Presentation in 2 parts:

Part 1: Calculus Made Easy

Part 2: Interactive Cryptography

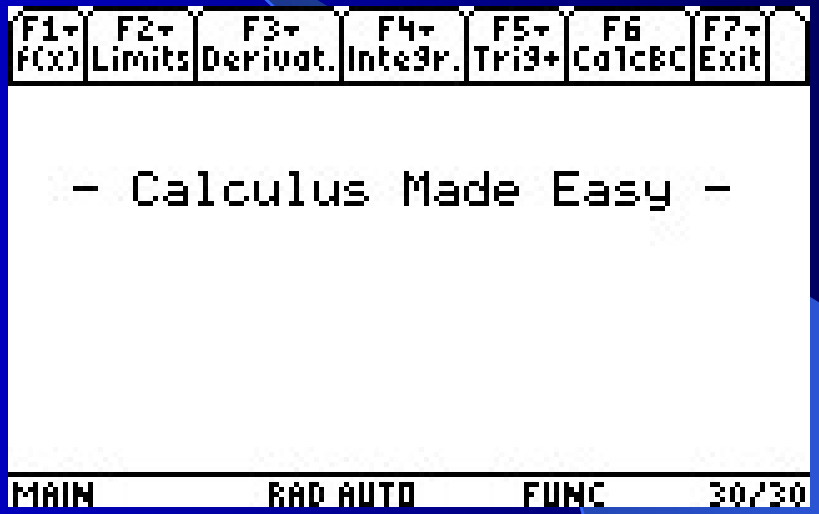
By Nils Hahnfeld

July 2004

Teaching Calculus I & II using Calculus Made Easy

(A teaching and learning tool for the TI89/Titanium, 92+, Voyage200)

CONTS

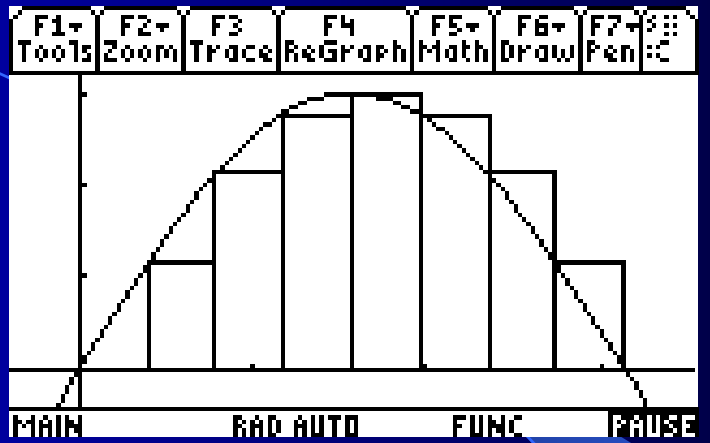


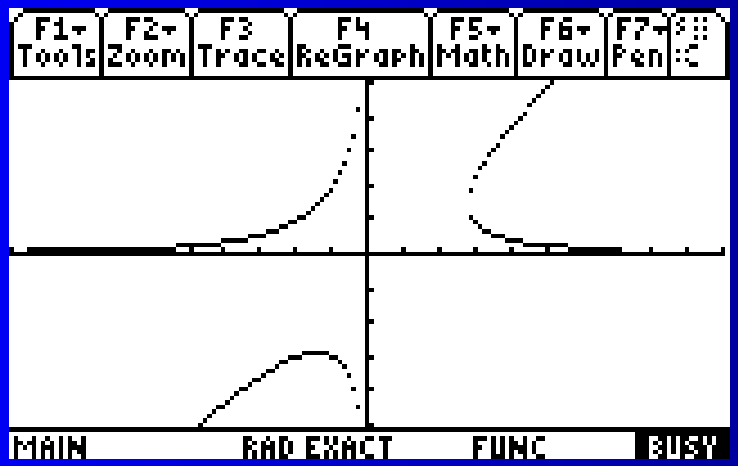
CONTS

Let's take a look at some examples ….

http://www.islands.vi/~shawn/ti_89.htm


F1▾ f(x)
F2▾ Limits
F3▾ Derivat.
F4▾ IntegProts
F5▾ Trig
F6 CalcBC
F7▾ Exit
1:Rules to Integrate
2:Find Antiderivat.
3:Definite (NetArea)
4:2 Equal Areas
5:TotalArea (∫|f|dx)
6:AverageValueTheor.
7:Area Approximation
8:Find Volume
TYPE OR USE ←→↑↓ + [ENTER] OR [ESC]

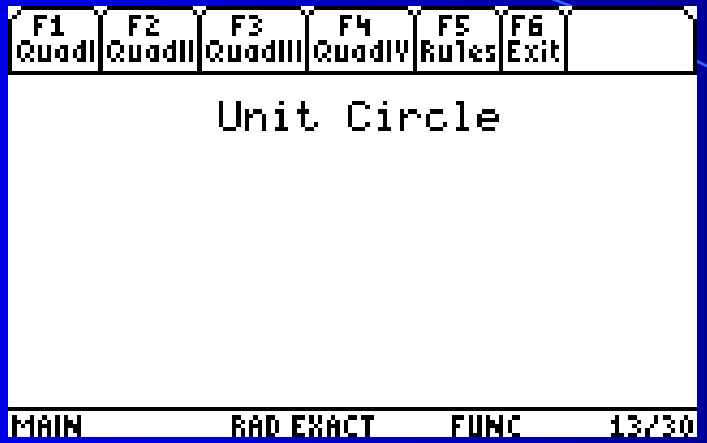

F1▾ Tools
F2▾ Zoom
F3 Trace
F4 ReGraph
F5▾ Math
F6▾ Draw
F7▾ Pen
MAIN
RAD AUTO
FUNC
PAUSE


F1▾ Tools
F2▾ Zoom
F3 Trace
F4 ReGraph
F5▾ Math
F6▾ Draw
F7▾ Pen
MAIN
RAD EXACT
FUNC
BUSY

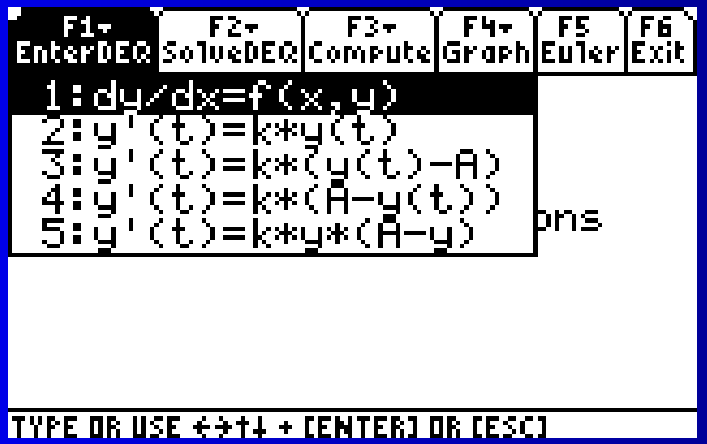

F1▾ EnterSeries
F2▾ Tests
F3▾ PowerSeries
F4▾ Taylor
F5 Exit
1:Test for Conv.
2:Geometric Series
3:Alternating Series
4:Integral Test
5:Comparison Test
6:Ratio Test
TYPE OR USE ←→↑↓ + [ENTER] OR [ESC]

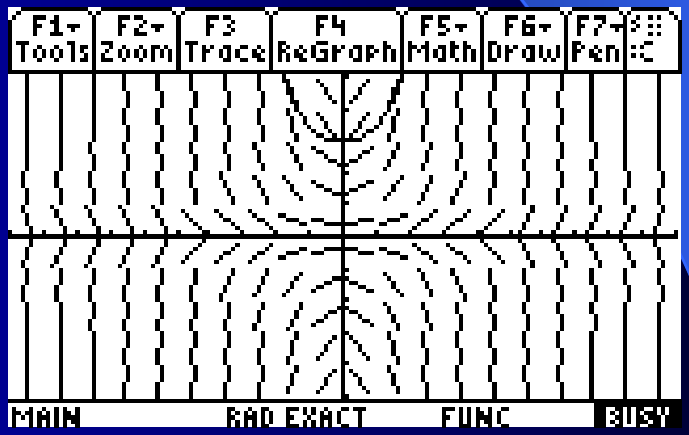
CONTS

CONTS


F1 Quadi
F2 QuadII
F3 QuadIII
F4 QuadIV
F5 Rules
F6 Exit
Unit Circle
MAIN
RAD EXACT
FUNC
13/30


Voyage200 PLT
TI89
TI92 Plus


F1 EnterDEQ
F2 SolveDEQ
F3 Compute
F4 Graph
F5 Euler
F6 Exit
1:dy/dx=f(x,y)
2:y'(t)=k*y(t)
3:y'(t)=k*(y(t)-A)
4:y'(t)=k*(A-y(t))
5:y'(t)=k*y*(A-y)
TYPE OR USE ↑↓ + [ENTER] OR [ESC]


F1 Tools
F2 Zoom
F3 Trace
F4 ReGraph
F5 Math
F6 Draw
F7 Pen
MAIN
RAD EXACT
FUNC
BUSY

CONTS

The Interactive Crypto-Tutorial

– a multimedia based online environment to learn cryptography at

http://www.antilles.k12.vi.us/math/cryptotut/home.htm

By Nils Hahnfeld

July 2004

CONTS

1) WHY Teaching Cryptography

Cryptography …

…is exciting to students.

… is crucial in today's life.

…allows discovery based learning and construction of own ciphers.

…triggers the discussion of current research problems.

CONTS

2) WHICH Ciphers shall be covered ?

UNIT 1:

Classical Cryptography -- Mono-alphabetic Ciphers

1.1 The Caesar Cipher

1.2 The Multiplication Cipher

1.3 The Linear Cipher

1.4 The Random Substitution Cipher

1.5 Reflection on Mono-alphabetic Ciphers

CONTS

UNIT 2: Classical Cryptography (II) -- Poly-alphabetical Ciphers

- **2.1 Vigenere Cipher**
- **2.2 The Homophonic Cipher**

Unit 3: Public-Key or Modern Cryptography

- **3.1 The RSA Cipher**
- **3.2 Digital Signatures with RSA**

Let's take a look …

3) Quantitative Analysis of Interactive Learning Environment:

Design of Statistical Analysis:

Post proficiency ratings of the tutorial vs classroom learners are compared using t-tests on the difference of the two means.

Cipher proficiencies after 10 day teaching trial.
Average rating of tutorial user group
Average rating of control group
p value resulting from t-test on difference of means

Caesar Cipher Proficiency

1.846
1.846
P=0.5

Multiplication Cipher Proficiency

2.692
2.769
p=0.403479

Linear Cipher?

2.692
2.769
p=0.427535

Mono-alphabetic Cipher?

2.462
2.616
p=0.355646

RSA Cipher?

3.538
3.616
p=0.437327

Table 1: Proficiency comparison of tutorial users vs. control group after 10 day teaching trial.

CONTS

Observation 1:

"Knowledge gain is independent of the learning environment."

Ratings
(range from 1=very good to 5 very bad)
Average rating of tutorial user group
P value resulting from T-test on difference of means with alternative mu=2 (good)
P value resulting from T-test on difference of means with alternative mu=3 (average)

CONTS

Q10: Questions posed

1.923
p<.37
p<.01

Q11:Explanations

1.923
p<.37
p<.01

Q12:Design

2.077
p<.64
p<.01

Q13:Navigation

1.846
p<.17
p<.01

Q14:Interactivity

1.769
p<.10
p<.01

Q15:Internet links

2
p<.5
p<.01

Q16:Multimedia tools

1.615

p<.05

p<.01

Q17:Length of text

2.538

p<.99

p<.03

Q18:Feedback

1.692

p<.06

p<.01

Q21:Overall rating

1.615

p<.01

p<.01

Q19: prior Knowledge

4.154

T-test on prior vs. post knowledge: p<.01

Q20: post Knowledge

2.308

Q24:Tutorial or textbook preference

1.08 (tutorial. I used +2,+1 for tutorial preference, -2, -1 for textbook preference)

T-test against alternative mu>0: p<.01

Table 2: Attribute ratings of tutorial users

CONTS

Observation 2:

"Interactivity level, the used multimedia tools and immediate feedback methods are effective enhancers resulting in a highly rated learning environment."

Observation 3:
"Lengthy texts and seemingly irrelevant Internet links are detractors."

Observation 4:
"Navigation, provided explanations and guiding questions are neutral attributes."

Observation 5:
"The students' knowledge gain by working the tutorial is significant."

Observation 6:
"Tutorial users prefer to study cryptography using a tutorial rather than using a textbook."

CONTS

THANK YOU FOR LISTENING.

Nils Hahnfeld
www.nilshahnfeld.com
nhahnfeld@hotmail.com