

LABORATION 3

Differentialiekvationer, Kryptoforcering

Deluppgifterna 1-3 redovisas i form av en rapport som gruppen lämnar in utskrivnen på papper till studentexpeditionen på Matematik senast 23/10 2013. Anvisningar för rapportens utformning, se kursens hemsida! Rapport som är godkänd och inlämnad i tid ger 1.5 bonuspoäng till tentan. Deluppgift 4 redovisas genom att gruppens MATLAB-program skickas till övningsassistenten för testkörning. Uppgiften ska skickas in senast den 11/11. Denna deluppgift ger inga bonuspoäng, men är obligatoriskt moment i Lab 3.

1. Numerisk integrering - svängningstiden för en pendel

I den här uppgiftsdelen skall du räkna ut svängningstiden för en pendel. En pendels svängningstid T beror av utslagsvinkeln φ_0 enligt formeln:

$$T = 4\sqrt{\frac{L}{g}} I(\varphi_0)$$

där L är pendelns längd, g är tyngdaccelerationen och

$$I(\varphi_0) = \int_0^{\pi/2} \frac{d\varphi}{\sqrt{1 - k^2(\sin \varphi)^2}}, \quad k = \sin \frac{\varphi_0}{2}$$

Låt $L = 1 \text{ m}$ och $g = 9.81 \text{ m/s}^2$. Skriv ett program som beräknar svängningstiden T för φ_0 -värdena 5, 10, ..., 90 grader. För att beräkna integralen $I(\varphi_0)$ används Matlabfunktionen `quad`. Plotta resultatet, dvs T som funktion av φ_0 i en graf (plotbild 1).

En ofta använd approximation av T är svängningstiden för små svängningar:

$$\tilde{T} = 2\pi\sqrt{\frac{L}{g}}$$

Denna approximation är bra för små utslagsvinklar, men relativfelet ökar med ökande utslagsvinkel. Plotta $\tilde{T}$ -värdet i samma graf som ovan, dvs plotbild 1.

Gör även en graf som visar det procentuella relativfelet i $\tilde{T}$, dvs $100 * (T - \tilde{T})/T$ som funktion av utslagsvinkeln då $5 \leq \varphi_0 \leq 90$ grader, plotbild 2.

2. Begynnelsevärdesproblem. Simulering av en pendelrörelse

I mekanik får man lära sig att rörelsen hos en pendel beskrivs av Newtons kraftekvation:

$$mL \frac{d^2\varphi}{dt^2} + mg \sin(\varphi) = 0$$

I ovanstående andra ordningens icke-linjära differentialekvation är m är massan, L är pendelns längd och g är tyngdaccelerationen.

Om pendeln startar från en given utslagsvinkel φ_0 utan begynnelsehastighet, ges begynnelsevillkoren av

$$\varphi(0) = \varphi_0, \quad \frac{d\varphi}{dt}(0) = 0$$

a) Skriv om systemet på vektorform, dvs

$$\frac{d\mathbf{u}}{dt} = \mathbf{f}(\mathbf{u})$$

Skriv den MATLAB-funktion som svarar mot högerledet.

b) Simulera pendelns rörelse genom att anropa MATLAB-funktionen `ode45`. Välj själv ett lämpligt tidsintervall och några startvinklar φ_0 och skriv ut en graf över vinkeln φ som funktion av tiden t . Låt parametrarna i problemet ha följande värden: $L = 1$, $m = 1$, $g = 9.81$. Avläs i grafen svängningstiden T och jämför med det värde du får i a).

3. Randvärdesproblem.

Betrakta nu samma differentialekvation som i deluppgift 2, men med följande randvillkor:

$$\varphi(0) = \varphi_0, \quad \frac{d\varphi}{dt}(\tau) = 0$$

Detta beskriver en pendel som startar med startvinkeln φ_0 och som vänder vid tiden τ .

Detta är ett randvärdesproblem, där vi för givna värden på φ_0 och τ vill bestämma hur vinkeln φ varierar med tiden t på intervallet $0 \leq t \leq \tau$.

Dela in intervallet $[0, \tau]$ i N delintervall av längden h , så att $Nh = \tau$. Beteckna punkterna på intervallet med $t_0, t_1, \dots, t_N$. Lägg även till en "spökpunkt" t_{N+1} . Motsvarande approximativa värden på vinkeln kallar vi $\varphi_0, \varphi_1, \dots, \varphi_{N+1}$. Om andraderivatan approximeras med en differenskvot

$$\frac{d^2\varphi}{dt^2}(t_i) \approx \frac{\varphi_{i+1} - 2\varphi_i + \varphi_{i-1}}{h^2}, i = 1, 2, \dots, N$$

och första derivatan approximeras med

$$\frac{d\varphi}{dt}(t_N) \approx \frac{\varphi_{N+1} - \varphi_{N-1}}{2h}$$

erhålles ett icke-linjärt ekvationssystem i $N + 1$ obekanta:

$$L(\varphi_{i+1} - 2\varphi_i + \varphi_{i-1}) + h^2 g \sin(\varphi_i) = 0, i = 1, 2, \dots, N$$

$$\varphi_{N+1} - \varphi_{N-1} = 0$$

Ställ upp ekvationssystemet så att Newtons metod kan användas för att lösa det. Låt parametrarna ha samma värden som i uppgift 2. Låt $\varphi_0 = \pi/6$ och $\tau = 1$. Vänsterledet i ekvationssystemet kommer att få strukturen:

$$A\varphi + \frac{h^2 g}{L} \sin(\varphi) + b = 0$$

där A är en tridiagonal matris, φ i detta fall är en kolumnvektor med vinkelvärdena och b en kolumnvektor med φ_0 som första element, resten av elementen är noll.

Kör programmet för 3 olika steglängder svarande mot $N = 10, 20, 40$. Hitta lämpligt startvärde, t ex genom att använda programmet i uppgift 2 på lämpligt

sätt. Plotta lösningen och beräkna speciellt värden på vinkelhastigheten då $t = 0$ (använd gärna en andra ordningens approximation, se EX1.3) och värdet på vinkeln då $t = \tau$. Extrapolera värdet på vinkeln vid tiden $t = 0.5$ och ange det.

Skriv en rapport om deluppgifterna 1 - 3 enligt anvisningar på hemsidan.

4. Kryptoforcering

Denna deluppgift behandlar hantering av text som data.

Kryptografi har blivit en del av vår vardag även om vi inte tänker så mycket på det. När du loggar in på din personliga banksida eller pratar i mobiltelefonen sker kommunikationen krypterat. När man använder kryptering konverterar man en klartext till en kryptotext med hjälp av en krypteringsmetod och vanligen dessutom en krypteringsnyckel. Att konvertera tillbaka kallas att dekryptera. Om man inte känner till krypteringsmetod eller nyckel måste man gissa för att återfinna klartexten. Att göra det systematiskt kallas att forcera kryptotexten. I denna laboration ska du skriva ett program som forcerar en krypterad text där vi vet krypteringsmetoden men själva måste hitta nyckeln och sedan dekryptera texten. Ditt program ska läsa och dekryptera en text på engelska som finns på fil. Det finns många olika algoritmer för kryptering men vi förutsätter att texten är krypterad med "caesarrullning" vilket innebär att varje bokstav har bytts ut mot en bokstav ett visst antal steg framåt i alfabetet. Nyckeln är antalet positioner man rullar. Med 2 positioners rullning blir "The zebra has stripes" krypterat till "Vjg bgdtc jcu uvtkrgr". Med vetskap om att "e" är den vanligaste bokstaven i engelsk text kan texten forceras med hjälp av ett frekvensdiagram. Om t ex bokstaven "g" är den mest frekventa i kryptotexten kan man gissa att rullningen är 2 steg.

Ditt program ska 1) läsa in den krypterade texten (inklusive blanktecken och radbytecken) från en fil till en vektor bestående av tecken. 2) Skriv även ut den krypterade texten på skärmen. 3) Därefter visas ett frekvensdiagram (använd t ex `pie` i MATLAB) över de 10 mest frekventa bokstäverna i den krypterade texten. Det blir enklare om du först gör om alla bokstäver till versaler. 4) Därefter väljer du antal rullningssteg och 5) skriver ut texten efter rullning. Ditt program bör lämna andra tecken än bokstäver oförändrade. När texten visar en vettig mening är rullningen korrekt. Programmet ska utföra alla momenten 1)-5) ovan.

När gruppen skrivit programmet och testat det på de två filer som finns på hemsidan, skicka programmet till er assistent för sluttest. Inled programmet med gruppens namn, samt personnummer. En trevlig bok om kryptering är Simon Singh, "Kodboken". I slutet av boken finns en dekrypteringstävling som var öppen för alla i hela världen att försöka knäcka. Först ut att lösa detta krypto var ett gäng Datalogi-doktorander från KTH.