19.02.

1 Basic notions

1.1. Describe sets V_f and $V_f(\mathbb{R})$ if

(a) $f = x^2 - y^2 \in \mathbb{R}[x, y]$,

(b) $f = (x^2 - y^2)(x + y) \in \mathbb{R}[x, y]$,

(c) $f = x^3 - y^3 \in \mathbb{R}[x, y]$

(a) Since linear polynomials $x+y$ and $x-y$ are irreducible and $x^2-y^2 = (x+y)(x-y)$, we have irreducible decomposition of the curve:

$$V_{x^2-y^2} = V_{x+y} \cup V_{x-y}, \quad V_{x^2-y^2}(\mathbb{R}) = V_{x+y}(\mathbb{R}) \cup V_{x-y}(\mathbb{R}),$$

where $V_{x+y} = \mathrm{Span}_{\mathbb{C}}((1, -1))$ and $V_{x-y} = \mathrm{Span}_{\mathbb{C}}((1, 1))$ are complex lines and $V_{x+y}(\mathbb{R}) = \mathrm{Span}_{\mathbb{R}}((1, -1))$ and $V_{x-y}(\mathbb{R}) = \mathrm{Span}_{\mathbb{R}}((1, 1))$ are real lines.

(b) Since

$$\sqrt{((x^2 - y^2)(x + y))} = \sqrt{((x - y)(x + y)^2)} = ((x - y)(x + y)) = (x^2 - y^2),$$

we have the same irreducible decomposition of V_f and $V_f(\mathbb{R})$ into two lines as in (a)

$$V_{(x^2-y^2)(x+y)} = V_{x+y} \cup V_{x-y}, \quad V_{(x^2-y^2)(x+y)}(\mathbb{R}) = V_{x+y}(\mathbb{R}) \cup V_{x-y}(\mathbb{R}),$$

(c) We can easily calculate the decomposition of $x^3 - y^3$ into linear factors in $\mathbb{C}[x, y]$:

$$x^3 - y^3 = (x - y)(x^2 + xy + y^2) = (x - y)(x + (\frac{1}{2} + \frac{\sqrt{3}}{2}i)y)(x + (\frac{1}{2} - \frac{\sqrt{3}}{2}i)y),$$

hence $V_{x^3-y^3} = V_{x-y} \cup V_{x+(\frac{1}{2}+\frac{\sqrt{3}}{2}i)y} \cup V_{x+(\frac{1}{2}-\frac{\sqrt{3}}{2}i)y}$ is an irreducible decomposition into three complex lines. If we consider $V_{x^3-y^3}(\mathbb{R}) = V_{x-y}(\mathbb{R}) \cup V_{x^2+xy+y^2}(\mathbb{R})$. Now revoking linear algebra we can show that the real quadratic form $g_2 = x^2 + xy + y^2$ is positively definite, since its matrix

$$\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \sim_s \begin{pmatrix} 1 & 0 \\ 0 & \frac{3}{4} \end{pmatrix}$$

is positively definite, hence $\{(x, y) \in \mathbb{R}^2 \mid g_2(x, y) = 0\} = \{(0, 0)\}$. It means that $V_{x^3-y^3}(\mathbb{R}) = V_{x-y}(\mathbb{R}) = \mathrm{Span}_{\mathbb{R}}((1, 1))$ is a real line. □

26.02.

1.2. Describe the function field $K(V_f)$ for a general field K and

(a) $f = x + y$,

(b) $f = ax + by + c$ where $(a, b) \neq (0, 0)$.

First note that any non-constant linear polynomial is irreducible and that the function field $K(V_f)$ is a filed of fractions of the coordinate ring $K[V_f]$. So it is enough to describe coordinate rings.

(a) To find the coordinate ring $K[V_{x+y}] \cong K[x,y]/(x+y)$, we intend to use the First Isomorphism Theorem. Consider evaluating homomorphism $\varphi : K[x,y] \to K[x]$ given by $\varphi(p) = p(x,-x)$, then, obviously $x+y \in \ker(\varphi)$, hence $(x+y) \subseteq \ker(\varphi)$. If $q(y) \in \ker(\varphi)$, where we consider q as o polynomial in variable y with coefficients in the domain $K[x]$, we can observe that $-x$ is a root of q, thus $(y+x) \mid q$ and so $q \in (x+y)$. Since $\varphi(p)$ is surjective and we have shown that $\ker(\varphi) = (x+y)$ and the First Isomorphism Theorem gives us

$$K[V_{x+y}] \cong K[x,y]/(x+y) = K[x,y]/\ker(\varphi) \cong K[x].$$

It means that the function field $K(V_{x+y})$ is isomorphic to the field of rational functions in one variable $K(x)$.

(b) W.l.o.g we may suppose that $b \neq 0$, otherwise we switch the variables x and y. We repeat the arguments of (a) for the evaluating homomorphism $\psi : K[x,y] \to K[x]$ given by the rule $\psi(p) = p(x, -\frac{a}{b}x - \frac{c}{b})$, which is onto $K[x]$. Then $\ker(\psi) = (ax+by+c)$ and by the First Isomorphism Theorem we get the isomorphism.

$$K[V_{ax+by+c}] \cong K[x,y]/(ax+by+c) = K[x,y]/\ker(\psi) \cong K[x].$$

Thus $K(V_{ax+by+c}) \cong K(x)$ again. $\square$

1.3. Let p be a prime number, $q = p^n$ for $n \in \mathbb{N}$ and $f \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$.

(a) If f is irreducible, describe a rupture field of f.

(b) If f is irreducible, describe a splitting field of f.

(c) For which k does the field $\mathbb{F}_{q^k}$ contain a root of f?

(d) Construct an algebraic closure of the field $\mathbb{F}_p$.

(a), (b) We know that the factor ring $\mathbb{F}_q[x]/(f)$ is a field containing a root of f, i.e. a rupture field of f. Note that $\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^{\deg f}}$ is even a splitting filed of polynomials f and $x^{q^{\deg f}} - x$ and that $f \mid x^{q^{\deg f}} - x$ in $\mathbb{F}_q[x]$.

(c) Since $\mathbb{F}_{q^k}$ is a splitting filed of a polynomial $x^{q^k} - x = \prod_{a \in \mathbb{F}_{q^k}} x - a$ and it contains all roots of irreducible polynomials of degree dividing k, $\mathbb{F}_{q^k}$ contain a root of f if and only if $\deg \gcd(f, x^{q^k} - x) > 0$, which is true if and only if there exists an irreducible factor of f of degree dividing k.

(d) Recall that $\mathbb{F}_{p^{k!}}$ is a subfield of $\mathbb{F}_{p^{(k+1)!}}$ since $\mathbb{F}_{p^a} \leq \mathbb{F}_{p^b}$ iff $a \mid b$. Put $K = \bigcup_{k \in \mathbb{N}} \mathbb{F}_{p^{k!}}$. Observer that for each $\alpha \in K$ there exists m for which α is a root of the polynomial $x^{p^m} - x$, hence $K \subseteq \overline{\mathbb{F}_p}$. On the other hand let $f \in K[x]$. Then there exist k such that $f \in \mathbb{F}_{p^{k!}}[x]$ and by (c) there is $l \leq \deg f$ such that $\mathbb{F}_{p^{k!l}} \leq \mathbb{F}_{p^{(kl)!}} \leq K$ contains a root of f. This proves that K is an algebraic closure of the field $\mathbb{F}_p$. $\square$

05.03.

1.4. Let $f \in \mathbb{R}[x,y]$ and $F \in \mathbb{R}[X,Y,Z]$ be its homogenization. Describe sets V_Z, $V_f(\mathbb{R})$, and points in infinity of V_F and $V_F(\mathbb{R})$ if

(a) $f = x^2 + y^2 - 1$,

(b) $f = x^2 + y$.

First observe that

$$V_Z = \{(a : b : c) \in \mathbb{P}^2 \mid c = 0\} = \{(a : b : 0) \in \mathbb{P}^2 \mid (a, b) \in \mathbb{C}^2 \setminus (0, 0)\} = \mathbb{P}^2 \setminus \mathbb{A}^2.$$

(a) Clearly, $V_f(\mathbb{R})$ is a unit circle. Now, we can easily determine the homogenization $F = X^2 + Y^2 - Z^2$ of f. The points in infinity $V_F \cap V_Z$ of V_F are those satisfying $X^2+Y^2 = Z^2 = 0$. Since $X^2+Y^2 = (X+iY)(X-iY)$, we get that $V_F \cap V_Z = \{(1, \pm i, 0)\}$ and $V_F(\mathbb{R}) \cap V_Z = \emptyset$

(b) This time $V_f(\mathbb{R})$ forms a parabola satisfying the equation $y = -x^2$. Since the homogenization of f is the polynomial $F = X^2 + YZ$ and the points in infinity $V_F \cap V_Z$ of V_F satisfy the equality $X^2 + YZ = X^2 = 0$, we can easily compute that $V_F \cap V_Z = V_F(\mathbb{R}) \cap V_Z = \{(0, 1, 0)\}$. □

1.5. Let $\beta = \frac{x^3+1}{(x^2-1)^2} \in \mathbb{R}(x)$. Calculate in the function field $\mathbb{R}(x)$ over $\mathbb{R}$ the values of valuations:

(a) $v_{x+1}(\beta)$,

(b) $v_{x-1}(\beta)$,

(c) $v_x(\beta)$,

(d) $v_{x^2-x+1}(\beta)$.

Recall that $v_p(a) = \max(k \mid p^k \mid a)$ and $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ for $a, b \in \mathbb{R}[x] \setminus \{(0)\}$.
(a) $v_{x+1}(\beta) = v_{x+1}(x^2 - 1) - v_{x+1}(x^2 - 1)^2 = 1 - 2 = -1$.
(b) $v_{x-1}(\beta) = v_{x-1}(x^2 - 1) - v_{x-1}(x^2 - 1)^2 = 0 - 2 = -2$.
(c) $v_x(\beta) = v_x(x^2 - 1) - v_x(x^2 - 1)^2 = 0 - 0 = 0$.
(d) $v_{x^2-x+1}(\beta) = v_{x^2-x+1}(x^2 - 1) - v_{x^2-x+1}(x^2 - 1)^2 = 1 - 0 = 1$. □

1.6. Let $v_\infty : K(x) \to \mathbb{Z} \cup \{\infty\}$ be defined by the rules

$$v_\infty(0) = \infty, \quad v_\infty(\frac{a}{b}) = \deg(b) - \deg(a)$$

for all $a, b \in K[x]\setminus\{(0)\}$. Prove that v_∞ is a normalized discrete valuation on the function field $K(x)$ over a field K.

First observe that the definition of v_∞ is correct. If $a, b, c, d \in K[x] \setminus \{(0)\}$ satisfies $\frac{a}{b} = \frac{c}{d}$ then

$$v_\infty(\frac{a}{b}) = \deg(b) - \deg(a) = \deg(d) - \deg(c) = v_\infty(\frac{c}{d}).$$

since $ad = bc$ and so $\deg(a) + \deg(d) = \deg(b) + \deg(c)$.

Let $a, b, c, d \in K[x] \setminus \{(0)\}$. Then

$$v_\infty(\frac{a}{b}\frac{c}{d}) = v_\infty(\frac{ac}{bd}) = \deg(bd)-\deg(ac) = \deg(b)+\deg(d)-\deg(a)-\deg(c) = v_\infty(\frac{a}{b})+v_\infty(\frac{c}{d})$$

and

$$v_\infty(\frac{a}{b} + \frac{c}{d}) = v_\infty(\frac{ad + bc}{bd}) = \deg(b) + \deg(d) - \deg(ad + bc).$$

As $\deg(ad+bc) \leq \max(\deg(ad), \deg(bc)) = \max(\deg(a)+\deg(d), \deg(b)+\deg(c))$ we get that

$$v_\infty(\frac{a}{b}+\frac{c}{d}) = \deg(b)+\deg(d)-\deg(ad+bc) \geq$$
$$\deg(b)+\deg(d)-\min(\deg(a)+\deg(d), \deg(b)+\deg(c)) =$$
$$= \min(\deg(b)-\deg(a), \deg(d)-\deg(c)) = \min(v_\infty(\frac{a}{b}), v_\infty(\frac{c}{d})).$$

Finally note that $v_\infty(\frac{1}{x}) = 1$ and that $v_\infty(a) = \infty$ if and only if $a = 0$, which finishes the proof that all axioms (DV1)–(DV4) are satisfied. $\square$

12.03.

2 Weierstrass equations

2.1. Find a short WEP which is $\mathbb{R}$-equivalent to the WEP

$$w = y^2 + y(2x+2) - (x^3 - 4x^2 + 1) \in \mathbb{R}[x, y].$$

We apply standard linear algebra machinery of Lemma 2.1. First, we remove the term $2xy$. Let $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in U_2(\mathbb{R})$, which represents replacement of y by $y - x$ and compute

$$\vartheta_A^*(w) = (y-x)^2 + (y-x)(2x+2) - (x^3 - 4x^2 + 1) = y^2 + 2y - (x^3 - 3x^2 + 2x + 1).$$

Now we use $b = (1, -1)$ to exclude monomials y and x^2:

$$\tau_b^* \vartheta_A^*(w) = (y-1)^2 + 2(y-1) - ((x+1)^3 - 3(x+1)^2 + 2(x+1) + 1) = y^2 - (x^3 - x + 2).$$

$\square$

2.2. Show that the real polynomial $\tilde{w} = y^2 - (x^3 - x + 2)$ is

(a) $\mathbb{R}$-equivalent to $y^2 - (x^3 - \frac{1}{16}x + \frac{1}{32})$,

(b) $\mathbb{C}$-equivalent to $y^2 - (x^3 - x - 2)$.

(a) It is enough to take the matrix $A_1 = \begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$ and compute $\vartheta_{A_1}^*(\tilde{w}) = 64y^2 - 64(x^3 - \frac{1}{16}x + \frac{1}{32})$, hence $y^2 - (x^3 - x + 2)$ and $y^2 - (x^3 - \frac{1}{16}x + \frac{1}{32})$ are $\mathbb{R}$-equivalent by the Fact from the lecture where we take $c = 2$ and $d = 0$.

(b) Now, we chose the complex matrix $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}$ and calculate

$$\vartheta_{A_2}^*(\tilde{w}) = -y^2 - (-x^3 + x + 2).$$

Then the same argument as in (a) proves that $\mathbb{C}$-equivalence of $\tilde{w}$ and $y^2 - (x^3 - x - 2)$. $\square$

19.03.

2.3. Decide which of the following WEPs are smooth and find all singularities of singular ones:

(a) $y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$,

(b) $(y + 1)^2 - (x^3 + 1) \in \mathbb{F}_3[x, y]$,

(c) $y^2 - (x^3 - x^2 - x + 1) \in \mathbb{R}[x, y]$,

(d) $y^2 + y(2x + 2) - (x^3 - 4x^2 + 1) \in \mathbb{R}[x, y]$ (from 2.1).

(a) $y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$ is a smooth short WEP by Proposition 2.2 since the polynomial $x^3 + 1$ is separable. The same result follows from the Corollary 2.3 as

$$4 \cdot 0^3 + 27 \cdot 1^2 = 1 \neq 0.$$

(b) $w = (y + 1)^2 - (x^3 + 1) \in \mathbb{F}_3[x, y]$ is a singular WEP, since w is $\mathbb{F}_3$-equivalent to $y^2 - (x^3 + 1)$ and the polynomial $x^3 + 1 = (x + 1)^3$ has the root 2 of multiplicity 3. It is easy to see that the only singularity is $(2, 2)$,

(c) $y^2 - (x^3 - x^2 - x + 1) \in \mathbb{R}[x, y]$ is also a singular WEP, since the root 1 of $x^3 - x^2 - x + 1$ has the multiplicity 2. Then the singularity is $(1, 0)$.

(d) Using the equivalent short form $y^2 - (x^3 - x + 2)$ computed in 2.1 we can easily see that the polynomial $f = x^3 - x + 2$ is separable. Indeed, the roots of $f' = 3x - 1$ are $\pm\frac{1}{\sqrt{3}}$ and $f(\pm\frac{1}{\sqrt{3}}) \neq 0$, so there is no multiple root of f. This means that $y^2 - (x^3 - x + 2)$ is smooth by Proposition 2.2, hence $y^2 + y(2x + 2) - (x^3 - 4x^2 + 1)$ is smooth by Fact from the lecture. □

2.4. Let $f = y - x^3 \in \mathbb{C}[x, y]$. Find all singularities of V_f and of the projective extension V_F.

Since $\frac{\partial f}{\partial y} = 1$, the tangent $t_\alpha(f) \neq 0$ for each $\alpha \in V_f$, hence V_f is a smooth affine curve.

Clearly, $F = YZ^2 - X^3$. Then $V_F \cap V_F = \{(0 : 1 : 0)\}$ since

$$F(\alpha : \beta : 0) = 0 \Leftrightarrow \alpha^3 = 0 \Leftrightarrow \alpha = 0 \Leftrightarrow (\alpha : \beta : 0) = (0 : 1 : 0).$$

We calculate

$$\frac{\partial F}{\partial X} = -3X^2, \quad \frac{\partial F}{\partial Y} = Z^2, \quad \frac{\partial F}{\partial Z} = 2YZ,$$

and so $t_{(0:1:0)}(F) = 0$. Thus F is singular at $(0 : 1 : 0)$ and V_F is a singular projective curve. □

26.03.

2.5. For the elliptic curve C given by the WEP $w = y^2 - (x^3 + x + 2) \in \mathbb{F}_5[x, y]$ compute the tables of the group operations $\ominus$, $\oplus$ on $C(\mathbb{F}_5)$.

Note that $f = x^3 + x + 2 = (x+1)(x^2 - x + 2)$ where $x^2 - x + 2$ is irreducible in $\mathbb{F}_5[x, y]$, which means that f is a separable polynomial. Hence w is a smooth WEP and so V_w is an elliptic curve. Now, we compute $f(x)$ for all $x \in \mathbb{F}_5$:

	0	1	2	−2	−1
x^3	0	1	−2	2	−1
$f(x)$	2	−1	2	2	0

Since $y^2 \in \{0, 1, -1\}$, we can easily find all zeros

$$V_w(\mathbb{F}_5) = \{(1, 2), (1, -2), (-1, 0)\},$$

which means that the group $C(\mathbb{F}_5) = \{o, (1, 2), (1, -2), (-1, 0)\}$ is of the order 4. Since w is of a short form, we know that $\ominus(x, y) = (x, -y)$ hence we have the table of the unary operation

$\ominus$	o	$(1,2)$	$(1,-2)$	$(-1,0)$
	o	$(1,-2)$	$(1,2)$	$(-1,0)$

From the table we can see that the group has exactly one element $(-1, 0)$ of the order 2, so $C(\mathbb{F}_5) \cong \mathbb{Z}_4$ is a cyclic group. We can directly draw the table of the operation $\oplus$

$\oplus$	o	$(1,2)$	$(1,-2)$	$(-1,0)$
o	o	$(1,2)$	$(1,-2)$	$(-1,0)$
$(1,2)$	$(1,2)$	$(-1,0)$	o	$(1,-2)$
$(1,-2)$	$(1,-2)$	o	$(-1,0)$	$(1,2)$
$(-1,0)$	$(-1,0)$	$(1,-2)$	$(1,2)$	o

□

2.6. Describe the group $C(\mathbb{F}_7)$ of the elliptic curve C given by the WEP w, and if it is cyclic, find its generator.

(a) $w = y^2 - (x^3 + 3) \in \mathbb{F}_7[x, y]$,

(b) $w = y^2 - (x^3 + 2x^2 - x - 2) \in \mathbb{F}_7[x, y]$.

(a) First we compute a table of values

	0	1	2	3	−3	−2	−1
y^2	0	1	−3	2	2	−3	1
x^3	0	1	1	−1	1	−1	−1
$f(x)$	3	−3	−3	2	−3	2	2

Since f has no root in $\mathbb{F}_7$ by the table, it is irreducible and so separable. It implies that w is a smooth WEP and we can easily find all $\mathbb{F}_7$-rational points of the curve

$$V_w(\mathbb{F}_7) = \{(1, \pm 2), (2, \pm 2), (3, \pm 3), (-3, \pm 2), (-2, \pm 3), (-1, \pm 3)\}.$$

Since $C(\mathbb{F}_7) = V_w(\mathbb{F}_7) \cup \{o\}$ has 13 elements, it is a cyclic group and $\langle a \rangle = C(\mathbb{F}_7)$ for each $a \in V_w(\mathbb{F}_7)$.

(b) Since $x^3 + 2x^2 - x - 2 = (x-1)(x+1)(x+2)$, the WEP is smooth and we have three zeros $(1, 0)$, $(-1, 0)$, $(-2, 0)$ compute the table of the binary group operation $\oplus$ on $C(\mathbb{F}_7)$. It remains to observe that $y^2 \in \{0, 1, -3, 2\}$ and compute $f(x)$ for $x \in \{0, 2, 3, -3\}$:

	0	2	3	−3
$f(x)$	−2	−2	−2	−1

which shows that $C(\mathbb{F}_7) = \{o, (1,0), (-1,0), (-2,0)\}$ is a group of the order 4. As $\ominus a = a$ for every $a \in C(\mathbb{F}_7)$, we can see that $C(\mathbb{F}_7) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

2.7. For the curve V_w from 2.6(a) describe all points of

(a) secant passing points $(1,2)$ and $(3,3)$, and compute $(1,2) \oplus (3,3)$,

(b) tangent at the point $(1,2)$, and compute $(1,2) \oplus (1,2) = [2](1,2)$.

(a) It is easy to calculate the slope $\lambda = \frac{2-3}{1-3} = -3$. Then the secant V_{y+3x+2} contains all points (x,y) satisfying $y = -3x - 2$, hence

$$V_{y+3x+2} = \{(0,-2), (1,2), (2,-1), (3,3), (-3,0), (-2,-3), (-1,1)\}.$$

To find $(1,2) \oplus (3,3)$ we can either find $V_{y+3x+2} \cap V_w = \{(1,2), (3,3), (-2,-3)\}$, hence $(1,2) \oplus (2,3) = \ominus(-2,-3) = (-2,3)$ or we can apply formula

$$\gamma_1 = \lambda^2 - \alpha_1 - \beta_1 = 2 - 1 - 3 = -2, \quad \gamma_2 = \lambda(\alpha_1 - \gamma_1) - \alpha_2 = -3(1+2) - 2 = -4 = 3,$$

and $(1,2) \oplus (2,3) = (\gamma_1, \gamma_2)$.

02.04.

(b) This time we calculate the slope $\lambda = \frac{3 \cdot 1^2}{2 \cdot 2} = -1$, hence the tangent is

$$V_{y+x-3} = \{(0,3), (1,2), (2,1), (3,0), (-3,-1), (-2,-2), (-1,-3)\}.$$

and $[2](1,2) = (\gamma_1, \gamma_2) = (-1,3)$ as

$$\gamma_1 = \lambda^2 - 2\alpha_1 = 1 - 2 = -1, \quad \gamma_2 = \lambda(\alpha_1 - \gamma_1) - \alpha_2 = -1(1+1) - 2 = 3.$$

□

09.04.

3 Montgomery curves

3.1. Find the Montgomery's ladder for (a) $n = 98$, (b) $n = 137$

(a) Note that $l_2(98) = \lfloor \log_2(98) \rfloor + 1 = 7$ and recall that the Montgomery's ladder $\{(n_i, n'_i)\}_{i=1}^{7}$ is done by the recurrent condition $n_{i-1} = \lfloor \frac{n_i}{2} \rfloor$ and by $n'_i = n_i + 1$. Thus we can easily compute

i	7	6	5	4	3	2	1
n_i	98	49	24	12	6	3	1
n'_i	99	50	25	13	7	4	2

(b) This time $l_2(137) = \lfloor \log_2(137) \rfloor + 1 = 8$, hence the table of the Montgomery's ladder is

i	8	7	6	5	4	3	2	1
n_i	137	68	34	17	8	4	2	1
n'_i	138	69	35	18	9	5	3	2

□

3.2. Describe the calculation of $[98]P$ for an element P of Montgomery curve of order greater then 98 using the Montgomery's ladder.

From the calculation of the Montgomery's ladder in 3.1 we obtain the binary notation $(98)_2 = a_6a_5a_4a_3a_2a_1a_0 = 1100010$ for $98 = \sum_{i=0}^{6} a_i 2^i$. Recall that the run of calculation $([n_j]P, [n'_j]P])$, depends on the value of the bit a_{7-j}, namely

- if $a_{7-j} = 0$ then $[n_j]P = [2][n_{j-1}]P$ and $[n'_j]P = [n_{j-1}]P \oplus [n'_{j-1}]P$,
- if $a_{7-j} = 1$ then $[n_j]P = [n_{j-1}]P \oplus [n'_{j-1}]P$ and $[n'_j]P = [2][n'_{j-1}]P$.

Thus we can describe the calculation in the following table, where we denote $P_j = [n_j]P$ and $P'_j = [n'_j]P$:

j	1	2	3	4	5	6	7
a_{7-j}	1	1	0	0	0	1	0
n_j	1	$1+2$	$2\cdot 3$	$2\cdot 6$	$2\cdot 12$	$24+25$	$2\cdot 49$
n'_j	2	$2\cdot 2$	$3+4$	$6+7$	$12+13$	$2\cdot 25$	$49+50$
P_j	P	$P_1 \oplus P'_1$	$[2]P_2$	$[2]P_3$	$[2]P_4$	$P_5 \oplus P'_5$	$[2]P_6$
P'_j	$[2]P$	$[2]P'_1$	$P_2 \oplus P'_2$	$P_3 \oplus P'_3$	$P_4 \oplus P'_4$	$[2]P'_5$	$P_6 \oplus P'_6$

$\square$

16.04.

3.3. Decide whether the WEP $w = y^2 - f \in \mathbb{F}_5[x, y]$ is $\mathbb{F}_5$-equivalent to some Montgomery polynomial if

(a) $f = x^3 + 1$,

(b) $f = x^3 + 2$,

(c) $f = x^3 + x$,

(d) $f = x^3 + x + 1$,

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

We apply Proposition 4.5 from the lecture (M.5 in the lecture notes) which says that smooth WEP $w = y^2 - f$ is $\mathbb{F}_5$-equivalent to some Montgomery polynomial if and only if there exists a root $\zeta \in \mathbb{F}_5$ of f such that $f'(\zeta)$ is a non-zero square in $\mathbb{F}_5$. Note that if we find all $\mathbb{F}_5$-rational roots ζ of f and check whether $f'(\zeta) \neq 0$, we will know that w is smooth.

Observe that $1 = 1^2 = (-1)^2, -1 = (2)^2 = (-2)^2$ are all non-zero squares in $\mathbb{F}_5$. We will search all $\mathbb{F}_5$-rational roots ζ of f and check whether $f'(\zeta) = \pm 1$:

(a) The only $\mathbb{F}_5$-rational root of $f = x^3 + 1$ is -1, $f' = 3x^2$ and $f'(-1) = -2$, which means that w is not $\mathbb{F}_5$-equivalent to any Montgomery polynomial.

(b) The only $\mathbb{F}_5$-rational root of $f = x^3 + 2$ is 2, and $f'(2) = 2$, hence w is not $\mathbb{F}_5$-equivalent to any Montgomery polynomial.

(c)The polynomial $y^2 - (x^3 + x)$ is already a Montgomery polynomial (for $A = 0$, $B = 1$), so the answer is yes.

(d) The polynomial $x^3 + x + 1$ has no $\mathbb{F}_5$-rational root, thus the answer is no.

(e) Since -1 is $\mathbb{F}_5$-rational root of $f = x^3 + x + 2$, the derivative $f' = 3x^2 + 1$ has no $\mathbb{F}_5$-rational root, and $f'(-1) = -1$, the WEP w is $\mathbb{F}_5$-equivalent to some Montgomery polynomial. $\square$

3.4. Find a Montgomery polynomial $\mathbb{F}_5$-equivalent to a WEP $w \in \mathbb{F}_5[x, y]$ if

(a) $w = y^2 - (x^3 + x + 2)$,

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

(a) We have found the root -1 of $f = x^3 + x + 2$ in the previous task and we use the idea of the proof of Proposition 4.5/M.5 and Lemma 4.1. First substitute $x - 1$ into f and we get $\hat{f} = f(x-1) = x^3 + 2x^2 - x$. Now, if we put $x^3 + 2x^2 - 1 = x^3 + ABx^2 + B^2x$, we can easily calculate $B = \pm 2$ and $A = 2 \cdot (\pm 2) = \pm 1$, hence by Lemma 4.1 we get

$$y^2 - (x^3 + x + 2) \sim_{\mathbb{F}_5} 2y^2 - (x^3 + x^2 + x)(\sim_{\mathbb{F}_5} -2y^2 - (x^3 - x^2 + x)).$$

(b) As in 3.3 we find roots ± 1, -2 of

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

Since $f' = 3x^2 - x - 1$, we calculate $f'(1) = 1$ and $f'(-1) = f'(-2) = -2$. As $f'(1) = 1$ is a square, we substitute $x \to x + 1$ and we obtain $\tilde{f} = f(x + 1) = x^3 + x$. We can see that the $\mathbb{F}_5$-equivalent WEP $y^2 - \tilde{f} = y^2 - (x^3 + x)$ is already Montgomery (cf. 3.3(c)), so we are done, i.e. $y^2 - (x^3 + 2x^2 - x - 2) \sim_{\mathbb{F}_5} y^2 - (x^3 + x)$. $\square$

3.5. Decide whether there exists $c \in \mathbb{F}_7$ such that the WEP $y^2 - (x^3 - c) \in \mathbb{F}_7[x, y]$ is $\mathbb{F}_7$-equivalent to some Montgomery polynomial.

Assume that there exists a root $\zeta \in \mathbb{F}_7$ of $f = x^3 - c$ and $b \in \mathbb{F}_7$ such that

$$f'(\zeta) = 3\zeta^2 = b^2 \in \mathbb{F}_7^*.$$

Then $3 = \frac{b^2}{\zeta^2} = (\frac{b}{\zeta})^2$, which contradicts to the fact that $1, 2, 4$ are the only non-zero squares in the field $\mathbb{F}_7$. $\square$

3.6. Explain for an arbitrary field K why Montgomery polynomials m and $\tilde{m}$ are K-equivalent if

$$m = By^2 - (x^3 + Ax^2 + x) \text{ and } \tilde{m} = -By^2 - (x^3 - Ax^2 + x) \in K[x, y].$$

It is enough to consider the affine transformation $(x, y) \to (-x, -y)$, on m:

$$m(-x, -y) = By^2 - (-x^3 + Ax^2 - x) = -(-By^2 - (x^3 - Ax^2 + x)) = (-1) \cdot \tilde{m}$$

and note that $B \in K^*$, $A \neq \pm 2$ if and only if $-B \in K^*$, $-A \neq \pm 2$. $\square$

4 Edwards curves

4.1. Show that the polynomial $x^2 + y^2 \in \mathbf{R}[x, y]$ is irreducible but it is not absolutely irreducible.

Clearly, $x^2 + y^2 = (x + iy)(x - iy) \in \mathbb{C}[x, y]$, which shows that $x^2 + y^2$ is not absolutely irreducible.

If $x^2 + y^2 = g_1 g_2$ was a nontrivial decomposition in $\mathbf{R}[x, y]$, then it would be a nontrivial decomposition in $\mathbb{C}[x, y]$ which would be associated to the prime decomposition $x^2 + y^2 = (x + iy)(x - iy)$. Hence $g_i \| (x + iy)$ which contradicts to the fact that $g_i \in \mathbf{R}[x, y]$, and so $x^2 + y^2$ is irreducible in $\mathbf{R}[x, y]$. $\square$

23.04.

4.2. Let $f = y^2 + ax^2 - (1 + dx^2y^2) \in \mathbf{R}[x, y]$ and $F = (Y^2 + aX^2)Z^2 - (Z^4 + dX^2Y^2)$ be the homogenization of f. Find all points of $V_F \cap V_Z$ and decide which are smooth.

Since $(a : b : c) \in V_F \cap V_Z$ if and only if $c = da^2b^2 = 0$ if and only if $c = a = 0$ or $c = b = 0$, we get $V_F \cap V_Z = \{(1 : 0 : 0), (0 : 1 : 0)\}$.

We can compute

$$\frac{\partial F}{\partial X} = 2X(aZ^2 - dY^2), \quad \frac{\partial F}{\partial Y} = 2Y(Z^2 - dX^2), \quad \frac{\partial F}{\partial Z} = 2Z(Y^2 + aX^2) - 4Z^3,$$

$$\frac{\partial F}{\partial X}(1, 0, 0) = \frac{\partial F}{\partial Y}(1, 0, 0) = \frac{\partial F}{\partial Z}(1, 0, 0) = 0,$$
$$\frac{\partial F}{\partial X}(0, 1, 0) = \frac{\partial F}{\partial Y}(0, 1, 0) = \frac{\partial F}{\partial Z}(0, 1, 0) = 0,$$

hence both the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ are singularities. □

4.3. If $f = y^2 + ax^2 - (1 + dx^2y^2) \in K[x, y]$ and $a = cb^2$ for $c, b \in K$ show that $f \sim_K y^2 + cx^2 - (1 + db^{-2}x^2y^2)$.

It is enough to apply affine transformation $(x, y) \to (b^{-1}x, y)$ to receive

$$y^2 + ax^2 - (1 + dx^2y^2) = y^2 + cb^2(b^{-1}x)^2 - (1 + d(b^{-1}x)^2y^2) = y^2 + cx^2 - (1 + db^{-2}x^2y^2),$$

which is K-rationally equivalent to f. □

30.04.

4.4. For the Montgomery curve given by $3y^2 - (x^3 + 3x^2 + x) \in \mathbb{F}_7[x, y]$ find a birationally equivalent (a) twisted Edwards curve (b) Edwards curve.

(a) We simply apply Theorem 5.8 (E.7) for $A = B = 3$:

$$(a, d) = \left(\frac{A + 2}{B}, \frac{A - 2}{B}\right) = \left(\frac{3 + 2}{3}, \frac{3 - 2}{3}\right) = (4, 5),$$

thus the birationally equivalent generalized Edwards curve satisfies the equation

$$4x^2 + y^2 = 1 + 5x^2y^2.$$

(b) This time we use the linear transformation $x \to 2x$ to receive a birationally equivalent Edwards curve given by $x^2 + y^2 = 1 - x^2y^2$, where the coefficient d is transformed by the rule $d \to \frac{b}{2^2}$ (see Lemma 5.5 (E.4)). □

4.5. For the Edwards curve given by the polynomial $x^2 + y^2 - x^2y^2 \in \mathbb{F}_7[x, y]$ compute a birationally equivalent Montgomery curve.

We apply the formulas from Theorem 5.8 (E.7) again

$$(A, B) = \left(2 \cdot \frac{a + d}{a - d}, \frac{4}{a - d}\right) = \left(2 \cdot \frac{1 - 1}{1 + 1}, \frac{4}{1 + 1}\right) = (0, 2),$$

hence we have found a birationally equivalent Montgomery curve given by the polynomial $2y^2 - (x^3 + x)$. □

4.6. If C is a curve given by the WEP $w = y^2 - (x^3 - x + 1) \in \mathbb{F}_7[x, y]$, prove there exists a birationally equivalent twisted Edwards curve and find the corresponding Edwards polynomial.

Put $f = x^3 - x + 1$ and observe that $(2, 0) \in V_w$, hence $f(2) = 0$. Since $f' = 3x^2 - 1$, we have $f'(2) = 4 = 2^2$. Using the transformation $x \to x + 2$ we get the $\mathbb{F}_7$-equivalent WEP $y^2 - (x^3 - x^2 + 4x) = y^2 - (x^3 + ABx^2 + B^2x)$, which is $\mathbb{F}_7$-equivalent to the Montgomery polynomial $By^2 - (x^3 + Ax^2 + x) = 2y^2 - (x^3 + 3x^2 + x)$. Now it remains to apply Theorem 5.8 (E.7) as in 4.4 to show that a birationally equivalent generalized Edwards curve exists and it is given by the equality $6x^2 + y^2 = 1 + 4x^2y^2$ since $(6, 4) = (\frac{3+2}{2}\frac{3-2}{2})$. □

Let $f = y^2 + ax^2 - (1 + dx^2y^2) \in K[x, y]$ for a general field K with $\mathrm{char}(K) \neq 2$ and define $\hat{F}(X_1, X_2, Y_1, Y_2) = X_2^2Y_1^2 + aX_1^2Y_2^2 - (X_2^2Y_2^2 + dX_1^2Y_1^2) \in K[X_1, X_2, Y_1, Y_2]$. Note that $\hat{F}$ is homogeneous of degree 4. Define

$$\hat{V}_{\hat{F}} = \{((\alpha_1 : \alpha_2), (\beta_1 : \beta_2)) \in \mathbb{P}^1 \times \mathbb{P}^1 \mid \hat{F}(\alpha_1, \alpha_2, \beta_1, \beta_2) = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^1$$

and $\nu : \mathbb{A}^2 \to \mathbb{P}^1 \times \mathbb{P}^1$ by the rule $\nu(\alpha, \beta) = ((\alpha : 1), (\beta : 1))$

4.7. Prove the following properties of $\hat{V}_{\hat{F}}$ and ν:

(a) $\hat{V}_{\hat{F}}$ is correctly defined,

(b) ν is an embedding and $\nu(V_f) = \hat{V}_{\hat{F}} \cap \nu(\mathbb{A}^2)$

(c) $\hat{V}_{\hat{F}} \setminus \nu(V_f) = \{((1 : \pm s), (1 : 0)), ((1 : 0), (1 : \pm t))\}$ where $s, t \in \overline{K}$ satisfy $s^2 = d$ and $t^2 = \frac{d}{a}$.

(a) It is enough to observe each $((\alpha_1 : \alpha_2), (\beta_1 : \beta_2)) \in \mathbb{P}^1 \times \mathbb{P}^1$ and non-zero $\lambda, \eta \in \overline{K}$ such that $\hat{F}((\alpha_1 : \alpha_2), (\beta_1 : \beta_2)) = 0$ that

$$\hat{F}((\lambda\alpha_1, \lambda\alpha_2, \eta\beta_1, \eta\beta_2)) = \lambda^2\eta^2\hat{F}(\alpha_1, \alpha_2, \beta_1, \beta_2) = \lambda^2\eta^2 \cdot 0 = 0.$$

(b) Clearly ν is injective. Observe that $(\alpha, \beta) \in V_f$ if and only if

$$\hat{F}(\nu(\alpha, \beta)) = \hat{F}(\alpha, 1, \beta, 1) = f(\alpha, \beta) = 0,$$

which holds if and only if $\nu(\alpha, \beta) \in \hat{V}_{\hat{F}}$. This shows that $\nu(V_f) = \hat{V}_{\hat{F}} \cap \nu(\mathbb{A}^2)$.

(c) First note that

$$\mathbb{P}^1 \times \mathbb{P}^1 \setminus \nu(\mathbb{A}^2) = (1 : 0) \times \mathbb{P}^1 \cup \mathbb{P}^1 \times (1 : 0).$$

We will discuss two intersections $((1 : 0) \times \mathbb{P}^1) \cap \hat{V}_{\hat{F}}$ $(\mathbb{P}^1 \times (1 : 0)) \cap \hat{V}_{\hat{F}}$.

Let $A = ((x_1 : x_2), (1 : 0)) \in \mathbb{P}^1 \times (1 : 0) \cap \hat{V}_{\hat{F}}$, then $x_2^2 = dx_1^2 = s^2x_1^2$ and so $A = \{((1, \pm s), (1 : 0))\}$

Let $B = ((1 : 0), (y_1 : y_2)) \in ((1 : 0) \times \mathbb{P}^1) \cap \hat{V}_{\hat{F}}$, then $ay_2^2 = dy_1^2$ which implies that $y_2^2 = \frac{d}{a}y_1^2 = t^2y_1^2$. Thus and so $B = \{((1 : 0), (1, \pm t))\}$. □

Recall that $(\hat{V}_{\hat{F}}, \oplus, \ominus, o)$ is a group with operations defined as follows:

$$o = \nu(0, 1) = ((0 : 1), (1 : 1))$$

$$\ominus((\alpha_1:\alpha_2),(\beta_1:\beta_2)) = ((-\alpha_1:\alpha_2),(\beta_1:\beta_2))$$

$$((\alpha_1:\alpha_2),(\beta_1:\beta_2)) \oplus ((\gamma_1:\gamma_2),(\delta_1:\delta_2)) = \begin{cases} ((\mu_1:\mu_2),(\nu_1:\nu_2)) & \text{if it has sense} \\ ((\mu_1':\mu_2'),(\nu_1':\nu_2')) & \text{otherwise} \end{cases}$$

where

$$\begin{array}{rlrl} \mu_1 = & \alpha_1\beta_2\gamma_2\delta_1 + \alpha_2\beta_1\gamma_1\delta_2, & \mu_1' = & \alpha_1\beta_1\gamma_2\delta_2\alpha_2\beta_2\gamma_1\delta_1, \\ \mu_2 = & \alpha_2\beta_2\gamma_2\delta_2 + d\alpha_1\beta_1\gamma_1\delta_1, & \mu_2' = & a\alpha_1\beta_2\gamma_1\delta_2 + \alpha_2\beta_1\gamma_2\delta_1, \\ \nu_1 = & \alpha_2\beta_1\gamma_2\delta_1 - a\alpha_1\beta_2\gamma_1\delta_2, & \nu_1' = & \alpha_1\beta_1\gamma_2\delta_2 - \alpha_2\beta_2\gamma_1\delta_1 \\ \nu_2 = & \alpha_2\beta_2\gamma_2\delta_2 - d\alpha_1\beta_1\gamma_1\delta_1, & \nu_2' = & \alpha_1\beta_2\gamma_2\delta_1 - \alpha_2\beta_1\gamma_1\delta_2. \end{array}$$

for each $(\alpha_1:\alpha_2),(\beta_1:\beta_2),(\gamma_1:\gamma_2),(\delta_1:\delta_2)$

4.8. Let $\sigma_\pm = ((1:\pm s),(1:0))$ and $\tau_\pm = ((1:0),(1:\pm t))$ for s,t satisfying $s^2 = d$ and $t^2 = \frac{d}{a}$. Prove the following properties of the group $(\hat{V}_{\hat{F}}, \oplus, \ominus, o)$:

(a) $\nu(\alpha \oplus \beta) = \nu(\alpha) \oplus \nu(\beta)$ if the left side has a sense,

(b) $\tau_\pm$ and $\nu(0,-1)$ are elements of the order 2,

(c) $\sigma_\pm$ and $\nu(\pm r, 0)$ for $r^2 = a^{-1}$ are elements of the order 4.

(a) If we apply the definition of adding on $\hat{V}_{\hat{F}}$ we get

$$\nu(u_1,u_2) \oplus \nu(v_1,v_2) = ((u_1:1),(u_2:1)) \oplus ((v_1:1),(v_2:1)) =$$

$$= \begin{cases} ((u_1v_2 + u_2v_1 : 1 + du_1u_2v_1v_2),(u_2v_2 - au_1v_1 : 1 - du_1u_2v_1v_2)) = \\ ((u_1u_2 + v_1v_2 : au_1v_1 + u_2v_2),(u_1u_2 - v_1v_2 : u_1v_2 + u_2v_1)) = \end{cases}$$

$$= \begin{cases} ((\frac{u_1v_2+u_2v_1}{1+du_1u_2v_1v_2} : 1),(\frac{u_2v_2-au_1v_1}{1-du_1u_2v_1v_2} : 1)) = \nu((u_1,u_2)\oplus(v_1,v_2)) \\ ((\frac{u_1u_2+v_1v_2}{au_1v_1+u_2v_2} : 1),(\frac{u_1u_2-v_1v_2}{u_1v_2+u_2v_1} : 1)) = \nu((u_1,u_2)\oplus(v_1,v_2)) \end{cases}$$

if the line has a sense, where on the first line we have exactly the closed formula and on the second line the generic formula, which means that at least one line is correct.

(b) Since $\tau_\pm, \nu(0,-1) \neq o = (0,1)$ and

$$\ominus\tau_\pm = ((-1:0),(1,\pm t)) = \tau_\pm, \quad \ominus\nu(0,-1) = \nu(0,-1),$$

all the elements are exactly of the order 2.

(c) It is enough to show that $[2]P = \nu(0,-1)$, as $\nu(0,-1)$ has the order 2. Let us apply the formulas of the addition

$$((1,\pm s),(1:0)) \oplus ((1,\pm s),(1:0)) = ((0,d),(d:-d)) = ((0,1),(-1:1)) = \nu(0,-1).$$

and

$$(\pm r, 0) \oplus (\pm r, 0) = (0, -ar^2) = (0:-1),$$

which can be computed in V_f. $\square$