Dr. Domenico Valloni
Dr. Alapan Mukhopadhyay
Léo Navarro Chafloque

EPFL, fall semester 2025
AG II - Schemes and sheaves

Hand-in 2

Exercise to hand in. *A family of curves of* $\mathrm{Spec}(\mathbb{Z})$. (Due Wednesday October 15, 12:00) Please write your solution in TEX.
Consider the closed sub-scheme of $\mathbb{P}^2_{\mathbb{Z}}$

$$C := V_+(X_0^2 + 5X_1^2 + 7X_2^2) = \mathrm{Proj}\left(\frac{\mathbb{Z}[X_0, X_1, X_2]}{(X_0^2 + 5X_1^2 + 7X_2^2)}\right) \subset \mathbb{P}^2_{\mathbb{Z}}.$$

For a prime number $p \in \mathbb{N}$, we denote by C_p the fiber of C at $(p) \in \mathrm{Spec}(\mathbb{Z})$.

(1) For which primes C_p is reduced?
(2) For which primes C_p is *geometrically* reduced?[1]
(3) Compute $\mathbb{F}_3$-rational points and $\mathbb{F}_5$-rational points of C_3 and C_5 respectively.
(4) We denote by $C_{\mathbb{Q}} = C \times \mathrm{Spec}(\mathbb{Q})$ the *generic fiber* of C. Show that $C_{\mathbb{Q}}$ has no $\mathbb{Q}$-rational points.

Solution key. Note the following.
Remark. Let A be an UFD. Suppose that $a \in A$ is square free. Then $t^2 - a$ is irreducible in $A[t]$.
We answer (1) and (2) at the same time by studying more precisely the behavior of the equations modulo p for each prime p.

(1) *The behavior for* $p = 2$. The equation modulo 2 is

$$X_0^2 + X_1^2 + X_2^2 = (X_0 + X_1 + X_2)^2.$$

We see that affine locally on $D_+(X_0)$ we have the equation $(1 + \frac{X_1}{X_0} + \frac{X_2}{X_0})^2$ which show that the (geometric) fiber is non-reduced.

(2) *The behavior for* $p = 5$. The equation modulo 5 is

$$X_0^2 - 3X_2^2.$$

By the remark above, because 3 is not a square in $\mathbb{F}_5$, this polynomial is irreducible, and therefore C_5 is integral, in particular, reduced. As 3 acquires a square-root α over $\mathbb{F}_{25}$, the equations becomes

$$(X_0 - \alpha X_2)(X_0 + \alpha X_2).$$

Therefore the base change to $\mathbb{F}_{25}$ is not integral. Namely it is the union of two reduced irreducible components, which are copies of $\mathbb{P}^1_{\mathbb{F}_{25}}$ intersecting at $(X_0, X_2) = [0 : 1 : 0]$. The same reasoning holds for the further base change to the algebraic closure. However it is reduced and geometrically reduced.

[1] This means that $C \times \mathrm{Spec}(\overline{\mathbb{F}}_p)$ is reduced.

(3) *The behavior for $p = 7$.* The equation modulo 7 is
$$X_0^2 - 2X_1^2.$$
But note that 3 is a square root of 2 modulo 7. Therefore we have
$$X_0^2 - 2X_1^2 = (X_0 - 3X_1)(X_0 + 3X_1).$$
Therefore C_7 is not integral being the union of two reduced irreducible components, which are copies of $\mathbb{P}^1_{\mathbb{F}_7}$. These two components intersect at $(X_0, X_1) = [0 : 0 : 1]$. Same holds for base change to the algebraic closure. However it is reduced and geometrically reduced.

(4) *The behavior for $p \neq 2, 5, 7$.* Because $-(5X_1^2+7X_2^2)$ is never a square in $\overline{\mathbb{F}}_p[X_0, X_1]$,[2] we see that C_p and $C \times \mathrm{Spec}(\overline{\mathbb{F}}_p)$ are irreducible, and therefore (geometrically) reduced.

Note that for any field k we have
$$C(k) = \{[a_0 \colon a_1 \colon a_2] \in \mathbb{P}^2_k(k) \mid a_0^2 + 5a_1^2 + 7a_2^2 = 0\}$$

(1) $p = 3$. Say $a_0 \neq 0$. We can suppose, because we are working in the projective space, that $a_0 = 1$. So we are looking for $a_1, a_2 \in \mathbb{F}_3$ such that
$$1 + a_2^2 = a_1^2.$$
As the only squares in $\mathbb{F}_3$ are 0 and 1, we see that $a_1 \neq 0$, and therefore $a_1^2 = 1$. So $a_2^2 = 0$, and then $a_2 = 0$. So we conclude that
$$[1 : 1 : 0] \quad [1 : 2 : 0]$$
are points and the only ones with $a_1 \neq 0$. The other case is when $a_0 = 0$. So we are looking for points $[0 : a_1 : a_2]$ with
$$a_2^2 = a_1^2$$
Because they can not be zero, we see that we have
$$[0 : 1 : 1] \quad [0 : 1 : 2]$$
This concludes.

(2) $p = 5$. We are looking for $\mathbb{F}_5$-projective points $[a_0 \colon a_1 \colon a_2]$ with
$$a_0^2 = 3a_2^2.$$
Squares in $\mathbb{F}_5$ are $0, 1$ and -1. In particular 3 and -3 are not squares. We deduce that $a_0 = a_2 = 0$. The only $\mathbb{F}_5$-rational points of C is therefore
$$[0 \colon 1 \colon 0].$$

(3) *Generic fiber.* Note that a $\mathbb{Q}$-point can be supposed to be with coefficients in $\mathbb{Z}$, because we can clear the denominators in the projective space. Also we can suppose that a_0, a_1, a_2 have no common divisors in $\mathbb{Z}$, because we would be able to divide by this common divisor and not change the $\mathbb{Q}$-projective point. We therefore suppose this below.

[2] Indeed if it was, say $g^2 = -(5X_1^2+7X_2^2)$ then the g would divide the partial derivative of $5X_1^2 + 7X_2^2$ with respect to X_1 and X_2 by the Leibniz rule. So g would divide X_1 and X_2 implying that g is a unit.

Reducing modulo 5, using the above analysis, we see that $5 \mid a_0$ and $5 \mid a_2$, say $a_0 = 5a_0'$ and $a_2 = 5a_2'$. So

$$25a_0'^2 + 5a_1^2 + 25a_2'^2 = 0$$

dividing by 5, we get that $5 \mid a_1$ a contradiction.

□