Elliptic Curves. MT 2024. Sheet 0 solutions.

1. Determine whether the following are groups.
(a). The set of all 2×2 matrices under matrix multiplication.
Solution: *No: no inverses for singular matrices.*

(b). The set of all 2×2 matrices under matrix addition.
Solution: *Yes!*

2. For each of the following, decide whether ϕ is a homomorphism. When ϕ is a homomorphism, decide whether ϕ is injective, surjective, bijective, and find the kernel of ϕ.
(a). $\phi : \mathbb{Z}, + \to \mathbb{Q}^*, \times : x \mapsto x^2 + 1$.
Solution: *No: for example,* $\phi(2) \neq \phi(1)^2$.

(b). $\phi : \mathbb{Q}, + \to \mathbb{R}, + : w \mapsto \sqrt{2}\, w$.
Solution: *Can check directly that this is a homomorphism. It is bijective ($\sqrt{2}$ is invertible, so multiplication by it is bijective), so the kernel is zero.*

(c). $\phi : \mathbb{Z}, + \to \mathbb{Z}/3\mathbb{Z}, + : x \mapsto 2x$.
Solution: *This is a surjective homomorphism, since* 2 *is coprime to* 3*. The kernel is* $3\mathbb{Z}$.

3.
(a). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, decide whether the following are true or false: $3 = 1/27$, $-4 = 4$, $3 = 5/6$.
Solution: $3 \times 27 = 3^4$ *is a square, so* $3 = 1/27$ *mod* $(\mathbb{Q}^*)^2$.
$4 = 1$ *and* $-4 = -1$ *mod* $(\mathbb{Q}^*)^2$*. But* -1 *is not a rational square, so* $-4 \neq 4$ *mod* $(\mathbb{Q}^*)^2$.
$5/18$ *is not a rational square (it has prime factors appearing with odd powers).*

(b). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, write each of the following as a square free integer: $-2/27$, 16, 12, $1/3$.
Solution: $-2 \cdot 3^{-3} = -2 \cdot 3 = -6$ *mod* $(\mathbb{Q}^*)^2$.
$16 = 1$ *mod* $(\mathbb{Q}^*)^2$.
$12 = 3$ *mod* $(\mathbb{Q}^*)^2$.
$1/3 = 3$ *mod* $(\mathbb{Q}^*)^2$.

(c). Perform each of the following in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, writing your answer as a square free integer: 6×10, $10/21$, 15^{101}, 3^{-1}.
Solution: $6 \times 10 = 2^2 \cdot 3 \cdot 5 = 15$ *mod* $(\mathbb{Q}^*)^2$.
$10/21 = 2 \cdot 5 \cdot 3^{-1} \cdot 7^{-1} = 2 \cdot 5 \cdot 3 \cdot 7 = 210$ *mod* $(\mathbb{Q}^*)^2$.
$15^{101} = 15$ *mod* $(\mathbb{Q}^*)^2$.
$3^{-1} = 3$ *mod* $(\mathbb{Q}^*)^2$.

(d). How many elements are in each of the groups: $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, $\mathbb{R}^*/(\mathbb{R}^*)^2$, $\mathbb{C}^*/(\mathbb{C}^*)^2$?
Solution: *The elements of* $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ *are in bijection with square free integers. So there are (countably) infinitely many.*
Every positive real is a square, so the sign map gives an isomorphism

$$\mathbb{R}^*/(\mathbb{R}^*)^2 \cong \{\pm 1\}.$$

Every complex number can be written as a square of another complex number, so the group $\mathbb{C}^*/(\mathbb{C}^*)^2$ *is trivial.*

4.
(a). Find all singular points on the curve (defined over $\mathbb{C}$)

$$\mathcal{C} : f(X,Y) = X^4 + Y^3 - 3X^2Y = 0.$$

Solution: *For (x,y) to be a singular point, we need $f(x,y) = \frac{\partial f}{\partial X}(x,y) = \frac{\partial f}{\partial Y}(x,y) = 0$. In particular, we have $4x^3 - 6xy = 0$ and $3y^2 - 3x^2 = 0$. We deduce from these two equations that $y^2 = x^2$, hence $y = \pm x$, and then $4x^3 \mp 6x^2 = 0$. This gives the possibilities $(x,y) = (0,0), (\pm 3/2, 3/2)$. Only the first is a point on the curve, so the unique singular point is $(0,0)$.*

Find all tangents to $\mathcal{C}$ at the point $(0,0)$.
Solution: *See Comment 0.100 for how to do this computation. We write*

$$f(X,Y) = Y^3 - 3X^2Y + (\text{higher order terms})$$

and then factorise $Y^3 - 3X^2Y = Y(Y - \sqrt{3}X)(Y + \sqrt{3}X)$. So we have three tangents: $Y = 0, Y = \sqrt{3}X, Y = -\sqrt{3}X$. Try sketching the graph (e.g. with Wolfram Alpha.)

(b). Find all singular points on the curve (defined over $\mathbb{C}$)

$$\mathcal{C} : f(X,Y) = Y^2 - X(X^2-1)^2 = 0.$$

Solution: *Computing the partial derivative with respect to Y, we see that $y = 0$ is necessary for a singular point. So the possible singular points are $(0,0), (1,0), (-1,0)$. We have $\frac{\partial f}{\partial X} = -(X^2-1)^2 - 2X(X^2-1)(2X)$, so the two singular points are $(x,y) = (\pm 1, 0)$.*

Find all tangents to $\mathcal{C}$ at the points $(0,0)$ and $(1,0)$.
Solution: *The unique tangent at $(0,0)$ is $X = 0$. At $(1,0)$ we compute*

$$f(1+X,Y) = Y^2 - (1+X)(X^2+2X)^2 = Y^2 - 4X^2 + (\text{higher order terms}).$$

So we have two tangent lines at $(1,0)$, $Y = \pm 2(X-1)$.

5. Show that $\mathcal{C} : Y^2 = X^3 + AX + B$ is smooth if $4A^3 + 27B^2 \neq 0$ and we work over a field with characteristic $\neq 2$. What happens in characteristic 2?
Solution: *We set $f(X,Y) = Y^2 - X^3 - AX - B$. So $\frac{\partial f}{\partial Y}(x,y) = 0$ implies $y = 0$ (if $2 \neq 0$). So the possible singular points are $(x,0)$ where x is a root of the cubic $X^3 + AX + B$. The vanishing $\frac{\partial f}{\partial X}(x,0) = 0$ is then equivalent to x being a repeated root of the cubic. The discriminant of the cubic polynomial is $4A^3 + 27B^2$, so that gives the desired criterion for smoothness.*

In characteristic 2, we have $\frac{\partial f}{\partial Y}(x,y) = 0$ for all points (x,y). The equation $\frac{\partial f}{\partial X}(x,y) = 0$ gives us $x^2 = A$. So we have singular points (x,y) when $x^2 = A$ and $y^2 = B$.

6. For each of the following curves, find the irreducible components over $\mathbb{Q}$ and the irreducible components over $\mathbb{C}$.
(a). $\mathcal{C} : Y^2 = X^5$.
Solution: *We have to factorise the polynomial $Y^2 - X^5$ over $\mathbb{Q}$ and $\mathbb{C}$. We claim that $Y^2 - X^5$ is irreducible over $\mathbb{C}$. Here is a long-winded proof (a more efficient argument might exist!). View $Y^2 - X^5$ as an element of $(\mathbb{C}[X])[Y]$,*

i.e. a polynomial in Y with coefficients in $\mathbb{C}[X]$. We cannot factor it as a product of polynomials in Y with positive degree, since X^5 does not have a square root in $\mathbb{C}[X]$. So we deduce that if $Y^2 - X^5 = f_1(X,Y)f_2(X,Y)$, then one of the factors, say f_1 is actually just a polynomial in X. But then f_1 must actually be a constant, otherwise there would be a (complex) root x_0 of f_1 which would satisfy $y^2 - x_0^5 = 0$ for all $y \in \mathbb{C}$.

(b). $\mathcal{C} : Y^3 = X^3$.

Solution: *We factorise $Y^3 - X^3 = (Y - X)(Y^2 + XY + X^2)$. So we get $Y = X$ as one component, and $Y^2 + XY + X^2 = 0$ as another. The latter is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{C}$. We factorise*

$$Y^2 + XY + X^2 = (Y - \omega X)(Y - \bar{\omega} X)$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$, a primitive third root of unity, satisfies $\omega + \bar{\omega} = -1$ and $\omega\bar{\omega} = 1$. So over $\mathbb{C}$ the components are $Y = X$, $Y = \omega X$ and $Y = \bar{\omega} X$.

(c). $\mathcal{C} : Y^2 = X^3 + 1$.

Solution: *As for part (a), we observe that the polynomial $Y^2 - X^3 - 1$ is irreducible viewed as a polynomial in Y with coefficients in $\mathbb{C}[X]$. Similarly to part (a), it is also not divisible by a non-constant element of $\mathbb{C}[X]$. So this curve is irreducible.*

7.

(a). Find the discriminant of $X^4 - 2$.

Solution: *Write down the resultant matrix for $(X^4 - 2, 4X^3)$. Repeatedly doing Laplace expansion down the columns (from right to left) gives determinant $(-2)^3 4^4 = -2^{11}$.*

(b). Find the resultant of $X^3 - a$ and $X^2 - b$, where a, b are constants.

Solution: $b^3 - a^2$.

8. Find all intersection points (with multiplicities) over $\mathbb{C}$ of the curves: $X^3 + Y^3 = Z^3$ and $X^2 + Y^2 = Z^2$.

Solution: *See Comment 0.122. We first compute intersection points with $Z \neq 0$. We compute the resultant of $f(x,y) = x^3 + y^3 - 1$ and $g(x,y) = x^2 + y^2 - 1$, viewed as polynomials in the variable y over $\mathbb{C}[x]$. By 8(b) we get resultant $(1 - x^2)^3 - (1 - x^3)^2 = -(x - 1)^2 x^2 (2x^2 + 4x + 3)$. Let's consider the multiple roots $x = 0, x = 1$. We get, respectively, $y^3 = 1, y^2 = 1$ and $y^3 = 0, y^2 = 0$. So we have intersection points $(0 : 1 : 1)$ and $(1 : 0 : 1)$, both with multiplicity 2, and two (complex conjugate) intersection points with multiplicity 1: $(-1 + \frac{\sqrt{2}}{2}i : -1 - \frac{\sqrt{2}}{2}i : 1), (-1 - \frac{\sqrt{2}}{2}i : -1 + \frac{\sqrt{2}}{2}i : 1)$. That gives all the sections, since we've found 6 with multiplicity. We can also check directly that there are no intersection points with $Z = 0$.*

9.

(a). Decide whether each of $2, 3, 5, 10, 15$ are quadratic residues modulo 1009 (if you use quadratic reciprocity, this should not involve any lengthy computations).

Solution: *Note that 1009 is prime. We have $\left(\frac{2}{1009}\right) = +1$, since $1009 = 1$ mod 8.*

We have $\left(\frac{3}{1009}\right) = \left(\frac{1009}{3}\right) = \left(\frac{1}{3}\right) = +1$.
We have $\left(\frac{5}{1009}\right) = \left(\frac{1009}{5}\right) = \left(\frac{4}{5}\right) = +1$.
We have $\left(\frac{10}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{5}{1009}\right) = +1$.
We have $\left(\frac{15}{1009}\right) = \left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right) = +1$.

(b). Describe all primes p such that 3 is a quadratic residue modulo p. Describe all primes p such that 5 is a quadratic residue modulo p. Describe all primes p such that 10 is a quadratic residue modulo p.

Solution: *For $p > 3$, we have $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. So 3 is a QR mod p if and only if $p = \pm 1$ mod 12.*

For an odd prime $p \neq 5$, we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. So 5 is a QR mod p if and only if $p = \pm 1$ mod 5.

For an odd prime $p \neq 5$, we have $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$. So 10 is a QR mod p if and only if one of the following holds:

- $p \equiv \pm 1 \bmod 5$ and $\pm 1 \bmod 8$
- $p \equiv \pm 3 \bmod 5$ and $\pm 3 \bmod 8$

Equivalently, 10 is a QR mod p if and only if p mod $40 \in \{\pm 1, \pm 3, \pm 9, \pm 13\}$. Note that this covers 8 of the 16 congruence classes in $(\mathbb{Z}/40\mathbb{Z})^{\times}$.

10. Are there integers a, b, c, not all 0, such that $2a^2 + 5b^2 = c^2$?

Solution: *We can reduce to looking for solutions which are pairwise coprime. Then consider the equation mod 5. It says $2a^2 = c^2$ mod 5, which implies that $a = c = 0$ mod 5 (since 2 is not a QR mod 5). This contradicts coprimality of a and c. So there are no non-trivial integer solutions.*

11. For any $n \in \mathbb{N}$ define, as usual, Euler's ϕ-function by:

$$\phi(n) = \#\{x : 1 \leqslant x \leqslant n \text{ and } \gcd(x, n) = 1\}.$$

For any prime p, what is $\phi(p^r)$? For any distinct primes p_1, p_2, what is $\phi(p_1 p_2)$?

Solution: *There are p^{r-1} multiplies of p in the interval $[1, p^r]$. So $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.*

For each of the following examples of the type $a^b \pmod{n}$, reduce $a^b \pmod{n}$ to a member of $\{0, \ldots, n-1\}$.
$2^{12} \pmod{13}$, $3^{12} \pmod{13}$, $3^{24} \pmod{13}$, $3^{12000} \pmod{13}$, $3^{12002} \pmod{13}$,
$4^{24} \pmod{35}$, $4^{48} \pmod{35}$, $4^{48000001} \pmod{35}$,
$7^{24} \pmod{35}$, $7^{48} \pmod{35}$, $7^{48000001} \pmod{35}$.

Solution: *The first eight follow easily from Fermat–Euler:* $1, 1, 1, 1, 9, 1, 1, 4$.

We have $7^{24} = 0$ mod 7 and 1 mod 5. So $7^{24} = 21$ mod 35.

Squaring, we also have $7^{48} = 0$ mod 7 and 1 mod 5. So $7^{48} = 21$ mod 35.

In fact, the same argument shows that $7^{24k} = 21$ mod 35 for any positive integer k. So $7^{48000001} = 7 \times 21 = 7$ mod 35.