ in $\mathcal{E}(\mathbb{Q}_p)$.

(d). Let $\mathcal{E} : Y^2 = X^3 + X^2 + p$ and $\tilde{\mathcal{E}} : Y^2 = X^3 + X^2$. Then the node $(0, 0)$ on $\tilde{\mathcal{E}}$ does not lift to any point in $\mathcal{E}(\mathbb{Q}_p)$ by the same argument as in Question 2.

- (5) By definition of a homomorphism, we need to show

$$[m]F(X, Y) \stackrel{?}{=} F([m](X), [m]Y).$$

This is true when $m = 0$, since $[0](T) := 0$. Now for $m \geq 1$ we can use the recursive definition to rewrite this as

$$F([m-1]F(X, Y), F(X, Y)) \stackrel{?}{=} F(F([m-1](X), X), F([m-1]Y, Y)).$$

By induction we can assume $[m-1]F(X, Y) = F([m-1](X), [m-1]Y)$. Starting from the LHS we compute

$$\begin{aligned} F([m-1]F(X, Y), F(X, Y)) &= F(F([m-1](X), [m-1](Y)), F(X, Y)) \\ &= F([m-1](X), F([m-1](Y), F(X, Y))) = F([m-1](X), F(F(X, Y), [m-1](Y))) \\ &= F([m-1](X), F(X, F(Y, [m-1](Y)))) = F(F([m-1](X), X), F(Y, [m-1](Y))) \end{aligned}$$

which by commutativity equals the RHS. Here we have used, in order, induction, associativity, commutativity, associativity, associativity.

- (6) (a) We can regard F as a formal group law over K , and then $\log_F$ is a homomorphism from F to $\widehat{\mathbb{G}}_a$. In particular, we have an identity of formal power series (with coefficients in K): $\log_F(X) + \log_F(Y) = \log_F(F(X, Y))$. When $x, y \in \mathfrak{m}$, it follows from the result in Question 10 that $\log_F(x) + \log_F(y) = \log_F(F(x, y))$. This gives the desired homomorphism.

(b) We have $\log_F(x) = x + \sum_{n \geq 2} \frac{c_n}{n} x^n$, with $c_n \in R$. So to show that $|\log_F(x)| = |x|$, it suffices to show that $|\frac{c_n}{n} x^n| < |x|$ for all $n \geq 2$. Using $|c_n| \leq 1$ and rearranging, we need to show $|x| < |n|^{1/(n-1)}$ for all $n \geq 2$. Write $n = p^k m$, so $|n|^{1/(n-1)} = |p|^{k/(p^k m - 1)}$. We have $k/(p^k m - 1) \leq k/(p^k - 1) = \frac{1}{p-1} \frac{k}{1 + \dots + p^{k-1}} \leq 1/(p-1)$. This shows that $\min_n (|n|^{1/(n-1)}) = |p|^{1/(p-1)}$. We deduce that a sufficient condition to ensure $|x| < |n|^{1/(n-1)}$

for all $n \geq 2$ is $|x| < |p|^{1/(p-1)}$. This gives the desired statement. We get injectivity because $\log_F(x) = 0$ implies $|x| = 0$.

(c) Suppose that $z \in F(\mathfrak{m})$ has exact order p . We deduce from part (a) that $p \log_F(z) = 0$, which implies that $\log_F(z) = 0$. We deduce from part (b) that $|z| \geq |p|^{1/(p-1)}$.

- (7) In all of the following, we use the result from lectures that (when the coefficients of $\mathcal{E}$ are in $\mathfrak{F}$) $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$ is isomorphic to a subgroup of $\tilde{\mathcal{E}} \bmod p$, where $p \neq 2$ is a prime not dividing the discriminant. Note that this typically gives a much faster way of computing $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$ than the Nagell-Lutz result. N.B. (a),(b),(c) are about the level that could be asked as part of a 3-hour exam.

(a). There are the obvious points $P = (0, 1)$ of order 3 and $Q = (-1, 0)$ of order 2 in $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$, which generate a subgroup of $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$ of size 6 (namely, the 6 points $mP + nQ$ for $0 \leq m \leq 2$ and $0 \leq n \leq 1$). Further, $\Delta = 4A^3 + 27B^2 = 27$, so we can reduce modulo any prime except 2 (which must always be avoided) and 3. Over $\mathfrak{F}_5$, there are only six points: $\mathfrak{o}, (0, \pm 1), (2, \pm 3), (4, 0)$. So, we conclude that $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$ has size at most 6, which means that it consists of precisely the $C_6 = C_2 \times C_3$ group of points we have found already.

Note that, if $P = (0, 1)$ and $Q = (-1, 0)$, then the complete list of torsion points is: $\mathfrak{o}, P = (0, 1), 2P = (0, -1), Q = (-1, 0), P + Q = (2, -3), 2P + Q = (2, 3)$.

(b). Here, the (birational over $\mathfrak{Q}$) transformation $(X, Y) \mapsto (X - 1, Y)$ takes the given curve to: $Y^2 = X(X + 1)(X - 1) = X^3 - X$, which has discriminant -4 , and so we can reduce modulo the prime 3. Over $\mathfrak{F}_3$ there are the points: $\mathfrak{o}, (0, 0), (1, 0), (2, 0)$ giving that $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$ has size at most 4. But, in fact, $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$ contains $\mathfrak{o}, (0, 0), (-1, 0), (1, 0)$, which means the this $C_2 \times C_2$ group gives all of $\mathcal{E}_{\text{tors}}(\mathfrak{Q})$. *[Alternatively, even without using a birational transformation to the form $Y^2 = X^3 + AX + B$, we could just work entirely with the given equation of the curve, noting that the original cubic $X(X - 1)(X - 2)$ has no repeated roots mod 3, so that $Y^2 = X(X - 1)(X - 2)$ is an elliptic curve mod 3, and then noting that the only points are: $\mathfrak{o}, (0, 0), (1, 0), (2, 0)$.]*

(c). The (birational over $\mathfrak{Q}$) transformation $(X, Y) \mapsto (3^2 X, 3^3 Y)$ takes the given curve to: $Y^2 = X^3 + 1$ which we have already seen in part (a) to have a $C_2 \times C_3$ group as its torsion group.

Note that, if $P = (0, 1/27)$ and $Q = (-1/9, 0)$ then the complete list of torsion points is given by: $\mathfrak{o}, P = (0, 1/27), 2P = (0, -1/27), Q = (-1/9, 0), P + Q = (2/9, -1/9), 2P + Q = (2/9, 1/9)$.

- (8) Take $F(X, Y) = X + Y + tXY^p$, clearly non-commutative. One only has to check associativity.

$$\begin{aligned} F(F(X, Y), Z) &= F(X + Y + tXY^p, Z) = X + Y + tXY^p + Z + t(X + Y + tXY^p)Z^p \\ &= X + Y + tXY^p + Z + tXZ^p + tYZ^p, \end{aligned}$$

since the remaining term $t^2XY^pZ^p \in I = t^2\mathfrak{F}_p[t]$ and so $t^2XY^pZ^p = 0$ in $R = \mathfrak{F}_p[t]/I$. Also:

$$\begin{aligned} F(X, F(Y, Z)) &= X + F(Y, Z) + tXF(Y, Z)^p = X + Y + Z + tYZ^p + tX(Y + Z + tYZ^p)^p \\ &= X + Y + Z + tYZ^p + tX(Y^p + Z^p + (tYZ^p)^p), \end{aligned}$$

since all other terms in the binomial expansion of $(Y + Z + tYZ^p)^p$ are divisible by p and so are equal to 0 in R , which has characteristic p . But $(tYZ^p)^p = t^p(t^{p-2}Y^pZ^{p^2}) \in I$ and so $(tYZ^p)^p = 0$ in R , so that the above are the same, giving associativity, as required.

- (9) We are going to use the fact that these curves admit unusual endomorphisms ('complex multiplication'), and therefore so do the associated formal groups. In the first example, $Y^2 = X^3 + AX$, the map $(x, y) \mapsto (-x, iy)$ induces an endomorphism of the curve (compatible with the group law). In the (z, w) -coordinates, this map is $(z, w) \mapsto (iz, -iw)$. This tells us that $f(z) = iz$ is an endomorphism of the formal group $F(X, Y)$ (regarded as a formal group law over $\mathbb{C}$, for example). This implies that $F(iX, iY) = iF(X, Y)$, so looking at each homogeneous piece we have $i^n F_n(X, Y) = iF(X, Y)$. We deduce that $F_n = 0$ unless $i^n = i$, i.e. $n \equiv 1 \pmod{4}$.

In the second case, our unusual endomorphism is given by $(x, y) \mapsto (\zeta x, -y)$, where $\zeta = e^{2i\pi/3}$ (we have changed the sign of y to get an endomorphism of maximal order, 6). In the (z, w) -coordinates, this map is $(z, w) \mapsto (-\zeta z, -w)$. This tells us that $f(z) = -\zeta z$ is an endomorphism of the formal group $F(X, Y)$. This implies that $F(-\zeta X, -\zeta Y) = -\zeta F(X, Y)$, so looking at each homogeneous piece we have $(-\zeta)^n F_n(X, Y) = -\zeta F(X, Y)$. We deduce that $F_n = 0$ unless $(-\zeta)^n = -\zeta$, i.e. $n \equiv 1 \pmod{6}$.

Here is a (perhaps) more direct solution, reproduced from an earlier version of these solutions: Recall from lectures that the first step in deriving the formal group of an elliptic curve is to write the equation $\mathcal{E} : Y^2 = X^3 + AX + B$ as: $\mathcal{E}' : w = f(z, w) = z^3 + Aw^2z + Bw^3$, where $z = -x/y, w = -1/y$. We then inductively define $f_n(z, w)$ by: $f_1(z, w) = f(z, w)$ and $f_{m+1}(z, w) = f_m(z, f_m(z, w))$ and define

$$w(z) = \lim_{m \rightarrow \infty} f_m(z, 0) \in \mathbb{Z}[A, B][[z]],$$

which satisfies $w(z) = f(z, w(z))$. The terms of $f_1(z, w) = z^3 + Aw^2z + Bw^3$ all have weighted degree $\equiv 3$ [where we give z weight 1, w weight 3, A weight -4 and B weight -6]. Suppose that this is also true of $f_m(z, w)$; then $f_{m+1}(z, w) = f_m(z, z^3 + Aw^2z + Bw^3)$, where z has weighted degree 1, $z^3 + Aw^2z + Bw^3$ is homogeneous of weighted degree 3, and so the same will be true of f_{m+1} . So, by induction, all terms of every f_m and so all terms of $w(z)$ will have weighted degree 3.

We now perform the addition $(z_1, w_1) + (z_2, w_2)$. As usual, we first write the line $z = \lambda w + \mu$ through the points, given by $\lambda = (w(z_1) - w(z_2))/(z_1 - z_2)$ and $\mu = (z_1w(z_2) - z_2w(z_1))/(z_1 - z_2)$, both in $\mathbb{Z}[A, B][[z_1, z_2]]$. Letting z_1 and z_2 each have weight 1, the numerator $w(z_1) - w(z_2)$ is homogeneous of weighted degree 3, and so λ is homogeneous of weighted degree 2. Similarly,

μ is homogeneous of weighted degree 3. As in lectures, substituting $w = \lambda z + \mu$ into $\mathcal{E}'$ gives $\lambda z + \mu = z^3 + A(\lambda z + \mu)^2 z + B(\lambda z + \mu)^3$, and so:

$$(1 + A\lambda^2 + B\lambda^3)z^3 + (2A\lambda\mu + 3B\lambda^2\mu)z^2 + \dots = 0.$$

Let $(z_3, w(z_3))$ be the third point of intersection of $\mathcal{E}'$ and the line $z = \lambda w + \mu$, so that z_1, z_2, z_3 are the roots of the above cubic, giving that $z_1 + z_2 + z_3 = -(\text{coeff of } z^2)/(\text{coeff of } z^3)$, so:

$$z_3 = -z_1 - z_2 - \frac{2A\lambda\mu + 3B\lambda^2\mu}{1 + A\lambda^2 + B\lambda^3} \in \mathbb{Z}[A, B][[z_1, z_2]],$$

since the denominator is of the form $1 + \phi(z)$, where $\phi(z)$ has no constant term [and so is an invertible power series, with $1/(1 + \phi(z)) = 1 - \phi(z) + \phi(z)^2 + \dots$]. The sum $(z_1, w_1) + (z_2, w_2) + (z_3, w_3) =$ the identity, and so $(z_1, w_1) + (z_2, w_2) = -(z_3, w_3)$. Negation $(x, y) \mapsto (x, -y)$ induces $(z, w) \mapsto (-z, -w)$ [since $z = -x/y, w = -1/y$], so that the z -coordinate of $(z_1, w_1) + (z_2, w_2)$ is given by $F_{\mathcal{E}}(z_1, z_2)$, where:

$$F_{\mathcal{E}}(z_1, z_2) = z_1 + z_2 + (\text{ terms of degree } \geq 2) \in \mathbb{Z}[A, B][[z_1, z_2]].$$

But note that the expression for z_3 above consists of the terms z_1, z_2 , both homogeneous of weighted degree 1, and the fraction whose numerator $2A\lambda\mu + 3B\lambda^2\mu$ is homogeneous of weighted degree 1, and whose denominator $1 + A\lambda^2 + B\lambda^3$ is homogeneous of weighted degree 0. Therefore the final power series giving the formal group must be homogeneous of weighted degree 1.

For the case when our curve is of the form $Y^2 = X^3 + AX$ (so that $B = 0$), each term of the formal group must be an integer multiple of $A^k z_1^{n_1} z_2^{n_2}$. Since the weighted degree is 1 and since A has weight -4 , we see that the degree purely in z_1, z_2 must be $\equiv 1 \pmod{4}$, as required.

When our curve is of the form $Y^2 = X^3 + B$ (so that $A = 0$) the fact that B has weight -6 similarly gives that each term of the formal group has degree $\equiv 1 \pmod{6}$ in z_1, z_2 .

- (10) First we show convergence of the right hand side. For each i , set $g_i = G_i(x_1, \dots, x_l)$. We have $|g_i| \leq \max(|x_i|) < 1$. Choose $\rho < 1$ such that $\max(|x_i|) = \rho\delta$ with $\delta < 1$. Since $\{|a_n| \rho^{\sum n_i}\}$ is bounded, say by C , we have

$$\left| \sum_{n: \sum n_i \geq N} a_n g_1^{n_1} \dots g_k^{n_k} \right| \leq C\delta^N.$$

It follows that the right hand side converges, and is the limit of the sequence

$$\sum_{n: \sum n_i \leq N-1} a_n g_1^{n_1} \dots g_k^{n_k}$$

as $N \rightarrow \infty$.

Write $G_i = \sum b_{i,m} X_1^{m_1} \dots X_l^{m_l}$ and for a positive integer M consider the finite truncations $G_{i,M} = \sum_{\sum m_i \leq M-1} b_{i,m} X_1^{m_1} \dots X_l^{m_l}$ with values $g_{i,M}$ when we substitute the x_i .

We have

$$\left| a_n g_1^{n_1} \cdots g_k^{n_k} - a_n g_{1,M}^{n_1} \cdots g_{k,M}^{n_k} \right| = \left| a_n (g_1^{n_1} \cdots g_k^{n_k} - g_{1,M}^{n_1} \cdots g_{k,M}^{n_k}) \right| \leq |a_n| \rho^M \delta^M,$$

since all the terms which appear in $g_1^{n_1} \cdots g_k^{n_k}$, but not in $g_{1,M}^{n_1} \cdots g_{k,M}^{n_k}$, have valuation $\leq \rho^M \delta^M$. We deduce that

$$\begin{aligned} F(g_1, \dots, g_k) - \sum_{n: \sum n_i \leq N-1} a_n g_{1,N}^{n_1} \cdots g_{k,N}^{n_k} \\ \leq \max(C\delta^N, |a_n| \rho^N \delta^N : \sum n_i \leq N-1) = C\delta^N. \end{aligned}$$

On the other hand, if we consider the formal power series $F \circ G$ then the difference

$$(F \circ G) - \sum_{n: \sum n_i \leq N-1} a_n G_{1,N}^{n_1} \cdots G_{k,N}^{n_k}$$

only contains terms of degree $\geq N$. From this and the condition on the $|a_n|$, it follows easily that $(F \circ G)(x_1, \dots, x_l)$ converges and its value is the limit of

$$\sum_{n: \sum n_i \leq N-1} a_n g_{1,N}^{n_1} \cdots g_{k,N}^{n_k}$$

as $N \rightarrow \infty$.