

# Use of Open-source Mathematics Software in degree level courses at Sheridan College Content delivery, assessment and evaluation

Victor Ralevich, Ph.D.  
Sheridan College, Oakville, Ontario, Canada

**THE ROLE OF TECHNOLOGY IN ASSESSMENT AND EVALUATION OF MATHEMATICS LEARNING  
FIELDS MATHEMATICS EDUCATION FORUM**

February 25, 2012, Fields Institute, 222 College Street, Toronto

## Introduction

---

Brief overview of mathematics software, with the emphasis on use of free and open-source software platform SAGE in some of the advanced courses taught at the Sheridan College, Ontario.

We use SAGE for:

Meaningful non-trivial exercises courses such as:

- Algorithms and data structures
- CPU architecture
- Introduction to Cryptology
- Advanced Cryptology, etc.

Bachelor of Applied Information Sciences (Information Systems Security) program includes in its curriculum:

- *Number theory* (divisibility, primality testing, Euler totient function, congruencies, simultaneous congruency equations, pseudoprimality testing on large numbers)
- *Abstract algebra* (groups, rings, integral domains, fields, finite, polynomials over finite fields)
- *Complexity theory*
- *Information theory*

Particularly sensitive and complex topics which cannot be covered properly without use of more mathematics software:

- Efficient implementation of multiple precision arithmetic computation with large integers, and in  $Z_m$
- Use in RSA, AES, ECC, ElGamal and other cryptographic algorithms
- Fast exponentiation of large integers (modulo  $n$ )
- Probabilistic primality testing (Miller-Rabin, etc)
- Discrete fast Fourier transforms

## What Math Software is Available and Useful?

---

### Magma

Software to Solve Computationally Hard Problems in Pure Mathematics

**Origins:** 1973 as Cayley, then renamed Magma in 1993. University setting – not a company. **Not for profit.**

**Mission:** “Develop computer techniques for solving symbolic problems in mathematics, with particular emphasis on the areas of algebra, number theory and geometry.”

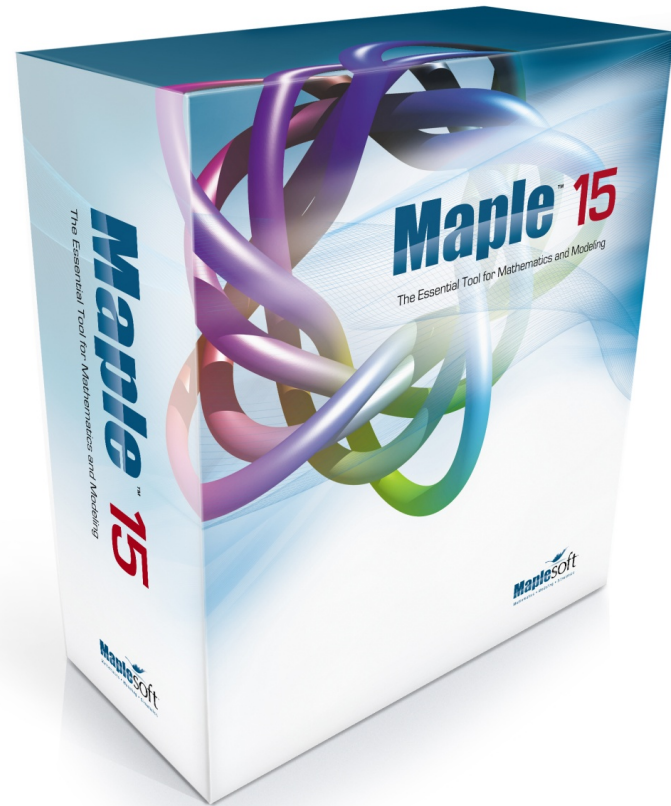
**Funding:** Australian Research Council and License Fees

**List price:** The educational price is \$1150 per copy.

## Maple

Maple is a general-purpose commercial computer algebra system. It was first developed in 1980 by the Symbolic Computation Group at the University of Waterloo in Waterloo, Ontario, Canada.

Since 1988, it has been developed and sold commercially by Waterloo Maple Inc. (also known as Maplesoft), a Canadian company also based in Waterloo, Ontario. The current major version is version 15 which was released in April 2011.



Maple 12 - C:\method of joints.mw - [Server 2]

File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help

Text Math Drawing Plot Animation

P Heading 1 Arial Black 18 B I U

### Static analysis of a truss: Method of joints

$$-F_{AB} - F_{AD} \cos(\theta) = 0 \quad (3.1)$$

$$-2000 \text{ [N]} + F_{AD} \sin(\theta) = 0 \quad (3.2)$$

$$-2000 \text{ [N]} + F_{AD} \sin(\theta) = 0$$

### Solve for unknown forces

$$\text{eval}\left(\text{eqlist}, \left[\sin(\theta) = \frac{8 \text{ [m]}}{10 \text{ [m]}}, \cos(\theta) = \frac{6 \text{ [m]}}{10 \text{ [m]}}\right]\right)$$

$$\left[60000 \text{ [N]} \text{ [m]} - 6 \text{ [m]} R_E = 0, R_{Cx} = 0, -3000 \text{ [N]} + R_E + R_{Cy} = 0, -F_{AB} - \frac{3}{5} F_{AD} = 0, -2000 \text{ [N]} + \frac{4}{5} F_{AD} = 0, F_{AB} - F_{BC} \right. \quad (4.1)$$

$$\left. - \frac{3}{5} F_{EB} + \frac{3}{5} F_{DB} = 0, -1000 \text{ [N]} + \frac{4}{5} F_{EB} + \frac{4}{5} F_{DB} = 0, R_{Cx} + F_{BC} + \frac{3}{5} F_{EC} = 0, R_{Cy} + \frac{4}{5} F_{EC} = 0, -F_{DE} - \frac{3}{5} F_{DB} + \frac{3}{5} F_{AD} = 0, -\frac{4}{5} F_{DB} - \frac{4}{5} F_{AD} = 0, F_{DE} + \frac{3}{5} F_{EB} - \frac{3}{5} F_{EC} = 0, R_E - \frac{4}{5} F_{EB} - \frac{4}{5} F_{EC} = 0\right]$$

$$\text{solve}$$

$$\{R_{Cy} = -7000 \text{ [N]}, F_{AB} = -1500 \text{ [N]}, F_{EB} = 3750 \text{ [N]}, F_{DE} = 3000 \text{ [N]}, F_{DB} = -2500 \text{ [N]}, R_E = 10000 \text{ [N]}, F_{EC} = 8750 \text{ [N]}, F_{AD} = 2500 \text{ [N]}, F_{BC} = -5250 \text{ [N]}, N = N, m = m, R_{Cx} = 0\} \quad (4.2)$$

$$3750. \text{ [N]} \xrightarrow{\text{replace units}} 843.0335366 \text{ [lbf]}$$

Memory: 0.43M Time: 0.06s Text Mode

Maple - Screenshot

# MathCad

Was the first to introduce live editing of typeset mathematical notation, combined with its automatic computations.

Mathcad includes some of the capabilities of a *computer algebra* system but is primarily oriented towards ease of use and *numerical engineering applications*.

The screenshot displays the Mathcad Prime 1.0 interface. The top menu bar includes Math, Input/Output, Functions, Matrices/Tables, Plots, Formatting, Calculation, Document, and Getting Started. A toolbar below the menu contains various function icons. The left sidebar shows a 'Functions' list with categories like Finance, Fourier Transform, Graphing, Hyperbolic, Interpolation and Prediction, Log and Exponential, Number Theory/Combinatorics, Piecewise Continuous, Probability Density, Probability Distribution, Random Numbers, Signal Processing, Solving, Sorting, Special, Statistics, String, and Trigonometric. The main workspace shows a worksheet titled 'cam\_worksheet\_rev2' with the following content:

The displacement of a follower for one cycle of cam's motion can be determined by the following logic:

$$s_i := \text{if}(0 \leq \phi_i, s_1, 0 \text{ m}) \quad s_i := \text{if}(\phi_r \leq \phi_i, s_1(\phi_i) \cdot s^2, s_i)$$
$$s_i := \text{if}(\phi_r + \phi_d \leq \phi_i, s_2, s_i) \quad s_i := \text{if}(\phi_r + \phi_d + \phi_f \leq \phi_i, 0 \text{ m}, s_i)$$

Figure 4. Displacement profile throughout one rotation

The pressure angle can be determined by following function:

$$f(\epsilon, s, v, R_0) := \text{atan}\left(\frac{\epsilon - v}{s + \sqrt{R_0^2 - \epsilon^2}}\right)$$

From equality  $f(0, s_i, v_i, r_i) = \epsilon_p$  one can find the formula:

$$r_i := \frac{-v_i \cdot s}{\tan(\theta_p) - s_i}$$

The values of pressure angle must be validated throughout a given rotation to make sure the restriction is not exceeded. This is checked for the base circle parameter, +/- 10%.

$$\theta_{01} := f(0 \text{ m}, s_i, v_i \cdot s, R_0) \quad \theta_{11} := f(0 \text{ m}, s_i, v_i \cdot s, 1.1 \cdot R_0) \quad \theta_{21} := f(0 \text{ m}, s_i, v_i \cdot \text{sec}, 0.9 \cdot R_0)$$

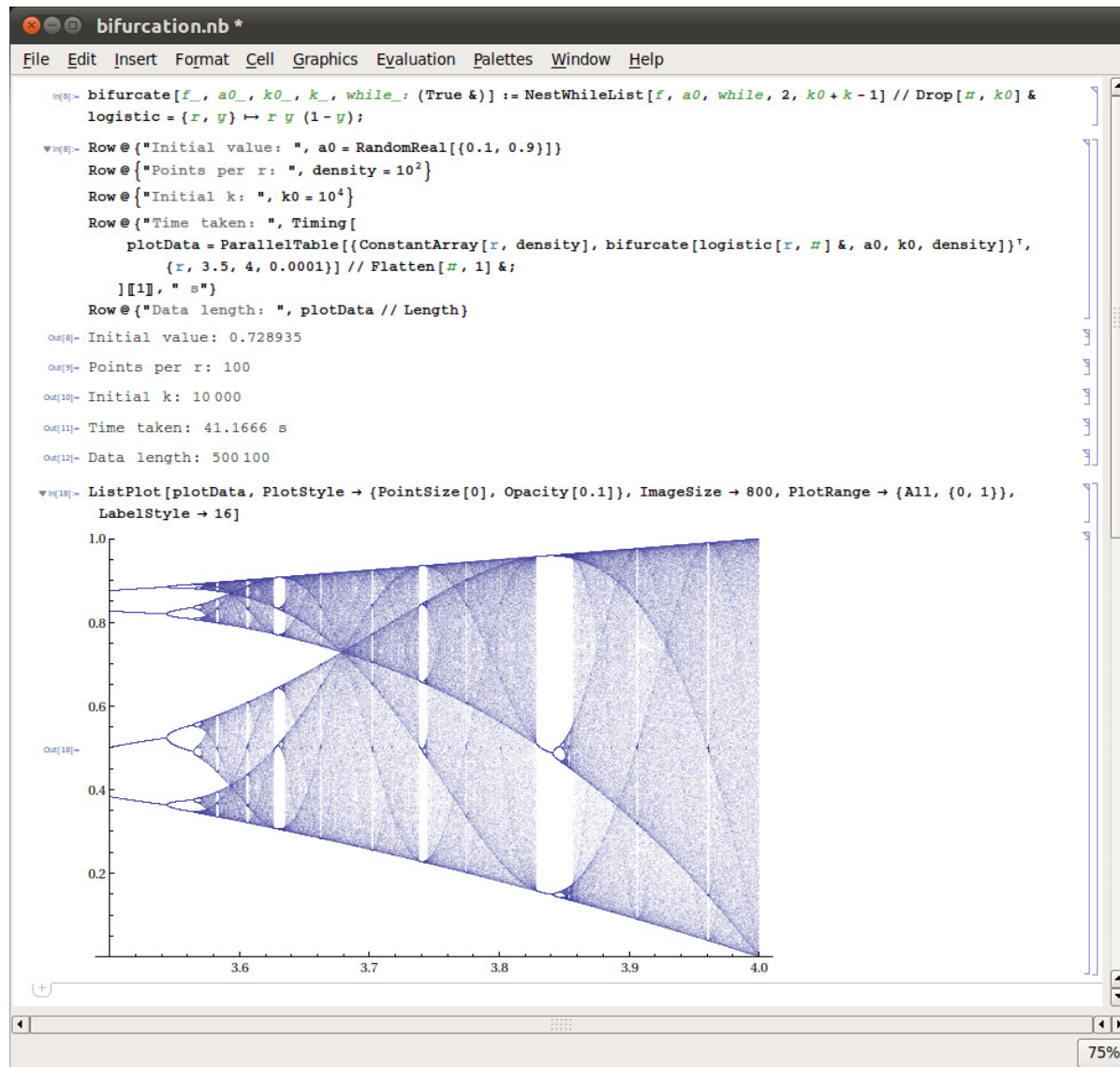
Figure 5. Validating pressure angles throughout one rotation of the cam

A tooltip for the 'atan(z)' function is visible, stating: 'Returns the angle (in radians) whose tangent is z. Principal value for complex z. Press F1 for help.'



## Mathematica

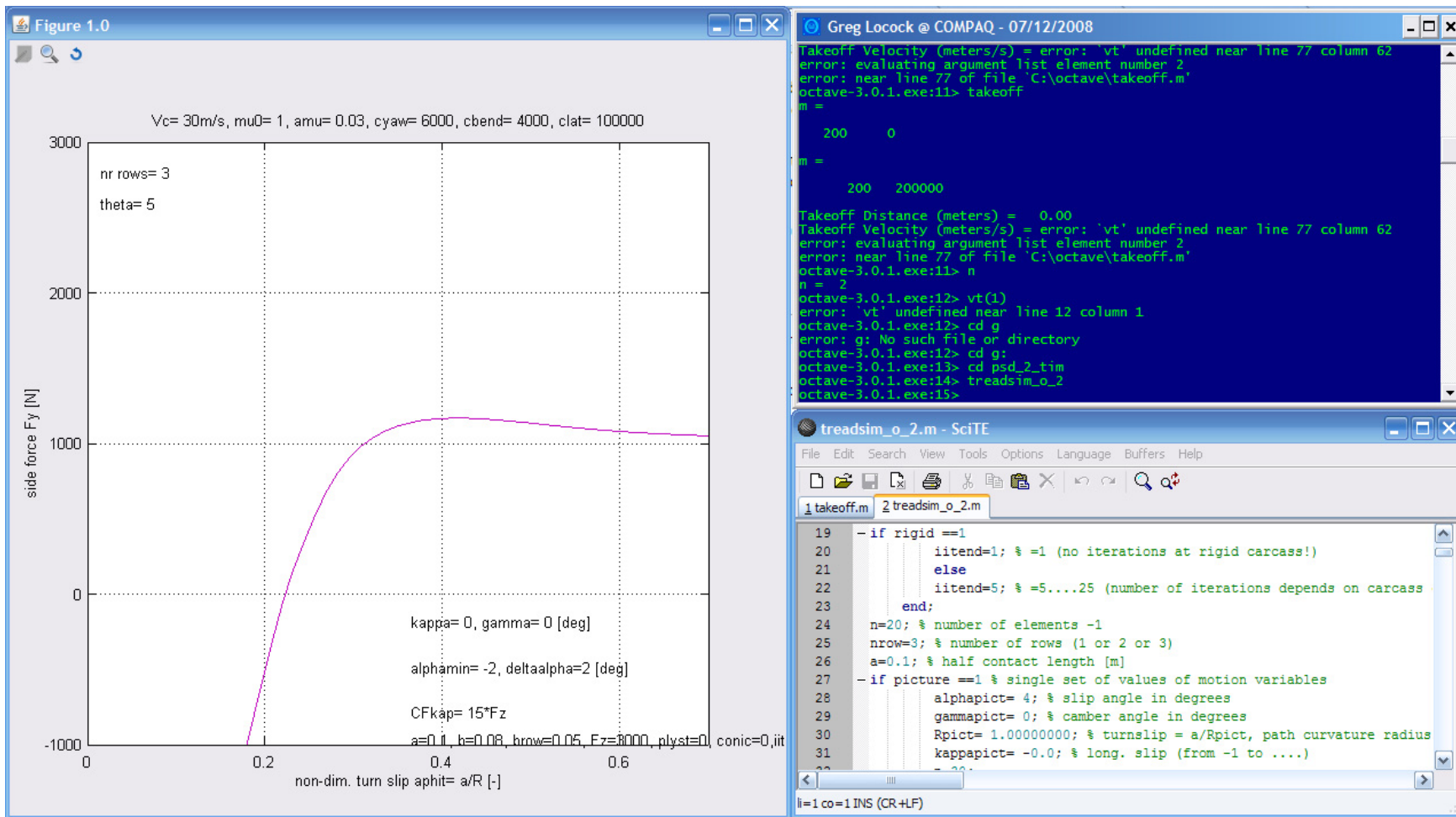
- Mathematica is a computational software program used in scientific, engineering, and mathematical fields and other areas of technical computing.
- It was conceived by Stephen Wolfram and is developed by Wolfram Research of Champaign, Illinois.
- List price: \$2,495/copy; \$1095/copy for professors; \$139.95/copy for students; \$1,995/copy for government employees.



Mathematica Screenshot

## GNU Octave

- Origins: Started in January 2005 by William Stein by combining together the open source programs PARI, Maxima, Python, Singular and GAP.
- Mission statement: “Create a viable open source free alternative to Magma, Maple, Mathematica, and MATLAB which uses a standard modern language.”
- List price: \$0
- Volunteers: About 50, with at least 20 regular contributors.
- Annual budget: Currently about \$50K.
- Estimated number of users: Between 200 and 1000.



Octave - Screenshot

## Sage

- **Sage** is an open source computer algebra system that supports teaching, study and research in mathematics.
- Its features cover many aspects of mathematics, including *algebra*, *combinatorics*, *numerical mathematics*, *number theory*, and *calculus*.
- It combines numerous open source packages and provides access to their functionalities via a common interface, namely, a *Python* based programming language supporting procedural, functional and object-oriented constructs..

- Sage can be used as a powerful desktop calculator, as a tool to help undergraduate students study mathematics, or as a programming environment for prototyping algorithms and research in algorithmic aspects of mathematics.
- Sage is available free of charge and can be downloaded from the following website:

<http://www.sagemath.org>

- The starter and leader of the Sage project, William Stein, is a mathematician at the University of Washington.

- Two modes of operation:
  - Downloadable install version for Linux or Oracle VM Virtualbox for MS Windows, or
  - Online command line or as Sage Notebook
- The default interface to Sage is command line based, but there is a graphical user interface to the software as well in the form of the Sage notebook.

### Untitled

last edited on April 11, 2011 05:45 PM by admin

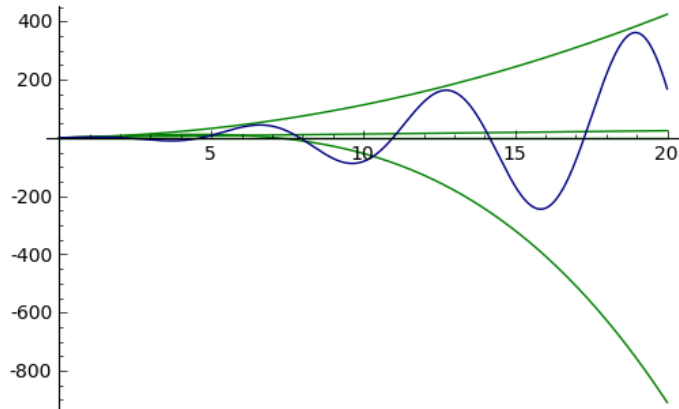
Save Save & quit Discard & quit

File... Action... Data... sage  Typeset

[Print](#) [Worksheet](#) [Edit](#) [Text](#) [Undo](#) [Share](#) [Publish](#)

```
var('x')
f = sin(x) + cos(x)*x^2 + sqrt(x)
fp = f.plot(xmin=0, xmax=20, rgbcolor=(0,0,.5))
tp = sum((f.taylor(x, 0, i).plot(xmin=0, xmax=20, rgbcolor=(0,.5,0)) for i in range(0, 4)))
(tp+fp).show()
```

[evaluate](#)



jsMath

Sage – Screenshot (graphics plotting)



## Use Sage to Solve Equations

last edited on April 11, 2011 05:45 PM by admin

Save Save & quit Discard & quit

File... Action... Data... sage  Typeset

Print Worksheet Edit Text Undo Share Publish

```
var('a b c d e f x y')
```

```
(a, b, c, d, e, f, x, y)
```

```
show(solve(a*x^2 + b*x + c == 0, x)[0])
```

$$x = -\frac{b + \sqrt{-4ac + b^2}}{2a}$$

```
show(solve(x^3 + a*x + b == 0, x)[0])
```

$$x = \frac{(-i\sqrt{3}+1)a}{6\left(\frac{1}{18}\sqrt{4a^3+27b^2}\sqrt{3}-\frac{1}{2}b\right)^{\frac{1}{3}}} - \frac{1}{2}(i\sqrt{3}+1)\left(\frac{1}{18}\sqrt{4a^3+27b^2}\sqrt{3}-\frac{1}{2}b\right)^{\frac{1}{3}}$$

```
solve([a*x + b*y == c, d*x + e*y == f], x, y)
```

```
[[x == -(b*f - c*e)/(a*e - b*d), y == (a*f - c*d)/(a*e - b*d)]]
```

[evaluate](#)

jsMath

Sage – Screenshot (typeset)

## Sage Features

- Sage is built out of nearly 100 open-source packages and features a unified interface.
- Sage can be used to study elementary and advanced, pure and applied mathematics.
- This includes a huge range of mathematics, including basic algebra, calculus, elementary to very advanced number theory, cryptography, numerical computation, commutative algebra, group theory, combinatorics, graph theory, exact linear algebra and much more.

## Using the Sage shell – Random Examples

---

```
sage: integral(x*sin(x^2), x)
-1/2*cos(x^2)
```

```
sage: integral(x/(x^2+1), x, 0, 1)
1/2*log(2)
```

---

```
sage: [sqrt(i) for i in srange(0,10,.1)]
```

---

```
sage: plot(sin,0,2)+plot(cos,0,2,rgbcolor='red')
```

## Elementary Number Theory Examples

---

```
sage: primes_first_n(20)
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,
41, 43, 47, 53, 59, 61,
67, 71]
```

```
sage: gcd(18, 27)
9
```

```
sage: mod(23, 5)
3
```

```
sage: euler_phi(20)
8
```

```
sage: factorial(50)
30414093201713378043612608166064768844377641
5689605120000000000000L
```

## Generating pair of keys for RSA

---

1. Choose two primes  $p$  and  $q$  and let  $n = pq$ .
2. Let  $e \in \mathbb{Z}, e > 0, \gcd(e, \varphi(n)) = 1$ .
3. Compute a values for  $d \in \mathbb{Z}, d > 0, de \equiv 1 \pmod{\varphi(n)}$ .
4. *Public key* is the pair  $(n, e)$  and *private key* is  $(p, q, d)$ .
5. For any two non-zero integer  $m < n$ , encrypt  $m$  using  $c \equiv m^e \pmod{n}$ .
6. Decrypt  $c$  using  $m \equiv c^d \pmod{n}$ .

## Use of Sage to generate RSA keys (example)

If  $p$  is prime and  $M_p = 2^p - 1$  is also prime, then  $M_p$  is called a Mersenne prime. For example, for primes  $p = 31$  and  $p = 61$ ,  $M_p$  are Mersenne primes.

```
sage: p = (2^31) - 1
```

```
sage: is_prime(p)
```

```
True
```

```
sage: q = (2^61) - 1
```

```
sage: is_prime(q)
```

```
True
```

```
sage: n = p * q ; n
```

```
4951760154835678088235319297
```

A word of warning: choice of  $p$  and  $q$  as Mersenne primes, and with so many digits far apart from each other, is a **very bad choice in terms of cryptographic security**.

```
sage: e = ZZ.random_element(euler_phi(n))
sage: while gcd(e, euler_phi(n)) != 1:
.....: e = ZZ.random_element(euler_phi(n))
.....:
sage: e
1850567623300615966303954877
sage: e < n
True
sage: bezout = xgcd(e, euler_phi(n)) ; bezout
(1, 4460824882019967172592779313, -
1667095708515377925087033035)
sage: d=Integer(mod(bezout[1],euler_phi(n))) ; d
4460824882019967172592779313
sage: mod(d * e, euler_phi(n))
```

In this example RSA public key is:

$$(n, e) = (4951760154835678088235319297, 1850567623300615966303954877)$$

and private key is:

$$(p, q, d) = (2147483647, 2305843009213693951, 4460824882019967172592779313)$$



## Example of Sage programming

---

Find two numbers, both greater than 100,000 that have a greatest common divisor of exactly 3.

```
sage: while (p < 100000): p = random_prime(1000000)
.....:
sage: p
586139
sage: q = 1
sage: while (q < 100000): q = random_prime(1000000)
.....:
sage: q
938591
sage: A = 3*p
sage: B = 3*q
sage: xgcd(A,B)
(3, -380028, 237323)
```

## How do we use Sage for evaluation?

---

1. In-class exercises
2. Homework and assignments
3. Group projects that involve use of Sage or similar tools

- Use of laptop during exams is not possible – we cannot isolate and control environment.
- Major concern may be – network communication among students in real-time.
- For the purpose of homework and projects, plagiarism among students is easy to recognize.
- Plagiarism accomplished by downloading solutions from the Web is virtually impossible to detect or prove.

Thank you!

Questions?

My contact information:

[victor.ralevich@sheridanc.on.ca](mailto:victor.ralevich@sheridanc.on.ca)