Mathematik I - Übungsblatt 04

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 $G=(19^{15}) \text{ MOD } 23$.

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

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

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

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?

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

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

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,

  $$ggT(e,\Phi(n))=1 \quad ,$$

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

  $$(d \cdot e) \text{ MOD } \Phi(n)=1 \quad .$$

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

a) Berechnen Sie n.

b) Berechnen Sie $\Phi(n)$.

c) Berechnen Sie den geheimen Schlüssel d.

d) Berechnen Sie die Geheimtextzahl G.

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

Aufgabe 3

Bestimmen Sie **alle** Lösungen zu

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

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

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.

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

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

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 $\cos(u\pm v)=\cos(u)\cdot\cos(v)\mp\sin(u)\cdot\sin(v)$.

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.

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

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.

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

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

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 mechanischen Gleichgewichtsbedingungen für die Ruhelage (=statisches Gleichgewicht der Platte) wurden als

$$\sigma \cdot \sin\phi + \tau \cdot \cos\phi = \sigma_{xx} \cdot \sin\phi + \sigma_{xz} \cdot \cos\phi$$

$$\sigma \cdot \cos\phi - \tau \cdot \sin\phi = \sigma_{zz} \cdot \cos\phi + \sigma_{xz} \cdot \sin\phi$$

ermittelt.

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

b) Welche Terme sind gegebene Konstanten?

c) Was sind die beiden Unbekannten?

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

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

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

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

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