1. Modulare Arithmetik I

Berechnen Sie jeweils ohne Taschenrechner. Die Ergebnisse sollen dabei im Bereich 0, . . . , Modulus-1 liegen. Beschreiben Sie kurz den Zusammenhang zwischen den einzelnen Aufgaben: (a) 19 · 23 mod 17 (b) −15 · 23 mod 17

A: (a) 19\*23 mod 17 = 2\*6 mod 17 = 12 mod 17

(b) -15\*23 mod 17=2\*6 mod 17 = 12 mod 17

Die Resultat ist gleich.

1. Vervollständigen Sie die Verknüpfungstafeln für Z/5Z

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| + | 0 | 1 | 2 | 3 | 4 |
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| \* | 0 | 1 | 2 | 3 | 4 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |
|  |  |  |  |  |  |

1. Modulare Arithmetik II (Multiplikative Inverse)

(a) Welche Elemente in Z/8Z, Z/11Z haben keine multiplikative Inverse?

(b) Wie unterscheidet sich Z/pZ von Z/8Z, falls p eine Primzahl ist?

(c) Gegeben sei die Primzahl 7. Berechnen Sie für 5 ∈ Z/7Z ∗ die Potenzen 5i , i = 1, 2, . . . bis zum ersten Mal 5i ≡ 1 mod 7 auftritt.

i. Ist die Existenz eines solchen i a priori klar? Begründen Sie Ihre Antwort.

ii. Was ändert sich, wenn man die Potenzen von 2 ∈ Z/8Z betrachtet. Warum existiert jetzt kein i mit 2i ≡ 1 mod 8.

A: (a) Z/8Z: 1,3,5,7.

Z/11Z: 1,2,3,4,5,6,7,8,9,10.

(b) Falls p eine Primzahl ist, die Elemente in Z/pZ von 1 zur p-1 sind.

1. Modulare Arithmetik III (Quer durch den Garten)

Berechnen Sie jeweils ohne Taschenrechner. Die Ergebnisse sollen dabei im Bereich 0, . . . , Modulus-1 liegen.

(a) mod 11

(b) 4 · x = 4 mod 8 (Geben Sie alle Lösungen an.)

(c) 3x + 4 = 2 mod 5

A: (a)

f) Stromchiffren

(a) Gegeben sei das LFSR mit der Rückkopplungsvorschrift: si+3 = si+2 + si mod 2, i ≥ 0 und der Anfangsbelegung r2 = 1, r1 = 0, r0 = 1. Vervollständigen Sie die Tabelle.

|  |  |  |  |
| --- | --- | --- | --- |
| Ausgabefolge Si | R2 | R1 | R0 |
| 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 |

(b) Bestimmen Sie die Periode, d.h. geben Sie an nach wie vielen Takten sich die Ausgabesequenz wiederholt.

A: Von der Form ist die Periode

(c) Bestimmen Sie die Frobeniusbegleitmatrix.

(d) Stellen Sie sich vor, dass obiges LFSR gemäß dem ersten Designprinzip für eine Stromchiffre aus der Vorlesung eingesetzt wird. Warum wäre das System gebrochen, wenn man z.B. s1, . . . , s3 kennt? Nehmen Sie nun an, dass Sie ein LFSR mit einer Länge von 128 bit verwenden. Wäre das System auch gebrochen, wenn man z.B. s3, . . . , s130 kennt?

A: Der Startvektor (Geheimer Schlüssel k) ist nur 3 Bits. Er ist S1,…S3. Alle Situationen Können mit dem Startvektor berechnet werden. Wenn man S3…S130 kennt, wird die Periode berechnet. Man kann von der Ausgabesequenz das System brechen.

(e) Nehmen Sie nun an, dass obiges LFSR wird wie in der gefilterten Schieberegisteranordnung aus der Vorlesung mit dem Filter x1 x0 + x2 x0 + x2 x1 + x2 + x1 + x0 kombiniert wird.

i. Berechnen Sie die ersten 3 Ausgabebits ausgehend von obiger Startbelegung.

ii. Wäre das System immer noch gebrochen, wenn man s1, . . . , s3 kennt? Begründen Sie Ihre Antwort.

i: Die ersten 3 Ausgabebits sind 1,1,1.

ii: Das System wäre noch gebrochen, weil die Länge des Startvektors zu kurz.(nur 3 bits)

(f) Warum bietet es sich an, bei der Implementierung einer gefilterten Schieberegisteranordnung die Ausgabefolgen des LFSRs mittels der fortgeführten Matrix-Vektor-Multiplikation des Startvektors mit der Frobeniusbegleitmatrix (vgl.Vorlesung) zu arbeiten bzw. einer effizienten Implementierung davon?

A: Die Ausgabebits hängt nicht nur von des Startvektors. Die gefilterte schieberegisteranordnung und Startvektor entscheiden die Ausgabebits.

（g）Gegeben sei nun das LFSR, welches durch die fortgeführte Matrix-Vektor-Multiplikation mit der Frobeniusbegleitmatrix F = und dem Startvektor beschrieben wird. Vervollständigen Sie die Tabelle.

|  |  |  |  |
| --- | --- | --- | --- |
| Ausgabefolge si | R2 | R1 | R0 |
| 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |

1. Welche Periode ergibt sich hier?

Die Periode ist 3.

1. Welche Dimension hat der von F i · er zeugte Untervektorraum? Welche Dimension ergibt sich bei a). Welcher Zusammenhang ergibt sich zu den Perioden?

A: Der erzeugte Untervektorraum von F i · ist {}

Untervektorraum ist {}

Dimension ist 2 .

Bei a) ergibt sich auch 3 Dimension.

2^Dimension – 1 = stets m-Sequenzen maximal Periode.

Die Periode hängt von der Startvektor und Rückkopplungsvorschrift.

1. Wie lautet die Rückkopplungsvorschrift?

Rückkpoplungsvorschrift: Si+3=Si mod 2, i>=0.