ALGEBRAIC GEOMETRY

HOMEWORK 1

Due Th 19.02.04

(1) Find all points on the following curves with coordinates in the fields $F_2$, $F_3$, $F_4$ and $F_5$:

- the line $L : 2X - Y + 1 = 0$;
- the unit circle $U : X^2 + Y^2 = 1$;
- the curve $C : X^2Y + XY^2 + 1 = 0$.

1. Consider the line $L : 2X - Y + 1 = 0$; over fields with characteristic 2 such as $F_2$ and $F_4$, the equation becomes $Y = 1$, hence $L(F_2) = \{(0,1), (1,1)\}$ and $L(F_4) = \{(a,1) : a \in F_4\}$. Note that a line over a finite field with $q$ elements always has $q$ points.

Also observe that $\mathbb{Z}/4\mathbb{Z}$ is not a field (it has zero divisors since $2 \cdot 2 \equiv 0 \text{ mod } 4$), in particular it is not the field $F_4$ with 4 elements.

Finally, straightforward calculations show that $L(F_3) = \{(0,1), (1,0), (2,1)\}$ and $L(F_5) = \{(0,1), (1,0), (2,1)\}$.

2. Consider the unit circle $U : X^2 + Y^2 = 1$. We find

- $U(F_2) = \{(0,1), (1,0)\}$,
- $U(F_3) = \{(0,0), (\pm 1,0)\}$,
- $U(F_4) = \{(0,0), (\pm 1,0)\}$,
- $U(F_5) = \{(0,0), (\pm 1,0)\}$.

3. Now let $C : X^2Y + XY^2 + 1 = 0$. We find

- $C(F_2) = \emptyset$;
- $C(F_3) = \{(1,1)\}$,
- $C(F_4) = \{(x,1), (x,x+1), (x,1), (x,x+1), (x+1,1), (x+1,x)\}$,
- $C(F_5) = \{(3,3), (3,4), (4,3)\}$.

Here’s how to do the last example with pari: type in

```
p=5;for(x=0,4,for(y=0,5,if(Mod(x^2*y+x*y^2+1,p),,print(x," ",y))))
```

and press Enter; you will get the three points as output. If you replace $p = 5$ by $p = 7$, you get six points.

(2) Determine the rational points on the hyperbola $X^2 - 2Y^2 = 1$ with as many methods as possible. Do the same for the circle $X^2 + Y^2 = 2$.

The geometric method definitely is the simplest. Start with $P = (-1,0)$, take a line $y = t(x+1)$ through $P$ with slope $t$, compute the second point of intersection with the hyperbola, and get

$$x = \frac{1 + 2t^2}{1 - 2t^2}, \quad y = \frac{2t}{1 - 2t^2}.$$
Such formulas for the equation $X^2 - dY^2 = 1$ were already known to the Hindus more than a thousand years ago. Note that the denominator does not vanish for rational $t$ since $\sqrt{2}$ is irrational.

For the circle with radius $\sqrt{2}$ you get similarly, if you start with $P = (1, 1)$, that

$$x = \frac{t^2 - 2t - 1}{1 + t^2}, \quad y = \frac{-t^2 - 2t + 1}{1 + t^2}.$$

You can check this with pari by typing

$$x = \frac{(t^2-2t-1)}{(1+t^2)}; \quad y = \frac{(-t^2-2t+1)}{(1+t^2)}; \quad x^2 + y^2.$$

The output will be the number 2.

The algebraic method only works for integers; thus we have to clear denominators by putting $x = \frac{a}{c}, \quad y = \frac{b}{c},$ and solve $a^2 - 2b^2 = c^2$. Since common divisors can be cancelled, we may assume that $(a, b) = (a, c) = 1$.

In particular, $a$ (and thus $c$) must be odd, since otherwise $2$ would divide $a$ and $c$. Now $2b^2 = a^2 - c^2 = (a - c)(a + c)$. Since both $a$ and $c$ are odd and coprime, we find gcd$(a, c) = 2$. Assume that $a - c$ is divisible exactly by $2$ (if it is divisible by $4$, then $a + c$ is divisible exactly by $2$); then $\frac{a-c}{2}$ and $a + c$ are coprime integers whose product is a square. Thus $a - c = 2r^2$, $a + c = 4s^2$, giving $a = r^2 + 2s^2$ and $c = 2s^2 - r^2$. Finally $b^2 = 4r^2s^2$, hence the general (primitive) solution is $(a, b, c) = (2s^2 + r^2, 2rs, 2s^2 - r^2)$.

Converting back to fractions we find

$$x = \frac{2s^2 + r^2}{2s^2 - r^2}, \quad y = \frac{2rs}{2s^2 - r^2},$$

or, by using $t = s/r$,

$$x = \frac{2t^2 + 1}{2t^2 - 1}, \quad y = \frac{2t}{2t^2 - 1}.$$

The Galois theory approach also works: if $x^2 - 2y^2 = 1$, then $x + y\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ has norm 1, so Hilbert 90 gives

$$x + y\sqrt{2} = \frac{a + b \sqrt{2}}{a - b \sqrt{2}} = \frac{a^2 + 2b^2 + 2ab \sqrt{2}}{a^2 - 2b^2},$$

and comparing the coefficients (note that $\mathbb{Q}(\sqrt{2})$ is a $\mathbb{Q}$-vector space with basis $1$ and $\sqrt{2}$) gives the solution

$$x = \frac{a^2 + 2b^2}{a^2 - 2b^2}, \quad y = \frac{2ab}{a^2 - 2b^2}.$$

(3) The parametrization

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}$$

of the unit circle $X^2 + Y^2 = 1$ over the field $\mathbb{Q}$ can be interpreted as a $\mathbb{Q}(t)$-rational point on the unit circle itself.

Use the group law to compute $2P$ and $P + Q$, where $P$ is the parametrization above and where $Q = \left(\frac{3}{4}, \frac{1}{4}\right)$. Do the points $2P$ and $P + Q$ also give
parametrizations of the unit circle? For example, do they give the point (3/5, 4/5)?

The group law is given by

\[(r, s) + (t, u) = (rt - su, rt + su).\]

Thus

\[2P = P + P = \left( \frac{t^4 - 6t^2 + 1}{(t^2 + 1)^2}, \frac{4t(1 - t^2)}{(t^2 + 1)^2} \right).\]

It is clear that this parametrization will give every rational point on the unit circle that can be written as 2Q for some rational point Q (because P will represent Q, hence 2P will represent 2Q). However, 2P will not parametrize the other points, such as \((3/5, 4/5)\): in fact, this leads to

\[5(t^4 - 6t^2 + 1) = 3((t^2 + 1)^2),\]

hence to \(t^4 - 18t^2 + 1 = 0\). The equation \(s^2 - 18s + 1\) has discriminant 320, which is not a square; thus the roots of the equation above are not rational.

Is it a parametrization? In classical algebraic geometry, a parametrization is a nonconstant rational map from the line to the curve; in this sense, 2P is a parametrization. A parametrization is called proper if it misses only finitely many points; the factorization 2P misses infinitely many points (all points \((\frac{3}{5}, \frac{4}{5}) + 2Q\)), hence is not proper.

Similarly, the group law gives

\[P + Q = \left( \frac{(t + 3)(1 - 3t)}{5(t^2 + 1)}, \frac{2(2 - t)(2t + 1)}{5(t^2 + 1)} \right).\]

This can be shown to be a proper parametrization.

(4) Use sing surf to sketch the following curves:

(a) \(y^2 - x^3 - x^2 = 0\);
(b) \(y^3 + y^2x - x^2 = 0\);
(c) Folium of Descartes: \(x^3 + y^3 - 3xy = 0\) (make sure you leave a blank space between x and y).
(d) 5-leaved rose: \((x^2 + y^2)^3 - 5x^2y + 10x^2y^3 - y^5\).

All these curves have the property that lines through (0, 0) intersect the curve in exactly one other point. Use the sweeping lines technique to find all rational points on these curves.

The origin O is a singular point (definition later) in all examples, and the lines \(y = tx\) intersect the curves in O and exactly one other point; thus the sweeping lines technique will give us a parametrization of these curves.

- \(y^2 - x^3 - x^2 = 0\): \(x = t^2 - 1, y = t^3 - t\).
- \(y^3 + y^2x - x^2 = 0\): \(x = \frac{1}{t^2 + 1}, y = \frac{1}{t^2 + 1}\).
- \(x^3 + y^3 - 3xy = 0\): \(x = \frac{3t}{t^2 + 1}, y = \frac{3t^2}{t^2 + 1}\).
- \((x^2 + y^2)^3 - 5x^2y + 10x^2y^3 - y^5\): \(x = \frac{t^2 - 10t^2 + 5t}{(t^2 + 1)^2}, y = \frac{t^2(t^4 - 10t^2 + 5t)}{(t^2 + 1)^3}\).