Wolfgang K. Seiler
Tel. 2515

B6, B4.08

30. April 2025

9. Übungsblatt Kryptologie

Aufgabe 1:

a) Finden Sie die kleinste dreistellige Primzahl $p \equiv 1 \bmod 11$!

b) Welche Primzahlen p zwischen 100 und 200 sind von der Form $2p'+1$ mit einer Primzahl p'?

Aufgabe 2:

a) Angenommen, ein DSA-Anwender wählt für die Unterschriften unter zwei verschiedene Nachrichten m und m' die gleiche Zufallszahl k. Zeigen Sie, daß jeder, der die beiden Nachrichten und die beiden Unterschriften kennt, den geheimen Schlüssel dieses Anwenders bestimmen kann!

b) Ein Anwender wählt für seine elektronischen DSA-Unterschriften die Parameter $q = 1\,009$, $p = 1\,124\,027$ und $g = 2\,952$. Sein öffentlicher Schlüssel ist $u = 9\,275$. Er unterschreibt die Nachricht 456 mit $(1006, 199)$, die Nachricht 789 mit $(1006, 202)$. Berechnen Sie seinen geheimen Schlüssel!

Aufgabe 3:

Vom vorigen Übungsblatt kennen wir die diskreten Logarithmen modulo 23 zur Basis fünf:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

Berechnen Sie mit Hilfe dieser Logarithmentafel die Zahlen

$$a = 13 \cdot 17 \bmod 23, \quad b = 13! \bmod 23 \quad \text{und} \quad c = 13^{100} \bmod 23\,!$$

Aufgabe 4:

a) Zeigen Sie, daß $p = 113$ eine Primzahl ist!

Lösung: Da $11^2 = 121$ größer ist als 113, wäre 113 durch eine der Primzahlen $2, 3, 5, 7$ teilbar, falls die Zahl zusammengesetzt wäre. Als ungerade Zahl ist 113 nicht durch zwei teilbar, durch drei auch nicht, da die Quersumme 5 keine Dreierzahl ist, und wenn 113 durch fünf teilbar wäre, müßte die letzte Ziffer 0 oder 5 sein. Da $113 : 7 = 16$ Rest 1 ist, kann die Zahl auch nicht durch sieben teilbar sein, ist also prim.

b) Modulo $p = 113$ gelten die Kongruenzen $3^8 \equiv 7 \bmod p$ und $2^{14} \equiv 3^{56} \equiv 112 \bmod p$ (die Sie *nicht* nachrechnen müssen). Bestimmen Sie die Ordnungen der Elemente zwei, drei und sechs in $(\mathbb{Z}/113)^\times$.

Lösung: Da p prim ist, hat $(\mathbb{Z}/113)^\times$ die Ordnung $p - 1 = 112 = 2^4 \cdot 7$. Die Ordnung eines jeden Elements ist nach Lagrange ein Teiler davon.
Da $2^{14} \equiv 112 \equiv -1 \bmod p$, ist $2^{28} \equiv 1 \bmod p$, die Ordnung der Zwei ist also ein Teiler von 28 und kann kein Teiler von 14 sein. Falls sie kleiner als 28 ist, muß sie also ein Teiler von $28/7 = 4$ sein, aber $2^4 = 16$ ist modulo p ungleich eins. Somit hat zwei die Ordnung 28.

Die Ordnung der Drei ist ein Teiler von 112, nicht aber von 56. Falls sie kleiner als 112 wäre, müßte sie Teiler von $112/7 = 16$ sein. Da $3^8 \equiv 7 \bmod p$, ist $3^{16} \equiv 49 \bmod p$. Somit hat drei die Ordnung 112.
Für jedes $n \in \mathbb{N}$ ist $6^n \equiv 2^n \cdot 3^n \bmod p$. Falls die Ordnung von sechs kleiner als 112 ist, muß entweder 6^{56} oder 6^{16} modulo p gleich eins sein. Da 28 ein Teiler von 56 ist, ist $2^{56} \equiv 1 \bmod p$, also $6^{56} \equiv 3^{56} \equiv -1 \bmod p$.

$$6^{16} \equiv 2^{16} \cdot 3^{16} \equiv 4 \cdot 2^{14} \cdot 3^{16} \equiv 4 \cdot (-1) \cdot 49 = -196 \equiv -83 \bmod 113\,,$$

also ist beides nicht der Fall, und die Ordnung ist 112.

c) Bestimmen Sie den diskreten Logarithmus modulo p von zwölf zur Basis drei!

Lösung: Hier bietet sich die *baby step - giant step*-Methode an: Die Wurzel von 113 ist knapp 11; da 113 ziemlich klein ist, bieten sich elf *baby steps* an. Die ersten elf Potenzen von drei modulo 113 sind

i	1	2	3	4	5	6	7	8	9	10	11
$3^i \bmod p$	3	9	27	81	17	51	40	7	21	63	76

12 kommt in dieser Liste nicht vor; wir brauche daher noch *giant steps* und dazu zunächst $3^{-11} \bmod 113$, also das Inverse von 76. Dies liefert der erweiterte EUKLIDische Algorithmus:

$$\begin{aligned} 113 : 76 = 1 \text{ Rest } 37 &\Longrightarrow 37 = 113 - 76 \\ 76 : 37 = 2 \text{ Rest } 2 &\Longrightarrow 2 = 76 - 2 \cdot (113 - 76) = 3 \cdot 76 - 2 \cdot 113 \\ 37 : 2 = 18 \text{ Rest } 1 &\Longrightarrow 1 = (113 - 76) - 18 \cdot (3 \cdot 76 - 2 \cdot 113) = 37 \cdot 113 - 55 \cdot 76 \end{aligned}$$

Das Inverse ist also $-55 \equiv 113 - 55 = 58 \bmod 113$, und für den ersten *giant step* erhalten wir $12 \cdot 3^{-11} \equiv 12 \cdot 58 \equiv 696 \equiv 18 \bmod 113$. Auch diese Zahl steht nicht in der Liste; wir machen weiter mit $18 \cdot 58 = 1044 \equiv 27 = 3^3 \bmod 113$. Also ist $12 \cdot 3^{-11 \cdot 2} \equiv 3^3 \bmod 113$, d.h. $12 \equiv 3^{22+3} = 3^{25} \bmod 113$. Der diskrete Logarithmus ist somit 25.

Aufgabe 5:

a) Zeigen Sie, daß die Zwei in $(\mathbb{Z}/295)^\times$ die Ordnung 116 hat!

Lösung: r sei die gesuchte Ordnung. Die Primzerlegung von 295 ist $295 = 5 \cdot 59$, also ist dann $2^r \equiv 1 \bmod 5$ und $2^r \equiv 1 \bmod 59$. Wegen $2^2 = 4 \equiv -1 \bmod 5$ hat die Zwei die Ordnung vier in $(\mathbb{Z}/5)^\times$, d.h. $r \equiv 0 \bmod 4$.
$59 - 1 = 2 \cdot 29$; nach LAGRANGE ist also die Ordnung eines Elements von $(\mathbb{Z}/59)^\times$ eine der Zahlen $1, 2, 29$ oder 58. Für die Zwei kommen 1 und 2 offensichtlich nicht in Frage.
$2^{29} = 2^{16} \cdot 2^8 \cdot 2^4 \cdot 2$. Modulo 59 ist

$$2^4 = 16, \quad 2^6 = 2^4 \cdot 4 = 64 \equiv 5, \quad 2^8 = 2^6 \cdot 4 \equiv 20, \quad 2^16 \equiv 20^2 = 400 \equiv 46\,.$$

Also ist $2^{29} \equiv 46 \cdot 20 \cdot 16 \cdot 2 = 29440 \equiv 58 \bmod 59$, so daß die Zwei nicht Ordnung 29 hat. Damit hat sie modulo 59 die Ordnung 58.
Die gesuchte Ordnung r ist also sowohl ein Vielfaches von vier als auch eines von 58, also eines von 116. Da 2^{116} sowhl modulo fünf als auch modulo 59 gleich eins ist, ist $2^{116} \equiv 1 \bmod 295$, die Zwei hat also Ordnung 116.

b) Lösen Sie die Gleichung $2^x \equiv 9 \bmod 295$ mit dem *baby step – giant step* Algorithmus und dem chinesischen Restesatz!
Hinweis: Bei so kleinen Werten von p empfiehlt es sich, die Anzahl der *baby steps* nicht viel größer als die Wurzel des Moduls zu wählen.

Lösung: Wegen des chinesischen Restesatzes reicht es, zunächst die beiden Kongruenzen $2^x \equiv 9 \bmod 5$ und $2^x \equiv 9 \bmod 59$ zu lösen. Die erste der beiden ist einfach: Wegen $9 \equiv 4 \bmod 5$, ist $x = 2$ die offensichtliche Lösung.

Modulo 59 empfiehlt es sich, mit der *baby step – giant step* Methode zu arbeiten. $8^2 = 64$ ist moderat größer als 59, also berechnen wir in den *baby steps* die Zahlen $2^i \bmod 59$ für $i \leq 8$:

i	1	2	3	4	5	6	7	8
$2^i \bmod 59$	2	4	8	16	32	5	10	20

Für die *giant steps* brauchen wir die Zahlen $9 \cdot 2^{-8j} = 20^{-j} \bmod 59$, also als Erstes das Inverse von 20 modulo 59. Da $3 \cdot 20 = 60 \equiv 1 \bmod 59$ ist, sehen wir auch ohne EUKLIDischen Algorithmus, daß dieses gleich drei ist. Wir müssen also die Zahlen $9 \cdot 3^j \bmod 59$ bestimmen bis wir eine erhalten, die bereits Ergebnis eines *baby steps* war.

j	1	2	3	4	5
$9 \cdot 2^{-8j} \bmod 59$	27	22	7	21	4

Das Ergebnis ist $9 \cdot 2^{-8 \cdot 5} = \equiv 2^2 \bmod 59$, also $2^{8 \cdot 5 + 2} = 2^{42} \equiv 9 \bmod 59$.

Modulo fünf hat die Zwei die Ordnung vier, also ist $2^{42} \equiv 2^2 = 4 \equiv 9 \bmod 5$. Somit ist $2^{42} \equiv 9 \bmod 295$.