

Vorlesung Diskrete Strukturen

Rechnen modulo n

Bernhard Ganter

WS 2009/10

1 Rechnen modulo n

1.1

modulo (Wiederholung)

Für eine natürliche Zahl $n > 0$ und eine ganze Zahl z bezeichnet

$$z \bmod n$$

diejenige Zahl in $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, um die z größer ist als eine durch n teilbare Zahl.

Mit Hilfe der Gaussklammer erhält man

$$z \bmod n := z - n \cdot \left\lfloor \frac{z}{n} \right\rfloor.$$

Informatiker schreiben statt $\left\lfloor \frac{z}{n} \right\rfloor$ gern $z \operatorname{div} n$.

Mit dieser Schreibweise ist dann

$$z \bmod n := z - n \cdot (z \operatorname{div} n).$$

Die Homomorphieregel

Wenn man umfangreiche Rechnungen modulo n auszuführen hat, dann ist die **Homomorphieregel** außerordentlich hilfreich. Sie besagt, dass man auch Zwischenergebnisse modulo n rechnen darf, ohne dass sich das Endergebnis ändert. Formal besagt sie, dass für ganze Zahlen a, b stets folgendes

gilt:

$$\begin{aligned}(a + b) \bmod n &= (a \bmod n + b \bmod n) \bmod n \\(a - b) \bmod n &= (a \bmod n - b \bmod n) \bmod n \\(a \cdot b) \bmod n &= (a \bmod n \cdot b \bmod n) \bmod n\end{aligned}$$

August, der Scherzkeks

König August treibt ein Späßchen mit seinen Hofdienern. Er lässt zwanzig Diener rufen und erklärt ihnen seine Regeln: Jeder Diener bekommt einen farbigen Hut aufgesetzt, wobei fünf verschiedene Farben möglich sind. Jeder Diener kann die Hüte der anderen sehen, nicht aber seinen eigenen. Nacheinander müssen sie vortreten und laut raten, welche Farbe der Hut auf dem eigenen Kopf hat. Dabei dürfen sie nicht miteinander sprechen oder sich sonstwie Hinweise geben. Je mehr richtige Antworten gegeben werden, desto größer wird die Belohnung für alle sein.

Die Diener sind schlau

Die Diener kennen das Spiel schon, denn der König spielt es nicht zum ersten Mal. Sie haben deshalb eine Zuordnung der fünf Farben zu den Zahlen 0, 1, 2, 3, 4 vereinbart und die folgende Strategie verabredet:

Der zuerst aufgerufene Diener addiert die Hutfarben der anderen Diener modulo 5 und nennt laut das Ergebnis. Das ist zwar wahrscheinlich nicht die Farbe seines eigenen Hutes, aber mit Hilfe dieser Information können alle anderen Diener die Farbe ihres Hutes herausfinden. Sie wissen nun nämlich, was die Summe modulo 5 über alle Hüte ist, dazu müssen sie ja nur die gegebene Antwort zu der Hutfarbe des ersten Dieners addieren. Wenn sie von dieser Summe die Summe aller Hüte, die sie sehen, subtrahieren (also alle außer ihrem eigenen), erhalten sie die Farbe ihres eigenen Hutes. Auf diese Weise ist also höchstens die erste Antwort falsch.

$$a \equiv r \pmod{n}$$

Der ständige Zusatz „mod n “ wird rasch lästig und gern weggelassen. Um Missverständnisse zu vermeiden, kann man ihn am Ende der Rechnung in Klammern angeben und die Gleichheitszeichen durch \equiv ersetzen, wie im folgenden Beispiel:

$$(108 \cdot 33) - 22 \equiv (3 \cdot 3) + 3 \equiv 9 + 3 \equiv 2 \pmod{5}.$$

Statt $a \bmod n = r$ schreibt man oft auch

$$a \equiv r \pmod{n}$$

und liest dies etwas altertümlich aber einprägsam als

a ist kongruent zu r modulo n.

Beispiel

Aufgabe: Was sind die letzten beiden Ziffern von $333333 \cdot 444444 \cdot 56789$?

Kunstgriff: Die letzten beiden Ziffern einer natürlichen Zahl n sind offenbar die Ziffern von $n \bmod 100$. Also:

$$\begin{aligned} 333333 \cdot 444444 \cdot 56789 &\equiv 33 \cdot 44 \cdot 89 \\ &\equiv 3 \cdot 11 \cdot 4 \cdot 11 \cdot 89 \\ &\equiv 12 \cdot 121 \cdot 89 \\ &\equiv 21 \cdot (890 + 178) \\ &\equiv 21 \cdot (90 + 78) \\ &\equiv 21 \cdot 68 \\ &\equiv 1428 \\ &\equiv 28 \pmod{100} \end{aligned}$$

Rechnen modulo n

Auf der Menge $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ der natürlichen Zahlen kleiner als n kann man zwei zweistellige Operationen definieren: Die Addition modulo n , die Subtraktion modulo n und die Multiplikation modulo n . Man definiert

$$\begin{aligned} a +_{\bmod n} b &:= (a + b) \bmod n \\ a -_{\bmod n} b &:= (a - b) \bmod n \\ a \cdot_{\bmod n} b &:= (a \cdot b) \bmod n. \end{aligned}$$

Allerdings ist es viel zu umständlich, die Operationszeichen mit den Indizes zu benutzen. Deshalb lässt man die gern weg, benutzt einfach die Zeichen $+$, $-$ und \cdot und sagt dazu, dass man modulo n rechnet.

Rechnen modulo 2

Der für die Informatik wichtigste Fall ist natürlich $n = 2$. In diesem Fall stimmen Addition und Subtraktion überein. Die beiden Operationen sind durch die folgenden Verknüpfungstabellen beschrieben:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Das Rechnen modulo 2.

Umgangssprachlich sind diese Operationen vertrauter, wenn man das Symbol 0 als „gerade“ und 1 als „ungerade“ liest. Man hat dann *gerade plus gerade gleich gerade*, *gerade plus ungerade gleich ungerade*, usw.

Rechnen modulo 5

+	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	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

·	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

Die Verknüpfungstabellen für die Rechenarten modulo 5.

Die Subtraktion kann man einfacher mit Hilfe der einstelligen Operation $x \mapsto -x$ definieren, die wie folgt gegeben ist:

x	0	1	2	3	4
$-x$	0	4	3	2	1

Offenbar gilt $a - b = a + (-b)$
für alle a, b .

Ein einfaches Rechenbeispiel

Aufgabe: Eine größere Menge Bauschotter wird mit einer Eisenbahn von A nach B transportiert, dafür sind 50 Fahrten erforderlich. Das Beladen des Zuges dauert vier Stunden, jede Fahrt zwei Stunden pro Richtung und das Abladen drei Stunden. Pausen werden nicht gemacht. Mit dem Beladen für

die erste Fahrt wurde mittags um 12:00 Uhr begonnen. Zu welcher Uhrzeit wird der letzte Zug zurück erwartet?

Antwort: Für jede Fahrt wird vom Beginn des Beladens bis zur Rückkehr ein Zeitraum von 11 Stunden benötigt, insgesamt also $50 \cdot 11$ Stunden. Da nur nach der Uhrzeit der Rückkehr gefragt ist, kann modulo 24 gerechnet werden, und man erhält, dass der Zug

$$12 + 50 \cdot 11 \equiv 12 + 2 \cdot 11 \equiv 34 \equiv 10 \pmod{24},$$

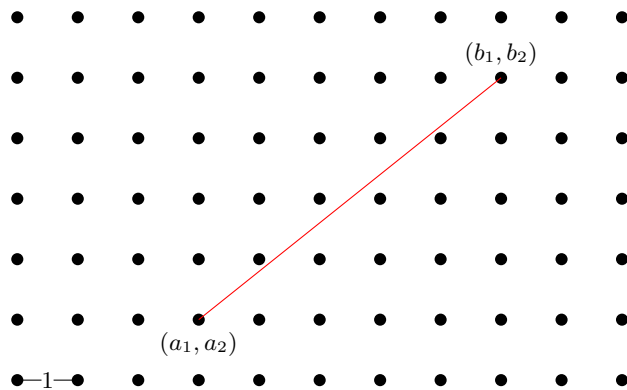
also zehn Stunden nach Mitternacht ankommt.

2 Summen von zwei Quadraten

2.1

Ein raffinierteres Beispiel

Frage: Welchen Abstand können zwei Gitterpunkte des karierten Papiers haben?



Ein raffinierteres Beispiel

Frage: Welchen Abstand können zwei Gitterpunkte des karierten Papiers haben?

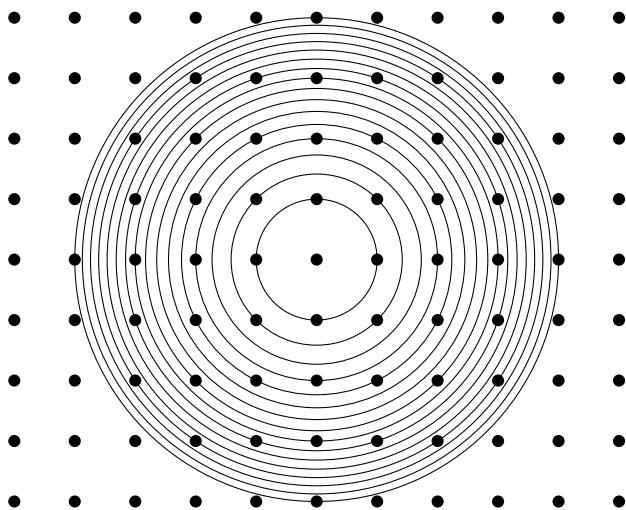
Teilantwort: Der Abstand zwischen den Punkten mit den Koordinaten (a_1, a_2) und (b_1, b_2) ist nach dem Satz von Pythagoras gleich

$$\text{dist}((a_1, a_2), (b_1, b_2)) = \sqrt{(b_1 - a_1)^2 + (b_2 - a_2)^2}.$$

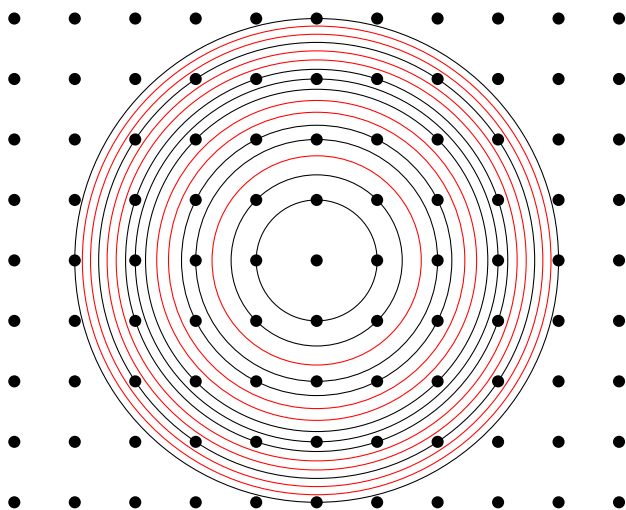
Wenn a_1, a_2, b_1, b_2 ganze Zahlen sind, dann ist der Abstand also notwendig von der Form \sqrt{n} für eine natürliche Zahl n .

Aber: Welche Zahlen n treten tatsächlich auf?

Kreise vom Radius \sqrt{n} um einen Gitterpunkt, $n \leq 16$.



Welche Kreise enthalten einen Gitterpunkt?



Was unsere Beobachtungen ergeben haben

- Der Abstand zweier Gitterpunkte des Einheitsgitters kann nur eine Zahl der Form \sqrt{n} sein, wobei n eine natürliche Zahl ist.
- Diese *notwendige Bedingung* ist aber nicht *hinreichend*: Es gibt Zahlen der Form \sqrt{n} , die nicht Abstand zweier Gitterpunkte sind.
- Für $n \leq 16$ gilt folgendes:
 - \sqrt{n} ist der Abstand zweier Gitterpunkte für $n = 0, 1, 2, 4, 5, 8, 9, 10, 13, 16$
 - \sqrt{n} ist *nicht* der Abstand zweier Gitterpunkte für $n = 3, 6, 7, 11, 12, 14, 15$.

Welches Gesetz steckt dahinter?

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, ...

Welche Zahlen sind Summe von zwei Quadraten?

Die Frage, welche Zahlen n von der Form

$$n = a^2 + b^2, \quad a, b \in \mathbb{N}$$

sind, ist etwas zu schwierig für diese Vorlesung.

Wir geben hier nur einen ersten, einfachen Schritt der Argumentationskette an und verraten dann die Antwort.

Die Frage gehört zur **elementaren Zahlentheorie**. Dieser Zweig der Mathematik hat viele schöne Anwendungen in der Informatik, insbesondere dafür, Daten gegen Störungen oder gegen Angriffe zu sichern (Kodierungstheorie, Kryptologie).

Eine notwendige Bedingung

Wir kommen der Antwort ein kleines Stück näher, wenn wir das Problem modulo 4 betrachten: Wenn

$$n = a^2 + b^2$$

gilt, dann muss natürlich auch folgendes gelten:

$$n \bmod 4 = ((a \bmod 4)^2 + (b \bmod 4)^2) \bmod 4.$$

a	0	1	2	3
a^2	0	1	4	9
$a^2 \bmod 4$	0	1	0	1

Quadratzahlen modulo vier sind nur die Zahlen 0 und 1.

Die Summe zweier Quadrate kann modulo 4 also nur die Werte 0, 1 oder 2 annehmen, niemals den Wert 3.

Ein Satz von J.P.Fermat

Satz 1 (Fermat). *Eine Primzahl p ist genau dann als Summe zweier Quadrate ganzer Zahlen darstellbar, wenn $p \not\equiv 3 \pmod{4}$.*

Davon haben wir die einfachere Richtung eben bewiesen. Von da ist es nicht mehr sehr weit zum allgemeinen Ergebnis:

Satz 2. *Eine natürliche Zahl n ist genau dann Summe zweier Quadrate ganzer Zahlen, wenn jeder Primteiler $\equiv 3 \pmod{4}$ in der kanonischen Darstellung von n einen geraden Exponenten hat.*

Beispiel: $240 = 2^4 \cdot 3 \cdot 5$ ist nicht Summe zweier Quadrate. Aber $720 = 2^4 \cdot 3^2 \cdot 5$ ist Summe zweier Quadrate (nämlich $12^2 + 24^2$).

3 Square and Multiply

3.1

Motivation

Bei Anwendungen der modularen Arithmetik z.B. in der Kryptographie hat man oft Ausdrücke der Form

$$98732752938752987523975^{983205820502051} \pmod{843980282093803}$$

auszuwerten (gewöhnlich sind die Zahlen viel größer als in diesem Beispiel, z.B. 1000-stellig).

Wie kann man so etwas ausrechnen?
Und wozu ist das gut?

Die erste Frage ist leicht zu beantworten. Für die zweite benötigen wir noch einiges an Theorie.

Zwei Hilfsmittel

Solche Berechnungen werden durch die Kombination zweier Überlegungen durchführbar:

- Man kann bei jedem Rechenschritt modular vereinfachen, dabei hilft besonders die Homomorphieregel, und
- man kann mittels “Square and Multiply” die Berechnung der Potenz in einfache Schritte zerlegen.

Wie das geht, erklären wir an einem ganz kleinen Beispiel: Wir rechnen

$$2^{100000} \bmod 100001$$

aus.

Square and Multiply

Wegen

$$100000 = 2^{16} + 2^{15} + 2^{10} + 2^9 + 2^7 + 2^5$$

gilt

$$\begin{aligned} 2^{100000} &= 2^{2^{16}} \cdot 2^{2^{15}} \cdot 2^{2^{10}} \cdot 2^{2^9} \cdot 2^{2^7} \cdot 2^{2^5} \\ &= ((((((2^{2^1} \cdot 2)^{2^5} \cdot 2)^{2^1} \cdot 2)^{2^2} \cdot 2)^{2^2} \cdot 2)^{2^5} \\ &= ((\dots (2^2 \cdot 2)^{2 \cdot 2 \cdot 2 \cdot 2} \cdot 2)^2 \cdot 2)^{2 \cdot 2} \cdot 2)^{2 \cdot 2 \cdot 2 \cdot 2}. \end{aligned}$$

Das ist nun leicht auszurechnen. Man erhält

$$2^{100000} \bmod 100001 = 1024.$$

Potenzieren modulo n

Das Potenzieren mit dem Exponenten $e \in \mathbb{N}$ kann mit $\lceil \log_2 e \rceil$ -maligem Quadrieren und Multiplizieren durchgeführt werden.

Beim Rechnen modulo n kann dabei bei jedem Rechenschritt $\bmod n$ reduziert werden.

Kein auch nur halbwegs schnelles Verfahren ist bekannt, um aus der Angabe von $2^e \bmod n$ den Exponenten e zu bestimmen („binary log“).

Das kann man ausnutzen, um Hacker auszutricksen!

Öffentlich ein Geheimnis vereinbaren

Problemstellung: Zwei Teilnehmer möchten abhörsicher miteinander kommunizieren und dazu ein Verschlüsselungsverfahren benutzen.

Dazu müssen sie einen gemeinsamen geheimen Schlüssel verwenden.

Wie können sie sich über eine nicht abhörsichere Verbindung auf ein gemeinsames Geheimnis einigen?

Öffentlich ein Geheimnis vereinbaren

Lösung:

Die beiden Teilnehmer A und B einigen sich zunächst öffentlich auf eine grosse Zahl n .

Dann erzeugt jeder Teilnehmer eine große Zahl:

- Teilnehmer A erzeugt die Zahl a und berechnet $2^a \bmod n$
- Teilnehmer B erzeugt die Zahl b und berechnet $2^b \bmod n$

Die Zahlen a und b behalten die Teilnehmer geheim für sich. Die Zahlen $2^a \bmod n$ und $2^b \bmod n$ teilen sie sich mit.

Danach

- kennt Teilnehmer A die Zahlen a und $2^b \bmod n$,
- kennt Teilnehmer B die Zahlen b und $2^a \bmod n$,
- kennt ein Angreifer die Zahlen $2^a \bmod n$ und $2^b \bmod n$.

Das gemeinsame Geheimnis

Die beiden Teilnehmer berechnen

$$2^{a \cdot b} \equiv (2^a)^b \equiv (2^b)^a \pmod{n}.$$

Dieses Ergebnis verwenden sie als gemeinsamen Schlüssel für das Verschlüsselungsverfahren.

Der Angreifer kennt lediglich $2^a \bmod n$ und $2^b \bmod n$.

Es ist kein brauchbares Verfahren bekannt, daraus

$$2^{a \cdot b} \bmod n$$

auszurechnen.

Beispiel

Achtung: Die in diesem Beispiel verwendeten Zahlen sind viel zu klein und bieten keinerlei Sicherheit gegen einen Angriff!

1. Die beiden Geheimnisträger A und B einigen sich öffentlich auf $n := 100001$ als Modul.

2. A wählt $a := 23456$ als sein persönliches Geheimnis,
 B wählt $b := 34567$ als sein persönliches Geheimnis.
3. A berechnet $2^a \bmod n = 5201$ und sendet diese Zahl an B .
 B berechnet $2^b \bmod n = 8642$ und sendet diese Zahl an A .
4. A kennt nun die Zahlen $a = 23456$ und $2^b = 8642$ und berechnet
 $(2^b)^a = 8642^{23456} = 41408$.
5. B kennt nun die Zahlen $b = 34567$ und $2^a = 5201$ und berechnet
 $(2^a)^b = 5201^{34567} = 41408$.
6. 41408 ist nun das gemeinsame Geheimnis.

4 Der Körper $\text{GF}(p)$

4.1

Regeln (1) für das Rechnen modulo n

Die Addition

- ist assoziativ: es gilt $(a + b) + c = a + (b + c)$ für alle a, b, c ,
- ist kommutativ: es gilt $a + b = b + a$ für alle a, b ,
- ist **kürzbar**: aus $a + b = a + c$ folgt stets $b = c$. Das ist wichtig, wenn man Gleichungen lösen will.
- hat 0 als **neutrales Element**: $a + 0 = 0 + a = a$ gilt für alle a .
- hat **inverse Elemente**: Zu jedem a ist $-a := 0 - a$ ein Element mit $a + (-a) = 0 = (-a) + a$. Daraus folgt übrigens die Kürzbarkeit.

$(\mathbb{Z}_n, +_{\bmod n}, -_{\bmod n}, 0)$ ist eine **abelsche Gruppe**.

Regeln (2) für das Rechnen modulo n

die Multiplikation

- ist assoziativ: es gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle a, b, c ,
- ist kommutativ: es gilt $a \cdot b = b \cdot a$ für alle a, b ,
- hat 1 als neutrales Element: $a \cdot 1 = a = 1 \cdot a$ gilt für alle a .

- ist über der Addition distributiv: $a \cdot (b + c) = a \cdot b + a \cdot c$ gilt für alle a, b, c (Leseregel: „Punktrechnung vor Strichrechnung“).

$$\mathbb{Z}_n := (\mathbb{Z}_n, +_{\text{mod } n}, -_{\text{mod } n}, \cdot_{\text{mod } n}, 0, 1)$$

ist ein **kommutativer Ring mit Eins**.

Regeln für das Rechnen modulo einer Primzahl p

Rechnet man modulo einer Primzahl p , dann hat man noch eine zusätzliche Rechenoperation zur Verfügung: Man kann auch **dividieren!**

Jede von Null verschiedene Zahl $a \in \mathbb{Z}_p$ hat nämlich ein **multiplikativ inverses** Element, d.h. eine Zahl $b \in \mathbb{Z}_p$ mit

$$a \cdot b \equiv 1 \pmod{p}.$$

Eine solche Zahl kann man als **Kehrwert** von a modulo p verstehen, denn das Multiplizieren mit b wirkt wie ein Dividieren durch a .

Existenz eines Inversen

Eine Primzahl p ist zu jeder nicht durch p teilbaren Zahl teilerfremd.

Ist also $a \in \mathbb{Z}_p$ ungleich Null, dann gilt $\text{ggT}(a, p) = 1$, und man kann Zahlen α, β berechnen mit

$$1 = \alpha \cdot a + \beta \cdot p.$$

Rechnet man beide Seiten dieser Gleichung modulo p , erhält man das gewünschte Ergebnis:

$$1 = (\alpha \bmod p) \cdot a.$$

Berechnung des Inversen

Man findet das multiplikativ inverse Element zu a mit Hilfe des erweiterten euklidischen Algorithmus.

Zu gegebener Primzahl p und $a \in \mathbb{Z}_p$ mit $a \neq 0$ errechnet man Zahlen α und β mit $1 = \alpha \cdot a + \beta \cdot p$.

Die Zahl

$$b := \alpha \bmod p$$

ist dann multiplikativ invers zu a .

Der Körper $\text{GF}(p)$, p prim

Beim Rechnen modulo einer Primzahl p hat man alle Struktur zur Verfügung, die man zum Rechnen braucht, denn

- \mathbb{Z}_p ist ein kommutativer Ring mit Eins,
- auf dem zusätzlich eine vollständige Division erklärt ist (durch jedes von Null verschiedene Element).

Eine solche Struktur, in der man mit den gewohnten Regeln

addieren, subtrahieren, multiplizieren und dividieren

kann, nennt man einen **Körper**. Andere Beispiele sind \mathbb{Q} , \mathbb{R} und \mathbb{C} .

Der Körper mit p Elementen wird mit $\text{GF}(p)$ bezeichnet („Galois-Field“).

Beispiel $\text{GF}(7)$, Addition und Subtraktion

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

−	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	1	0	6	5	4	3	2
2	2	1	0	6	5	4	3
3	3	2	1	0	6	5	4
4	4	3	2	1	0	6	5
5	5	4	3	2	1	0	6
6	6	5	4	3	2	1	0

Beispiel GF(7), Multiplikation und Division

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

:	1	2	3	4	5	6
1	1	4	5	2	3	6
2	2	1	3	4	6	5
3	3	5	1	6	2	4
4	4	2	6	1	5	3
5	5	6	4	3	1	2
6	6	3	2	5	4	1

Primitives Element

Man kann das Rechnen mit Hilfe eines **primitives Elements** vereinfachen. Darunter versteht man ein Element des Körpers, dessen Potenzen alle von Null verschiedenen Elemente durchlaufen.

Beispiel: Sind die Elemente 2 und 3 primitiv in GF(7)?

n	0	1	2	3	4	5
2^n	1	2	4	1	2	4

Die Zahl 2 ist *nicht* primitiv.

n	0	1	2	3	4	5
3^n	1	3	2	6	4	5

Die Zahl 3 ist primitiv.

Rechnen mit Potenzen

Für die Potenzen ein beliebiges Elements α von GF(p) gilt

- $\alpha^m \cdot \alpha^n = \alpha^{m+n}$ und
- $\alpha^n = \alpha^{n \bmod p-1}$.

Der Multiplikation von Potenzen entspricht also die *Addition der Exponenten modulo $p - 1$* .

Deshalb kann man Multiplikation und Division modulo p auf Addition und Subtraktion modulo $p - 1$ zurückführen.

Beispiel für $p := 7$:

$$\frac{2 \cdot 3}{5 \cdot 5} \equiv \frac{3^2 \cdot 3^1}{3^5 \cdot 3^5} \equiv \frac{3^3}{3^4} \equiv 3^5 \equiv 5 \pmod{7}.$$

“Logarithmentafel”

Kennt man ein primitives Element α , so kann man eine Tafel der Potenzen dieses Elements (salopp gesagt: eine „Logarithmentafel“ modulo p) zur vereinfachten Rechnung von Multiplikation und Division benutzen.

Der „Logarithmus“ (zur Basis α) eines Elements $z \neq 0$ von $\text{GF}(p)$ ist dann diejenige Zahl $e \in \mathbb{Z}_{p-1}$, für die $\alpha^e = z$ gilt. Für $z = 0$ schreibt man den symbolischen Wert $-\infty$ auf. Im Fall $p := 7, \alpha := 3$ ergibt sich folgende Tafel:

z	0	1	2	3	4	5	6
$\log_3 z$	$-\infty$	0	2	1	4	5	3