# Course MA342P — Sample Paper 1

Timothy Murphy

May 2, 2016

*Attempt 4 questions. All carry the same mark. The word 'curve' always means* projective curve.

1. Explain informally how two points on an elliptic curve are added.

   Find the sum $P+Q$ of the points $P=(0,1),\ Q=(1,2)$ on the curve

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

   over the rationals $\mathbb{Q}$. What is $2P$?

   **Answer:** *Let $\mathcal{E}$ be the elliptic curve. We choose any point $O \in \mathcal{E}$ as the zero point.*

   *Suppose $P, Q \in \mathcal{E}$, the elliptic curve in question. The line $PQ$ meets $\mathcal{E}$ in a third point $R$ (which may coincice with $P$ or $Q$). We set*

   $$P * Q = R.$$

   *If $P = Q$ then we take the tangent at $P$ in place of the line $PQ$.*

   *Now we set*

   $$P + Q = O * (P * Q).$$

   *Suppose the elliptic curve is given in the standard Weierstrass form*

   $$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6.$$

   *More precisely, $\mathcal{E}$ is the projective curve*

   $$Y^2Z + c_1XYZ + c_3YZ^2 = X^3 + c_2X^2Z + c_4XZ^2 + c_6Z^3.$$

   *In this case we normally take $O = [0,1,0]$. If now*

   $$R = P * Q = (x, y)$$

   *then*

   $$P + Q = (x, -y).$$

*Now consider the points*

$$P = (0, 1),\ Q = (1, 2)$$

*on the elliptic curve*

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + 2x + 1.$$

*Suppose $PQ$ is the line*

$$y = mx + c.$$

*Then*

$$m = \frac{2-1}{1-0} = 1.$$

*Thus the line is*

$$y - 1 = x,$$

*ie*

$$y = x + 1.$$

*This line meets the curve where*

$$(mx + c)^2 = x^3 + 2x + 1.$$

*Thus if $P * Q = (x_2, y_2)$ then*

$$0 + 1 + x_2 = m^2 = 1,$$

*ie*

$$x_2 = 0.$$

*Hence*

$$y_2 = x_2 + 1 = 1.$$

*Thus*

$$P * Q = (0, 1) = P,$$

*and so*

$$P + Q = (0, -1).$$

*Since the line $PQ$ meets the curve again at $P$, this line is the tangent at $P$. Hence*

$$P * P = Q = (1, 2),$$

*and so*

$$2P = (1, -2).$$

2. Show that all cubics through 8 given points in general position in the plane pass through a 9th point.

   Hence or otherwise show that addition on an elliptic curve is associative.

   **Answer:**

   (a) *Let the points be* $P_i$ $(i = 1 - 10)$. *A cubic curve* $\Gamma$ *has 10 coefficients:*

$$c_1X^3+c_2X^2Y+c_3X^2Z+C_4XY^2+C_5XYZ+C_6XZ^2+c_7Y^3+c_8Y^2Z+c_9YZ^2+C_{10}Z^3 = 0.$$

   *The requirement that* $\Gamma$ *passes through* $P_i$ *gives 8 homogeneous linear conditions on these 10 coefficients. The solution space has dimension* $\geq 10 - 8 = 2$. *In other words the cubics form a pencil of homogeneous dimension* $\geq 1$.

   *We may suppose that no 4 of the points are collinear, and that the points do not all lie on a conic.*

   *We claim this in this case the dimension must be exactly 1. For suppose it is* $\geq 2$. *Then we can find a cubic in the pencil passing through any further 2 points. Let us choose 2 points* $U, V$ *on the line* $P_7P_8$. *Then the line* $\ell = P_7P_8UV$ *must lie entirly in the cubic, which must therefore split into*

$$\Gamma = \ell C,$$

   *where* $C$ *is a conic. Thus the 6 points* $P_i(i = 1 - 6)$ *must lie on a conic.*

   *By the same argument, any 6 of the 8 given points must lie on a conic.*

   *But there is only one conic through 5 points* $Q_j(j = 1 - 5)$, *no 4 of which are collinear.*

   *For suppose first that three of the points are collinear, say*

$$m = Q_1Q_2Q_3.$$

   *Then the only conic through the 5 points is*

$$C = mn,$$

   *where*

$$n = Q_4Q_5.$$

   *Now suppose no three of the points are collinear; and suppose there are two conics through the 5 points. Then the conics through the points form a pencil of projective dimension* $\geq 1$, *and we can find a conic in the pencil through any further point* $W$.

*Choose $W$ on $m = Q_1Q_2$. Then the conic must degenerate into two lines,*

$$C = mn,$$

*and $Q_3, Q_4, Q_5$ must lie on the line $n$, contrary to hypothesis.*

*Thus, returning to the 8 points $P_i$, there is a unique conic through $P_1, P_2, P_3, P_4, P_5$. But as we have seen, this conic must pass through $P_6$; and by the same argument it must also pass through $P_7$ and $P_8$. Hence all 8 points lie on a conic, contrary to hypothesis.*

*Therefore the pencil is of dimension 1; and if $\Gamma_1, \Gamma_2$ are two curves in the pencil then the general curve in the pencil is*

$$\Gamma = \lambda\Gamma_1 + \mu\Gamma_2.$$

*The curves $\Gamma_1, \Gamma_2$ meet in the 8 points $P_i$. Let the curves have equations*

$$F_1(X, Y, Z) = 0,\ F_2(X, Y, Z) = 0.$$

*We can regard these as cubics in $Z$ with coefficients in $X, Y$. If we form the resultant of the two cubics we obtain a homogeneous polynomial $R(X, Y)$ of degree 9 in $X, Y$, whose vanishing is a condition for the two cubics to have a root in common.*

*The 8 points $P_i$ will provide 8 roots for this equation. By considering the sum of the roots, it follows that there is a 9th root in the field $k$ we are working over. Thus the two cubics meet in a 9th point $P_9 = [X_9, Y_9, Z_9]$. Moreover, by the argument above $Y_9/X_9 \in k$; and similarly $Z_9/X_9 \in k$. Hence $P_9$ is defined over $k$.*

*(b) Suppose $P, Q, R \in \mathcal{E}$. We have to show that*

$$(P + Q) + R = P + (Q + R).$$

*By definition,*

$$P + Q = O * (P * Q),$$

*where $P * Q$ is the point where $PQ$ meets the curve again, and $O$ is the point chosen as zero point. Thus we have to show that*

$$O * ((P + Q) * R) = O * (P * (Q + R)).$$

*Since*

$$U * V = U * W \iff V = W$$

*it is sufficient to show that*

$$(P + Q) * R = P * (Q + R),$$

*ie*

$$(O * (P * Q)) * R = P * (O * (Q * R)).$$

*Note that*

$$U * V = W \iff V * W = U.$$

*Thus if we set*

$$P * Q = X,\ Q * R = Y$$

*then*

$$P = Q * X,\ R = Q * Y,$$

*and our equation becomes*

$$(O * X) * (Q * Y) = (Q * X) * (O * Y),$$

*ie (since $V * U = U * V$)*

$$(O * X) * (Y * Q) = (O * Y) * (X * Q).$$

*Thus the result will follow if we show that*

$$(P * Q) * (R * S) = (P * R) * (Q * S) \qquad (\dagger)$$

*for any 4 points $P, Q, R, S \in \mathcal{E}$.*
*[Conversely, if the operation $+$ is associative then it defines an abelian group structure on $\mathcal{E}$, with*

$$-P = O * P$$

*and*

$$P * Q = -(P + Q).$$

*In this case,*

$$(P * Q) * (R * S) = P + Q + R + S = (P * R) * (Q * S).$$

*Thus the identity (†) holds if and only if the operation is associative.]*
*Now let us apply the 8-point theorem to the points,*

$$P, Q, R, S, U = P * Q, V = R * S, W = P * R, X = Q * S.$$

*Let us define lines as follows:*

$$\ell = PQU, m = RSV, n = WX,$$
$$f = PRW, g = QSX, h = UV.$$

*Then the degenerate cubics*

$$\ell mn,\ fgh$$

*pass through the 8 points, and so must have a 9th point in common. This 9th point must be where the line $n$ meet $\mathcal{E}$ again, ie the point*

$$W * X = (P * R) * (Q * S).$$

*But by the same argument, it must be the point where the line $h$ meet $\mathcal{E}$ again, ie the point*

$$U * V = (P * Q) * (R * S).$$

*We conclude that*

$$(P * Q) * (R * S) = (P * R) * (Q * S),$$

*as required.*

*[This argument assumes, on the face of it, that the 9 points arising in this was are distinct. There are several ways of extending the reult to cover the special cases when some of the points coincide.*

*Thus we could extend the definition of the pencil of cubics so that if eg $P = Q$ then our pencil consisted of the cubics which had the same tangent at $P$ as $\mathcal{E}$.*

*Alternatively, we could justify the general result when $k = \mathbb{C}$, say, by continuity. The result must then be an algebraic identity which will hold over all fields.*

*Thirdly, we could appeal to the "Irrelevance of Algebraic Inequalities", which states that if an identity $f(x_1, \ldots, x_n) = 0$ holds subject to an inequailty $g(x_1, \ldots, x_n) \neq 0$ then it must hold in all cases.*

*But the question is long enough as it is, and I think one can assume that no examiner would expect the student to go into this issue.]*

3. Define the discriminant of a polynomial, and find the discriminant of

$$f(x) = x^3 + x^2 - x + 2.$$

How many real roots does this polynomial have?

Define the resultant of two polynomials, and find the resultant of

$$f(x) = x^2 + 3,\ g(x) = x^3 + 2.$$

**Answer:** *The discriminant $\Delta(f)$ of the polynomial*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

*with roots $\alpha_1, \ldots, \alpha_n$ is*

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

*The resultant $R(f, g)$ of two polynomials*

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m,\ g(x) = x^n + b_1 x^{n-1} + \cdots + b_n$$

*with roots $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ is*

$$R(f, g) = \prod_{i,j} (\alpha_i - \beta_j).$$

*There are various ways of computing the discriminant, eg removing the term in $x^2$ by changing to $x' = x + a/3$ (which won't alter the discriminant) and using the fact that if $a = 0$ then $\Delta = -(4b^3 + 27c^2)$. But the following trick is probably quicker in this case. Note that*

$$\begin{aligned} g(x) = \prod_i (x - \beta_j) &\implies g(\alpha_i) = \prod_j (\alpha_i - \beta_j) \\ &\implies R(f, g) = \prod_j \prod_i (\alpha_i - \beta_j) = \prod_i g(\alpha_i). \end{aligned}$$

*Also*

$$\begin{aligned} R(f, g) &= \prod_{i,j} (\alpha_i - \beta_j) \\ &= (-1)^{mn} \prod_{i,j} (\beta_j - \alpha_i) \\ &= (-1)^{mn} R(g, f) \\ &= (-1)^{mn} \prod_j f(\beta_j). \end{aligned}$$

*Since*

$$f'(x) = \sum_i \prod_{j \neq i} (x - \alpha_j),$$

*it follows that*

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j),$$

*and so*

$$\begin{aligned}\Delta(f) &= \prod_{i<j}(\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2}\prod_{i\neq j}(\alpha_i - \alpha_j) \\ &= (-1)^{n(n-1)/2}\prod_{i}\prod_{j\neq i}(\alpha_i - \alpha_j) \\ &= (-1)^{n(n-1)/2}\prod_{i} f'(\alpha_i)\end{aligned}$$

*Setting $g(x) = f'(x)/n$ (so that $g(x)$ is monic),*

$$\Delta(f) = (-1)^{n(n-1)/2}n^n\prod_i g(\alpha_i) = (-1)^{n(n-1)/2}n^n R(f,g).$$

*But now (since $n(n-1)$ is even)*

$$R(f,g) = \prod_j f(\beta_j),$$

*and so*

$$\Delta(f) = (-1)^{n(n-1)/2}n^n\prod_j f(\beta_j).$$

*Applying this with*

$$f(x) = x^3 + x^2 - x + 2,\ g(x) = \frac{1}{3}f'(x) = \frac{1}{3}(x+1)(x-1/3),$$

*we get*

$$\begin{aligned}\Delta(f) &= -3^3\prod_j f(\beta_j) \\ &= 27f(-1)f(1/3) \\ &= 27\cdot 3\cdot(1/27 + 1/9 - 1/3 + 2) \qquad = 3(1+3-9+54) \\ &= 3\cdot 49 \\ &= 3\cdot 7^2.\end{aligned}$$

*Finally, uppose*

$$f(x) = x^2 + 3,\ g(x) = x^3 + 2.$$

*The roots of $f(x)$ are $\pm\sqrt{3}i$. It follows that*

$$\begin{aligned}R(f,g) &= g(\sqrt{3}i)g(-\sqrt{3}i) \\ &= (-3\sqrt{3}i + 2)(3\sqrt{3}i + 2) \\ &= 27 + 4 = 31.\end{aligned}$$

4. What is meant by saying that a point on the curve

$$y^2 + Ax + B = x^3 + ax^2 + bx + c$$

is *singular*? What are the points at infinity on this curve? Are any of them singular?

Find a condition on $A, B, a, b, c$ for the curve to contain a singular point.

**Answer:**

*(a) A point on the projective curve*

$$F(x, y, z) = 0$$

*(where $F(x, y, z)$ is a homogeneous polynomial) is said to be singular if*

$$\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0.$$

*The given curve $\Gamma$ takes the homogeneous form*

$$F(x, y, z) \equiv y^2 z - x^3 - ax^2 z - bxz^2 - cz^3 = 0.$$

*It follows that the point $P = (x, y) \in \Gamma$ is singular if*

$$3x^2 + 2axz + bz^2 = 0,\ 2yz = 0,\ y^2 - ax^2 - 2bxz - 3cz^2 = 0.$$

*If $z = 0$ then $x = 0$ from the first equation and so $y = 0$ from the third equation. This is impossible. Hence $y = 0$, and so*

$$3x^2 + 2axz + bz^2 = 0,\ ax^2 + 2bxz + 3cz^2 = 0.$$

*Reverting to non-homogeneous notation,*

$$3x^2 + 2ax + b = 0,\ ax^2 + 2bx + 3c = 0.$$

*If*

$$f(x) = x^3 + ax^2 + bx + c$$

*then first equation can be written $f'(x) = 0$, while $x$ times the first plus the second is just $3f(x) = 0$.*

*It follows that the point $P = (x, y)$ on $\Gamma$ is singular if and only if $y = 0$ and*

$$f(x) = f'(x) = 0,$$

*in other words $x$ is a double root of $f(x)$.*

(b) *The point* $[x, y, z]$ *is 'at infinity' if* $z = 0$. *The point* $[x, y, 0]$ *is on* $\Gamma$ *if*

$$x^3 = 0.$$

*Thus* $\Gamma$ *has just one point at infinity,* $[0, 1, 0]$.

(c) *This point is not singular, since*

$$y^2 - ax^2 - 2bxz - cz^2 = y^2 \neq 0.$$

(d) *As we have seen, there is a singular point on* $\Gamma$ *if and only if* $f(x)$ *has a double root, ie* $f(x)$ *and* $f'(x)$ *have a root in common.*
*Two polynomials* $f(x)$ *and* $g(x)$ *have a root in common if and only if their* resultant $R(f, g)$ *vanishes.*
*The resultant of* $f(x)$ *and* $f'(x)$ *is*

$$R(f, f') = \det \begin{pmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 3 & 2a & b & 0 & 0 \\ 0 & 3 & 2a & b & 0 \\ 0 & 0 & 3 & 2a & b \end{pmatrix}.$$

*Thus we have to compute this determinant. Expanding with respect to the first column,*

$$\begin{aligned} R(f, f') &= \det \begin{pmatrix} 1 & a & b & c \\ 2a & b & 0 & 0 \\ 3 & 2a & b & 0 \\ 0 & 3 & 2a & b \end{pmatrix} + 3 \det \begin{pmatrix} a & b & c & 0 \\ 1 & a & b & c \\ 3 & 2a & b & 0 \\ 0 & 3 & 2a & b \end{pmatrix} \\ &= 1(b^3) - a(2ab^2) + b(4a^2b - 3b^2) - c(8a^3 - 12ab) \\ &\quad +3a(-ab^2 + 4a^2c - 3bc) - 3b(-2b^2 + 6ac) + 3c(-ab + 9c) \\ &= -a^2b^2 - 18abc + 4a^3C + 4b^3 + 27c^2, \end{aligned}$$

*which is just the given expression, multiplied by* $-1$.

5. Find the order of the point $P = (0, 0)$ on the elliptic curve

$$y^2 + y = x^3 - x.$$

**Answer:** *We have*

$$(2y + 1)\frac{dy}{dx} = 3x^2 - 1.$$

*Thus the slope at* $(x, y)$ *is*

$$m = \frac{3x^2 - 1}{2y + 1}.$$

*The tangent*

$$y = mx + c$$

*at* $(x, y)$ *meets the curve where*

$$(mx + c)^2 + (mx + c) = x^3 - x.$$

*If this meets the curve again at* $(x_2, y_2)$ *then*

$$2x + x_2 = m^2.$$

*In particular the slope at* $P$ *is*

$$m = \frac{-1}{1} = -1,$$

*so the tangent*

$$y = -x$$

*meets the curve again where*

$$x_2 = 1,$$

*ie at*

$$Q = (1, -1).$$

*Hence*

$$Q = -2P.$$

*The slope at* $Q$ *is*

$$m = \frac{2}{-1} = -2.$$

*Thus the tangent at* $Q$ *is*

$$y + 1 = -2(x - 1),$$

*ie*

$$y = -2x + 1,$$

*and this meets the curve again where*

$$2 + x_2 = 4,$$

*ie*

$$x_2 = 2,$$

*ie at* $(2,-3)$. *Thus*

$$-2Q = R = (2,-3).$$

*The slope at* $R$ *is*

$$m = \frac{12-1}{-6+1} = -\frac{11}{5}.$$

*It follows that* $R$ *is of infinite order, and so therefore is* $P$.

6. Show that the elliptic curve

$$E : y^2 + xy = x^3 - x^2 - 2x - 1$$

has good reduction modulo 2 and 5; and determine the groups $\mathcal{E}(\mathbb{F}_2)$ and $\mathcal{E}(\mathbb{F}_5)$.

What can you deduce about the group of points of finite order on $\mathcal{E}(\mathbb{Q})$?

**Answer:** *The curve takes homogeneous form*

$$F(X,Y,Z) \equiv Y^2Z + XYZ - X^3 - X^2Z - 2XZ^2 - Z^3 = 0.$$

*At a singular point,*

$$\begin{aligned} &\partial F/partial X = YZ - 3X^2 - 2XZ - 2Z^2 = 0, \\ &\partial F/partial Y = 2YZ + XZ = 0, \\ &\partial F/partial Z = Y^2 + XY - X^2 - 4XZ - 3Z^2 = 0. \end{aligned}$$

*(a) In characteristic 2, the second equation gives*

$$XZ = 0 \implies X = 0 \text{ or } Z = 0.$$

*If* $Z = 0$ *the first equation gives* $X = 0$, *and then the third equation gives* $Y = 0$. *Thus* $X = Y = Z = 0$, *which is impossible.*
*If* $X = 0$ *then the first equation gives*

$$YZ = 0 \implies Y = 0 \text{ or } Z = 0.$$

*We have excluded* $Z = 0$, *so*

$$X = Y = 0 \implies Z = 0$$

*from the third equation, so again* $X = Y = Z = 0$, *which is impossible.*
*We conclude that there is no singular point, ie the reduction at 2 is good.*

*(b) In characteristic 5, the second equation gives*

$$Z(2Y + X) = 0 \implies Z = 0 \text{ or } X = -2Y.$$

*If $Z = 0$, then as before the first equation gives $X = 0$, and then the third gives $Y = 0$.*
*Thus $X = -2Y \implies Y = 2X$ (as $-1/2 = 4/2 = 2$), and the first equation gives*

$$2X^2 = 2Z^2 \implies X = \pm Z.$$

*The third equation now gives*

$$(4 + 2 - 1 \mp 4 - 3)X^2 = 0 \implies X = 0.$$

*Thus $X = Y = Z = 0$, which is impossible.*
*We conclude that the curve is non-singular, ie the reduction at 5 is good.*
*[Alternatively, one could bring the curve to reduced form since the characteristic is neither 2 nor 3. Thus the equation can be written*

$$y^2 - 4xy = x^3 - x^2 - 2x - 1,$$

*ie*

$$(y - 2x)^2 = x^3 + 3x^2 - 2x - 1.$$

*Writing $y$ for $y - 2x$, and continuing the reduction,*

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

*ie*

$$y^2 = (x + 1)^3 - 2.$$

*Hence the discriminant*

$$D \bmod 5 = -27 \cdot (-2)^2 \neq 0,$$

*ie 5 is a good prime.]*

*In any characteristic, the only point on the line at infinity $Z = 0$ is $[0, 1, 0]$.*

*(a) In characteristic 2 there are just 4 finite points: $(0, 0), (1, 0), (0, 1), (1, 1)$. Of these, $(0, 1)$ and $(1, 1)$ lie on the curve. Thus*

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(3).$$

*(b) In characteristic 5 we can write the equation*

$$y^2 - 4xy = x^3 - x^2 - 2x - 1,$$

*ie*

$$(y - 2x)^2 = x^3 + 3x^2 - 2x - 1.$$

*Setting* $y' = y - 2x$,

$$y'^2 = x^3 + 3x^2 + 3x - 1,$$

*ie*

$$y'^2 = x'^3 - 2,$$

*where* $x' = x + 1$.
*Dropping the* $'$*s, we have to determine the group on the curve*

$$\mathcal{E}(\mathbb{F}_5) : y^2 = x^3 - 2.$$

*The quadratic residues* mod5 *are:* $0, 1, 4$, *ie* $0, \pm 1$. *We have the following table.*

| $x$ | $x^3 - 2$ | $y$ | *points* |
|---|---|---|---|
| 0 | $-2$ | $-$ | |
| 1 | $-1$ | $\pm 2$ | $(1, \pm 2)$ |
| 2 | 1 | $\pm 1$ | $(2, \pm 1)$ |
| $-2$ | 0 | 0 | $(-2, 0)$ |
| $-1$ | 2 | $-$ | |

*With* $O = [0, 1, 0]$,

$$\|\mathcal{E}(\mathbb{F}_5)\| = 6.$$

*It follows that*

$$\mathcal{E}(\mathbb{F}_5) = \mathbb{Z}/(6).$$

*If* $T \subset \mathcal{E}(\mathbb{Q})$ *is the torsion subgroup, and* $p$ *is a good prime, then the map*

$$T \to \mathcal{E}(\mathbb{F}_p)$$

*is an injective homomorphism.*

*Thus in this case* $p = 2$ *gives an injective homomorphism*

$$T \to \mathbb{Z}/(3).$$

*It follows that*

$$T = \{0\} \text{ or } \mathbb{Z}/(3).$$

*(The prime* $p = 5$ *does not give any further information.)*

7. Define a *lattice* $L \subset \mathbb{C}$. Show that the series

$$\frac{1}{z^2} + \sum_{\omega \in L,\, \omega \neq 0} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

defines a function $\varphi(z)$ which is periodic with respect to $L$.

Show also that $\varphi(z)$ satisfies the functional equation

$$\varphi'(z)^2 = 4\varphi(z)^3 + A\varphi(z) + B$$

for certain constants $A, B$.

**Answer:**

*(a) A lattice is a subgroup*

$$L = \langle \omega_1, \omega_2 \rangle$$

*of the additive group $\mathbb{C}$ generated by two non-zero complex numbers $\omega_1, \omega_2$ such that*

$$\omega_2/\omega_1 \notin \mathbb{R}.$$

*[One could equally well define a lattice as a discrete subgroup of $\mathbb{C}$ of rank 2. A discrete subgroup of $\mathbb{C}$ is isomorphic to $\mathbb{Z}^r$ where $r \leq 2$. In this subject we would normally exclude lattices of rank 0 (ie the group $\{0\}$) or 1 (ie the group $\langle \omega \rangle$ consisting of multiples of some $\omega \in \mathbb{C}$).]*

*(b) Let*

$$\varphi(z) = \frac{1}{z^2} + \sum{}' \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

*Then*

*i. The series converges absolutely for any $z \notin L$;*

*ii. the convergence is uniform in any bounded closed region excluding lattice points, and so the series defines a merormorphic function on $\mathbb{C}$ with a double pole at each lattice point;*

*iii. The function is periodic with respect to $L$, ie*

$$\omega \in L \implies \varphi(z+\omega) = \varphi(z).$$

*To prove (i), note that*

$$\begin{aligned} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega(1-z/\omega)^2} - \frac{1}{\omega^2} \\ &= \omega^{-2} \left( (1-z/\omega)^{-2} - 1 \right) \\ &= \omega^{-2} \left( 2z/\omega + 3z^2/\omega^2 + \cdots \right) \\ &= 2z/\omega^3 + 3z^2/\omega^4 + \cdots . \end{aligned}$$

*If*

$$\omega = m\omega_1 + n\omega_2$$

*then*

$$\begin{aligned} |\omega|^2 &= \omega\bar{\omega} \\ &= Q(m,n), \end{aligned}$$

*where $Q(m,n)$ is a positive-definite quadratic form. It follows that*

$$C_1(m^2+n^2) \leq |\omega|^2 \leq C_2(m^2+n^2)$$

*for some $C_1, C_2 > 0$.*
*In particular*

$$\left|\omega^{-r}\right| \leq C(m^2+n^2)^{-r/2}.$$

*But*

$$\sum{}'(m^2+n^2)^{-r/2}$$

*converges for $r > 2$, eg by comparison with*

$$\int (x^2+y^2)^{-r/2} dx\, dy.$$

*It follows that*

$$\sum{}' \omega^{-r}$$

*converges absolutely for $r \geq 3$; and so the series for $\varphi(z)$ converges absolutely for $z \notin L$.*
*This argument also shows that the convergence is uniform in any bounded region where say*

$$|z-\omega| \geq \epsilon > 0$$

*for all $\omega \in L$.*
*[It is a little more difficult to prove periodicity than one might think. If one could completely separate the terms*

$$\frac{1}{(z-\omega)^2} \text{ and } \frac{1}{\omega^2}$$

*it would be trivial, but unfortunatele these two series do not converge.]*
*Suppose $z \notin L = \langle \omega_1, \omega_2 \rangle$. We regard $z$ as fixed. It is sufficient to show that*

$$\varphi(z+\omega_1) = \varphi(z).$$

*Given $\epsilon > 0$ we can find $R$ such that*

$$\sum_{m^2+n^2>R^2} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| < \epsilon$$

*and*

$$\sum_{m^2+n^2>R^2} \left| \frac{1}{((z+\omega_1)-\omega)^2} - \frac{1}{\omega^2} \right| < \epsilon$$

*Thus it is sufficient to consider the terms with $m^2+n^2 \leq R^2$. But now the terms in the finite sums can be split in two. Now all the terms will cancel except for the terms*

$$\frac{1}{(m\omega_1 + n\omega_2)^2}$$

*when one of*

$$m^2+n^2 \text{ and } (m+1)^2+n^2$$

*is $\leq R$ and the other is $> R$. But this implies that*

$$|m| \leq R+1.$$

*Hence*

$$(m,n) \in A = \{(x,y) : R^2 - 3R < x^2+y^2 < R^2+3R\}.$$

*Since*

$$\left|(m\omega_1 + n\omega_2)^2\right| \geq C(m^2+n^2),$$

*the discrepancy will be*

$$< C' \sum_{(m,n)\in A} \frac{1}{m^2+n^2}.$$

*But this is*

$$< C' \int_{(x,y)\in A'} \frac{dx\, dy}{x^2+y^2}$$

*where*

$$A' = \{(x,y) : R^2 - 4R < x^2+y^2 < R^2+4R\},$$

*say. But the area of $A'$ is $8\pi R$, while the value of the integrand is always $\geq 1/(R^2-4R)$. Thus the integral is of order $O(1/R)$ and so $\to 0$ as $R \to \infty$. Hence the discrepancy can be ignored, and*

$$\varphi(z+\omega_1) = \varphi(z).$$

*Similarly*

$$\varphi(z+\omega_2)=\varphi(z),$$

*and so*

$$\varphi(z+\omega)=\varphi(z)$$

*for all* $\omega\in L$.

*(c) Since*

$$\begin{aligned}\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}&=\frac{1}{\omega^2}\left((1-z/\omega)^{-2}-1\right)\\&=\frac{2z}{\omega^3}+\frac{3z^2}{\omega^4}+\frac{4z^3}{\omega^5}+\cdots,\end{aligned}$$

*in the neighbourhood of* $z=0$

$$\varphi(z)=\frac{1}{z^2}+2G_3z+3G_4z^2+\cdots,$$

*where*

$$G_r=\sum{}'\frac{1}{\omega^r}$$

*(for* $r\geq 3$*). If* $r$ *is odd then*

$$G_r=0,$$

*since the terms in* $\pm\omega$ *cancel out. Thus*

$$\varphi(z)=\frac{1}{z^2}+3G_4z^2+5G_6z^4+O(z^6).$$

*Hence*

$$\varphi'(z)=\frac{-2}{z^3}+6G_4z+20G_6z^3+O(z^5),$$

*and so*

$$\varphi'(z)^2=\frac{4}{z^6}-\frac{24G_4}{z_2}+O(1).$$

*On the other hand,*

$$\varphi(z)^3=\frac{1}{z^6}+\frac{9G_4}{z^2}+O(1).$$

*Thus*

$$\varphi'(z)^2-4\varphi(z)^3=-\frac{60G_4}{z^2}+O(1).$$

*Hence*

$$\varphi'(z)^2-4\varphi(z)^3+60G_4\varphi(z)=O(1).$$

*Thus the periodic function on the left has no poles. But such a function is bounded on a fundamental parallelogram, and so on the whole of* $\mathbb{C}$*. Hence it is constant, say*

$$\varphi'(z)^2 - 4\varphi(z)^3 + 60G_4\varphi(z) = B,$$

*ie*

$$\varphi'(z)^2 = 4\varphi(z)^3 + A\varphi(z) + B,$$

*where* $A = 60G_4$.