Notationstabelle zur Vorlesung "Elliptische Kurven und Kryptographie"

V2:

R^* Menge der Einheiten in einem Ring mit 1 = Menge der Teiler von 1
Def.: $R^* = \{u \in R;\ \exists v \in R: uv = 1 = vu\}$
Einheit = invertierbares Ringelement = Teiler von 1

$c_k c_{k-1} \cdots c_0{}_{(g)}$ g-adische Darstellung der Zahl $n = \sum_{i=0}^{k} c_i g^i$ zur Basis g, die $c_i \in \{0, \ldots, g-1\}$ heißen Ziffern
Bsp.: $2B_{(16)} = 2 \cdot 16^1 + 11 \cdot 16^0 = 43_{(10)}$

$a \mid b$ a teilt b, für $a, b \in \mathbb{Z}$
Def.: $a \mid b :\Leftrightarrow \exists c \in \mathbb{Z}: ac = b$

p prim p Primzahl, Def.: $p \in \mathbb{N}$ prim $:\Leftrightarrow \#\{t \mid p;\ t \in \mathbb{N}\} = 2$

$p^k \| n$ p^k teilt n exakt $:\Leftrightarrow p^k \mid n$ und $p^{k+1} \nmid n$

$ggT(a,b)$ größter gemeinsamer Teiler von a und b, wo $a, b \in \mathbb{Z}$
Def.: $ggT(a,b) := \max\{t \in \mathbb{N};\ t \mid a \text{ und } t \mid b\}$, falls existent

V3:

$a \equiv b \bmod m$ oder $a \equiv b\ (m)$ a kongruent zu b modulo m,
Def.: $a \equiv b\ (m) :\Leftrightarrow m \mid (b-a)$

$x + m\mathbb{Z} := \{x + ma;\ a \in \mathbb{Z}\}$ Restklasse von x mod m
kurz: $\underline{x} := x + m\mathbb{Z}$, falls $m > 1$ geg., Bsp.: $m = 10 \rightsquigarrow \underline{2} = 2 + 10 \cdot \mathbb{Z} = \{\ldots, -8, 2, 12, \ldots\}$

$\mathbb{Z}_m := \{x + m\mathbb{Z};\ x \in \mathbb{Z}\}$ Menge der Restklassen mod m,
Bsp.: $\mathbb{Z}_{10} = \{x + 10 \cdot \mathbb{Z};\ x \in \mathbb{Z}\} = \{\underline{x};\ x \in \mathbb{Z}\}$
$= \{\underline{0}, \underline{1}, \ldots, \underline{9}\} = \{\underline{-4}, \underline{-3}, \ldots, \underline{3}, \underline{4}, \underline{5}\} = \ldots$

$\underline{x} + \underline{y} := \underline{x+y}$ Addition auf $\mathbb{Z}_m$
$\underline{x} \cdot \underline{y} := \underline{x \cdot y}$ Multiplikation auf $\mathbb{Z}_m$

$\underline{x}^*$ oder $\underline{x}^{-1}$ Inverses von $\underline{x} \in \mathbb{Z}_m$ in $\mathbb{Z}_m$, d.h. $\underline{x}^* := \underline{y} \in \mathbb{Z}_m$ mit $\underline{x} \cdot \underline{y} = \underline{1}$, definiert, falls $ggT(x,y) = 1$, explizit berechenbar mit Euklidischem Algorithmus

$\mathbb{Z}_m^*$ Menge der Einheiten im Ring $(\mathbb{Z}_m,+,\cdot)$,
Def.: $\mathbb{Z}_m^* := \{\underline{x}\in\mathbb{Z}_m;\ \exists y\in\mathbb{Z}_m:\ \underline{x}\cdot y = \underline{1}\}$
$\mathbb{Z}_m^* = \{\underline{x}\in\mathbb{Z}_m;\ ggT(x,m)=1\}$

φ Eulersche φ-Funktion, $\varphi:\mathbb{N}\to\mathbb{N}$, Def.: $\varphi(m) := \#\mathbb{Z}_m^*$

$\mathbb{F}_p$ endlicher Körper mit p Elementen, Def.: $\mathbb{F}_p := \mathbb{Z}_p$, p prim

$\mathrm{char}(k)$ Charakteristik eines Körpers k,
Def.: $\mathrm{char}(k) := \begin{cases}\min\{m;\ m\cdot 1 = 0\}, & \text{falls min existiert,}\\ 0, & \text{sonst}\end{cases}$

$\boxed{\text{V4}}$:

$\mathrm{ord}(G) := \#G$ Ordnung einer Gruppe G

$\langle a\rangle$ Erzeugnis eines Elements $a\in G$ in einer Gruppe G
= die von a in G erzeugte Untergruppe

Def.: $\langle a\rangle := \{m\cdot a;\ m\in\mathbb{Z}\}$, auch $\langle a\rangle = \mathbb{Z}\cdot a$, falls $(G,+)$ additiv geschrieben
bzw. $\langle a\rangle := \{a^m;\ m\in\mathbb{Z}\}$, auch $\langle a\rangle = a^{\mathbb{Z}}$, falls $(G,\cdot)$ multiplikativ geschrieben

$\mathrm{ord}(a) := \#\langle a\rangle$ Ordnung eines Elements, falls $\langle a\rangle$ endlich

$\boxed{\text{V7}}$: k Körper

$f(x_1,\dots,x_n) = \sum_{\nu_1,\dots,\nu_m \geq 0} \alpha_{\nu_1,\dots,\nu_m} X_1^{\nu_1}\cdots X_m^{\nu_m}$ Polynom in m Variablen/Unbestimmten $x_1,\dots,x_m$ mit Koeffizienten $\alpha_{\nu_1,\dots,\nu_m}\in k$, wo höchstens endlich viele $\alpha_{\nu_1,\dots,\nu_m}\neq 0$

Kurz: $f(\underline{X}) = \sum_{\underline{\nu}\in\mathbb{N}_0^m} \alpha_{\underline{\nu}} \underline{X}^{\underline{\nu}} = \sum_{\underline{\nu}\in\mathbb{N}_0^m} \alpha_{\underline{\nu}} X_1^{\nu_1}\cdots X_m^{\nu_m}$ mit $\underline{X} = (X_1,\dots,X_m)$, $\underline{\nu} = (\nu_1,\dots,\nu_m)$

$\deg f$ Grad eines Polynoms f = höchste Exponentensumme eines in f vorkommenden Monoms, d.h. $\deg f := \max\{\nu_1+\dots+\nu_m;\ \alpha_{\nu_1,\dots,\nu_m}\neq 0\}$, falls ex. ($f\neq 0$)

$k[X_1,\dots,X_m]$ bzw. $k[\underline{X}]$ Menge aller Polynome in m Variablen über k
$\leadsto$ schreibe $f\in k[\underline{X}]$ für "Sei f ein Polynom in m Var. über k"

$\frac{\partial f}{\partial x_i}\in k[\underline{X}]$ formale Ableitung von $f\in k[\underline{X}]$ nach der Variablen X_i, $1\leq i\leq m$,
Def.: $\frac{\partial f}{\partial x_i}(\underline{X}) := \sum_{\underline{\nu}\in\mathbb{N}_0^m} \alpha_{\underline{\nu}}\cdot\nu_i\cdot X_1^{\nu_1}\cdots X_{i-1}^{\nu_{i-1}} X_i^{\nu_i-1} X_{i+1}^{\nu_{i+1}}\cdots X_m^{\nu_m}$

$f\,|\,g \;:\Leftrightarrow\; \exists h\in k[\underline{X}]:\ fh = g$

Bez. Polynomring $k[X]$ in einer Variablen:

a kongruent b modulo f — Für $a,b,f\in k[X]$: $f \mid (b-a)$ als Polynome

$a+f\cdot k[X]$ — Restklasse von a mod f, Def.: $a+f\cdot k[X]=\{a+f\cdot g;\ g\in k[X]\}$

Kurz: $\underline{a}$, falls $f\neq 0$ geg., Bsp.: $f=X^2+1 \rightsquigarrow \underline{\underline{X^3+1}}=\underline{-X+1}$
weil X^3+1 kongr. zu $-X+1$ ist mod X^2+1

$k[X]/(f)$ — Menge der Restklassen modulo f in $k[X]$,
Def. $k[X]/(f):=\{a+f\cdot k[X];\ a\in k[X]\}=\{\underline{a};\ a\in k[X]\}$
Bsp.: $k=\mathbb{R}$, $f=X^2+1 \rightsquigarrow \mathbb{R}[X]/(f)=\{\underline{g};\ g\in\mathbb{R}[X],\ g=0 \text{ oder } \deg g\leq 1\}$

$\mathbb{F}_{p^r}$ — endlicher Körper mit p^r vielen Elementen
Konstruktion: $\mathbb{F}_{p^r}:=\mathbb{F}_p[X]/(f)$, wo $f\in\mathbb{F}_p[X]$ irreduzibel mit $\deg f=r\geq 1$ ist

$\boxed{V8}$: k Körper

$\mathbb{A}^2(k):=\{\underbrace{(x,y)}_{\text{affiner Punkt}};\ x,y\in k\}=k^2$ — affine Ebene

$g(a,b,c):=\{(x,y)\in\mathbb{A}^2(k);\ ax+by+c=0\}$ — affine Gerade,
Steigung $-\frac{a}{b}$ falls $b\neq 0$

$[x:y:z]$ — projektiver Punkt mit projektiven Koordinaten $(x,y,z)\in k^3\setminus\{(0,0,0)\}$,
Def.: $[x:y:z]:=\{(u,v,w)\in k^3\setminus\{(0,0,0)\};\ (u,v,w)\sim(x,y,z)\}$,
wobei $(u,v,w)\sim(x,y,z) :\Leftrightarrow \exists\lambda\in k\setminus\{0\}: (u,v,w)=(\lambda x,\lambda y,\lambda z)$
$=\lambda\cdot(x,y,z)$
$\rightsquigarrow$ Kurz: $[x:y:z]:=\{\lambda\cdot(x,y,z);\ \lambda\in k\setminus\{0\}\}$

$\mathbb{P}^2(k):=\{[x:y:z];\ x,y,z\in k,\ \text{nicht } x=y=z=0\}$
projektive Ebene: Menge aller projektiven Punkte $[x:y:z]$

Erhalten: Erweiterung von $\mathbb{A}^2(k)$ als $i(\mathbb{A}^2(k))\subseteq\mathbb{P}^2(k)$,
$i(x,y):=[x:y:1]$.

Es gilt: $i(\mathbb{A}^2(k))=\{[u:v:1];\ u,v\in k\}$
$=\{[x:y:z];\ x,y,z\in k;\ z\neq 0\}$

$g_\infty:=\{[x:y:0];\ x,y\in k\}\subseteq\mathbb{P}^2(k)$
unendlich ferne Gerade mit $\mathbb{P}^2(k)=\underbrace{g_\infty}_{\rightsquigarrow z=0}\cup\underbrace{i(\mathbb{A}^2(k))}_{\rightsquigarrow z\neq 0}$

$G(a,b,c)$ projektive Gerade in $\mathbb{P}^2(k)$, für $a,b,c \in k$, nicht $a=b=c=0$,

Def.: $G(a,b,c) := \{[x:y:z] \in \mathbb{P}^2(k);\ ax+by+cz=0\}$.

Es ist $i(g(a,b,c)) \subseteq G(a,b,c)$

und $G(a,b,c) \setminus i(g(a,b,c)) = \{[x:y:0] \in g_\infty;\ ax+by=0\}$

$= \{[ax:ay:0] \in g_\infty;\ ax+by=0\} = \{[-by:ay:0];\ y \in k\} = [-b:a:0]$.

Falls $b \neq 0$, ist dies $= \{[x:-\frac{a}{b}x:0];\ x \in k\} = [1:-\frac{a}{b}:0]$.

$C_f(k) := \{(x,y) \in \mathbb{A}^2(k);\ f(x,y)=0\}$ zu $f \in k[x,y]$

affine Kurve in $\mathbb{A}^2(k)$, geg. als Nullstellenmenge eines Polynoms f in 2 Variablen x und y

$t_{(a,b)}(C_f)$ (affine) Tangente an eine affine Kurve $C_f(k)$ im Punkt $(a,b) \in C_f(k)$, falls existent

(Tangente ex., falls C_f nicht singulär in (a,b) ist)

Def.: $t_{(a,b)}(C_f) := \{(x,y) \in \mathbb{A}^2(k);\ \frac{\partial f}{\partial x}(a,b)\cdot x + \frac{\partial f}{\partial y}(a,b)\cdot y + d = 0\}$,

mit $d \in k$ so, dass $(a,b) \in t_{(a,b)}(C_f)$

Es gilt: $t_{(a,b)}(C_f) = g\left(\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b), d\right)$, d passend

$\boxed{\text{V9}}$:

F_f Homogenisierung des Polynoms $f \in k[x,y]$, $f = \sum_{\nu,\mu \geq 0} a_{\nu,\mu} x^\nu y^\mu$, $\deg f = d$

Def.: $F_f := \sum_{\nu,\mu \geq 0} a_{\nu,\mu} X^\nu Y^\mu Z^{d-\nu-\mu} \in k[X,Y,Z]$

Bsp.: $f(x,y) = y^3 - x^2 + 4xy - xy^2$

$\Rightarrow F_f(X,Y,Z) = Y^3 - X^2Z + 4XYZ - XY^2$

$C_F(k) := \{[u:v:w] \in \mathbb{P}^2(k);\ F(u,v,w)=0\}$ projektive Kurve in $\mathbb{P}^2(k)$, geg. als Nullstellenmenge eines <u>homogenen</u> Polynoms F in 3 Variablen X, Y und Z.

$T_P(C_F)$ (projektive) Tangente an eine projektive Kurve $C_F(k)$
im Punkt $P \in C_F(k)$, falls existent
(Tangente ex., falls C_F nicht singulär in P ist)

Def.: $T_P(C_F) := \{[x:y:z] \in \mathbb{P}^2(k);\ \frac{\partial F}{\partial x}(P)\cdot x + \frac{\partial F}{\partial y}(P)\cdot y + \frac{\partial F}{\partial z}(P)\cdot z = 0\}$

Es gilt: $T_P(C_F) = G\left(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P), \frac{\partial F}{\partial z}(P)\right)$.

$m(P; G, C_F)$ $\in \mathbb{N}_0$, Schnittmultiplizität bzw. Vielfachheit,
mit der sich eine Gerade G und eine Kurve C_F im
Punkt P schneiden (alle Objekte in $\mathbb{P}^2(k)$ betrachtet;
m existiert, wenn $G \nmid C_F$ in $k[X,Y,Z]$ ist).

Def.: $m(P; G, C_F) := 0$, falls $P \notin G \cap C_F$,
und sonst ist $m(P; G, C_F)$ die Nullstellenordnung von $t=0$ des
Polynoms $\varphi(t) := F(a+ta', b+tb', c+tc')$,
wenn $P=[a:b:c]$ und $P'=[a':b':c'] \in G\setminus\{P\}$ ist;
d.h. $m(P; G, C_F)$ ist die maximale Zahl $m \in \mathbb{N}_0$, für die
$t^m \in k[t]$ ein Teiler des Polynoms $\varphi(t) \in k[t]$ ist,
falls ex.

$\boxed{\text{V10}}$:

$\mathrm{Res}(f,g)$ Resultante von $f,g \in k[X]$, $f = a_m X^m + \dots + a_0$, $g = b_n X^n + \dots + b_0$

Def.:

$$\mathrm{Res}(f,g) := \det \left[\ \underbrace{\begin{matrix} a_0 & & \\ \vdots & a_0 & \\ a_m & \vdots & \ddots \; a_0 \\ & a_m & \vdots \\ & & \ddots \; a_m \end{matrix}}_{n\text{ Spalten}} \ \middle|\ \underbrace{\begin{matrix} b_0 & & \\ \vdots & \ddots & \\ b_n & & b_0 \\ & \ddots & \vdots \\ & & b_n \end{matrix}}_{m\text{ Spalten}}\ \right]$$

$\boxed{V11}$:

$\mathcal{O}$ "unendlich ferner" Punkt $\mathcal{O} := [0:1:0] \in g_\infty \subseteq \mathbb{P}^2(k)$

$E(k)$ Elliptische Kurve: $C_F(k)$ zu einem kubischen, homogenen, irred. Polynom $F \in k[X,Y,Z]$, nicht-singulär mit Wendepunkt $\in \mathbb{P}^2(k)$

Δ bzw. $\Delta(C_F(k))$ Diskriminante der Kurve $C_F(k)$, wobei F ein langes Weierstraßpolynom ist
Es ist $\Delta = -16(4a^3+27b^2)$, falls $F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$

$\boxed{V12}$:

$disc(\sigma)$ $\in k$, Diskriminante eines Polynoms $\sigma \in k[X]$, $\deg \sigma = m$
Def.: $disc(\sigma) := \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j)^2$, falls $\alpha_1, \dots, \alpha_m \in \bar{k}$ die Nst. von σ in $\bar{k}$ sind,
d.h. wenn $\sigma(X) = c \cdot (X-\alpha_1) \cdot (X-\alpha_2) \cdots (X-\alpha_m)$ mit $\alpha_1, \dots, \alpha_m \in \bar{k}$, $c \in k$.

$\boxed{V13}$: $E(k)$ elliptische Kurve, $P, Q \in E(k)$

$G(P,Q)$ (projektive) Verbindungsgerade der Punkte $P, Q \in \mathbb{P}^2(k)$, $P \neq Q$, d.h. projektive Gerade mit $P, Q \in G(P,Q)$

$P * Q$ 3. Schnittpunkt, den die Gerade $G(P,Q)$, $P \neq Q$, mit $E(k)$ hat, gemäß Beachtung von Vielfachheiten

$P * P$ 3. Schnittpunkt, den die Tangente $T_P(E)$ mit $E(k)$ hat, gemäß Beachtung von Vielfachheiten

$P + Q$ Summe zweier Punkte $P, Q \in E(k)$,
Def.: $P + Q := \mathcal{O} * (P * Q)$

$-P$ Inverses von $P \in E(k)$ bzgl. Addition "+" auf $E(k)$,
es gilt $-P = \mathcal{O} * P \rightsquigarrow P + Q = -(P * Q)$.
Ist $E(k)$ symmetrisch zur x-Achse, gilt für $P = [a:b:c] \in E(k)$ dann $-P = [a:-b:c]$.

$\boxed{V15}$: Seien $c, d \in \mathbb{N}$

$(x:y:z)$ projektiver Punkt zu (c,d), Def.: $(x:y:z) := \{(\sigma^c x, \sigma^d y, \sigma z);\ \sigma \in k \setminus \{0\}\}$

$\mathbb{P}^2_{(c,d)}(k)$ projektive Ebene zu (c,d)

$m \cdot P$ m-faches von $P \in E(k)$ auf $E(k)$, Def.: $m \cdot P := \overbrace{P + \dots + P}^{m \text{ mal}}$

$\boxed{\text{V16}}$:

$r(E)$ Rang von $E(\mathbb{Q})$, d.h. $r(E) \in \mathbb{N}_0$ mit $E(\mathbb{Q}) \cong \mathbb{Z}^{r(E)} \times T$, wo $T := \{ P \in E(\mathbb{Q});\ \mathrm{ord}(P) \in \mathbb{N} \}$ die Torsionsgruppe von E ist.

$\boxed{\text{V17}}$:

N_p Anzahl der Punkte von $E(\mathbb{F}_p)$, d.h. $N_p := \# E(\mathbb{F}_p)$

a_p Defekt, bzw. Spur des Frobenius, nämlich $a_p := p + 1 - N_p$ von $E(\mathbb{F}_p)$. Für $E(\mathbb{F}_{p^r})$ ist entsprechend $a_{p^r} := p^r + 1 - N_{p^r}$

$\left(\frac{u}{\mathbb{F}_p}\right)$ verallgemeinertes Legendresymbol, $= +1$ falls u ein qR mod p, $= -1$ falls u ein qNR mod p, $= 0$ falls $p \mid u$.

ϕ, Φ Frobeniusendomorphismus $\phi : \mathbb{P}^2(\overline{\mathbb{F}_{p^r}}) \to \mathbb{P}^2(\overline{\mathbb{F}_{p^r}})$, $[x:y:z] \mapsto [x^{p^r} : y^{p^r} : z^{p^r}]$
$\leadsto \Phi := \phi_{/E(\overline{\mathbb{F}_{p^r}})}$

P_w Punkt einer elliptischen Kurve, der einem Textblock w entspricht