Wolfgang K. Seiler
Tel. 2515

B6, B4.18

28. April 2020

8. Übungsblatt Elliptische Kurven

Aufgabe 1: *(5 Punkte)*
Stellen Sie für die folgenden elliptischen Kurven aus $\mathbb{P}^2(\mathbb{F}_5)$ die Gruppentafeln auf und entscheiden Sie, welche der Gruppen zyklisch sind!

a) $Y^2Z = X^3 + XZ^2$

Lösung: Alle drei Gleichungen sind in Weierstrass-Form, haben also $O = (0 : 1 : 0)$ als einzigen unendlichfernen Punkt. Abgesehen davon können wir uns also auf den affinen Teil der Kurve beschränken; hier suchen wir also Punkte $(x, y) \in \mathbb{F}_5^2$ mit $y^2 = x^3 + x$. Die Quadrate in $\mathbb{F}_5$ sind $0 = 0^2$, $1 = 1^2 = 4^2$ und $4 = 2^2 = 3^2$. $x^3 + x = x(x^2 + 1)$ verschwindet für $x = 0, 2$ und 3, also sind $(0,0)$, $(2,0)$ und $(3,0)$ affine Punkte der Kurve. Für $x = 1$ ist $x^3 + x = 2$ kein Quadrat; für $x = 4$ ist $x^3 + x = 3$ auch keines. Also besteht die Kurve aus den vier Punkten O, $(0,0)$, $(2,0)$ und $(3,0)$. Bei einer Kurve in Weierstrass-Form haben die Punkte mit y-Koordinate Null stets die Ordnung zwei, und damit muß die Summe aus zweien dieser Punkte stets gleich dem dritten sein, denn in jeder Gruppe ist die Addition eines festen Elements eine bijektive Abbildung der Gruppe auf sich selbst. Dies führt auf die Gruppentafel

$+$	O	$(0,0)$	$(2,0)$	$(3,0)$
O	O	$(0,0)$	(2.0)	$(3,0)$
$(0,0)$	$(0,0)$	O	$(3,0)$	$(2,0)$
$(2,0)$	$(2,0)$	$(3,0)$	O	$(0,0)$
$(3,0)$	$(3,0)$	$(2,0)$	$(0,0)$	O

Die Gruppe ist natürlich nicht zyklisch, denn es gibt kein Element der Ordnung vier.

b) $Y^2Z = X^3 + 2XZ^2$

Lösung: Hier erfüllen die affinen Punkte (x, y) die Gleichung $y^2 = x^3 + 2x$. Für $x = 0$ erhalten wir somit den Punkt $(0,0)$. Für $x = 1$ ist $x^3 + 2x = 3$ kein Quadrat; für $x = 2$ ist $x^3 + 2x = 2$, für $x = 3$ ist es drei, für $x = 4$ auch, also in keinem Fall ein Quadrat. Somit enthält die Kurve nur die beiden Punkte O und $(0,0)$, und $(0,0) + (0,0) = O$. Die Gruppe ist zyklisch mit $(1,1)$ als erzeugendem Element.

c) $Y^2Z = X^3 + 2XZ^2 + Z^3$

Lösung: Hier erfüllen die affinen Punkte die Gleichung $y^2 = x^3 + 2x + 1$. Die Werte der rechten Seite in folgender Tabelle zusammengefaßt:

x	0	1	2	3	4
$x^3 + 2x + 1$	1	4	3	4	2

Wir bekommen also die sieben Punkte $(0,1)$, $(0,4)$, $(1,2)$, $(1,3)$, $(3,2)$, $(3,3)$ und O. Da sieben eine Primzahl ist, haben alle Punkte außer dem Neutralelement O die Ordnung sieben, d.h. jeder dieser Punkte erzeugt die Gruppe. Wenn wir also von einem dieser Punkte ausgehen und seine Vielfache berechnen, sollten wir die gesamte Gruppe bekommen.

Beginnen wir mit dem Punkt $P = (0,1)$ und berechnen wir seine Vielfachen! Zur Berechnung von $2P$ brauchen wir die Steigung m der Tangente im Punkt P; allgemein ist das für eine Kurve in WEIERSTRASS-Normalform $(3x^2 + a)/2y$, hier also mit $x = 0, y = 1$ und $a = 2$

$$m = \frac{3 \cdot 0 + 2}{2} = 1 .$$

Der Punkt $2P$ hat nach der Verdoppelungsformel die Koordinaten $x_3 = m^2 - 2x$ und $y_3 = m(x - x_3) - y$, hier also $x_3 = 1$ und $y_3 = (0 - 1) - 1 = -2 = 3$. Somit ist $2P = (1,3)$. Die weiteren Vielfachen lassen sich nun durch sukzessive Addition von P nach der gewöhnlichen Additionsformel berechnen; wir erhalten nacheinander

$$3P = 2P + P = (3,3), \quad 4P = (3,2), \quad 5P = (1,2) \quad \text{und} \quad 6P = (0,4) .$$

$7P = 0P$ ist natürlich gleich O, was man auch daran sieht, daß P und $6P$ die gleiche x-Koordinate, aber entgegengesetzt gleiche y-Koordinaten haben. Die Gruppe ist also zyklisch von der Ordnung sieben; die Addition geht nach der Formel

$$aP + bP = (a + b \bmod 7)P$$

mit $a, b \in \{0,1,2,3,4,5,6\}$.

Aufgabe 2: *(4 Punkte)*
Die elliptische Kurve E über dem Körper $\mathbb{F}_7$ sei gegeben durch die Gleichung

$$Y^2 = X^3 + 2XZ^2 + 3Z^3 .$$

Bestimmen Sie die Ordnungen aller Punkte von E und identifizieren Sie E als abstrakte Gruppe!

Lösung: Die Quadrate modulo sieben sind $0 = 0^2$, $1 = 1^2 = 6^2$, $4 = 2^2 = 5^2$ und $2 = 3^2 = 4^2$. Die affine WEIERSTRASS-Gleichung ist $y^2 = x^3 + 2x + 3$, wobei die linke Seite folgende Werte annimmt:

x	0	1	2	3	4	5	6
$x^3 + 2x + 3$	3	6	1	1	5	5	0

Nur 0 und 1 sind Quadrate; wir erhalten also die Punkte $(2,1)$, $(2,6)$, $(3,1)$, $(3,6)$, $(6,0)$, und natürlich den Punkt O. Letzterer hat als Neutralelement die Ordnung eins, und $(6,0)$ hat, wegen der y-Koordinate Null, die Ordnung zwei. Für die vier Punkte muß die Ordnung größer als zwei sein (Für Kurven in WEIERSTRASS-Normalform ist Ordnung zwei äquivalent zu $y = 0$); da die Gruppe insgesamt sechs Elemente hat, ist sie also entweder drei oder sechs.

Die Verdoppelungsformel zeigt, daß für $P = (2,1)$ gilt $2P = (3,6)$, und nach der Additionsformel ist $3P = 2P + P = (6,0)$ ein Punkt der Ordnung zwei. Somit hat $P = (2,1)$ die Ordnung sechs und $2P = (3,6)$ die Ordnung drei. Mit P hat auch $-P = (2,6)$ die Ordnung sechs, und entsprechend hat auch $-2P = (3,1)$ die Ordnung drei. Damit sind die Ordnungen aller Elemente bestimmt.

Da es ein Element der Ordnung sechs gibt, ist die Gruppe zyklisch; nach obigen Rechnungen können wir die Punkte explizit als Vielfache von $P = (2,1)$ angeben:

$$2P = (3,6), \quad 3P = (6.0), \quad 4P = -2P = (3,1), \quad 5P = -P = (2,6) \quad \text{und} \quad 6P = O .$$

Aufgabe 3: *(5 Punkte)*
Die elliptische Kurve E über dem Körper $\mathbb{F}_{103}$ sei gegeben durch die affine Gleichung

$$y^2 = x^3 + 3x - 1\,,$$

und P sei der Punkt $(5,6)$. Berechnen sie 20P nach dem Algorithmus von MONTGOMERY!

Lösung: Im Zweiersystem ist $20 = 16 + 4 = 2^4 + 2^2 = (10100)_2$, d.h. $a_4 = a_2 = 1$ und $a_2 = a_1 = a_0 = 0$. In der WEIERSTRASS-Gleichung ist $a = 3$ und $b = -1 = 102$, und $P = (x, y) = (5, 6)$, d.h. $x = 5$. Mit diesen Werten gehen wir in den Algorithmus.
Bei der Initialisierung im ersten Schritt setzen wir $n_1 = 1$, $u_1 = x = 5$ und

$$v_1 = \frac{(x^2 - a)^2 - 8bx}{4(x^3 + ax + b)} = \frac{(25-3)^2 + 8\cdot 5}{4(125 + 15 - 1)} = \frac{524}{556} = \frac{9}{41}\,.$$

Der erweiterte EUKLIDische Algorithmus, am besten auf einem Computeralgebrasystem, gibt uns $98 = -5$ als Inverses von 41 modulo 103, also ist $v_1 = 9 \cdot (-5) = -45 = 58$ in $\mathbb{F}_{103}$.
Im zweiten Schritt setzen wir $n_2 = 2n_1 + a_3 = 2$. Da a_3 verschwindet, wird wegen $u_1 = 5$ und $v_1 = 58$

$$u_2 = \frac{(u_1^2 - a)^2 + 8bu_1}{4(u_1^3 + au_1 + b)} = 58$$

und

$$v_2 = \frac{(u_1v_1 - a)^2 - 4b(v_1 + u_1)}{(v_1 - u_1)^2 x} = 70\,.$$

Im dritten Schritt wird $n_3 = 2n_2 + a_2 = 5$, und da a_2 nicht verschwindet, werden die Formeln nun anders herum angewendet:

$$v_3 = \frac{(v_2^2 - a)^2 + 8bv_2}{4(v_2^3 + av_2 + b)} = 79$$

und

$$u_3 = \frac{(u_2v_2 - a)^2 - 4b(v_2 + u_2)}{(v_2 - u_2)^2 x} = 51\,.$$

Im vierten Schritt wird $n_4 = 2n_3 + a_1 = 10$; da a_1 verschwindet, verwenden wieder dieselben Formeln wie beim zweiten Schritt:

$$u_4 = \frac{(u_3^2 - a)^2 + 8bu_3}{4(u_3^3 + au_3 + b)} = 53$$

und

$$v_4 = \frac{(u_3v_3 - a)^2 - 4b(v_3 + u_3)}{(v_3 - u_3)^2 x} = 83\,.$$

Auch im fünften Schritt ist $a_0 = 0$, also $n_5 = n = 20$, wie es sein muß, und

$$u_5 = \frac{(u_4^2 - a)^2 + 8bu_4}{4(u_4^3 + au_4 + b)} = 55$$

und

$$v_5 = \frac{(u_4v_4 - a)^2 - 4b(v_4 + u_4)}{(v_4 - u_4)^2 x} = 23\,.$$

Die x-Koordinate von 20P ist somit 55; für den sechsten Schritt bleibt noch die Bestimmung der y-Koordinate. Sie ist

$$y_* = \frac{u^3 + au + b - y^2 - (v + u + x)(u - x)^2}{2y}\,;$$

Einsetzen von $x = 5$, $y = 6$, $a = 3$ und $b = -1$ ergibt das Ergebnis 83. Somit ist $20P = (55, 83)$.

Aufgabe 4: *(6 Punkte)*

a) Die öffentlichen Parameter eines Kryptosystems nach KOYAMA, MAURER, OKAMOTO und SCOTT seien $N = 55$ und $e = 5$. Verschlüsseln Sie den Nachrichtenblock $(7, 13)$!

Lösung: $13^2 - 7^3 = -174 \equiv -9 \bmod 55$; wir arbeiten also mit der WEIERSTRASS-Gleichung $y^2 = x^3 - 9$ über $\mathbb{Z}/55$ und dem Punkt $P = (7, 13)$. Da der Parameter a in der Gleichung Null ist, erhalten wir die in $\mathbb{Z}/55$ zu berechnende Tangentensteigung

$$m = \frac{3 \cdot 7^2}{2 \cdot 13} = \frac{3 \cdot (-6)}{26} = -\frac{18}{26} = -\frac{9}{13}\,.$$

Wir wenden den erweiterten EUKLIDischen Algorithmus an auf 55 und 13:

$$\begin{aligned} 55 : 13 = 4 \text{ Rest } 3 &\implies 3 = 55 - 4 \cdot 13 \\ 13 : 3 = 4 \text{ Rest } 1 &\implies 1 = 13 - 4 \cdot (55 - 4 \cdot 13) = 17 \cdot 13 - 44 \cdot 55 \end{aligned}$$

Somit ist

$$m = -\frac{9}{13} = -9 \cdot 17 = -153 = 12$$

in $\mathbb{Z}/55$, und $m^2 = 34$. Der Punkt $2P$ hat somit die Koordinaten

$$x_3 = m^2 - 2x_1 = 34 - 14 = 20 \quad \text{und} \quad y_3 = m(x_1 - x_3) - y_1 = -12 \cdot 13 - 13 = 169 = 51\,,$$

d.h. $2P = (20, 51)$. Genauso berechnet man $4P = 2P + 2P = (20, 4)$. Da $4P$ und $2P$ die gleiche x-Koordinate, aber verschiedene y-Koordinate haben, ist ihre Summe sowohl über $\mathbb{F}_5$ als auch über $\mathbb{F}_{11}$ jeweils der unendlichferne Punkt der entsprechenden elliptischen Kurve; P hat also auf beiden Kurven die Ordnung sechs. Deshalb müssen wir $5P = 4P + P$ nicht mühsam nach der Additionsformel berechnen, sondern wegen $6P = 5P + P = O$ als $5P = -P = (7, -13) = (7, 42)$. Die Nachricht wird also verschlüsselt als $(7, 42)$.

b) Finden Sie die Entschlüsselungsabbildung dazu, und entschlüsseln Sie den Chiffretext $(3, 7)$!

Lösung: $55 = 5 \cdot 11$; das kgV von 6 und 12 ist 12. Zur Berechnung der Entschlüsselungsabbildung müssen wir also EUKLID auf 12 und 5 anwenden:

$$\begin{aligned} 12 : 5 = 2 \text{ Rest } 2 &\implies 2 = 12 - 2 \cdot 5 \\ 5 : 2 = 2 \text{ Rest } 1 &\implies 1 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 \end{aligned}$$

Somit ist der geheime Exponent hier gleich dem öffentlichen. Zur Entschlüsselung der Nachricht $Q = (3, 7)$ müssen wir zunächst die elliptische Kurve identifizieren: $7^2 - 3^3 = 22$; wir haben also die WEIERSTRASS-Gleichung $y^3 = x^3 + 22$. Damit müssen wir den Punkt $5Q$ berechnen; wie in *a)* berechnen wir zunächst mit der Verdoppelungsformel $2Q = (53, 38)$ und $4Q = (38, 2)$; zur Berechnung von $5Q$ müssen wir jetzt aber die Additionsformel anwenden auf $4Q$ und Q. Sie liefert uns den Klartext $(23, 43)$.