Mathematik I - Übungsblatt 04

Lösungsvorschläge

Aufgabe 1

Die Verfahren der asymmetrischen Verschlüsselung, der Authentifizierung (= Feststellung, ob eine Person diejenige ist, für die sie sich ausgibt), der elektronischen Unterschrift und anderer verlangen das Berechnen modularer Potenzen von ganzen Zahlen

$$G=(K^e) \text{ MOD } n \quad .$$

Dabei sind K, e und n natürliche Zahlen mit einigen 100 Dezimalstellen. Kein heutiger Digitalrechner ist in der Lage, die Operation K^e dann auch nur annähernd schnell auszuführen und das Zwischenergebnis in seiner Länge auf einem der heute verfügbaren Medien zu speichern. Mit einem Trick wird es aber möglich, die Operation in gut ausführbare Teile zu zerlegen und diese zusammen zu fassen. Man verwendet dazu die Eigenschaft der Vertauschbarkeit der Modulo-Operation, siehe Kapitel 18.9 im Skript.

a) Berechnen Sie $G=\left(19^{15}\right) \text{ MOD } 23$.

Tipp: Zerlegen Sie den Exponenten 15 in eine Summe von 2-er-Potenzen und wenden Sie die Rechenregeln für Potenzen an.

$$G=\left(19^{(8+4+2+1)}\right) \text{ MOD } 23=\left[\left(19^4\right)^2 \text{ MOD } 23\cdot\left(19^2\right)^2 \text{ MOD } 23\cdot\left(19^2\right)^1 \text{ MOD } 23\cdot(19)^1 \text{ MOD } 23\right] \text{ MOD } 23 \quad .$$

Hierin ist

$$(19^1) \text{ MOD } 23=19$$

$$(19^2) \text{ MOD } 23=\left((19^1)^2\right) \text{ MOD } 23=16$$

$$(19^2)^2 \text{ MOD } 23=(19^4) \text{ MOD } 23=3$$

$$(19^4)^2 \text{ MOD } 23=(19^8) \text{ MOD } 23=9$$

$$G=\left(19^{(8+4+2+1)}\right) \text{ MOD } 23=[9\cdot3\cdot16\cdot19] \text{ MOD } 23=19$$

Hinweis: Die 4-fach-Multiplikation im letzten Ausdruck wird bei großen Zahlen ebenfalls in Teilschritten durchgeführt, so dass in den Zwischenergebnissen nicht mehr als $22\cdot22=484$ auftreten kann.

b) Berechnen Sie $G=\left(34^{24}\right) \text{ MOD } 39$. (selbst durchführen)

c) Wie viele Stellen werden in den Teilrechnungen im Vergleich mit der Stellenzahl der Module höchstens gebraucht?

Mit dem Modul n höchstens die Stellenzahl von $(n-1)\cdot(n-1)=(n-1)^2$.

d) Könnte man die Zerlegung des Exponenten auch mit 3-er-Potenzen, 4-er-Potenzen usw. machen? Was wäre die Folge für die maximal benötigte Stellenzahl bei den Teilrechnungen?

Ja, bei 3-er-Potenzen ergibt sich mit dem Modul n aber bereits die Stellenzahl von $(n-1)^3$ usw.

Tipp: Verwenden Sie die Scilab-Funktion ***modulo(x,y)***.

Aufgabe 2

Die RSA-Verschlüsselung einer „Klartextzahl“ K in eine „Geheimtextzahl“ G erfolgt über die Operation

$$G=(K^e) \text{ MOD } n \quad ,$$

die Entschlüsselung über

$K = (G^d)$ MOD n .

Das funktioniert,

- wenn $n = p \cdot q$ und p und q Primzahlen sind,
- der öffentliche Schlüssel e eine beliebige, zu $\Phi(n) = (p-1) \cdot (q-1)$ teilerfremde Zahl ist,

  $ggT(e, \Phi(n)) = 1$,
- der geheime Schlüssel d die Bedingung der modularen inversen Zahl zu e bezüglich $\Phi(n)$ erfüllt, also

  $(d \cdot e)$ MOD $\Phi(n) = 1$.

Gegeben sind $p = 13$, $q = 19$, $e = 113$ und die Klartextzahl $K = 7$.

a) Berechnen Sie n. → 247

b) Berechnen Sie $\Phi(n)$. → 216

c) Berechnen Sie den geheimen Schlüssel d.

$\Phi_0 = a_1 \cdot \Phi_1 + \Phi_2$: $216 = 1 \cdot 113 + 103$

$\Phi_1 = a_2 \cdot \Phi_2 + \Phi_3$: $113 = 1 \cdot 103 + 10$

$\Phi_2 = a_3 \cdot \Phi_3 + \Phi_4$: $103 = 10 \cdot 10 + 3$

$\Phi_3 = a_4 \cdot \Phi_4 + \Phi_5$: $10 = 3 \cdot 3 + 1$

$\Phi_5 = 1 = ggT(\Phi_0, \Phi_1) = ggT(\Phi(n), e)$

m = 5 = Index von Rest 1

Rekursion:

$z_i = -a_{m-i} \cdot z_{i-1} + z_{i-2}$

mit i = 2, 3, …, m-1 = **2,3,4**

Startwerte:

$z_0 = 1$

$z_1 = -a_{m-1} = -a_4 = \mathbf{-3}$

Durchführung der Rekursion:

$z_2 = -a_3 \cdot z_1 + z_0$: $31 = -10 \cdot (-3) + 1$

$z_3 = -a_2 \cdot z_2 + z_1$: $-34 = -1 \cdot 31 + (-3)$

$z_4 = -a_1 \cdot z_3 + z_2$: $65 = -1 \cdot (-34) + 31$

z_4 ist die gesuchte modulare inverse Zahl

Probe: $(13 \cdot 34)$ MOD 63 = 1

d) Berechnen Sie die Geheimtextzahl G.

$G = 7^{113}$ MOD $247 = 7^{(64+32*16+1)}$ MOD 247

$7^2 \text{ MOD } 247 = 49$

$49^2 \text{ MOD } 247 = 7^4 \text{ MOD } 247 = 178$

$178^2 \text{ MOD } 247 = 7^8 \text{ MOD } 247 = 68$

$68^2 \text{ MOD } 247 = 7^{16} \text{ MOD } 247 = 178$

$178^2 \text{ MOD } 247 = 7^{32} \text{ MOD } 247 = 68$

$68^2 \text{ MOD } 247 = 7^{64} \text{ MOD } 247 = 178$

$G = 7^{113} \text{ MOD } 247 = 7^{(64+32*16+1)} \text{ MOD } 247 = (178 \cdot 68 \cdot 178 \cdot 7) \text{ MOD } 247 = 11$

e) Zeigen Sie für dieses Beispiel, dass $K = (G^d) \text{ MOD } n$ erfüllt ist.

$K = 11^{65} \text{ MOD } 247 = 11^{(64+1)} \text{ MOD } 247$

Wie bei Punkt d):

$11^2 \text{ MOD } 247 = 121$

$121^2 \text{ MOD } 247 = 11^4 \text{ MOD } 247 = 68$

$68^2 \text{ MOD } 247 = 11^8 \text{ MOD } 247 = 178$

$178^2 \text{ MOD } 247 = 11^{16} \text{ MOD } 247 = 68$

$68^2 \text{ MOD } 247 = 11^{32} \text{ MOD } 247 = 178$

$178^2 \text{ MOD } 247 = 11^{64} \text{ MOD } 247 = 68$

$K = 11^{65} \text{ MOD } 247 = 11^{(64+1)} \text{ MOD } 247 = (68 \cdot 11) \text{ MOD } 247 = 7$

Vorschlag: Man sieht, dass der Rechenablauf systematisch aufgebaut ist. Versuchen Sie, diesen als Algorithmus in einer **Scilab-Funktion** (***function***) zu formulieren.

Aufgabe 3

Bestimmen Sie **alle** Lösungen zu

a) $\sin(\gamma) = \frac{\sqrt{3}}{2}$

$\arcsin\left(\frac{\sqrt{3}}{2}\right) = \mathbf{60}° \pm k \cdot 360°$ **und** $\mathbf{120}° \pm k \cdot 360°, \quad k = 0,\ 1,\ 2,\ \ldots$

Hinweis: Die sin-Funktion (und die cos-Funktion) sind mit $k \cdot 360°$ periodisch.

In Grad Bogenmaß:

$\arcsin\left(\frac{\sqrt{3}}{2}\right) = \frac{\boldsymbol{\pi}}{\mathbf{3}} \pm k \cdot 2 \cdot \pi$ **und** $\frac{\mathbf{2\pi}}{\mathbf{3}} \pm k \cdot 2 \cdot \pi, \quad k = 0,\ 1,\ 2,\ \ldots$

Tipp: Schauen Sie sich mit Hilfe von **Scilab** ein Diagramm der sin-Funktion an.

b) $\tan(\psi) = \frac{1}{\sqrt{3}}$.

$\arctan\left(\frac{1}{\sqrt{3}}\right) = \mathbf{30}° \pm k \cdot 180°, \quad k = 0,\ 1,\ 2,\ \ldots$

Hinweis: Die tan-Funktion (und die cotan-Funktion) sind mit 180° periodisch.

Tipp: Schauen Sie sich mit Hilfe von **Scilab** ein Diagramm der tan-Funktion an.

Aufgabe 4

Bestimmen Sie **alle** Lösungen folgender Gleichungen (im Allgemeinen gibt es hier wegen der Periodizität trigonometrischer Funktionen eine Haupt- und unendlich viele weitere Lösungen):

a) $\sin(2x+\frac{\pi}{9})=\frac{1}{2}$ **Tipp:** Ersetzen Sie das Argument durch $2x+\frac{\pi}{9}=y$, dann wird es übersichtlicher.

$$\sin(y)=\frac{1}{2} \quad \rightarrow \quad y=\arcsin\left(\frac{1}{2}\right)=30°\pm k\cdot 360° \quad \textbf{und} \quad 150°\pm k\cdot 360°, \quad k=0,\ 1,\ 2,...$$

Substition nach x auflösen und y einsetzen:

$$x=\frac{y-20°}{2}=\frac{y}{2}-10°=15°-10°\pm k\cdot 360° \quad \textbf{und} \quad 75°-10°\pm k\cdot 360° \ = \ 5°\pm k\cdot 360° \quad \textbf{und} \quad 65°\pm k\cdot 360°$$

Tipp: Probe mit einigen Werten für x machen.

b) $2\cdot[\sin(x)]^2-2\cdot\cos(x)=2$

Nach Kürzung durch 2 und mit der trigonometrischen Beziehung $[\sin(x)]^2+[\cos(x)]^2=1$ erhält man

$$1-[\cos(x)]^2-\cos(x)=1$$

$$-[\cos(x)]^2-\cos(x)=0 \qquad \rightarrow \qquad [\cos(x)]^2+\cos(x)=0$$

Substitutuion : $x=\cos(x)$ $\rightarrow$ $y^2+y=0$ $\rightarrow$ $y_1=0,\quad y_2=-1$

$$\cos(x)=0 \qquad \rightarrow \qquad x=90°\pm k\cdot 360°, \quad k=0,\ 1,\ 2,....$$

$$\cos(x)=-1 \qquad \rightarrow \qquad x=180°\pm k\cdot 180°, \quad k=0,\ 1,\ 2,....$$

Hinweis: Die Nullstellen der sin- und cos-Funktion haben eine Periode von 180°.

c) $\sin(2x)+3\sin(x)-2\cdot\tan(x)=0$.

Triogonometrische Umformungen: $\sin(2x)=2\cdot\sin(x)\cdot\cos(x)$, $\tan(x)=\frac{\sin(x)}{\cos(x)}$

$$2\cdot\sin(x)\cdot\cos(x)+3\cdot\sin(x)-2\cdot\frac{\sin(x)}{\cos(x)}=0$$

Lösung 1: $\sin(x)=0$ $\rightarrow$ $x=0°\pm k\cdot 180°, \quad k=0,\ 1,\ 2,....$

Lösung 2: Gleichung durch $\sin(x)$ dividieren, dabei $\sin(x)=0$ **ausschließen!**

$$2\cdot\cos(x)+3-\frac{1}{\cos(x)}=0 \qquad \rightarrow \qquad 2[\cos(x)]^2+3\cdot\cos(x)-1=0$$

Substitution: $y=\cos(x)$ $\rightarrow$ $2\cdot y^2+3\cdot y-1=0$

Lösungen: $y_{1,2}=-\frac{3}{4}\pm\sqrt{\left(\frac{3}{4}\right)^2+1}=-\frac{3}{4}\pm\frac{5}{4} \quad \rightarrow \quad y_1=\frac{1}{2} \quad , \quad y_2=-2$.

Für $y_2=\cos(x)=-2$ gibt es im Reellen keine Lösung, es bleibt $y_1=\cos(x)=\frac{1}{2}$

$$x=60°\pm k\cdot 360°, \quad k=0,1,2,... \quad \textbf{und} \quad x=-60°\pm k\cdot 360°, \quad k=0,1,2,... \ .$$

Noch ein **Tipp**: Formen Sie Gleichungen so um, dass auf den rechten Seiten 0 steht und nennen Sie die linken Seiten f(x). Stellen Sie die Graphen der Funktionen f(x) mit Scilab dar, z. B. mit

x= linspace(-2*%pi, 2*%pi,1000); plot(x, f(x)); xgrid;

Dann haben Sie eine anschauliche Kontrollmöglichkeit zu den gesuchten Nullstellen. Mit der Zoom-Funktion im ***Grafik-Fenster*** können Sie außerdem einzelne Bereiche feiner auflösen, z. B., um die Lage von Nullstellen genauer sichtbar zu machen.

Aufgabe 5

a) Zeigen Sie die Gültigkeit von $[\sin(x)]^2+[\cos(x)]^2=1$ für $x\in R$ mit Hilfe der trigonometrischen Additionstheoreme. **Tipp:** Verwenden Sie das Theorem $\cos(u\pm v)=\cos(u)\cdot\cos(v)\mp\sin(u)\cdot\sin(v)$.

$\cos(x-x)=\cos(0)=1=[\cos(x)\cdot\cos(x)]+[\sin(x)\cdot\sin(x)]$

b) Zeigen Sie die Gültigkeit von $\sin[\arccos(x)]=\sqrt{1-x^2}$ für $x\in[-1,1]$

Tipp: Ersetzen Sie zur Vereinfachung $\arccos(x)=y$ und verwenden Sie trigonometrische Umformungen.

$\sin(y)=\sqrt{1-x^2}$ → $[\sin(y)]^2=1-x^2=1-[\cos(y)]^2$ → $[\cos(y)]^2=x^2$

$[\cos(\arccos(x))]^2=x^2$ → $x^2=x^2$ → linke und rechte Seite stimmen überein:

→ Gültigkeit erwiesen.

c) Zeigen Sie, dass $\arccos(x)=\arcsin(\sqrt{1-x^2})$ für $x\in[-1,1]$ gilt.

$\sin[\arccos(x)]=\sin[\arcsin(\sqrt{1-x^2})]=\sqrt{1-x^2}$:

Die Gültigkeit wurde unter Punkt b) gezeigt, daher ist auch Aussage gültig.

Aufgabe 6

In der Ingenieurtechnik müssen oft zu einem, in einem rechtwinkligen x-y-Koordinatensystem gegebenen Objekt (z. B. einem Kraftvektor oder einem Spannungszeiger aus dem Koordinatenursprung heraus) die Winkel bezüglich der positiven x-Achse bestimmt werden. Die trigonometrischen Umkehrfunktionen liefern dazu aus den Achsenabschnitten (= Komponenten) der Objekte die **Hauptwerte,** die je nach Lage im Quadranten des Koordinatensystems noch zu korrigieren sind, siehe Kapitel 18.1.4 im Skript.

Bestimmen Sie für die Komponenten eines ebenen Vektors a mit

a) $a_x=2$, $a_y=-4$ die Winkel über die arccos- und arctan- Funktion.

Hinweis. Die Winkel müssen natürlich gleich groß sein.

$\alpha=\arcsin\left(\frac{a_y}{\sqrt{a_x^2+a_y^2}}\right)=\arcsin\left(\frac{-4}{\sqrt{20}}\right)$ → Q IV → keine Korrektur → Scilab ergibt $\alpha=-63.4°$.

$\alpha=\arctan\left(\frac{a_y}{a_x}\right)=\arctan\left(\frac{-4}{2}\right)=\arctan(-2)$ → Q IV → keine Korrektur → Scilab → $\alpha=-63.4°$.

b) $a_x=-3$, $a_y=-5$ die Winkel über die arcsin- und arccot-Funktion.

$\alpha=\arcsin\left(\frac{a_y}{\sqrt{a_x^2+a_y^2}}\right)=\arcsin\left(\frac{-5}{\sqrt{34}}\right)$ → Q III → Korrektur erforderlich, siehe Kapitel 18.1.4.

Scilab ergibt $\alpha'=-59.0°$ → $\alpha=180°-\alpha'=239.0°$ → Probe machen!

Die arccot-Funktion ist nicht in jedem Taschenrechner vorhanden, daher verwendet man wegen $\operatorname{arccot}\left(\frac{a_x}{a_y}\right)=\arctan\left(\frac{a_y}{a_x}\right)$ die arctan-Funktion:

$\alpha=\arctan\left(\frac{a_y}{a_x}\right)=\arctan\left(\frac{-5}{-3}\right)=\arctan\left(\frac{5}{3}\right)$ → Q III → Korrektur erforderlich, siehe Kapitel 18.1.4.

Scilab ergibt $\alpha'=59.0°$ → $\alpha=180°+\alpha'=239.0°$ → Probe machen!

c) $a_x=-1$, $a_y=3$ die Winkel über die arcsin- arccos- und arctan-Funktion.

$\alpha=\arcsin\left(\frac{a_y}{\sqrt{a_x^2+a_y^2}}\right)=\arcsin\left(\frac{3}{\sqrt{10}}\right)$ → Q II → Korrektur erforderlich, siehe Kapitel 18.1.4.

Scilab ergibt $\alpha'=71.6°$ → $\alpha=180°-\alpha'=108.4°$ → Probe machen!

$\alpha=\arccos\left(\frac{a_x}{\sqrt{a_x^2+a_y^2}}\right)=\arccos\left(\frac{-1}{\sqrt{10}}\right)$ → Q II → keine Korrektur erforderlich

Scilab ergibt $\alpha'=108.4°=\alpha$.

$\alpha=\arctan\left(\frac{a_y}{a_x}\right)=\arctan\left(\frac{3}{-1}\right)=\arctan(-3)$ → Q II → Korrektur erforderlich, siehe Kapitel 18.1.4

Scilab ergibt $\alpha'=-71.6°$ → $\alpha=180°+\alpha'=108.4°$ → Probe machen!

Aufgabe 7

Eine ebene rechteckige Metallplatte, die in den beiden Koordinatenrichtungen x und z durch gegebene mechanische Normalspannungen σ_{xx}, σ_{zz} (= griechisch „sigma") senkrecht zu den Kanten und durch Scherspannungen σ_{xz} längs der Kanten belastet ist, besteht aus zwei Teilen, die unter einem Winkel ϕ verschweißt sind. In der Schweißnaht entstehen durch die äußere Belastung ebenfalls eine Normalspannung (σ = sigma) und ein Scherspannung (= Schubspannung) τ (= griechisch „tau"). Die Gleichgewichtsbedingungen werden als

$$\sigma\cdot\sin\phi+\tau\cdot\cos\phi=\sigma_{xx}\cdot\sin\phi+\sigma_{xz}\cdot\cos\phi \quad \text{(I)}$$

$$\sigma\cdot\cos\phi-\tau\cdot\sin\phi=\sigma_{zz}\cdot\cos\phi+\sigma_{xz}\cdot\sin\phi \quad \text{(II)}$$

ermittelt.

Achtung: Zur Wahrung einer einfacheren Übersicht werden die Argumente der trigonometrischen Funktion **ausnahmsweise nicht** in Klammern gesetzt und statt der korrekten Schreibweise

$[\cos(\phi)]^2$ die abkürzende, aber nicht korrekte Schreibweise $\cos^2\phi$ verwendet.

a) Skizzieren Sie grob die Platte,
   1. tragen Sie eine angenommenen Lage der Schweißnaht ein,
   2. legen Sie ein x-z-Koordinatensystem parallel zu den Kanten fest,
   3. versuchen Sie, sich vorzustellen, wo und in welchen Richtungen die genannten Spannung wirken.

   → selber machen.

b) Welche Terme sind gegebene Konstanten? → ϕ , σ_{xx}, σ_{zz} , σ_{xz}

c) Was sind die beiden Unbekannten? → σ und τ

d) Warum ist das Gleichungssystem in den beiden Unbekannten linear? → Da die beiden

Unbekannten nur in der ersten Potenz und jeweils nur als einfache mit Konstanten multiplizierte Summenterme erscheinen.

e) Bestimmen Sie für einen gegebenen Winkel ϕ die unbekannten Spannungen σ, τ in der Schweißnaht.

Elimination von σ durch Multiplikation von (I) mit $\cos(\phi)$ und von (II) mit $-\sin(\phi)$:

$$\sigma \cdot \sin\phi \cdot \cos\phi + \tau \cdot \cos^2\phi = \sigma_{xx} \cdot \sin\phi \cdot \cos\phi + \sigma_{xz} \cdot \cos^2\phi \quad \text{(III)}$$

$$-\sigma \cdot \sin\phi \cdot \cos\phi + \tau \cdot \sin^2\phi = -\sigma_{zz} \cdot \sin\phi \cdot \cos\phi - \sigma_{xz} \cdot \sin^2\phi \quad \text{(IV)}$$

Addition (III) + (IV):

$$\tau \cdot (\cos^2\phi + \sin^2\phi) = \sigma_{xx} \cdot \sin\phi \cdot \cos\phi - \sigma_{zz} \cdot \sin\phi \cdot \cos\phi + \sigma_{xz} \cdot (\cos^2\phi - \sin^2\phi)$$

Anwenden von

$$\cos^2\phi + \sin^2\phi = 1 \quad , \quad \cos^2\phi - \sin^2\phi = \cos(2\cdot\phi) \quad , \quad 2\cdot\sin\phi\cdot\cos\phi = \sin(2\cdot\phi) \quad :$$

$$\tau = \frac{(\sigma_{xx} - \sigma_{zz})}{2} \cdot \sin(2\cdot\phi) + \sigma_{xz} \cdot \cos(2\cdot\phi)$$

f) Unter welchem Winkel ϕ wird die Scherspannung $\tau = 0$?

$$0 = \frac{(\sigma_{xx} - \sigma_{zz})}{2} \cdot \sin(2\cdot\phi) + \sigma_{xz} \cdot \cos(2\cdot\phi)$$

Trennen der beiden Terme und Verwendung von $\tan(2\cdot\phi) = \frac{\sin(2\cdot\phi)}{\cos(2\cdot\phi)}$:

$$\tan(2\cdot\phi) = -2 \cdot \frac{\sigma_{xz}}{\sigma_{xx} - \sigma_{zz}} = 2 \cdot \frac{\sigma_{xz}}{\sigma_{zz} - \sigma_{xx}}$$

arctan-Funktion auf beide Seiten anwenden:

$$2\cdot\phi = \arctan\left[2 \cdot \frac{\sigma_{xz}}{\sigma_{zz} - \sigma_{xx}}\right] \quad \text{oder} \quad \phi = \frac{1}{2} \cdot \arctan\left[2 \cdot \frac{\sigma_{xz}}{\sigma_{zz} - \sigma_{xx}}\right]$$

g) Wie groß ist der Winkel ϕ für folgende mechanische Spannungen:

$$\sigma_{xx} = 30\left[\frac{N}{mm^2}\right] \quad , \quad \sigma_{zz} = 50\left[\frac{N}{mm^2}\right] \quad , \quad \sigma_{zx} = 15\left[\frac{N}{mm^2}\right]$$

→ 28,15°