Elliptic Curves. MT 2024. Sheet 0.

This sheet is not intended to be handed in or discussed in classes. It is for you to use to reinforce the background material discussed in the preliminary reading file.

1. Determine whether the following are groups.
(a). The set of all 2×2 matrices under matrix multiplication.
(b). The set of all 2×2 matrices under matrix addition.

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). $\phi : \mathbb{Z}, + \to \mathbb{Q}^*, \times : x \mapsto x^2 + 1$.
(b). $\phi : \mathbb{Q}, + \to \mathbb{R}, + : w \mapsto \sqrt{2}\, w$.
(c). $\phi : \mathbb{Z}, + \to \mathbb{Z}/3\mathbb{Z}, + : x \mapsto 2x$.

3.
(a). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, decide whether the following are true or false: $3 = 1/27$, $-4 = 4$, $3 = 5/6$.
(b). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, write each of the following as a square free integer: $-2/27$, 16, 12, $1/3$.
(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}.
(d). How many elements are in each of the groups: $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, $\mathbb{R}^*/(\mathbb{R}^*)^2$, $\mathbb{C}^*/(\mathbb{C}^*)^2$?

4.
(a). Find all singular points on the curve

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

Find all tangents to $\mathcal{C}$ at the point $(0, 0)$.
(b). Find all singular points on the curve

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

Find all tangents to $\mathcal{C}$ at the points $(0, 0)$ and $(1, 0)$.

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?

6. For each of the following curves, find the irreducible components over $\mathbb{Q}$ and the irreducible components over $\mathbb{C}$.
(a). $\mathcal{C} : Y^2 = X^5$.
(b). $\mathcal{C} : Y^3 = X^3$.
(c). $\mathcal{C} : Y^2 = X^3 + 1$.

7.
(a). Find the discriminant of $X^4 - 2$.
(b). Find the resultant of $X^3 - a$ and $X^2 - b$, where a, b are constants.

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

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).

(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.

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

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 $\phi(p_1 p_2)$?

For each of the following examples of the type $a^b \pmod n$, reduce $a^b \pmod n$ to a member of $\{0, \ldots, n-1\}$.

$2^{12} \pmod{13}$, $3^{12} \pmod{13}$, $3^{24} \pmod{13}$, $3^{12000} \pmod{13}$, $3^{12002} \pmod{13}$,
$4^{24} \pmod{35}$, $4^{48} \pmod{35}$, $4^{48000001} \pmod{35}$,
$7^{24} \pmod{35}$, $7^{48} \pmod{35}$, $7^{48000001} \pmod{35}$.