Elliptische-Kurven-Kryptographie, 1. Teil: Punkteaddition auf diskreten elliptischen Kurven[1]

https://youtu.beCoJNk_nr4Mc

Name: ..... Vorname: .....

Individuelle Parameter: a: ..... , b: ..... , p: .....

Anzahl Punkte: ..... Nr. .....

1. Punkteaddition auf reellen elliptischen Kurven

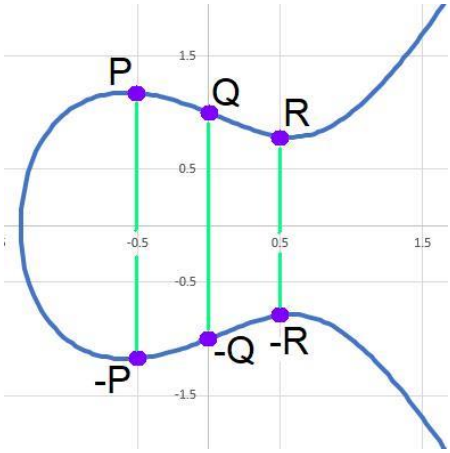
Elliptische Kurven werden definiert durch die Weierstrass-Gleichung

$$y^2 = x^3 + ax + b$$

Dabei sind a und b Parameter, welche die Gestalt der Kurve festlegen. Es muss

$$4a^3 + 27b^2 \neq 0$$

Auf elliptischen Kurven kann man eine Punkteaddition definieren. Spiegelbildliche Punkte mit gleichen x-Koordinaten erhalten unterschiedliche Vorzeichen.



Die Summe von einem Punkt und seinem spiegelbildlichen Gegenpunkt ist bei dieser Addition gleich "null". Die Rolle von "null" , d.h. das neutrale Element der Addition, spielt in dieser Punkteaddition allerdings ein Punkt im Unendlichen, den man als "uneigentlichen Punkt im Unendlichen" (UPU) bezeichnet. Für diesen Punkt werden verschiedene spezielle mathematische Symbole verwendet, die man nicht in vielen Schriftarten kennt. Wir verwenden hier das Symbol P_∞. Gemäss obigen Erläuterungen gilt

$$P + (-P) = Q + (-Q) = R + (-R) = \ldots\ldots = P_\infty$$

Ausserdem gilt $P + P_\infty = P$, $Q + P_\infty = Q$, $R + P_\infty = R$, ……

[1] https://www.mathepauker.com/Musterex/Benedict/Projektarbeiten/Punkteaddition-auf-diskreten-ellipt-Kurven.pdf

Diese Operation mit Punkten wird als Punkteaddition bezeichnet, unter anderem, weil sie Gesetzmässigkeiten gehorcht, die wir von der Addition kennen

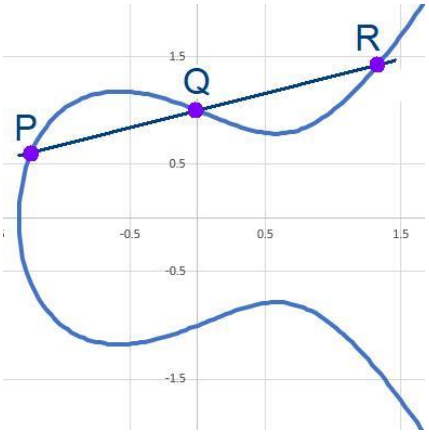
Kommutativgesetz: $P + Q = Q + P$

Assoziativgesetz: $(P + Q) + R = P + (Q + R)$

Man kann folgendes zeigen:

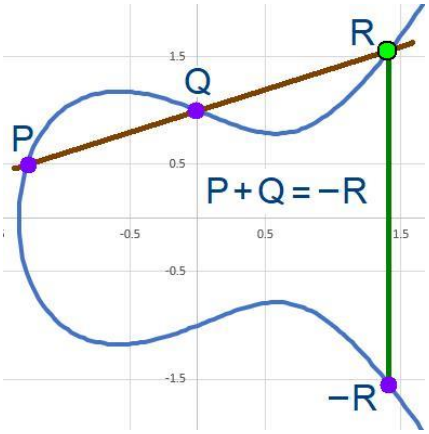
- Eine Gerade kann eine elliptische Kurve in höchstens drei Punkten schneiden. Eine Gerade, welche die elliptische Kurve in drei Punkten schneidet, bezeichnen wir hier als Sekante. Wenn eine Sekante die Kurve in den drei Punkten P, Q und R schneidet, dann gilt

$$P + Q + R = P_\infty$$



Dann gilt auch

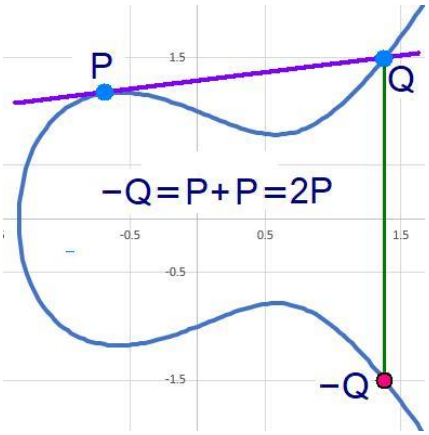
$$P + Q = -R$$
$$P + R = -Q$$
$$Q + R = -P$$



- Wenn eine Gerade die Kurve in einem Punkt B berührt, der nicht ein Wendepunkt ist, dann schneidet sie die Kurve in genau einem weiteren Punkt Q. Den Berührungspunkt könnten wir als zwei zusammen fallende Schnittpunkte 2P betrachten. Anstatt B schreiben wir also 2P. Es gilt also

$$2P + Q = P_\infty, \text{ resp.}$$

$$2P = -Q$$

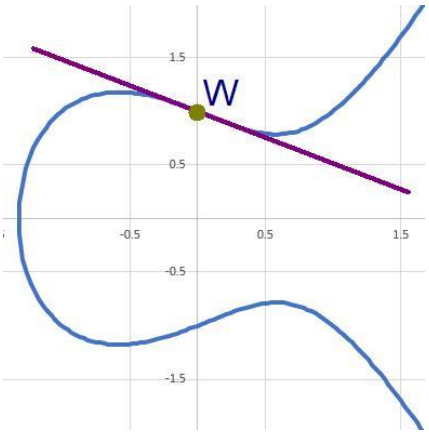


- Wenn eine Gerade die Kurve in einem Wendepunkt W berührt, dann sprechen wir von einer Wendetangente. Für einen Wendepunkt gilt

$$3W = P_\infty, \text{ resp.}$$

$$2W = -W$$

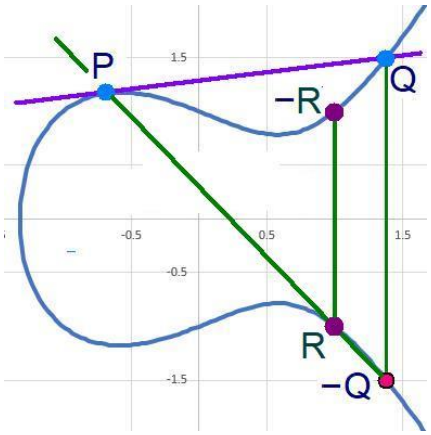
Die y-Koordinate des Wendepunkts darf dann allerdings nicht null sein. Wenn die y-Koordinate gleich null ist, handelt es sich um eine "unzulässige" Kurve mit $4a^3 + 27b^2 = 0$



Durch die Punktverdoppelung (mithilfe einer Tangenten) ist es möglich Punkte mit natürlichen Zahlen skalar zu multiplizieren. Um z.B. 3P zu berechnen kann man zunächst mithilfe einer Tangente P verdoppeln und zum Ergebnis, 2P, P addieren. In nebenstehender Figur ist z.B. $2P = -Q$ und $-Q + P + R = 2P + P + R = 3P + R = P_\infty$. Somit gilt

$$-R = 3P$$

Der Punkt $-R$ ist also das Dreifache von P.



Auf diese Weise kann man für beliebige natürliche n das skalare Produkt nP berechnen. Diese Punktadditionen und Punktvervielfachungen kann man rechnerisch durchführen.

2. Diskrete elliptische Kurve aus der modularen Arithmetik

Die Weierstrass-Gleichung ist erfüllt durch unendlich viele Wertepaare $(x \mid y)$. Betrachtet man die Weierstrass-Gleichung mit ganzen Zahlen für die Parameter a und b als Kongruenzgleichung

$$(y^2 - x^3 - ax - b) \bmod p = 0$$

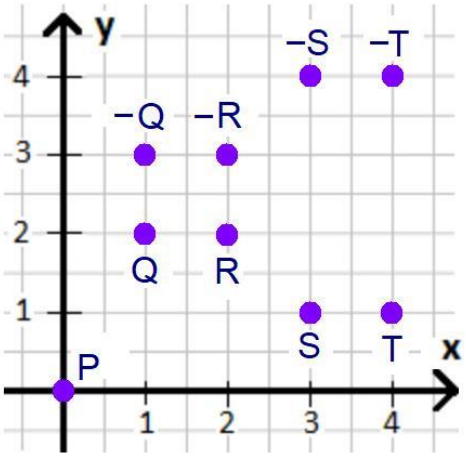
so erhält man eine endliche Anzahl Wertepaare $(x \mid y)$ als Lösungsmenge. Für p, d.h. für das Modul der Kongruenzgleichung muss für unsere Zwecke eine Primzahl verwendet werden. Wenn man für p eine beliebige natürliche Zahl verwendet, die nicht eine Primzahl ist, erhält man für viele unserer Berechnungen in modularer Arithmetik kein Ergebnis.

Z.B. für die Kongruenzgleichung

$$(y^2 - x^3 + 2x - 5) \bmod 5 = 0$$

erhält man als Lösungsmenge die neun Wertepaare

$P\binom{0}{0}$, $Q\binom{1}{2}$, $-Q\binom{1}{3}$, $R\binom{2}{2}$, $-R\binom{2}{3}$, $S\binom{3}{1}$, $-S\binom{3}{4}$, $T\binom{4}{1}$ und $-T\binom{4}{4}$



Die durch Lösung der Kongruenzgleichung erzeugte "Kurve" besteht also aus einer endlichen Punktemenge. Bei der Punkteaddition gehört formal der UPU zu dieser Punktmenge.

Man kann nun, mit denselben Algorithmen wie bei der Punkteaddition und Punktevervielfachung auf reellen Kurven, auf der diskreten Kurve Punkte addieren und vervielfachen, allerdings in modularer Arithmetik. Dabei ist bemerkenswert, dass durch die Addition und Vervielfachung von Punkten auf der diskreten Kurve keine neuen Punkte erzeugt werden. Die durch Addition und Vervielfachung berechneten Punkte gehören also zur Punktmenge, die als Lösung der Kongruenzgleichung bestimmt wurde. Ausserdem zeigen die Additionstabellen eine attraktive Gruppenstruktur, die in dieser Übung untersucht werden soll.

2. Eine Additionstabelle erstellen

Das Programm ECC.exe löst die Kongruenzgleichung und berechnet die Summe aller möglichen Punktepaare ausser Summen der Art P + (– P). Im Programm werden die Grössen IA (für a), IB (für b) und IP (für p) mit dem Format (I3) eingelesen. Mit diesem Format muss z.B. eine Zahl 5 mit zwei Leerzeichen und "5" eingegeben werden. Die Zahl -5 würde mit einem Leerzeichen gefolgt von "-5" eingegeben.

Zuerst soll die erhaltene Punktmenge aufgelistet werden.

Wertepaar Nr.	1.	2.	3.	4.	5.	6.	7.
Wertepaar $\binom{x}{y}$							

Wertepaar Nr.	8.	9.	10.	11.	12.	13.	14.
Wertepaar $\binom{x}{y}$							

Danach wird, basierend auf dem Output von ECC.exe[2], eine Additionstabelle erstellt.

2.1 Ein Beispiel

Das Beispiel ist für a = 1, b = 3 und p = 13. Die Kongruenzgleichung ergab eine Punktmenge mit 14 Punkten. Der Output von ECC.exe war wie folgt:

IA = ? 1 IB = ? 3 IP = ? 13

1. (0|4)	8. (8|4)
2. (0|9)	9. (8|9)
3. (2|0)	10. (9|0)
4. (5|4)	11. (10|5)
5. (5|9)	12. (10|8)
6. (6|2)	13. (12|1)
7. (6|11)	14. (12|12)

Sekanten

1. (0|4) + (5|4) = (8|9)	61. (5|4) + (0|4) = (8|9)
2. (0|4) + (5|9) = (9|0)	62. (5|9) + (0|4) = (9|0)
3. (0|4) + (6|2) = (10|8)	63. (6|2) + (0|4) = (10|8)
4. (0|4) + (6|11) = (8|4)	64. (6|11) + (0|4) = (8|4)
5. (0|4) + (8|4) = (5|9)	65. (8|4) + (0|4) = (5|9)
6. (0|4) + (8|9) = (6|2)	66. (8|9) + (0|4) = (6|2)
7. (0|4) + (9|0) = (5|4)	67. (9|0) + (0|4) = (5|4)
8. (0|4) + (10|5) = (6|11)	68. (10|5) + (0|4) = (6|11)
9. (0|4) + (10|8) = (12|12)	69. (10|8) + (0|4) = (12|12)
10. (0|4) + (12|1) = (10|5)	70. (12|1) + (0|4) = (10|5)
11. (0|9) + (5|4) = (9|0)	71. (5|4) + (0|9) = (9|0)
12. (0|9) + (5|9) = (8|4)	72. (5|9) + (0|9) = (8|4)
13. (0|9) + (6|2) = (8|9)	73. (6|2) + (0|9) = (8|9)
14. (0|9) + (6|11) = (10|5)	74. (6|11) + (0|9) = (10|5)
15. (0|9) + (8|4) = (6|11)	75. (8|4) + (0|9) = (6|11)
16. (0|9) + (8|9) = (5|4)	76. (8|9) + (0|9) = (5|4)
17. (0|9) + (9|0) = (5|9)	77. (9|0) + (0|9) = (5|9)
18. (0|9) + (10|5) = (12|1)	78. (10|5) + (0|9) = (12|1)
19. (0|9) + (10|8) = (6|2)	79. (10|8) + (0|9) = (6|2)
20. (0|9) + (12|12) = (10|8)	80. (12|12) + (0|9) = (10|8)
21. (5|4) + (6|11) = (12|12)	81. (6|11) + (5|4) = (12|12)
22. (5|4) + (8|4) = (0|9)	82. (8|4) + (5|4) = (0|9)
23. (5|4) + (8|9) = (10|5)	83. (8|9) + (5|4) = (10|5)
24. (5|4) + (9|0) = (0|4)	84. (9|0) + (5|4) = (0|4)
25. (5|4) + (10|8) = (8|4)	85. (10|8) + (5|4) = (8|4)
26. (5|4) + (12|1) = (6|2)	86. (12|1) + (5|4) = (6|2)
27. (5|9) + (6|2) = (12|1)	87. (6|2) + (5|9) = (12|1)
28. (5|9) + (8|4) = (10|8)	88. (8|4) + (5|9) = (10|8)
29. (5|9) + (8|9) = (0|4)	89. (8|9) + (5|9) = (0|4)
30. (5|9) + (9|0) = (0|9)	90. (9|0) + (5|9) = (0|9)
31. (5|9) + (10|5) = (8|9)	91. (10|5) + (5|9) = (8|9)
32. (5|9) + (12|12) = (6|11)	92. (12|12) + (5|9) = (6|11)
33. (6|2) + (8|4) = (0|4)	93. (8|4) + (6|2) = (0|4)
34. (6|2) + (9|0) = (10|5)	94. (9|0) + (6|2) = (10|5)
35. (6|2) + (10|5) = (0|9)	95. (10|5) + (6|2) = (0|9)

[2] ECC.exe von http://www.mathepauker.com/Blockchain/ECC/ECC.exe auf Downloads herunterladen und von dort ausführen.

36. (6|2) + (10|8) = (9|0)	96. (10|8) + (6|2) = (9|0)
37. (6|2) + (12|12) = (5|4)	97. (12|12) + (6|2) = (5|4)
38. (6|11) + (8|9) = (0|9)	98. (8|9) + (6|11) = (0|9)
39. (6|11) + (9|0) = (10|8)	99. (9|0) + (6|11) = (10|8)
40. (6|11) + (10|5) = (9|0)	100. (10|5) + (6|11) = (9|0)
41. (6|11) + (10|8) = (0|4)	101. (10|8) + (6|11) = (0|4)
42. (6|11) + (12|1) = (5|9)	102. (12|1) + (6|11) = (5|9)
43. (8|4) + (9|0) = (12|12)	103. (9|0) + (8|4) = (12|12)
44. (8|4) + (10|5) = (5|4)	104. (10|5) + (8|4) = (5|4)
45. (8|4) + (10|8) = (12|1)	105. (10|8) + (8|4) = (12|1)
46. (8|4) + (12|1) = (9|0)	106. (12|1) + (8|4) = (9|0)
47. (8|4) + (12|12) = (10|5)	107. (12|12) + (8|4) = (10|5)
48. (8|9) + (9|0) = (12|1)	108. (9|0) + (8|9) = (12|1)
49. (8|9) + (10|5) = (12|12)	109. (10|5) + (8|9) = (12|12)
50. (8|9) + (10|8) = (5|9)	110. (10|8) + (8|9) = (5|9)
51. (8|9) + (12|1) = (10|8)	111. (12|1) + (8|9) = (10|8)
52. (8|9) + (12|12) = (9|0)	112. (12|12) + (8|9) = (9|0)
53. (9|0) + (10|5) = (6|2)	113. (10|5) + (9|0) = (6|2)
54. (9|0) + (10|8) = (6|11)	114. (10|8) + (9|0) = (6|11)
55. (9|0) + (12|1) = (8|9)	115. (12|1) + (9|0) = (8|9)
56. (9|0) + (12|12) = (8|4)	116. (12|12) + (9|0) = (8|4)
57. (10|5) + (12|1) = (8|4)	117. (12|1) + (10|5) = (8|4)
58. (10|5) + (12|12) = (0|4)	118. (12|12) + (10|5) = (0|4)
59. (10|8) + (12|1) = (0|9)	119. (12|1) + (10|8) = (0|9)
60. (10|8) + (12|12) = (8|9)	120. (12|12) + (10|8) = (8|9)

Tangenten:

121. 2 * (0|4) = (12|1)	139. 2 * (8|4) = (6|2)
122. (0|4) + (12|12) = (0|9)	140. (8|4) + (6|11) = (8|9)
123. (12|12) + (0|4) = (0|9)	141. (6|11) + (8|4) = (8|9)
124. 2 * (0|9) = (12|12)	142. 2 * (8|9) = (6|11)
125. (0|9) + (12|1) = (0|4)	143. (8|9) + (6|2) = (8|4)
126. (12|1) + (0|9) = (0|4)	144. (6|2) + (8|9) = (8|4)
127. 2 * (5|4) = (12|1)	145. 2 * (10|5) = (5|9)
128. (5|4) + (12|12) = (5|9)	146. (10|5) + (5|4) = (10|8)
129. (12|12) + (5|4) = (5|9)	147. (5|4) + (10|5) = (10|8)
130. 2 * (5|9) = (12|12)	148. 2 * (10|8) = (5|4)
131. (5|9) + (12|1) = (5|4)	149. (10|8) + (5|9) = (10|5)
132. (12|1) + (5|9) = (5|4)	150. (5|9) + (10|8) = (10|5)
133. 2 * (6|2) = (5|9)	151. 2 * (12|1) = (6|11)
134. (6|2) + (5|4) = (6|11)	152. (12|1) + (6|2) = (12|12)
135. (5|4) + (6|2) = (6|11)	153. (6|2) + (12|1) = (12|12)
136. 2 * (6|11) = (5|4)	154. 2 * (12|12) = (6|2)
137. (6|11) + (5|9) = (6|2)	155. (12|12) + (6|11) = (12|1)
138. (5|9) + (6|11) = (6|2)	156. (6|11) + (12|12) = (12|1)

Wendepunkte:

3 * (2|0) = "null"

Wendetangenten:

157. (2|0) + (0|4) = (2|0)	170. (0|4) + (2|0) = (2|0)
158. (2|0) + (0|9) = (2|0)	171. (0|9) + (2|0) = (2|0)
159. (2|0) + (5|4) = (2|0)	172. (5|4) + (2|0) = (2|0)
160. (2|0) + (5|9) = (2|0)	173. (5|9) + (2|0) = (2|0)
161. (2|0) + (6|2) = (2|0)	174. (6|2) + (2|0) = (2|0)
162. (2|0) + (6|11) = (2|0)	175. (6|11) + (2|0) = (2|0)
163. (2|0) + (8|4) = (2|0)	176. (8|4) + (2|0) = (2|0)
164. (2|0) + (8|9) = (2|0)	177. (8|9) + (2|0) = (2|0)
165. (2|0) + (9|0) = (2|0)	178. (9|0) + (2|0) = (2|0)
166. (2|0) + (10|5) = (2|0)	179. (10|5) + (2|0) = (2|0)
167. (2|0) + (10|8) = (2|0)	180. (10|8) + (2|0) = (2|0)
168. (2|0) + (12|1) = (2|0)	181. (12|1) + (2|0) = (2|0)
169. (2|0) + (12|12) = (2|0)	182. (12|12) + (2|0) = (2|0)

Berechne 525 · (6|11)

Daraus ergibt sich folgende Additionstabelle:

	(0|4)	(0|9)	(2|0)	(5|4)	(5|9)	(6|2)	(6|11)	(8|4)	(8|9)	(9|0)	(10|5)	(10|8)	(12|1)	(12|12)
(0|4)	(12|1)	UPU	(2|0)	(8|9)	(9|0)	(10|8)	(8|4)	(5|9)	(6|2)	(5|4)	(6|11)	(12|12)	(10|5)	(0|9)
(0|9)	UPU	(12|12)	(2|0)	(9|0)	(8|4)	(8|9)	(10|5)	(6|11)	(5|4)	(5|9)	(12|1)	(6|2)	(0|4)	(10|8)
(2|0)	(2|0)	(2|0)	UPU	(2|0)	(2|0)	(2|0)	(2|0)	(2|0)	(2|0)	(2|0)	(2|0)	(2|0)	(2|0)	(2|0)
(5|4)	(8|9)	(9|0)	(2|0)	(12|1)	UPU	(6|11)	(12|12)	(0|9)	(10|5)	(0|4)	(10|8)	(8|4)	(6|2)	(5|9)
(5|9)	(9|0)	(8|4)	(2|0)	UPU	(12|12)	(12|1)	(6|2)	(10|8)	(0|4)	(0|9)	(8|9)	(10|5)	(5|4)	(6|11)
(6|2)	(10|8)	(8|9)	(2|0)	(6|11)	(12|1)	(5|9)	UPU	(0|4)	(8|4)	(10|5)	(0|9)	(9|0)	(12|12)	(5|4)
(6|11)	(8|4)	(10|5)	(2|0)	(12|12)	(6|2)	UPU	(5|4)	(8|9)	(0|9)	(10|8)	(9|0)	(0|4)	(5|9)	(12|1)
(8|4)	(5|9)	(6|11)	(2|0)	(0|9)	(10|8)	(0|4)	(8|9)	(6|2)	UPU	(12|12)	(5|4)	(12|1)	(9|0)	(10|5)
(8|9)	(6|2)	(5|4)	(2|0)	(10|5)	(0|4)	(8|4)	(0|9)	UPU	(6|11)	(12|1)	(12|12)	(5|9)	(10|8)	(9|0)
(9|0)	(5|4)	(5|9)	(2|0)	(0|4)	(0|9)	(10|5)	(10|8)	(12|12)	(12|1)	UPU	(6|2)	(6|11)	(8|9)	(8|4)
(10|5)	(6|11)	(12|1)	(2|0)	(10|8)	(8|9)	(0|9)	(9|0)	(5|4)	(12|12)	(6|2)	(5|9)	UPU	(8|4)	(0|4)
(10|8)	(12|12)	(6|2)	(2|0)	(8|4)	(10|5)	(9|0)	(0|4)	(12|1)	(5|9)	(6|11)	UPU	(5|4)	(0|9)	(8|9)
(12|1)	(10|5)	(0|4)	(2|0)	(6|2)	(5|4)	(12|12)	(5|9)	(9|0)	(10|8)	(8|9)	(8|4)	(0|9)	(6|11)	UPU
(12|12)	(0|9)	(10|8)	(2|0)	(5|9)	(6|11)	(5|4)	(12|1)	(10|5)	(9|0)	(8|4)	(0|4)	(8|9)	UPU	(6|2)

Wenn zwei Punkte mit gleicher x-Koordinate addiert werden ist die Summe der UPU. Ebenso wenn man einen Punkt mit einer y-Koordinate 0 verdoppelt.

Es gibt auch Webseiten auf welchen man eine Additionstabelle online erstellen kann, z.B. https://graui.de/code/elliptic2/.

3. Einen Punkt vervielfachen

Am Schluss des Outputs von ECC.exe erscheint eine Aufforderung man soll einen Punkt vervielfachen. Im obigen Beispiel steht man soll $525 \cdot (6|11)$ berechnen. Dazu muss man nicht 524 Mal P zu P addieren. Man arbeitet mit Punktverdoppelungen.

$$P\begin{pmatrix} & \\ & \end{pmatrix}$$

2P	4P	8P	16P	32P	64P	128P	256P	512P
$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$

Für das hier gezeigte Beispiel gilt $P\begin{pmatrix} 6 \\ 11 \end{pmatrix}$ erhält man aus der Additionstabelle

2P	4P	8P	16P	32P	64P	128P	256P	512P
$\begin{pmatrix} 5 \\ 4 \end{pmatrix}$	$\begin{pmatrix} 12 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 6 \\ 11 \end{pmatrix}$	$\begin{pmatrix} 5 \\ 4 \end{pmatrix}$	$\begin{pmatrix} 12 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 6 \\ 11 \end{pmatrix}$	$\begin{pmatrix} 5 \\ 4 \end{pmatrix}$	$\begin{pmatrix} 12 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 6 \\ 11 \end{pmatrix}$

Man erhält dann

$$525P = 512P + 8P + 4P + P = \begin{pmatrix} 6 \\ 11 \end{pmatrix} + \begin{pmatrix} 6 \\ 11 \end{pmatrix} + \begin{pmatrix} 12 \\ 1 \end{pmatrix} + \begin{pmatrix} 6 \\ 11 \end{pmatrix}$$

$$= 2\begin{pmatrix} 6 \\ 11 \end{pmatrix} + \left(\begin{pmatrix} 12 \\ 1 \end{pmatrix} + \begin{pmatrix} 6 \\ 11 \end{pmatrix}\right) = \begin{pmatrix} 5 \\ 4 \end{pmatrix} + \begin{pmatrix} 5 \\ 9 \end{pmatrix} = P_\infty$$

Das Ergebnis dieser Multiplikation ist der UPU.

Meine Multiplikation: .....

Berechnung:

Ergebnis: ..... $\cdot \begin{pmatrix} & \\ & \end{pmatrix} = \begin{pmatrix} & \\ & \end{pmatrix}$