



蘇昱丞

2015.10.13



數學軟體簡介

SAGE



簡報大綱

- 安裝與使用
- 一般操作
- 橢圓曲線



安裝與使用

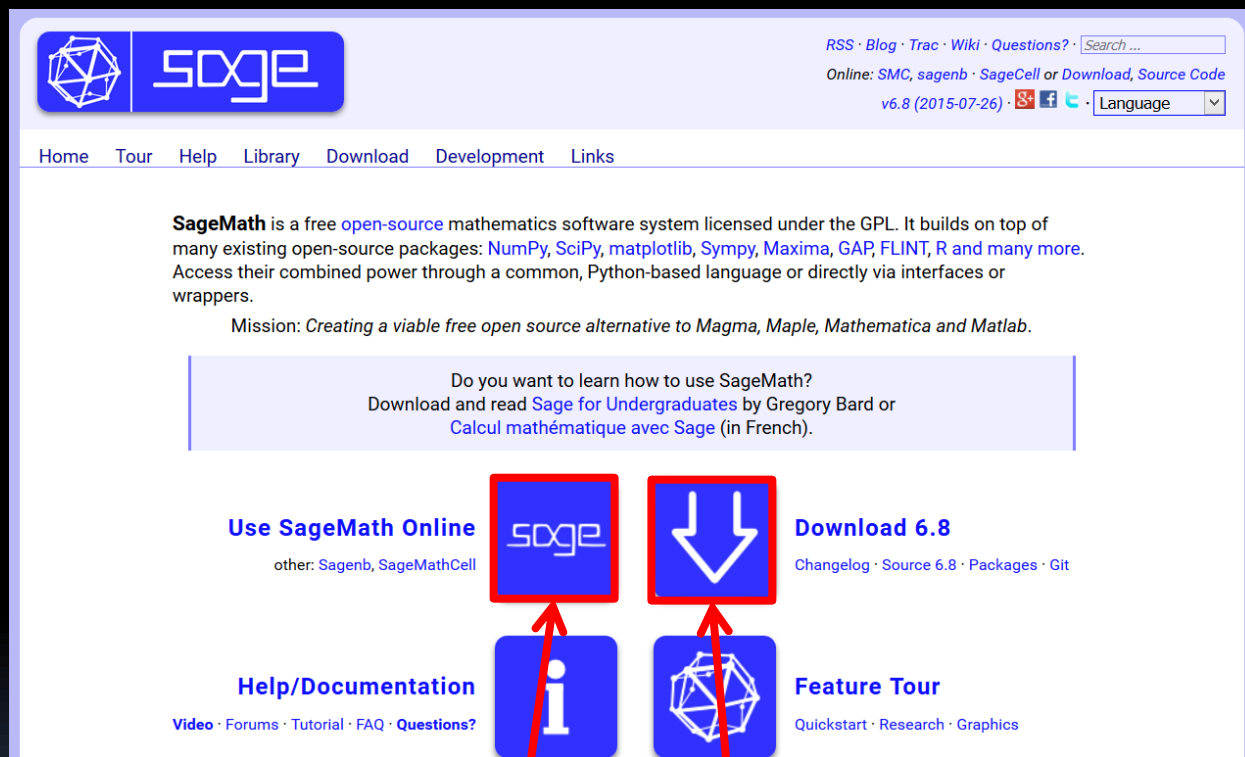
- 線上使用註冊
- 下載安裝

安裝與使用

- 首先連線到官方網站
 - <http://www.sagemath.org/>



安裝與使用



點選可以線上使用

點選可以下載

安裝與使用 – 線上使用

■ 註冊帳號

Create account (or [sign in](#))

✓ ☐ First, agree to the [Terms of Service](#)

Use your email address

Name

✓

Email

✓

Choose a password

✓

Create account for free

Or use

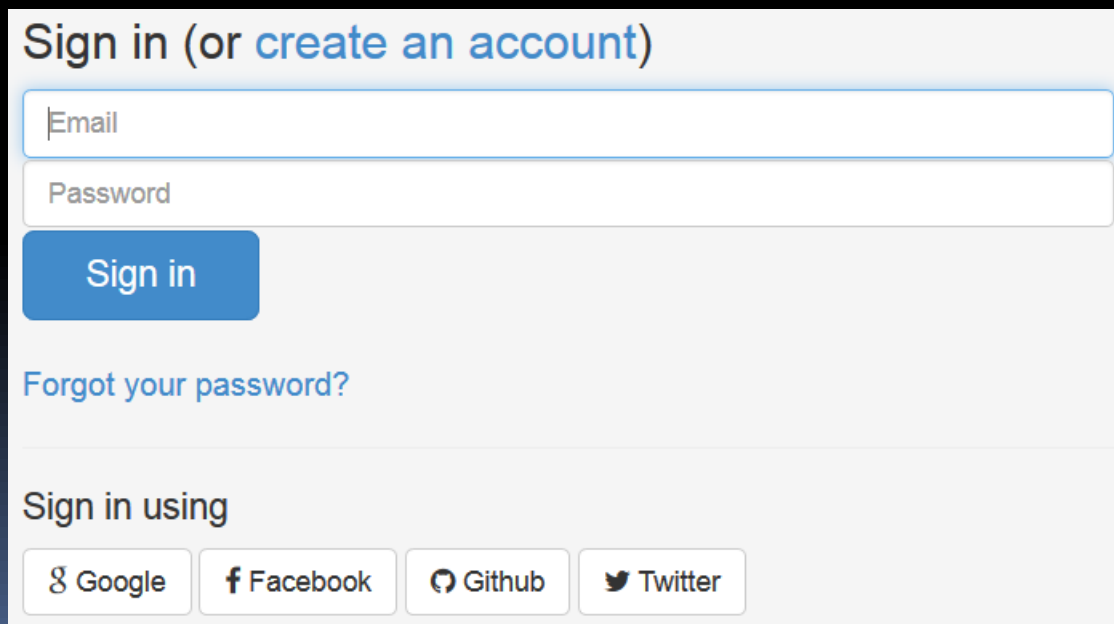
2018/12/24

安裝與使用 - 線上使用

■ 登入頁面

- 點選“sign in”
- 輸入帳號密碼

Create account (or [sign in](#))



Sign in (or [create an account](#))





Email

Password

Sign in

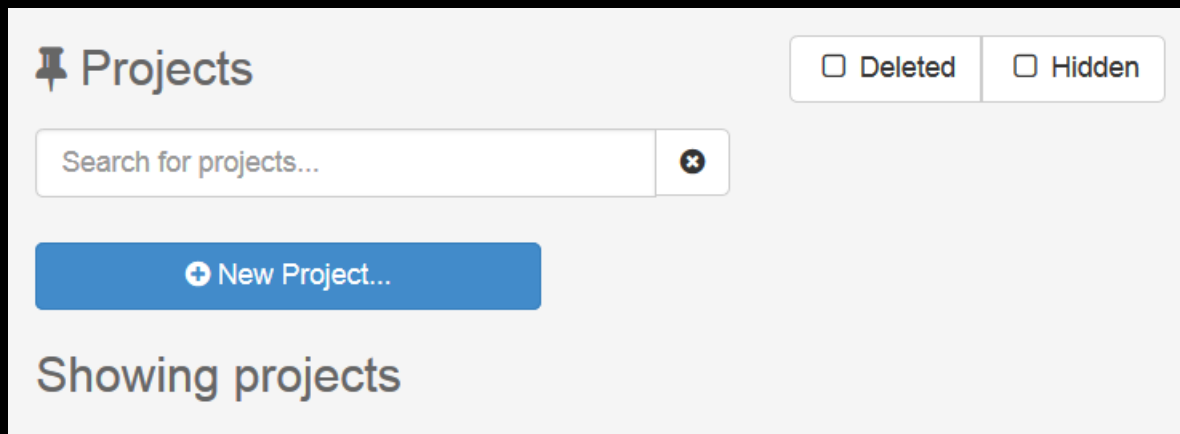
[Forgot your password?](#)

Sign in using

 Google  Facebook  Github  Twitter

安裝與使用 - 線上使用

- 登入後畫面



- 點選 New Projects 開始使用 (後述)

安裝與使用 - 下載


■ 下載頁面 - Windows

其他作業系統請按此

Download Binaries for Microsoft Windows

Click [here for other systems](#) or here to download source distribution.

Please select a download server close to your location below

Africa	 Polytechnic of Namibia
	 Tertiary Education Network, Johannesburg, South Africa
	 University of Cape Town, South Africa
	 University of the Free State, South Africa
America, North	 Go-Parts, Michigan, USA
	 MIT, Cambridge, MA, USA
	 Simon Fraser University, B.C., Canada

安裝與使用 - 下載

- 選擇伺服器後，會看到下列檔案

Filename	Other	Size	Date
sage-6.8.ova MD5: f6afebbaf82ec172a02c0e0ab3c33463	torrent	2173.58 MB	2015-07-31 23:01
sage-x.y.z.ova.txt MD5: ba10b2592d6c8232f1bb99f62aca8e4d		0.00 MB	2015-04-17 15:13
README-virtualbox.txt MD5: 162e147669c40a948735494f241e8125		0.00 MB	2015-04-17 15:13
README.txt MD5: 162e147669c40a948735494f241e8125		0.00 MB	2015-04-17 15:13

- 下載 sage-6.8.ova 檔案
 - 6.8 為版本號
 - ova 檔案為虛擬機器映像檔

安裝與使用 - 下載

- 需要安裝虛擬機器，點選前往 Oracle VirtualBox 官方網站

Usage

To run SageMath on Microsoft Windows you need the following:

1. [VirtualBox](#) for Windows
2. Download the "SageMath" .ova file from one of the Download Mirrors
3. Follow these [additional instructions](#).

The current VirtualBox solution provides you with an encapsulated and tested system. It allows to use the SageMath notebook in your web browser with no noticeable speed loss compared to a native Linux install.

安裝與使用 - 下載

■ Oracle VirtualBox 下載頁面



The screenshot shows the Oracle VirtualBox download page. On the left is a sidebar with navigation links: About, Screenshots, Downloads, Documentation, End-user docs, Technical docs, and Contribute. The main content area features the VirtualBox logo, the heading 'Download VirtualBox', and a paragraph stating that links to binaries and source code will be found there. Below this is a section for 'VirtualBox binaries' with a disclaimer about the license. A list of platform packages follows, including Windows, OS X, Linux, and Solaris hosts, each with a download link and architecture specification (x86/amd64).

VirtualBox

Download VirtualBox

Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox platform packages.** The binaries are released under the terms of the GPL version 2.
 - VirtualBox 5.0.4 for Windows hosts → x86/amd64
 - VirtualBox 5.0.4 for OS X hosts → amd64
 - VirtualBox 5.0.4 for Linux hosts
 - VirtualBox 5.0.4 for Solaris hosts → amd64

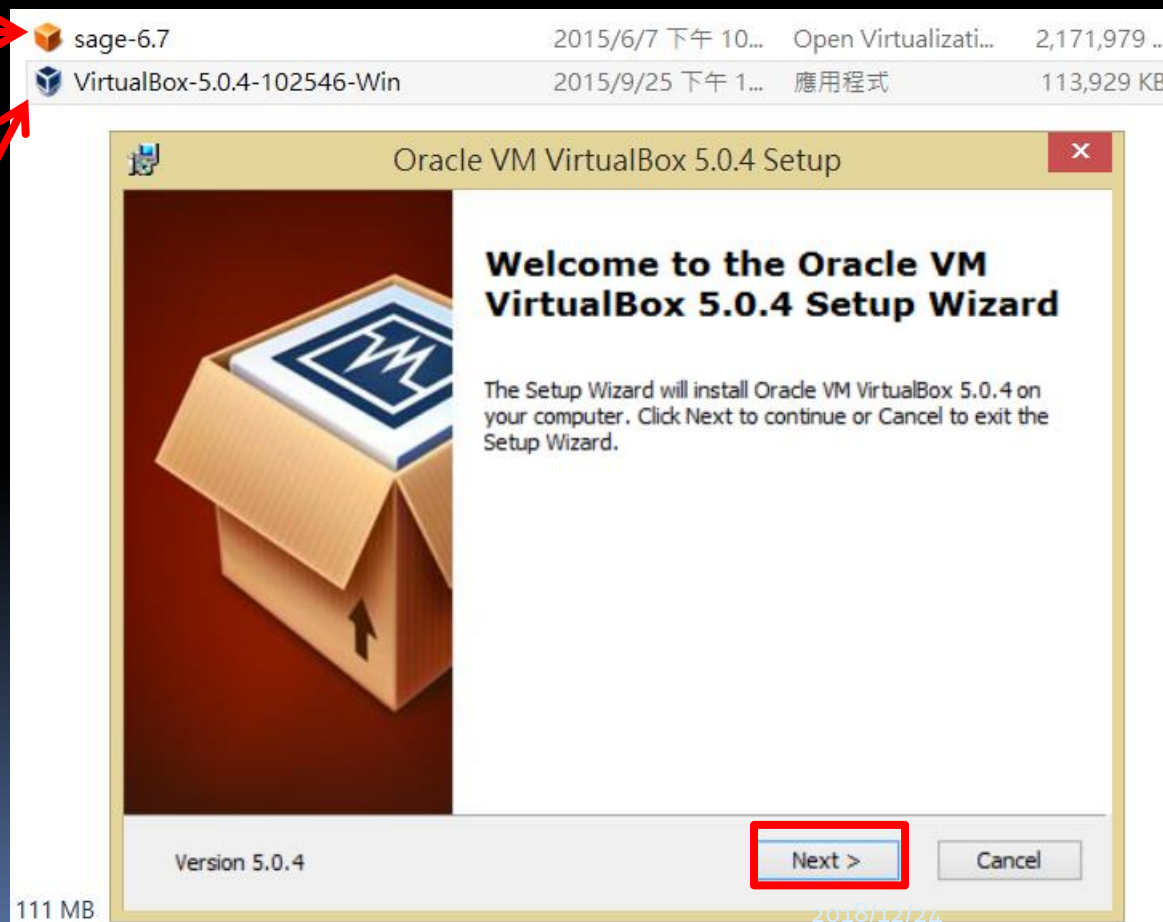
■ 選取適當作業系統並下載

安裝與使用 - 下載

- 下載完成後進行安裝

先放著

點兩下開始安裝



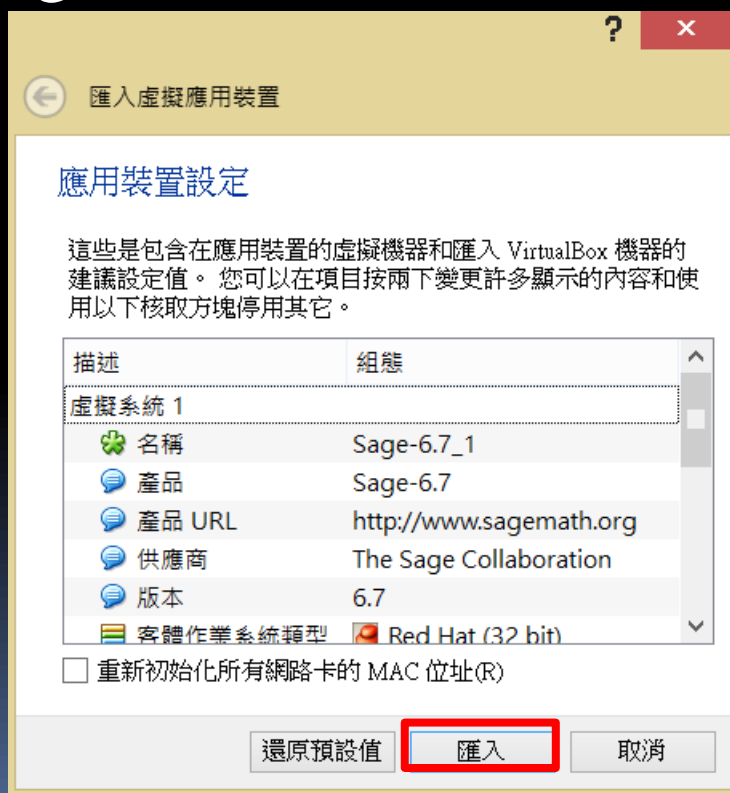
安裝與使用 - 下載

- Next 到底
 - 會警告暫時切斷網路連線 (不要理他)



安裝與使用 - 下載

- Oracle VirtualBox 安裝完成後，找到一開始下載的 sage-6.8.ova，點兩下打開，匯入

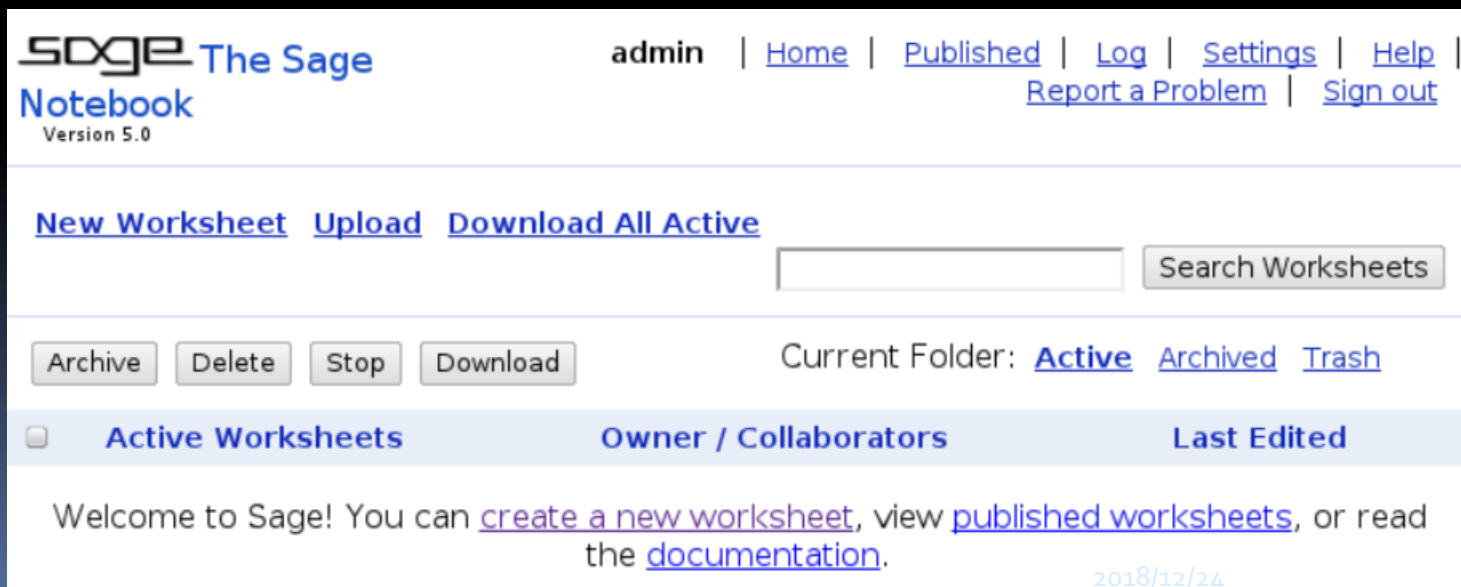


安裝與使用 - 下載

- 匯入後選擇啟動



- 會開啟另一個視窗，等一陣子





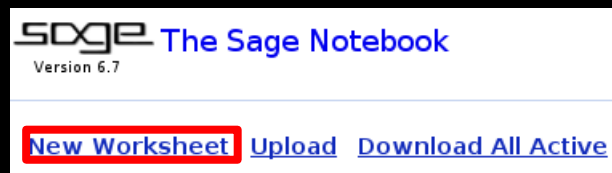
一般操作

- 建立 Worksheet
- 資料型態
- 基本指令

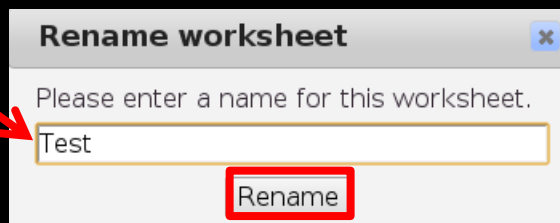
一般操作 - 單機建立 Worksheet

■ 單機使用

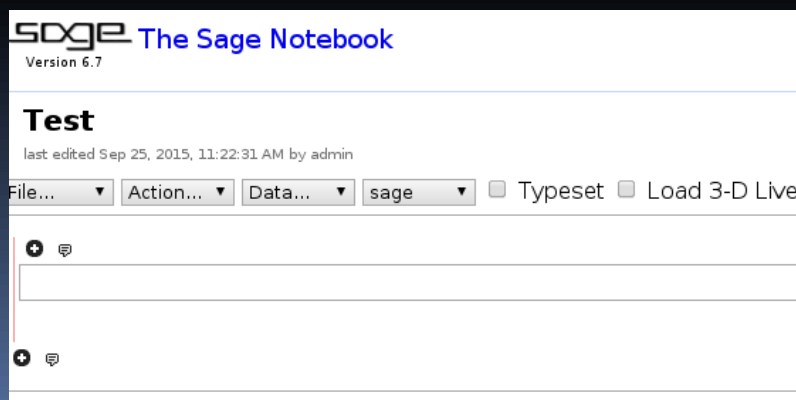
□ New Worksheet



□ 取名字

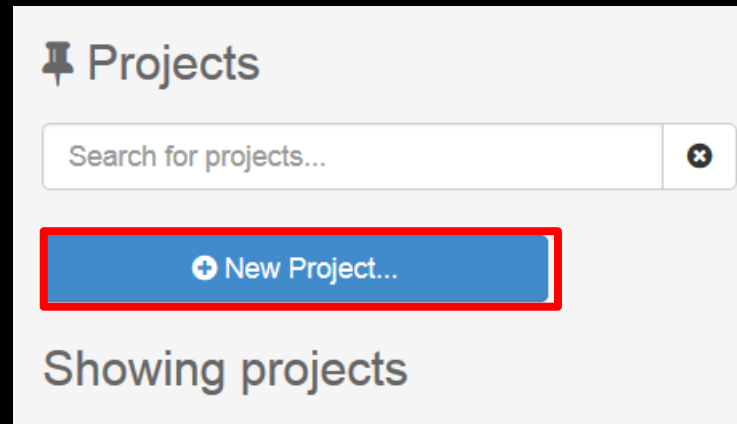


□ 開始程式寫作 (指令後述)

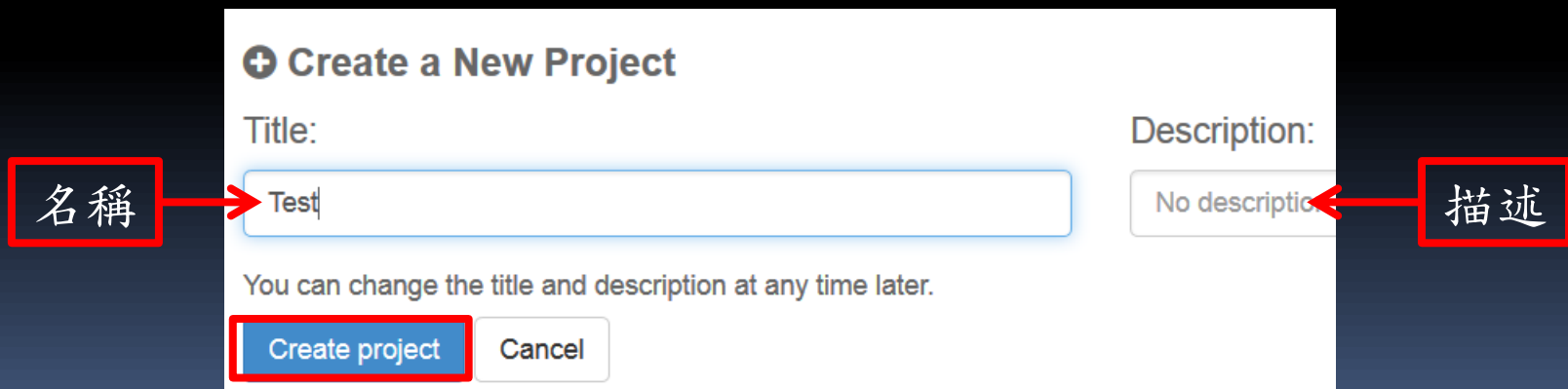


一般操作 - 線上建立 Worksheet

- 線上使用
 - New Project

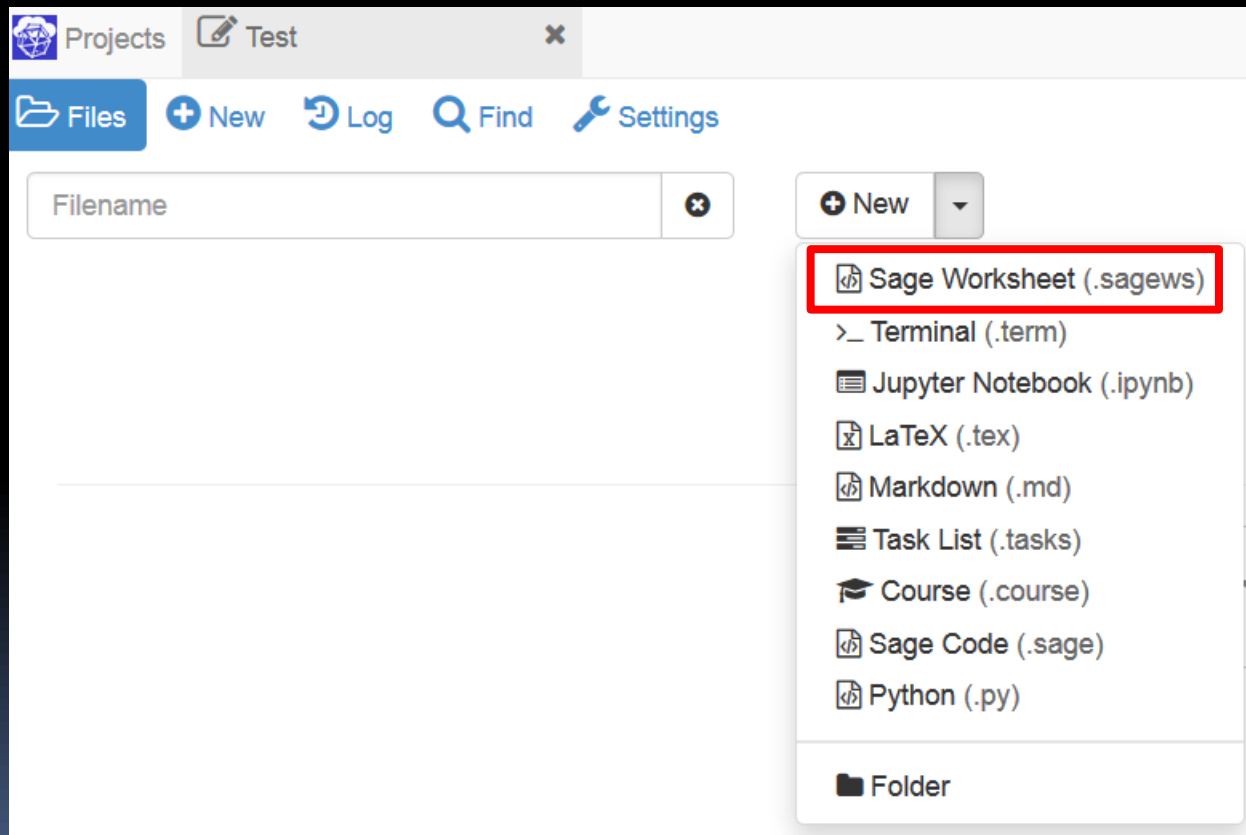


- 輸入名稱、描述

A screenshot of a 'Create a New Project' dialog box. It has a title bar with a plus icon and the text 'Create a New Project'. Below the title bar are two input fields: 'Title:' and 'Description:'. The 'Title:' field contains the text 'Test'. The 'Description:' field contains the text 'No description'. Below these fields is a line of text: 'You can change the title and description at any time later.' At the bottom are two buttons: 'Create project' and 'Cancel'. A red box labeled '名稱' (Name) with an arrow points to the 'Title:' field. Another red box labeled '描述' (Description) with an arrow points to the 'Description:' field.

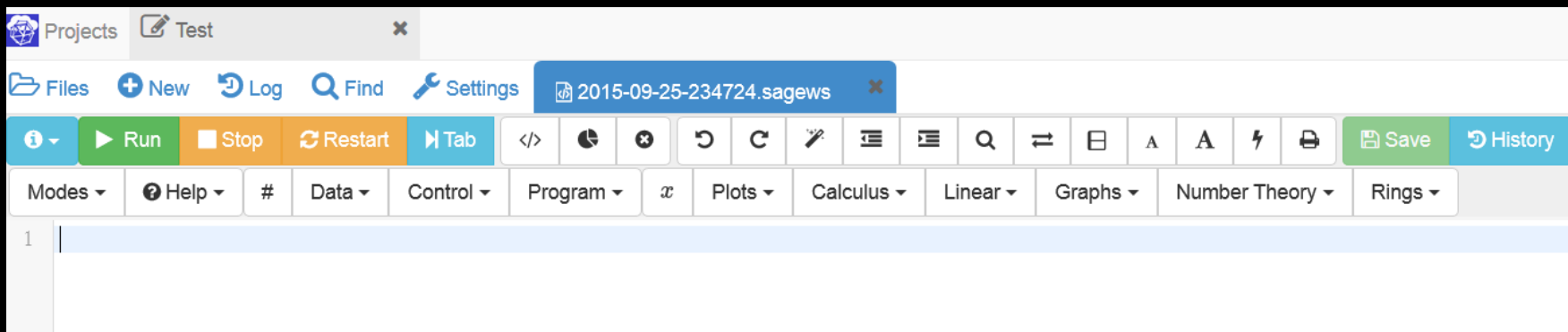
一般操作 - 線上建立 Worksheet

- 從下拉式選單選取 Sage Worksheet



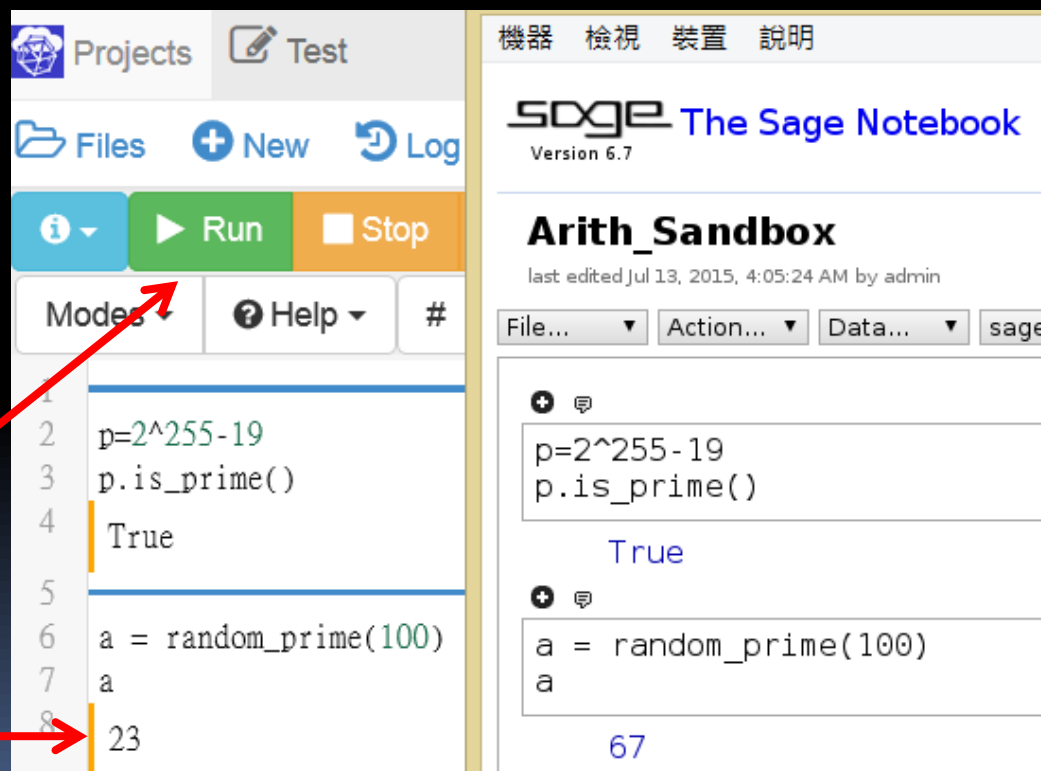
一般操作 - 線上建立 Worksheet

- 開始程式寫作 (指令後述)



一般操作 - 基本指令

- 由於是否上線無關程式，以下僅以單機版截圖說明
- 換行使用 Enter 鍵
- 執程式用 Shift + Enter 或按 Run



一般操作 - 整數

- 最簡單的資料型態為整數，可以直接進行四則運算

- 整數
- 有理數
- 實數

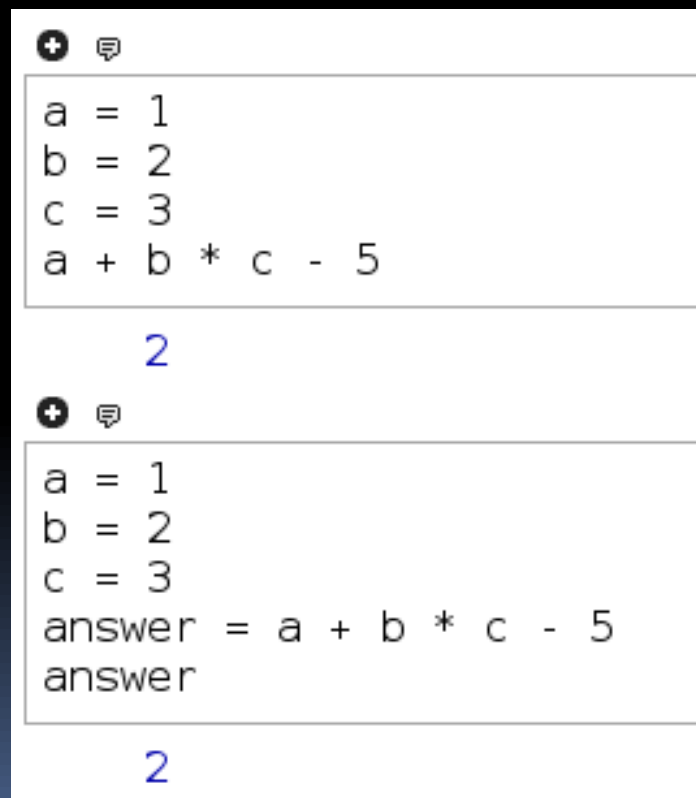
```
print 1/2
print 0.75
print 3 + 1/2
print 1/2 + 0.75
```

1/2
0.7500000000000000
7/2
1.2500000000000000

```
1 + 2
3
2 - 1
1
2 * 3
6
9 / 3
3
9 % 5
4
```

一般操作 - 整數

- 也可以使用變數 (variables) 進行運算



The image shows two screenshots of a code editor, likely from a presentation. Each screenshot has a header with a plus icon and a speech bubble icon. The first screenshot shows the following code: `a = 1`, `b = 2`, `c = 3`, and `a + b * c - 5`. Below the code, the number `2` is displayed in blue. The second screenshot shows the following code: `a = 1`, `b = 2`, `c = 3`, `answer = a + b * c - 5`, and `answer`. Below the code, the number `2` is also displayed in blue.

```
+ ⓘ  
a = 1  
b = 2  
c = 3  
a + b * c - 5  
  
2  
  
+ ⓘ  
a = 1  
b = 2  
c = 3  
answer = a + b * c - 5  
answer  
  
2
```


一般操作 - 整數

- 特別要注意的是，Sage 只會顯示最後一行的結果
 - 使用 print 指令

```
+ ⓘ  
a = 2; b = 3; c = 4  
a  
b  
c
```

4

```
+ ⓘ  
a = 2; b = 3; c = 4  
print a  
print b  
print c
```

2
3
4

- 可 print 多個值

```
+ ⓘ  
a = 2; b = 3; c = 4  
print a, b, c
```

2 3 4

一般操作 - 字串

- 另一種資料型態為字串
 - 需用單引號或雙引號標註
 - 也可以設變數



```
msg = "Hello, I am a string."  
print msg
```

```
Hello, I am a string.
```

一般操作 - 表單與向量

- 表單 (list) 以中括號表示
 - 起始為第 0 位置
 - 可修改內容
 - 可以增刪

```
+ ⓘ  
x = [1,2]; y = [3,4]  
x + y  
  
[1, 2, 3, 4]
```

```
+ ⓘ  
x = [1,3,5,7]  
print x  
print x[0]  
print x[3]  
x[3] = 100  
print x  
  
[1, 3, 5, 7]  
1  
7  
[1, 3, 5, 100]
```

一般操作 - 表單與向量

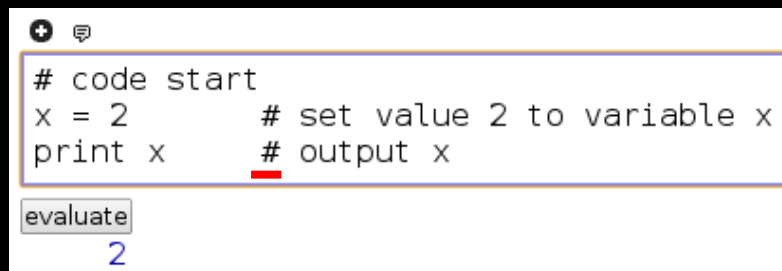
- 向量 (tuple) 和表單相似
 - 以小括號表示
 - 不可改變內容

```
+  ☰  
x = (1,3,5,7)  
print x  
print x[0]  
print x[3]  
  
(1, 3, 5, 7)  
1  
7
```

一般操作 - 註解

- 為使程式好讀，或寫作時提醒自己，通常會使用註記

- 以井字號起頭

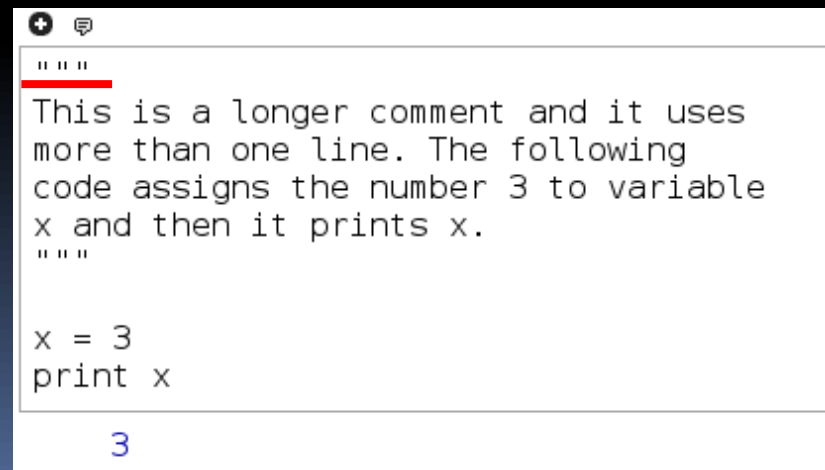


```
# code start
x = 2      # set value 2 to variable x
print x    # output x
```

evaluate

2

- 或以三個「'''」區隔開



```
'''
This is a longer comment and it uses
more than one line. The following
code assigns the number 3 to variable
x and then it prints x.
'''

x = 3
print x
```

3

一般操作 - 條件運算子


Operator	Description
<code>x == y</code>	Returns True if the two objects are equal and False if they are not equal. Notice that <code>==</code> performs a comparison and not an assignment like <code>=</code> does.
<code>x <> y</code>	Returns True if the objects are not equal and False if they are equal.
<code>x != y</code>	Returns True if the objects are not equal and False if they are equal.
<code>x < y</code>	Returns True if the left object is less than the right object and False if the left object is not less than the right object.
<code>x <= y</code>	Returns True if the left object is less than or equal to the right object and False if the left object is not less than or equal to the right object.
<code>x > y</code>	Returns True if the left object is greater than the right object and False if the left object is not greater than the right object.
<code>x >= y</code>	Returns True if the left object is greater than or equal to the right object and False if the left object is not greater than or equal to the right object.

一般操作 - 條件運算子

- 利用 `print` 的特性，可以寫成敘述的樣子，方便閱讀

```
+ ⓘ  
x = 1; y = 2  
print x == y  
print x <= y  
  
False  
True
```

```
+ ⓘ  
x = 1; y = 2  
print x, "==", y, ":", x == y  
print x, "<=", y, ":", x <= y  
  
1 == 2 : False  
1 <= 2 : True
```



一般操作 - if

- 文法為在 if 後加上判斷式，並以冒號結尾
 - if 指令中，所有敘述應在左方加上空白或 tab
 - 敘述應對齊

```
x = 6
if x > 5:
    print x
    print "Greater"
print "This program ends."
```

6
Greater
This program ends.

```
x = 2
if x > 5:
    print x
    print "Greater"
print "This program ends."
```

This program ends.

一般操作 - if, elif, else

- 仿照 if 的文法，可以依序判斷不同條件

- if <判斷式>:

.....

elif <判斷式>:

.....

else <判斷式>:

.....

```
x = -5

if x < 0:
    print x, "is negative."
elif (x % 2) == 0:
    print x, "is even."
else:
    print x, "is odd."

-5 is negative.
```

```
x = 1016842460

if x < 0:
    print x, "is negative."
elif (x % 2) == 0:
    print x, "is even."
else:
    print x, "is odd."

1016842460 is even.
```


```
x = 17

if x < 0:
    print x, "is negative."
elif (x % 2) == 0:
    print x, "is even."
else:
    print x, "is odd."

17 is odd.
```

一般操作 - and, or, not

- 需要多於一個判斷式時，可以使用這些運算子

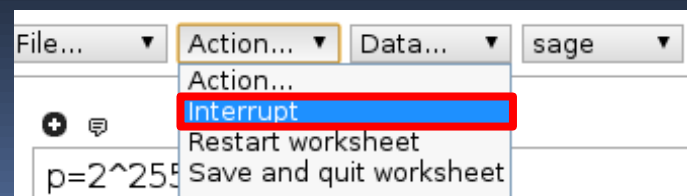
```
+   
a = 7; b = 9  
print (a < 5) and (b > 5)  
print (a < 5) or (b > 5)  
print not ((a < 5) or (b > 5))  
  
False  
True  
False
```

一般操作 - while 迴圈

- 文法與 if 類似
 - 會重複執行指令，直到後方判斷式為 False
 - 因此需要 $x = x + 1$ 避免無限迴圈
 - 若出現無限迴圈，或需要中斷程式時，線上版請按 Stop、單機版請選 Interrupt

```
x = 1
while x <= 10:
    print x
    x = x + 1
```

1
2
3
4
5
6
7
8
9
10



一般操作 - for 迴圈

- 文法為 for <目標> in <物件>:
 - 通常目標是變數、物件是表單
 - 敘述也要對齊並空格

```
+ ⓘ  
for x in [50,51,52,53,54,55,56,57,58,59]:  
    print x,  
  
50 51 52 53 54 55 56 57 58 59
```

```
+ ⓘ  
for i in range(50,60):  
    print i,  
  
50 51 52 53 54 55 56 57 58 59
```

一般操作 - 自訂函數

- `def <函數名>(變數 1, 變數 2, ..., 變數 n):`
 <運算指令>
 ...
 `return <答案>`

```
+ [icon]  
def addnum(num1, num2):  
    answer = num1 + num2  
    return answer  
  
addnum(5, 9)  
  
14
```

一般操作 - 整合使用

- 尋找 53 是否在表單中

```
+ ⓘ  
x = [50,51,52,53,54,55,56,57,58,59]  
y = 0  
  
while y <= 9:  
    if x[y] == 53:  
        print "53 was found in the list at position", y  
        y = y + 1
```

53 was found in the list at position 3



橢圓曲線

- 定義橢圓曲線
- 點運算
- ECDLP

橢圓曲線 - 有限體

■ 呼叫函數

- `GF(order, name, modulus)`
- `FiniteField(order, name, modulus)`

- `order` 代表群的大小

```
+ ⓘ  
K = GF(97)  
K  
  
Finite Field of size 97
```

- 若 `order` 是質數次方，則須給定變數名稱 `name`，以及模多項式

```
+ ⓘ  
K = GF(97^2, 'x', modulus = x^2 + x + 5)  
t = K.gen()  
print t  
print t^2  
  
x  
96*x + 92
```


橢圓曲線 - 有限體

- 會自動偵測是否 irreducible

```
+ 
K = GF(97^2, 'x', modulus = x^2 + 96*x + 0)
t = K.gen()
print t
print t^2
```

Traceback (click to the left of this block for traceback)
...
ValueError: finite field modulus must be irreducible but it is not

- 若不指定多項式，則預設使用 Conway polynomial

```
+ 
K = GF(97^2, 'x')
t = K.gen()
print t
print t^2
```

x
x + 92

橢圓曲線 - 橢圓曲線

- 呼叫函數 `EllipticCurve(體, 係數)`
 - 若不給定體，則使用有理數體
 - 係數若給
 - 5 項，則使用 long Weierstrass equation
 - 2 項則用 short Weierstrass equation

```
K = GF(97)

E = EllipticCurve(K, [2,3,4,5,6])
print "E is an", E

F = EllipticCurve(K, [2,3])
print "F is an", F
```

E is an Elliptic Curve defined by $y^2 + 2xy + 4y = x^3 + 3x^2 + 5x + 6$ over Finite Field of size 97
F is an Elliptic Curve defined by $y^2 = x^3 + 2x + 3$ over Finite Field of size 97

橢圓曲線 - 曲線上的點

- 定義曲線後，點表示法為 $\langle \text{曲線名} \rangle (x \text{ 座標}, y \text{ 座標})$
- 也可輸入投影座標
- 在程式內部會轉換為投影座標
- 會自動檢查點是否符合方程式

```
K = GF(103)
E = EllipticCurve(K,[1,18])
P = E(33, 91)
Q = E(66, 79, 2)

print "P =",P
print "Q =",Q
```

P = (33 : 91 : 1)
Q = (33 : 91 : 1)

```
K = GF(103)
E = EllipticCurve(K,[1,18])
P = E(33,90)
P
```

Traceback (click to the left of this block for traceback)
...
TypeError: Coordinates [33, 90, 1] do not define a point on Elliptic Curve defined by $y^2 = x^3 + x + 18$ over Finite Field of size 103

橢圓曲線 - 曲線上的點

- 點運算可直接以符號運算取代

```
K = GF(103)
E = EllipticCurve(K,[1,18])
P = E(33,91)
Q = E(70,60)

print P
print Q
print P + Q
print 2*P
print 7*P
```

(33 : 91 : 1)
(70 : 60 : 1)
(8 : 69 : 1)
(87 : 52 : 1)
(93 : 55 : 1)

加法和倍數就直接打+, *

橢圓曲線 - order

- 由於 Sage 建立於 Python 之上，所有的物件都有「屬性」
- 以 `.order()` 呼叫物件 `order` 屬性

```
K = GF(103)
E = EllipticCurve(K, [1, 18])
P = E(33, 91)

print E.order()
print P.order()
```

114
19

橢圓曲線 - ECDLP

- 離散對數內建函數

`discrete_log(真數, 底數, 運算)`

```
K = GF(103)
E = EllipticCurve(K,[1,18])
print E

P = E(33, 91)
print "P =", P
print "the point P has order", P.order()

Q = 13*P
print "Q =", Q

print discrete_log(Q,P,operation = '+')
```

Elliptic Curve defined by $y^2 = x^3 + x + 18$ over Finite Field of size 103
P = (33 : 91 : 1)
the point P has order 19
Q = (81 : 67 : 1)
13

橢圓曲線 - 整合使用 1

- 以課本習題為例，欲計算 $[n]P$

(d) $E : Y^2 = X^3 + 1541X + 1335$, $p = 3221$, $P = (2898, 439)$, $n = 3211$.

```
+ ③
p = 3221                                # prime field size
a = 1541                                # curve coefficients
b = 1335

EC = EllipticCurve(GF(p),[a,b])          # elliptic curve
P = EC(2898,439)                         # base point
n = 3211                                 # scalar

print "The point P has order", P.order()
print "[n]P =", n*P
print "n =", n % P.order(), "mod (order of P)." # same result with
print (n % P.order())*P                   # doing modulus first

The point P has order 1621
[n]P = (243 : 1875 : 1)
n = 1590 mod (order of P).
(243 : 1875 : 1)
```

橢圓曲線 - 整合使用 2

- 以 NIST P-192 曲線為例
 - 首先定義橢圓曲線

```
p = 6277101735386680763835789423207666416083908700390324961279 # define prime p for finite field
print "p is a prime:", p.is_prime() # test p is a prime
print "p has", p.nbits(), "bits." # bit-length of p
print

K = GF(p) # define finite field

a = -3 # define coefficients of elliptic curve
b = 0x64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1 # using P-192 parameters
EC = EllipticCurve(K,[a,b]) # define elliptic curve
print EC

p is a prime: True
p has 192 bits.

Elliptic Curve defined by  $y^2 = x^3 + 6277101735386680763835789423207666416083908700390324961276x + 2455155546008943817740293915197451784769108058161191238065$  over Finite Field of size 6277101735386680763835789423207666416083908700390324961279
```


橢圓曲線 - 整合使用 2

□ 計算橢圓曲線群大小

```
+ [icon]
m = EC.order()                                     # compute group order (a few seconds)
n = 6277101735386680763835789423176059013767194773182842284081 # order given in the P-192 parameters

print m
print "n = m:", n==m
print "m is a prime:", m.is_prime()

6277101735386680763835789423176059013767194773182842284081
n = m: True
m is a prime: True
```

□ 群大小和有限體大小相當

```
+ [icon]
print hex(p)
print hex(m)

ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffff99def836146bc9b1b4d22831
```

橢圓曲線 - 整合使用 2

□ 定義 Base Point

```
+ ⓘ
GX = 0x188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012    # x coordinate
GY = 0x07192b95ffc8da78631011ed6b24cdd573f977a11e794811    # y coordinate

G = EC(GX, GY)                                                # define point

print "G =", G
print
print G.order()
print G.order() == EC.order()
```

```
G = (602046282375688656758213480587526111916698976636884684818 :
174050332293622031404857552280219410364023488927386650641 : 1)

6277101735386680763835789423176059013767194773182842284081
True
```

橢圓曲線 - 整合使用 2

□ 計算點的倍數



```
G2 = 2*G
G3 = 3*G

print G2
print
print G3
print
print "[3]G = [2]G + G:", G3 == G2+G
print
print n*G
```

```
(5369744403678710563432458361254544170966096384586764429448 :
5429234379789071039750654906915254128254326554272718558123 : 1)
```

```
(2915109630280678890720206779706963455590627465886103135194 :
2946626711558792003980654088990112021985937607003425539581 : 1)
```

```
[3]G = [2]G + G: True
```

```
(0 : 1 : 0)
```

橢圓曲線 - 整合使用 2

□ 生成公私鑰對



```
sk = ZZ.random_element(n)
pk = sk * G

print "The secret key is the number"
print sk
print
print "The public key is the point"
print pk
```

```
The secret key is the number
465790366131782197125051796373531468982091692821174298183
```

```
The public key is the point
(6035183668853086651266560506855783079390512754326832314175 :
897358300060317104093930130570028055498348673116644433880 : 1)
```

橢圓曲線 - 整合使用 2

- 直接解 ECDLP，當機！



```
print discrete_log(pk,G,operation = '+')
```

參考資料

- Sage 官方網站
<http://www.sagemath.org/>
- Oracle VirtualBox 官方網站
<https://www.virtualbox.org/wiki/Downloads>
- Ted Kosan, SAGE For Newbies.
https://www.uam.es/personal_pdi/ciencias/pangulo/laboratorio/sage_for_newbies_v1.23.pdf
- Sage 官方說明文件
http://doc.sagemath.org/html/en/reference/plane_curves/sage/schemes/elliptic_curves/ell_point.html