

# pen and pencil

Copyright © 2003 by Read Pen Inc., [www.readpen.ca](http://www.readpen.ca)  
MITACS Industrial Workshop, Ottawa, Ontario, Canada.  
Read Pen offers writing, editing, and training services to industry and government.

## card trick

requires 3 players:  
the mathematician, the assistant, and the person being tricked

A limited supply of free playing cards will be available from the Read Pen booth at the MITACS conference.

1. The person being tricked selects five cards and gives them to the assistant. Both may see the cards. The mathematician may not see the cards.
2. The assistant silently assigns numeric values to each of the five cards by representing Ace through King respectively with values 1 to 13.
3. The assistant silently selects a suit which appears twice among the five cards, and two cards of that suit, say  $i$  and  $j$ ,  $i > j$ .
4. The assistant chooses the first card as follows: choose  $j$  if  $i - j < 6$ , in which case  $k = i - j$ , otherwise, choose  $i$  if  $i - j > 6$ , in which case  $k = 13 - (i - j)$ . Note:  $1 \leq k \leq 6$ .
5. The assistant shows the first card to the mathematician.
6. The assistant shows the 2nd, 3rd, and 4th (but not the 5th) card to the mathematician in an order which corresponds to the desired number  $k$ . Let L=low, M=middle, H=high, and assign LMH=1, LHM=2, MLH=3, MHL=4, HLM=5, and HML=6. (permutation values). Note: Break ties uses the standard suit order: hearts, spades, clubs, diamonds.
7. The mathematician deduces the unknown 5th card, from the 4 known cards as follows: the suit is that of the first card shown. From the 2nd, 3rd, and 4th cards, the mathematician deduces the permutation value  $k$  and adds  $k$  to the value of the first card shown. (If this result is more than 13, then subtract 13.) The result is the value of the 5th card.

## quiz

for answers, visit

[http://www.cert.org/encyc\\_article/tocencyc.html](http://www.cert.org/encyc_article/tocencyc.html)

1. What do the letters in ARPANET stand for?
2. Who wrote The Cuckoo's Egg?
3. What is a packet sniffer?
4. What makes NFS (network filing system) vulnerable?
5. How is a checksum calculated?

## math challenge 1

If  $a, b$  are integers with the property that  $x = (a^2 + b^2) / (ab + 1)$  is an integer, show that  $x$  must be the square of an integer.

## links

math trading cards

<http://www.mathcards.com/index.jsp>

comp.security.unix and comp.security.misc frequently asked questions

<http://www.faqs.org/faqs/computer-security/most-common-qs/index.html>

the RSA factoring challenge

<http://www.rsasecurity.com/rsalabs/challenges/factoring/faq.html>

elliptic curves

<http://www.fermigier.com/fermigier/elliptic.html>

history of mathematics archive

University of St Andrew's, Scotland

<http://www-groups.dcs.st-and.ac.uk/~history/index.html>

the math geneology project

<http://genealogy.math.ndsu.nodak.edu/>

codes and ciphers in the second world war

<http://www.codesandciphers.org.uk/>

pioneer computer scientist Grace Murray Hopper (1906 - 1992)

<http://www.cs.yale.edu/homes/tap/Files/hopper-story.html>

CISSP practice exam

<http://www.cissp.com/exam/practice1.asp>

## quotes

"Machines take me by surprise with great frequency." - Turing

"Silence is better than unmeaning words." - Pythagoras

"There is no branch of mathematics which may not be applied to the real world." - Lobachevsky

"I have the result, but I do not yet know how to get it." - Gauss

"A mathematician is a device for turning coffee into theorems."  
- Erdos

### match each algorithm to its definition

1. Euclidean algorithm
  2. Polynomial-time algorithm
  3. Randomized algorithm
  4. Schoof's algorithm
  5. Symmetric algorithm
- A. Execution paths may differ each time this algorithm is invoked.
  - B. Used by two parties sharing the same key.
  - C. Used to count the number of points on an elliptic curve over a finite field.
  - D. Used for computing the greatest common divisor of two integers.
  - E. Worst-case running time function of this algorithm is of the form  $O(n^k)$ , where  $n$  is the input size and  $k$  is a constant.

### match each test to its aim

1. Miller's test
  2. Lucas-Lehmer test
  3. Primality test
  4. Pepin's test
- A. Determines whether a number is composite
  - B. Determines whether a given Fermat number is prime or composite
  - C. Determines whether a given number is prime
  - D. Determines whether a given Mersenne number is prime or composite

### read about algorithms and tests

1997, Menezes, A. J., van Oorshot, P., and Vanstone, S.  
*Handbook of Applied Cryptography*

1999, Coutinho, S. C.  
*The Mathematics of Ciphers : number theory and RSA cryptography*

Schoof, Rene. *Elliptic curves over finite fields and the computation of square roots mod p*. *Math. Comp.* 44 (1985), no. 170, 483-494.

### find-a-word puzzle

The leftover squares are highlighted and spell out Read Pen Inc.

P	R	O	T	O	C	O	L	E	N	C	R	Y	P	T	I	O	N
A	R	S	V	C	O	O	H	S	A	M	P	E	R	S	C	K	P
S	F	I	E	L	D	P	L	A	R	K	I	K	I	S	A	F	E
S	M	I	M	E	E	R	E	E	C	D	T	V	S	A	I	T	
W	R	E	E	E	W	E	A	K	H	O	O	T	A	L	P	P	N
O	I	S	R	U	L	E	N	I	P	L	R	F	C	C	I	S	E
R	T	L	S	U	I	D	N	A	I	B	O	B	Y	F	S	R	T
D	R	P	E	N	O	I	T	A	C	I	T	N	E	H	T	U	A
T	A	A	N	S	N	A	T	E	R	U	T	A	N	G	I	S	P
N	P	R	N	I	M	T	C	V	N	A	I	S	E	T	R	A	C
E	D	T	E	P	A	I	E	E	H	T	U	N	K	G	D	L	H
M	O	Y	E	C	L	M	Y	C	I	L	O	P	S	D	Q	L	A
E	O	R	K	A	C	E	C	I	B	U	C	I	I	S	N	A	N
L	R	O	T	C	E	V	N	L	E	A	R	N	R	N	C	W	N
E	W	O	R	C	S	E	L	A	M	A	G	R	O	R	R	E	E
S	S	E	R	D	D	A	I	M	O	N	O	L	O	G	Y	R	L
M	O	D	U	L	U	S	T	O	C	H	A	S	T	I	C	I	U
N	O	N	O	I	T	I	S	O	P	S	N	A	R	T	N	F	C

### on this day in history

On May 8, 1945 V-E Day; Germany signs unconditional surrender, WWII ends in Europe.

The following mathematicians were born on May 8:

- 1859 - Johan Ludwig William Valdemar Jensen
- 1905 - Karol Borsuk
- 1923 - Dionisio Gallarati

The following mathematicians died on May 8:

- 1960 - Henry Whitehead
- 1936 - Lorna Mary Swain
- 1951 - Gilbert Ames Bliss
- 1953 - Benjamin Fedorovich Kagan
- 1959 - John Henry Constantine Whitehead

Source for born and died on this date:  
University of St. Andrews archive

## math challenge 2

If  $N$  is a positive integer with  $2^k$  significant bits and exactly 2 of the bits are zero, prove that  $N$  cannot be a prime number.

One example of  $N$  is 11010111 (has  $2^3$  significant bits with exactly two zeroes, is equal to 215, which is not a prime number.)

## high school math problems

A positive integer  $n$ , when written in base  $b$ , has the form 211. When  $n$  is written in base  $b+2$ , it has the form 110. Determine  $n$  and  $b$  (in base 10).

In how many ways can the numbers 1, 2, 3, 4, 5, 6 be arranged as a sequence  $u, v, w, x, y, z$  such that  $u + x = v + y = w + z$ ?

Source:

*Santa Clara University High School Mathematics Contest*  
<http://math.scu.edu/activities/hscontest.html>

Related resources:

*Canadian Mathematics Competition*  
<http://www.cemc.uwaterloo.ca>

*Math Teacher Home Page*  
<http://westview.tdsb.on.ca/Mathematics/contests.html>

## classics from Ancient Greece

Submitted by XMLsec  
<http://www.xmlsec.com>

Prove for a right angle triangle that the hypotenuse squared is the sum of the squares of the two sides.

Prove that the square root of two is irrational.

## something for epsilons

<http://pbskids.org/cyberchase/games.html>

## guess the next number

Consider the following sequence:

1, 11, 21, 1211, 111221

What is the next number and why?

## meet today's featured experts

Read Pen Inc. features a versatile and dynamic talent pool. Today's featured experts specialize in technical communication:

Debbie Hackett, B. Math, B. Ed.  
Training and Facilitation Services  
hackett@readpen.ca  
<http://www.readpen.ca/pool.html#debbie>

Dr. Erma Petrova  
Technical Editor  
petrova@readpen.ca  
<http://www.readpen.ca/pool.html#erma>

Liz Waterfall  
Senior Business/Marketing Writer  
waterfall@readpen.ca  
<http://www.readpen.ca/pool.html#liz>

Janice Yerxa, B. Math, B. Ed.  
Instructional Design and E-Learning  
yerxa@readpen.ca  
<http://www.readpen.ca/pool.html#janice>

## about Read Pen Inc.

Read Pen Inc. is a service company, based in Ottawa, Canada.

Are you looking for opportunity?

Contact:  
jobs@readpen.ca  
<http://www.readpen.ca/careers.html>  
<http://www.readpen.ca/tips.html>

Are you looking for advice or assistance?

Contact:  
Tina Walsh, B. Math, B. A.  
Director of Professional Services  
walsh@readpen.ca  
<http://www.readpen.ca/contact.html>

