Fun with Certificates part II

a Deep Dive into Elliptic Curve Cryptography for all ages

Brian Epstein
(he/him/his)

Institute for Advanced Study

Computer Manager, Network and Security

Information Security Officer

bepstein@ias.edu - @epepepep

Topics

- Explain why ECC came about
- ECC deep dive
- Safe Curves and Trust
- Certs
- Demo

So I was browsing the Interwebs...

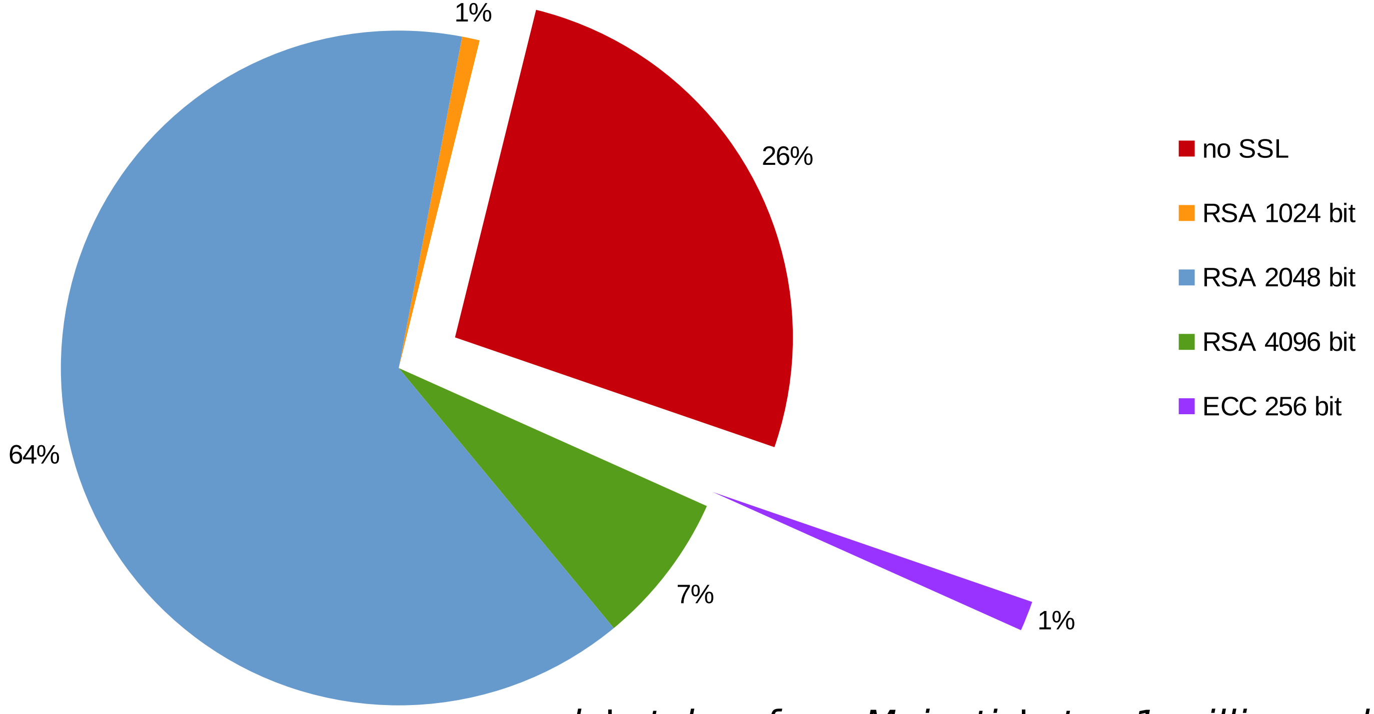
File Edit View Search Terminal Help

```
[2]epmacpro:~$ echo | openssl s_client -connect www.ias.edu:443 2>/dev/null | awk '/BEGIN/,/END/' | openssl x509
 -text -noout | awk '/Subject Public Key Info/,/Exponent/'
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ba:fb:a8:3d:9e:09:a4:97:9a:d6:e3:de:9c:86:
                    ef:91:69:95:4d:25:22:01:a1:f4:c9:a4:8c:2e:51:
                    b0:1c:1c:9f:8a:5a:9d:9a:85:25:05:b0:8e:c7:12:
                    7f:55:d7:e9:b1:06:7a:16:fe:88:05:9c:9c:53:3f:
                    85:c0:15:15:dd:2a:bb:f2:b7:13:34:5c:18:dd:ee:
                    a7:d0:11:2f:40:a5:ec:d2:3a:64:7c:4e:4f:fc:20:
                    b6:a3:dd:7c:7a:a5:8f:e5:9e:ad:27:42:ab:75:76:
                    1f:25:8c:3d:1b:0a:84:1c:1d:51:f5:fe:db:28:47:
                    5e:3e:1a:2e:d0:f5:56:10:ee:4e:26:08:05:9c:a1:
                    26:7f:b3:56:bd:f0:d3:87:0a:bf:7d:c5:5f:74:03:
                    2e:b2:75:28:f7:df:fb:64:2a:e1:76:34:15:d8:f9:
                    9c:ff:70:58:c2:e9:e1:ac:13:a1:d4:15:ae:10:a0:
                    05:bf:2d:69:b5:70:94:3b:b6:ab:b9:e9:b7:d2:39:
                    d6:66:c5:5d:62:90:f7:e4:9e:14:6f:d8:60:97:99:
                    3e:1e:f7:ac:0b:0c:d6:44:78:66:48:7f:23:01:1c:
                    76:04:8c:7d:86:a0:48:59:08:d1:ba:4e:48:6f:cf:
                    4d:36:55:ed:5c:80:38:48:2a:9c:cd:1a:6f:cc:49:
                    72:a3:0a:13:85:6e:75:a8:4b:3d:96:48:76:20:45:
                    17:30:dc:1a:6d:08:5f:0a:e6:4f:d6:cf:42:61:10:
                    92:d9:3a:12:73:85:62:75:a8:ae:3e:7f:d6:fd:3f:
                    00:11:2e:8a:5b:72:dc:cc:39:0e:8a:a3:6c:ac:66:
                    fd:d7:33:58:c5:34:3b:74:7b:12:f2:17:e6:d6:dc:
                    17:ad:2a:29:1f:59:a2:2e:6c:b4:28:29:b1:b3:f5:
                    1d:ee:b3:12:43:33:a7:bd:d3:79:d1:7b:f2:8a:45:
                    68:b4:07:86:35:83:d5:1a:45:16:c7:bd:60:ae:d9:
                    ab:60:17:aa:12:85:11:73:24:5b:87:6a:6c:a1:43:
                    39:60:99:a7:db:ba:98:f3:b2:83:6b:39:20:a6:e6:
                    ad:2c:95:66:82:50:22:b4:17:2e:78:34:66:21:db:
                    34:68:9b:92:fe:eb:12:42:46:72:38:ec:1e:fd:7e:
                    13:0e:58:d8:d6:11:f8:99:43:c6:5f:18:b3:5e:e2:
                    2a:45:37:12:20:3a:22:bb:da:d8:30:a5:a4:7c:85:
                    33:f0:30:40:7c:7d:e4:4e:12:09:58:03:6f:ba:1f:
                    f6:81:ad:7b:d0:52:29:d8:a8:d6:5f:66:34:58:eb:
                    33:0c:aa:d3:b4:27:41:c5:fb:62:ee:d0:7a:72:ab:
                    1c:38:b5
                Exponent: 65537 (0x10001)
[2]epmacpro:~$
```

File Edit View Search Terminal Help

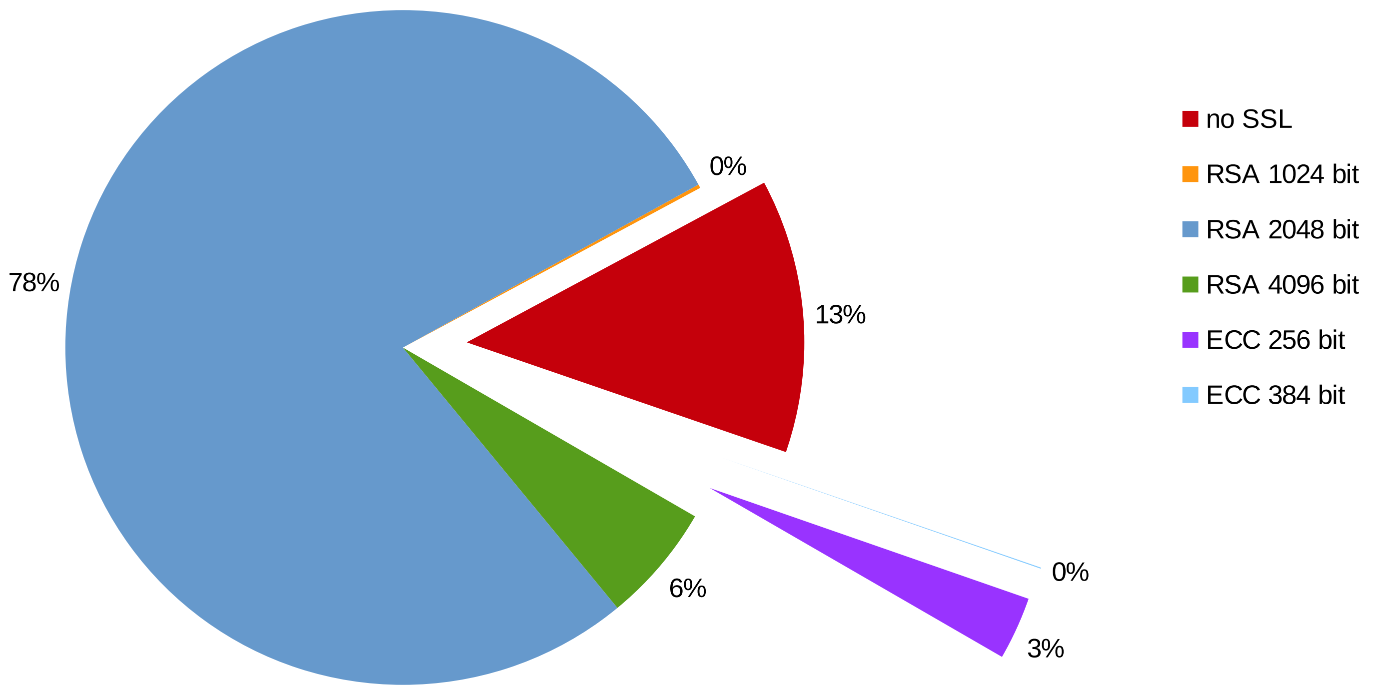
```
[2]epmacpro:~$ echo | openssl s_client -connect www.harvard.edu:443 2>/dev/null | awk '/BEGIN/,/END/' | openssl x509 -text -noout | awk '/Subject Public Key Info/,/X509/'
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:20:00:c7:c2:74:49:14:2f:15:64:cc:bd:be:4b:
                    b4:4d:41:02:fc:85:fd:4e:fa:5d:ca:cf:5e:84:3d:
                    f5:be:f0:04:b1:92:89:26:95:65:04:10:1b:2e:07:
                    3b:5c:47:68:fc:24:0d:52:50:87:a0:81:b6:53:1d:
                    4c:29:f1:94:d8
                ASN1 OID: prime256v1
        X509v3 extensions:
[2]epmacpro:~$
```

2017 TLS Certificate Breakdown for Edu's



.edu's taken from Majestic's top 1 million websites (3096 total)

2018 TLS Certificate Breakdown for Edu's



.edu's taken from Majestic's top 1 million websites (4008 total)

Why create ECC, we have RSA?

- If RSA breaks, what then?
- Faster computers force increased key size
- Speed is faster with ECC (for most things)

Key Length Comparison

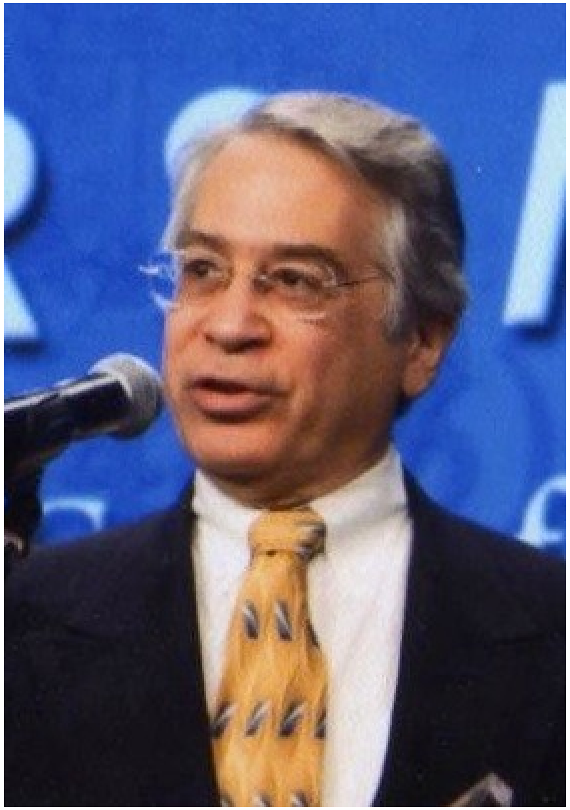
Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Elliptic Curve Cryptography

Neal Koblitz

1985



Victor Miller

Elliptic Curve Cryptography (ECC)

- Explain the end goal for ECC
- Review a little math
- Show how to get to our end goal

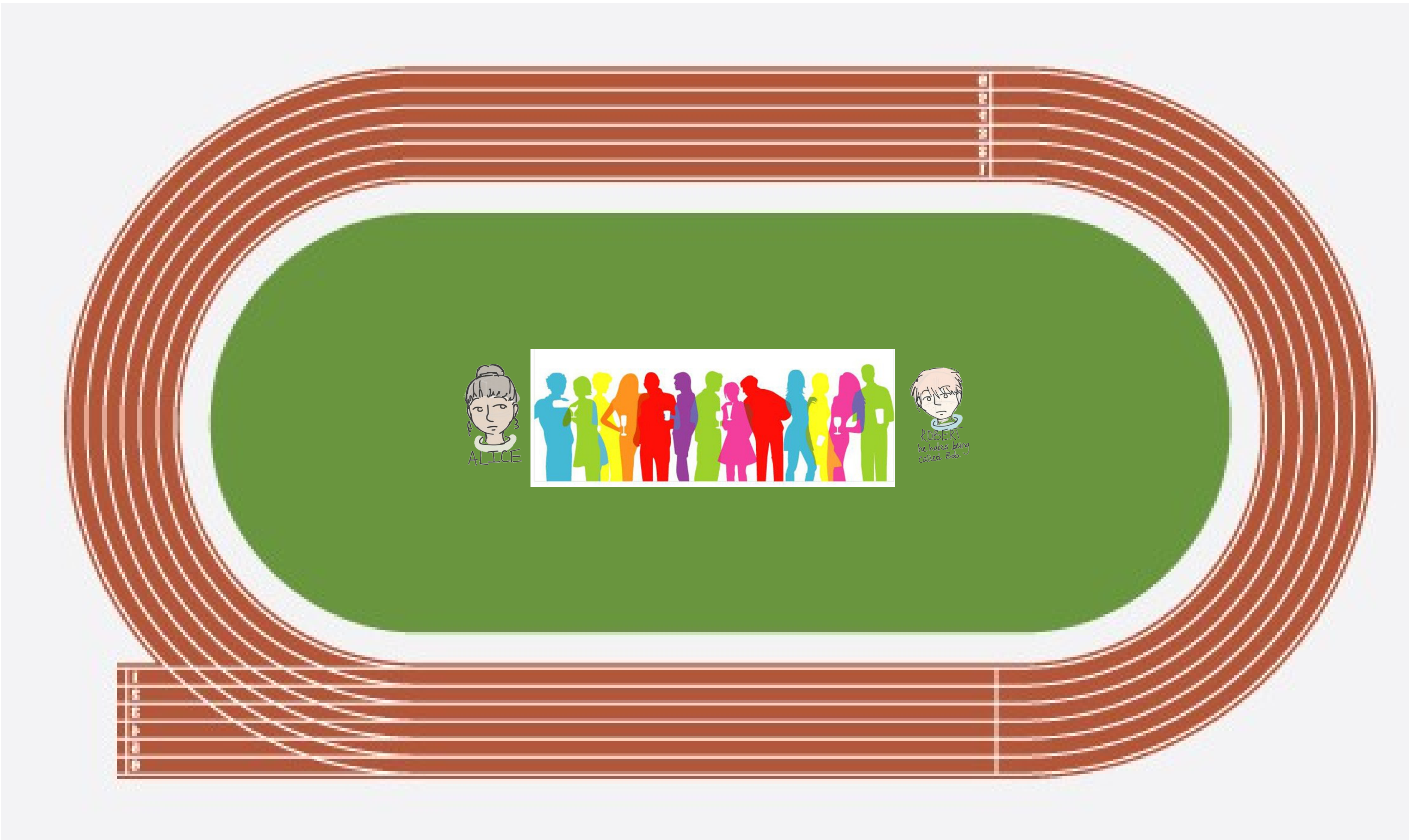
So, let's begin at the end...

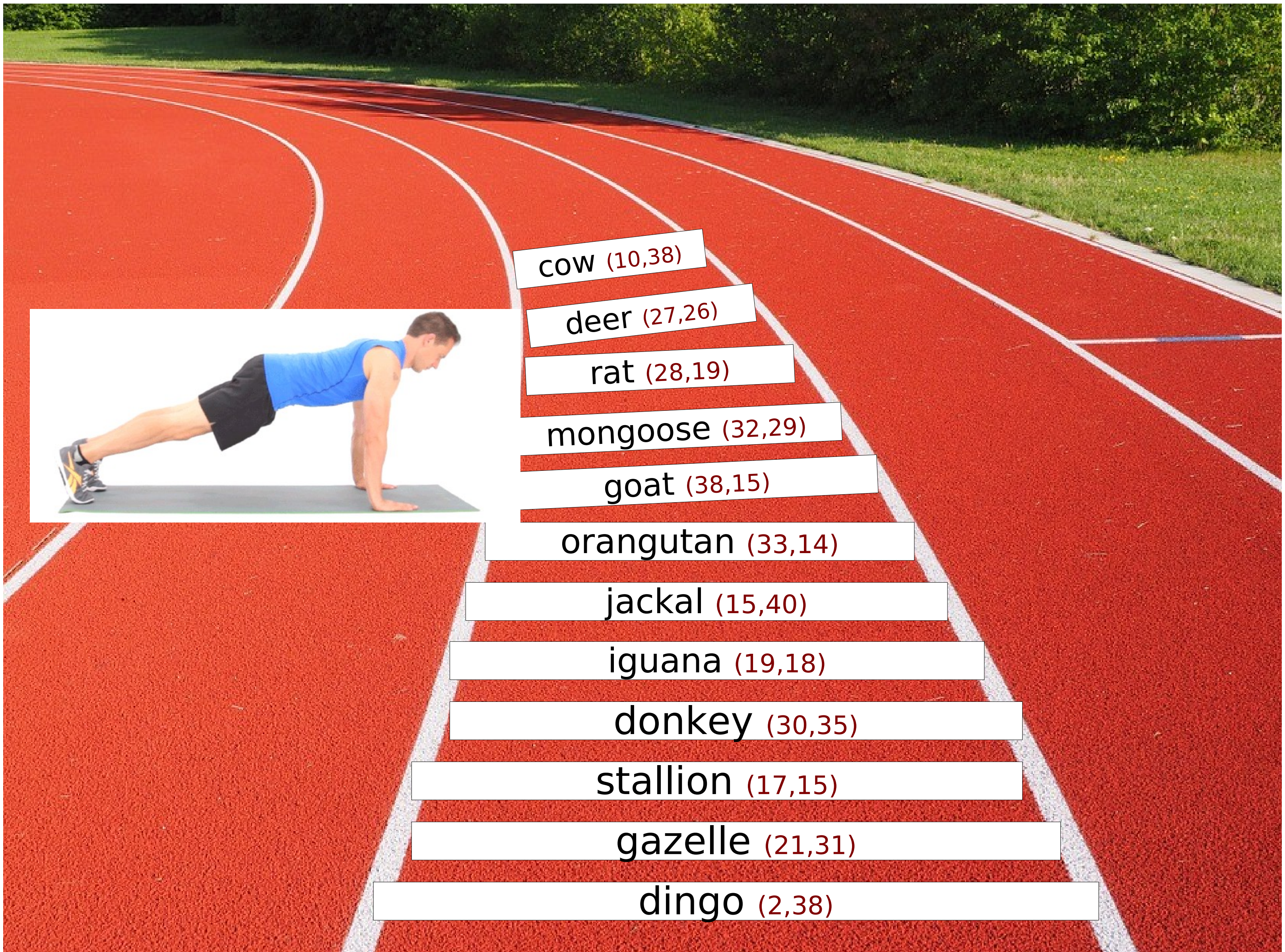
Secret Exchange

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

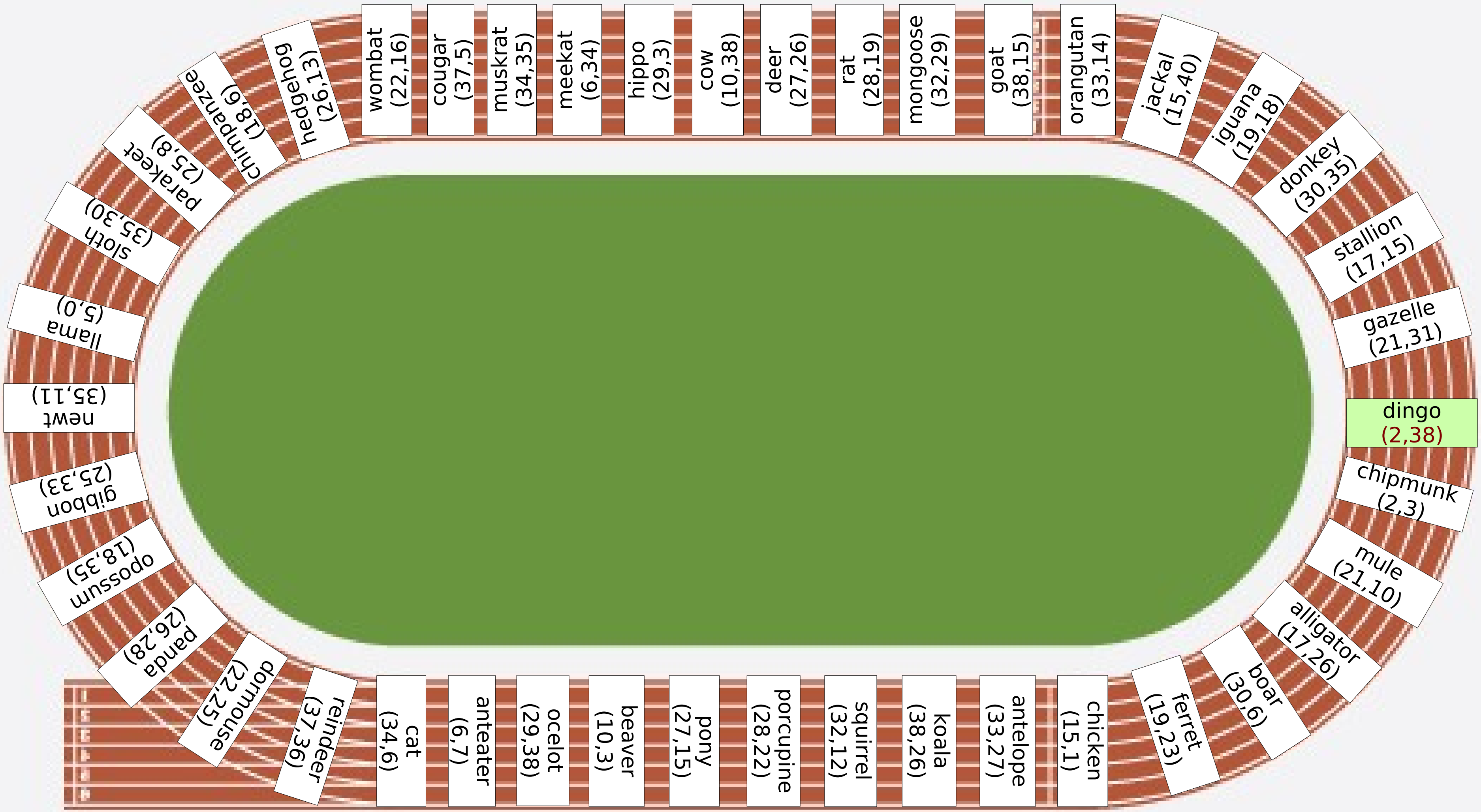



cow (10,38)
deer (27,26)
rat (28,19)
mongoose (32,29)
goat (38,15)
orangutan (33,14)
jackal (15,40)
iguana (19,18)
donkey (30,35)
stallion (17,15)
gazelle (21,31)
dingo (2,38)

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

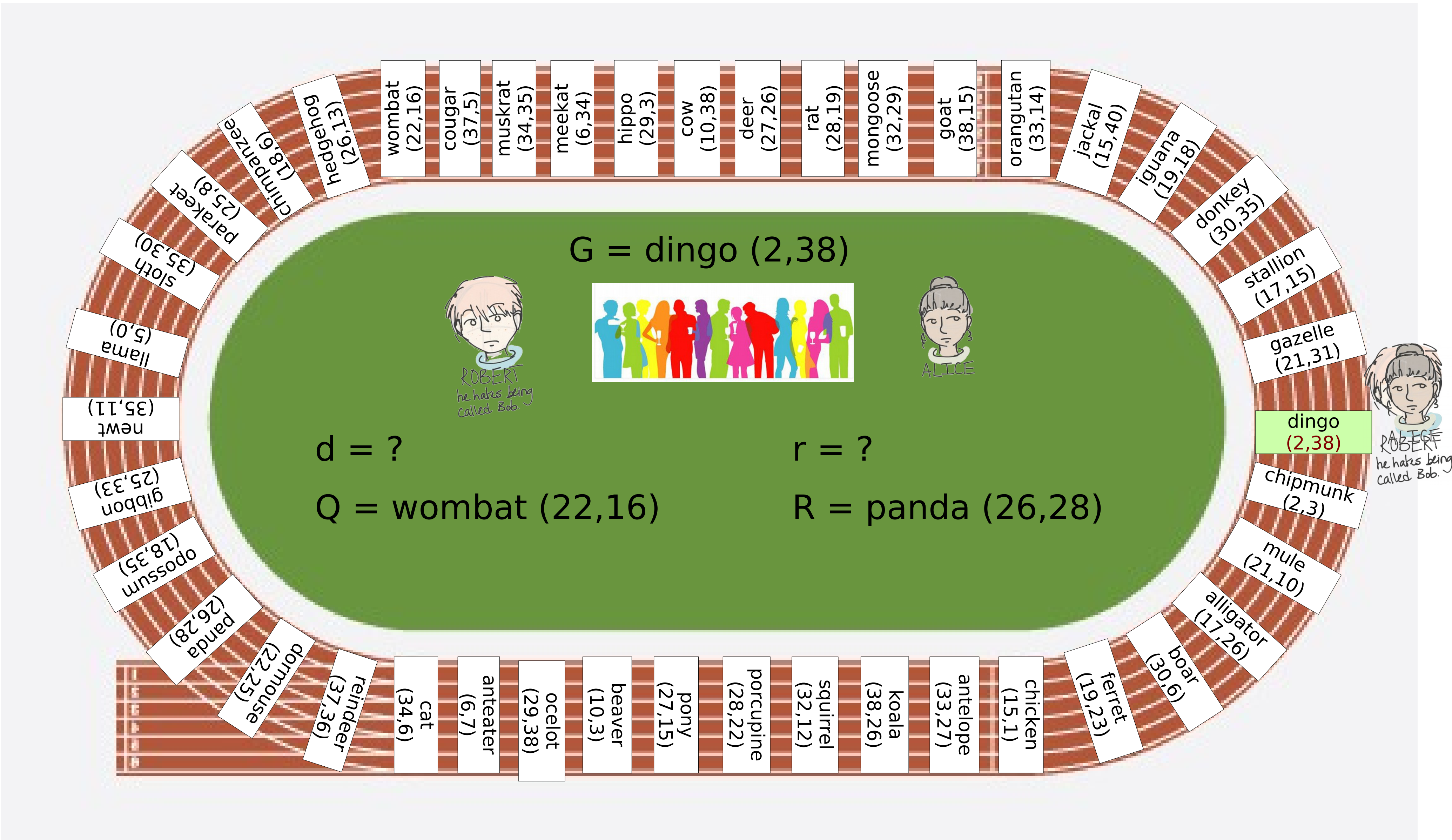


Network Security
Institute for Advanced Study

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

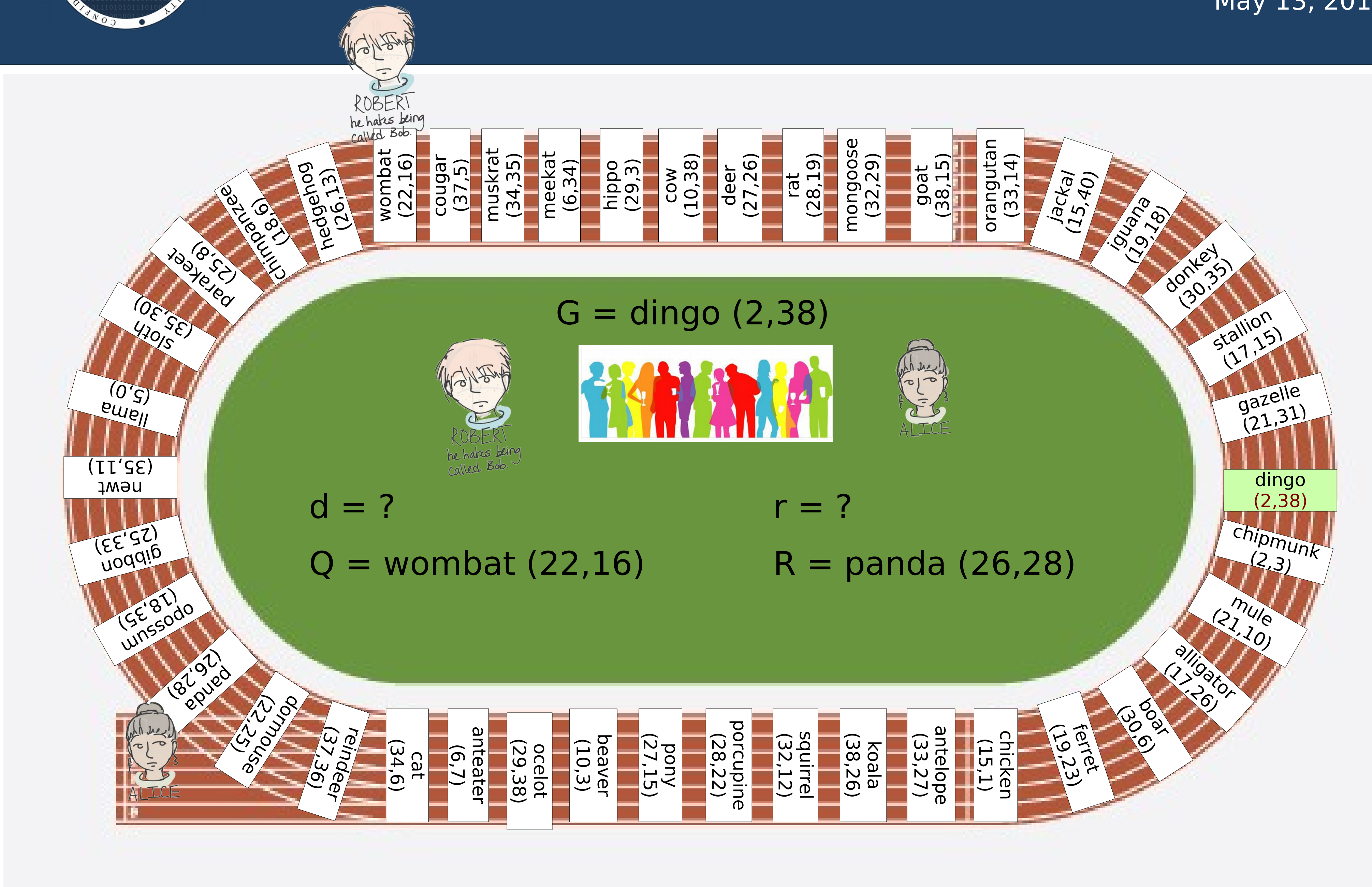


Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

Network Security
Institute for Advanced Study

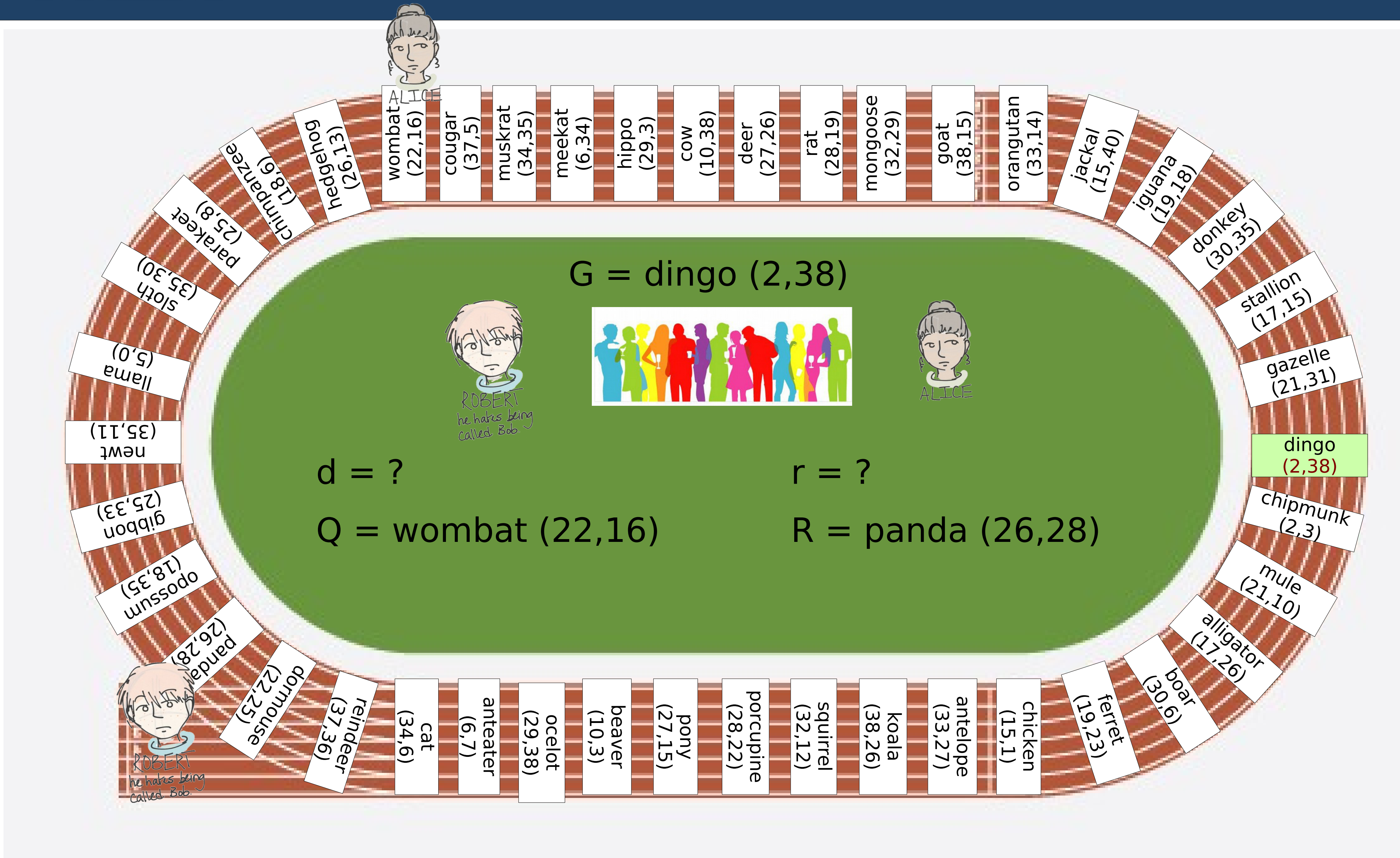


Network Security
Institute for Advanced Study

Fun with Certificates part II

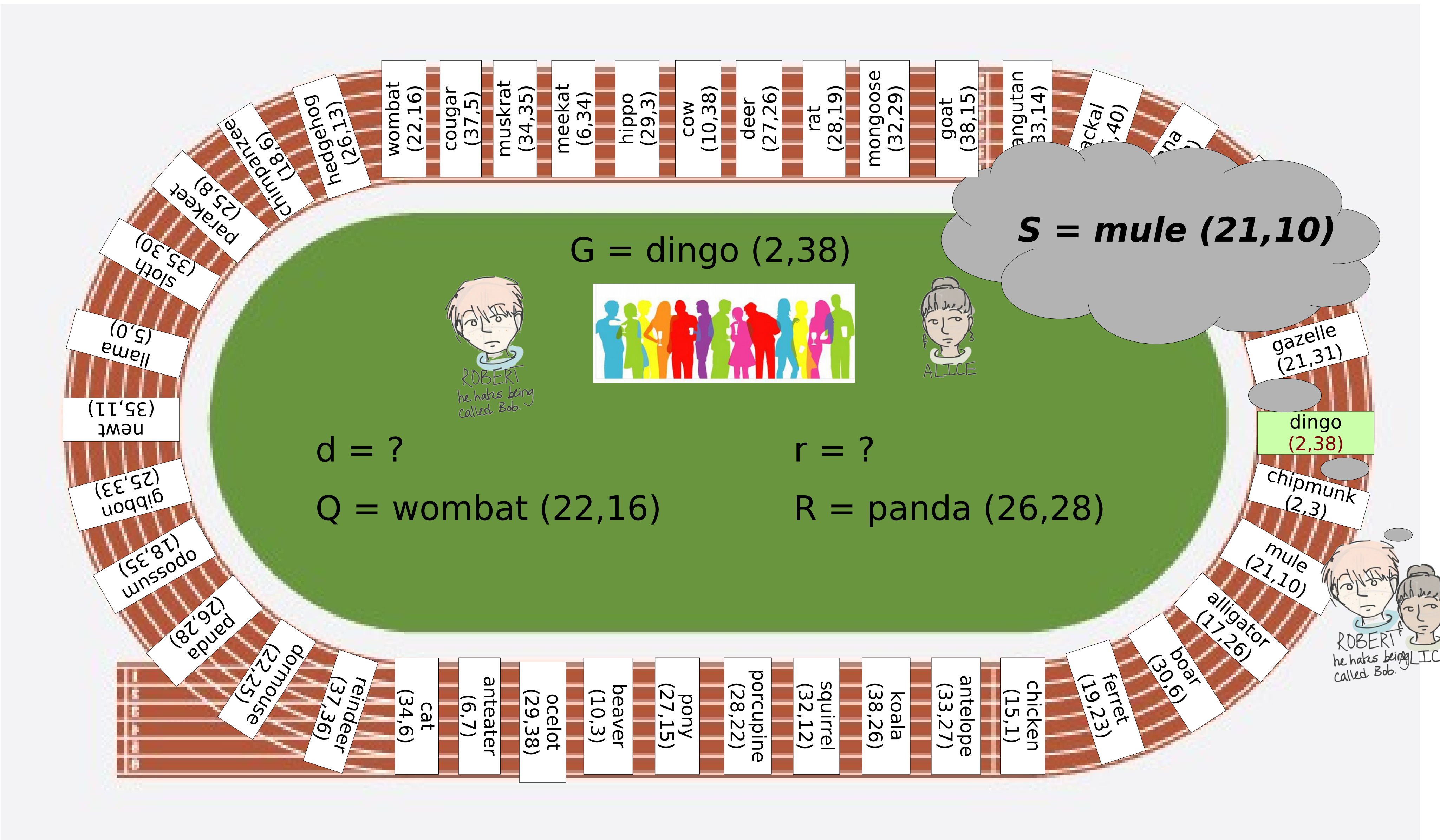
Elliptic Curve Cryptography

May 13, 2019



Network Security
Institute for Advanced Study

Fun with Certificates part II
Elliptic Curve Cryptography
May 13, 2019



G = dingo (2,38)

d = 16

Q = wombat (22,16)

r = 25

R = panda (26,28)

d

r

+ d Why does this work? = s

25 + 16 =

16 + 25 = 41

S = mule (21,10)

Humpf,
how romantic...

I should've
picked a better
number.

Math

- Square and Square root
- Graphing
- Elliptic Curves with point math
- Finite Fields

Square and Square Root

$$3^2 = 3 \cdot 3 = 9$$

$$(-3)^2 = -3 \cdot -3 = 9$$

$$\sqrt{9} = 3$$

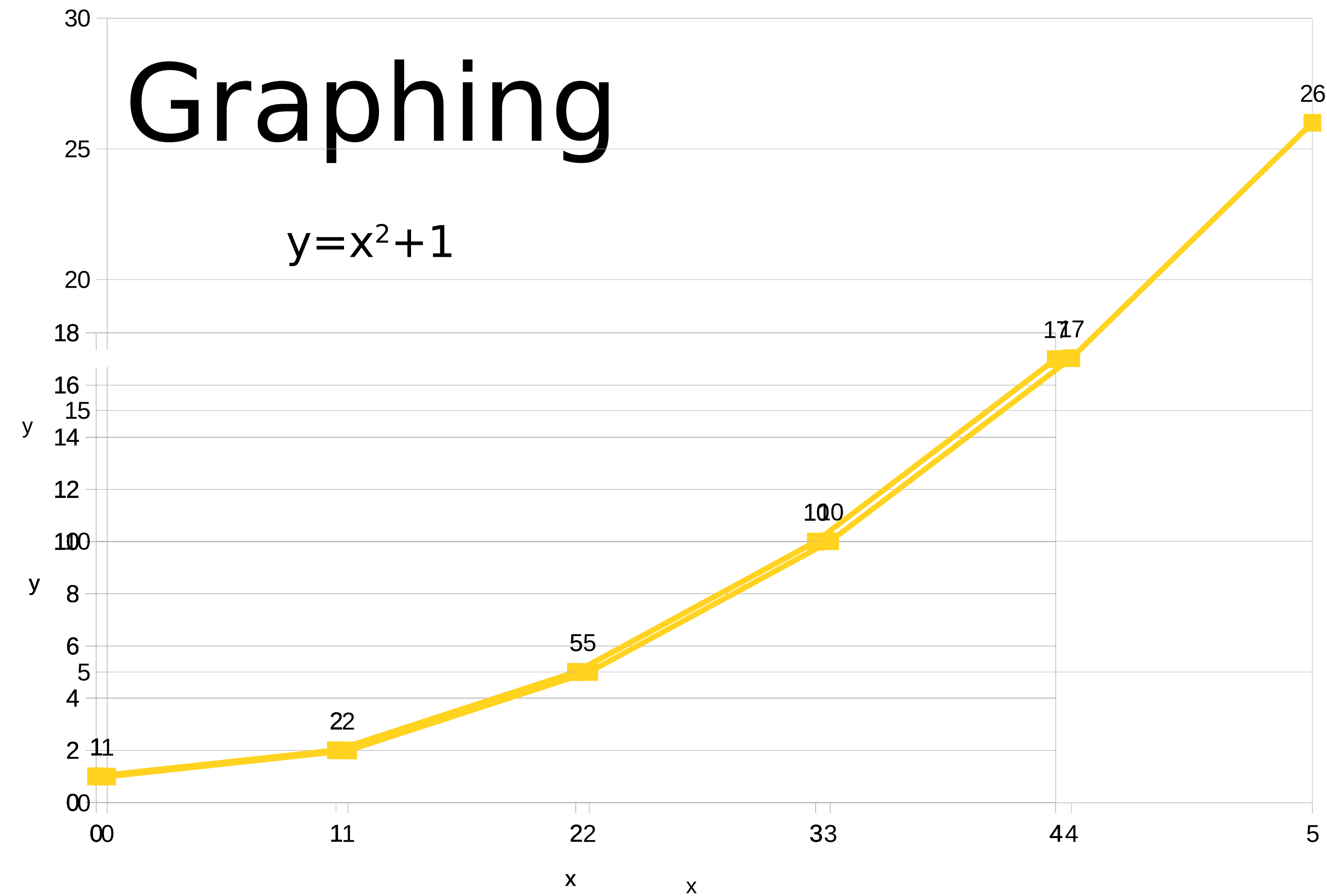
$$\sqrt{9} = \pm 3$$

$$\sqrt{9} = -3$$

Graphing

$y=x^2+1$

x	x^2+1 / y
0	0^2+1 / 1
1	1^2+1 / 2
2	2^2+1 / 5
3	10
4	17
5	26

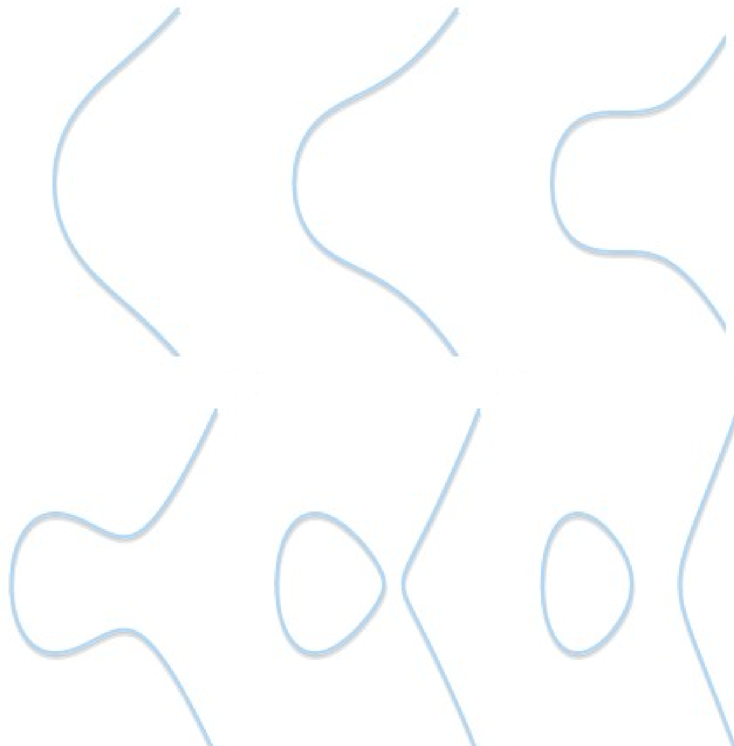


Elliptic Curves

An Elliptical Machine

Elliptic Curves

$$\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0\} \cup \{0\}$$



Elliptic Curve Math

- Create “point addition” ⊕

$$P \oplus Q \oplus R = 0$$

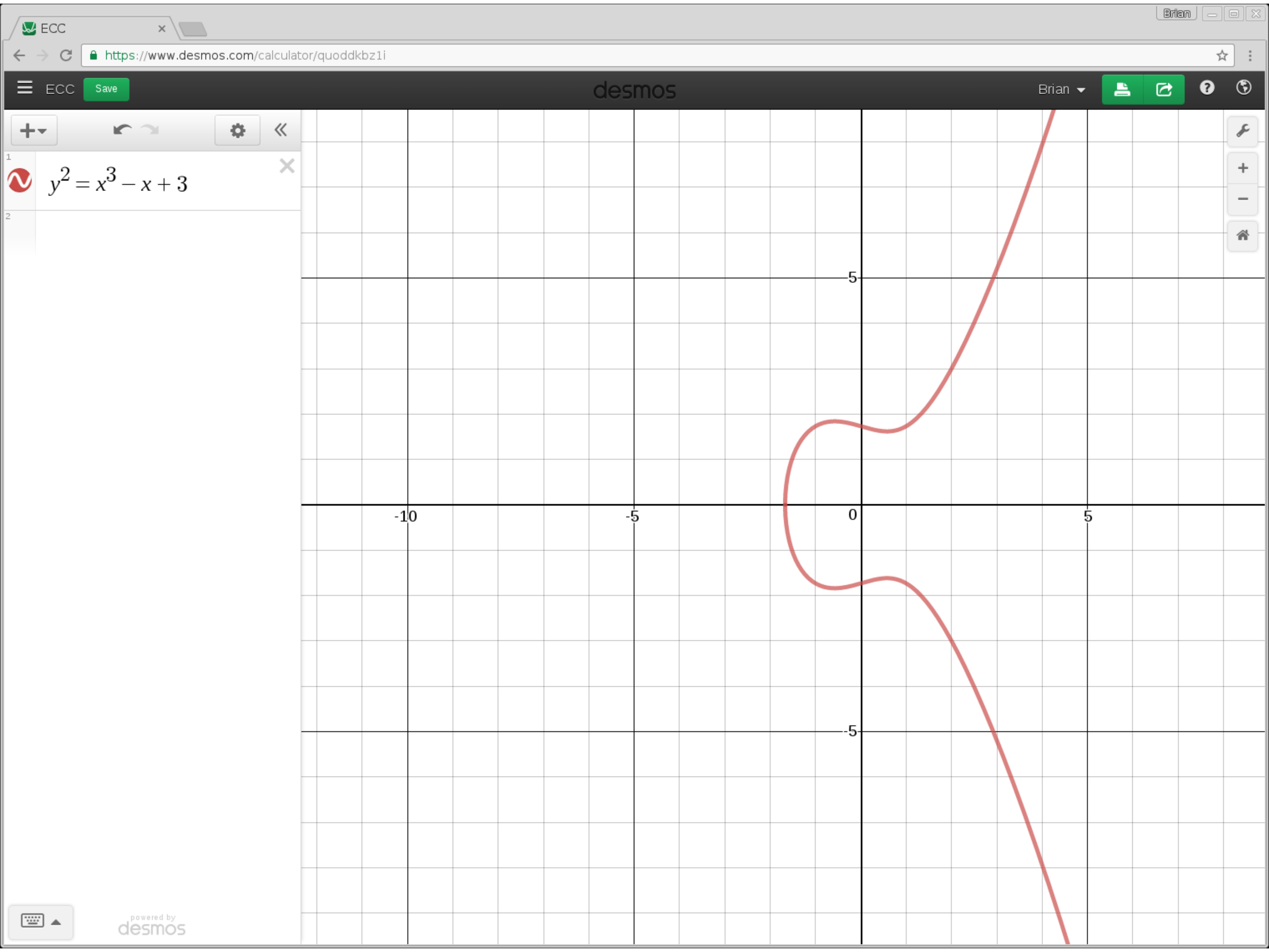
$$P \oplus Q = -R$$

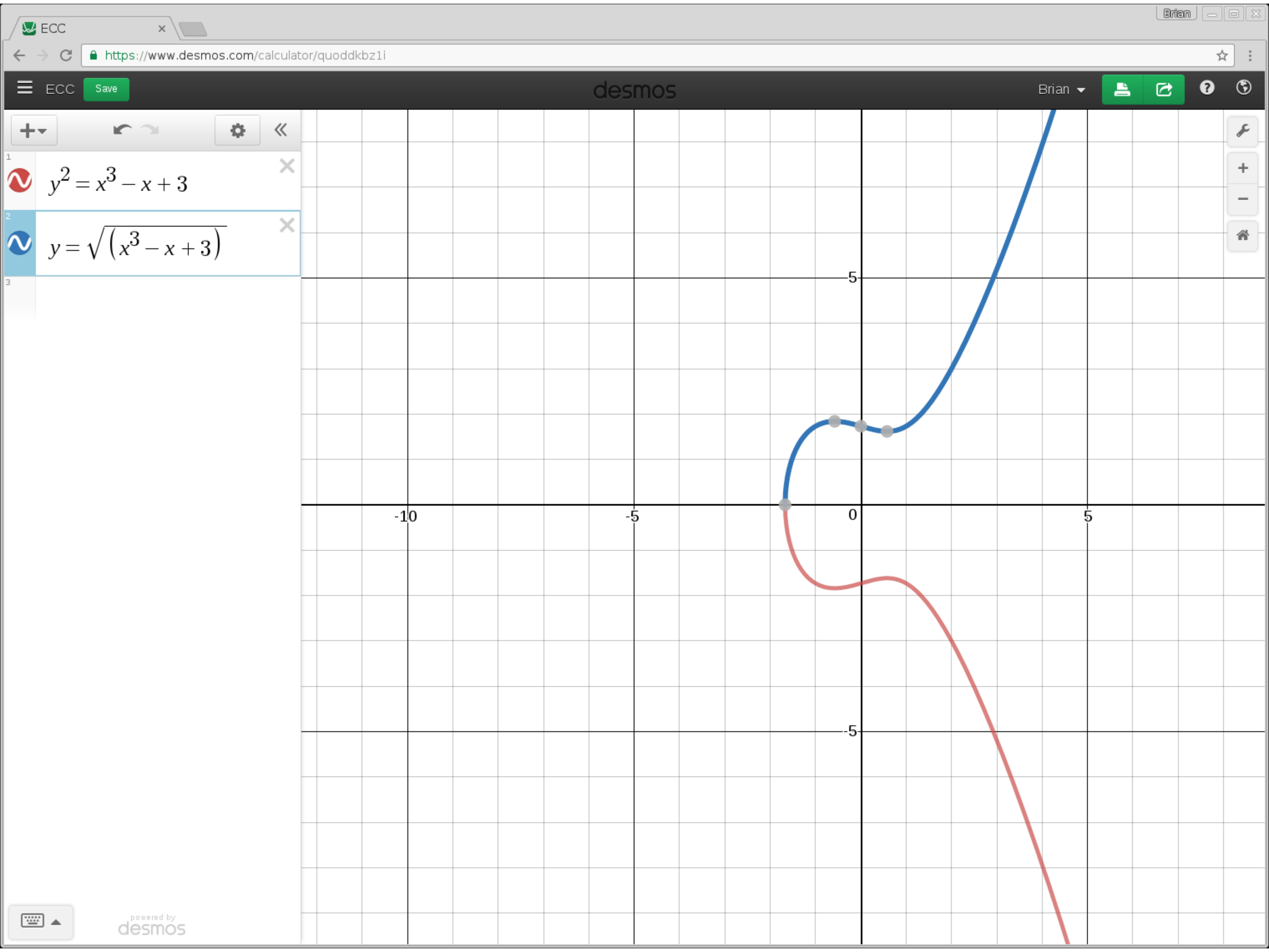
- Create “point multiplication” ⊙

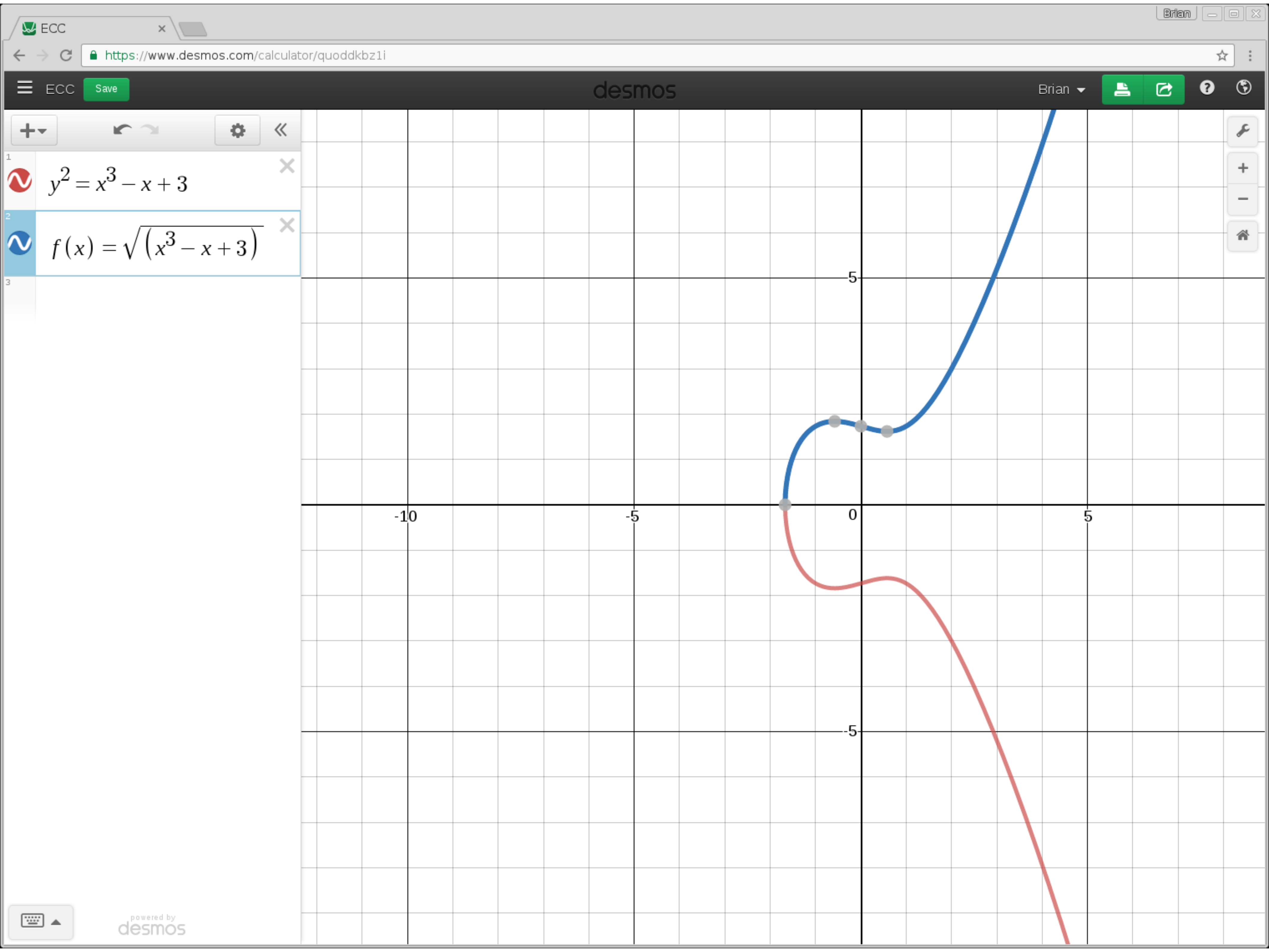
$$2 \odot P = P \oplus P$$

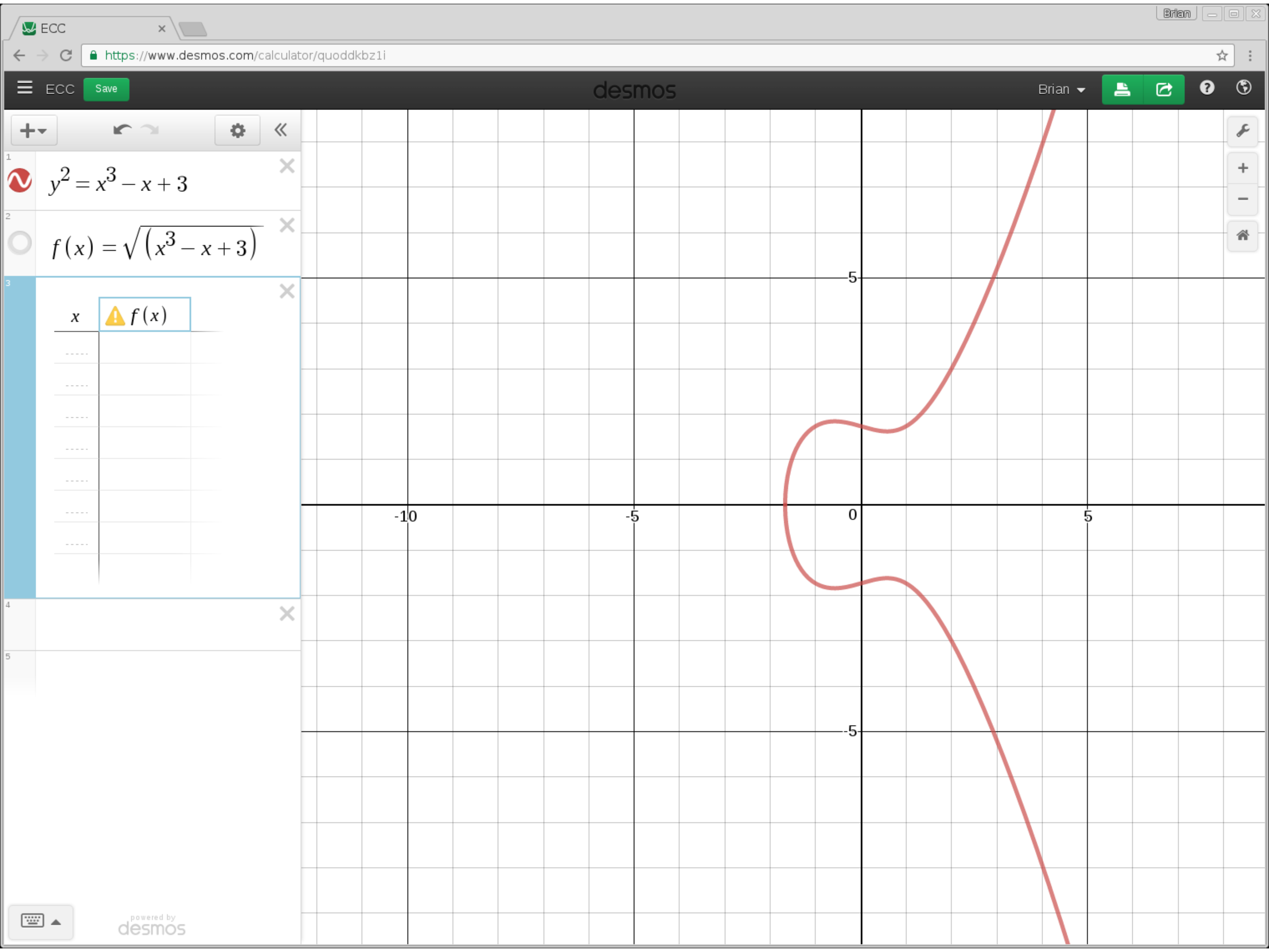
$$5 \odot P = P \oplus P \oplus P \oplus P \oplus P$$

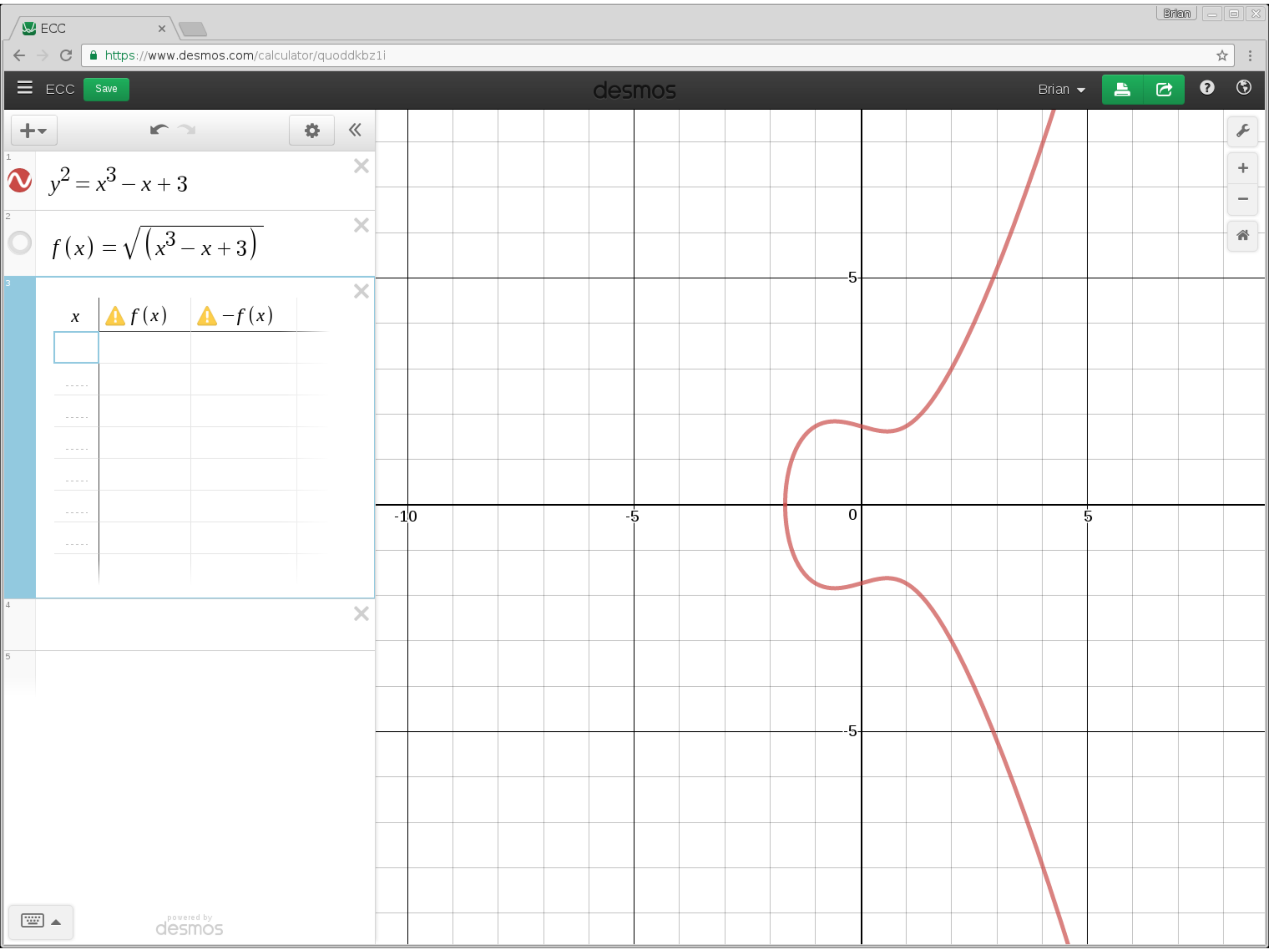
- Demo D

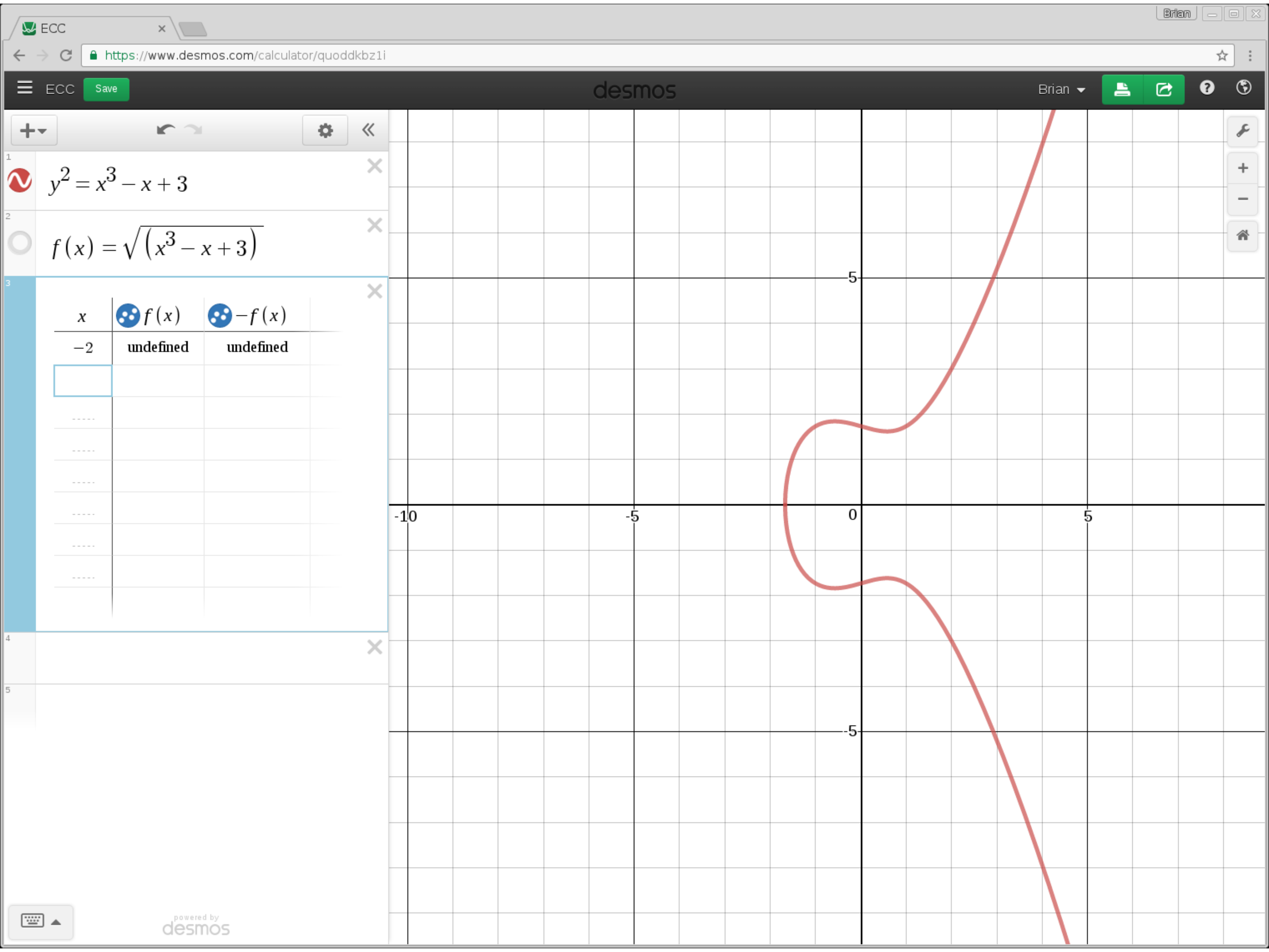

ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
$y^2 = x^3 - x + 3$
5
-10
-5
0
5
-5
powered by desmos

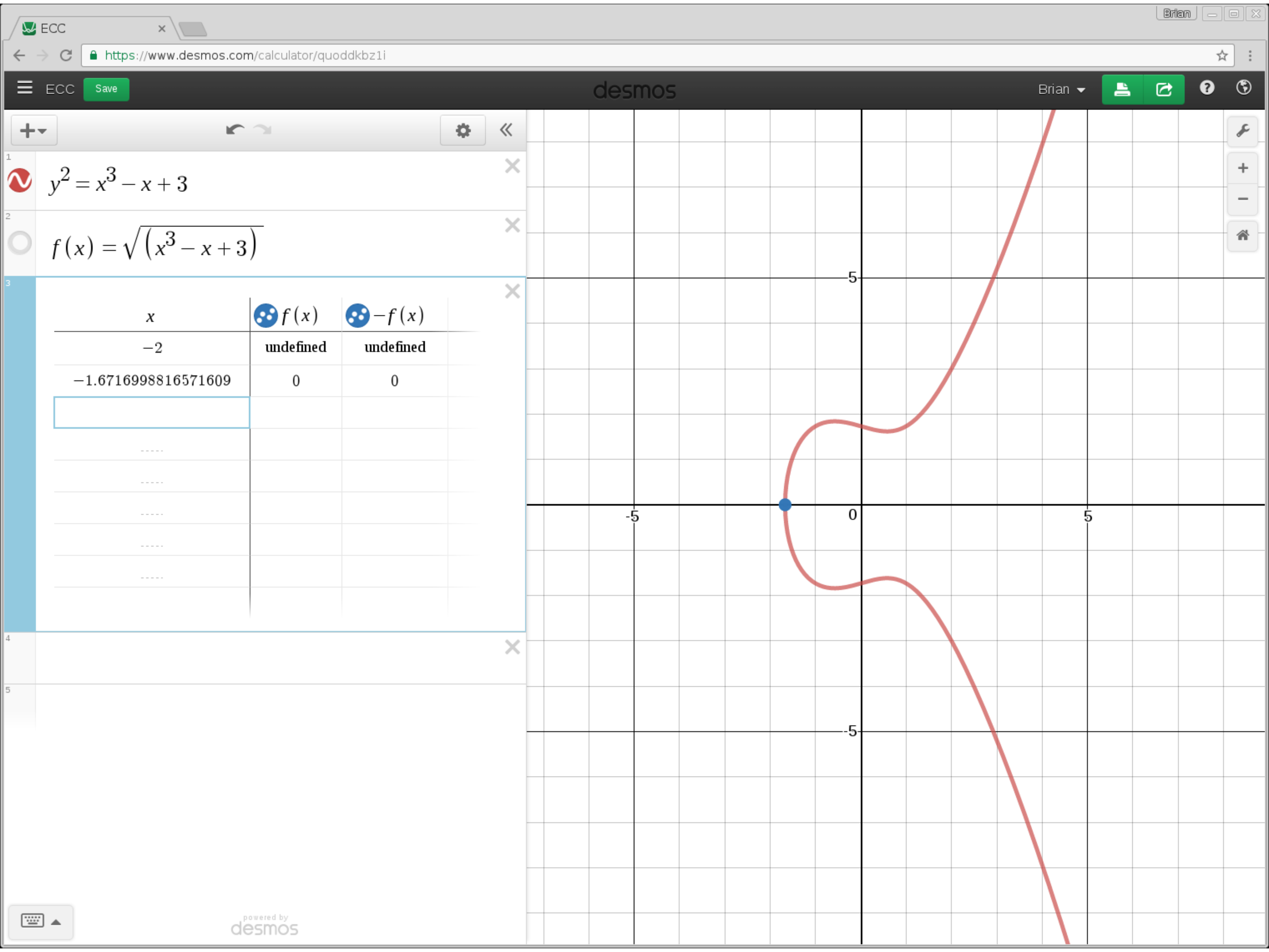

ECC
https://www.desmos.com/calculator/quoddkbz1i
Brian
ECC
Save
desmos
Brian
$y^2 = x^3 - x + 3$
$y = \sqrt{(x^3 - x + 3)}$
5
-10
-5
0
5
-5
powered by
desmos

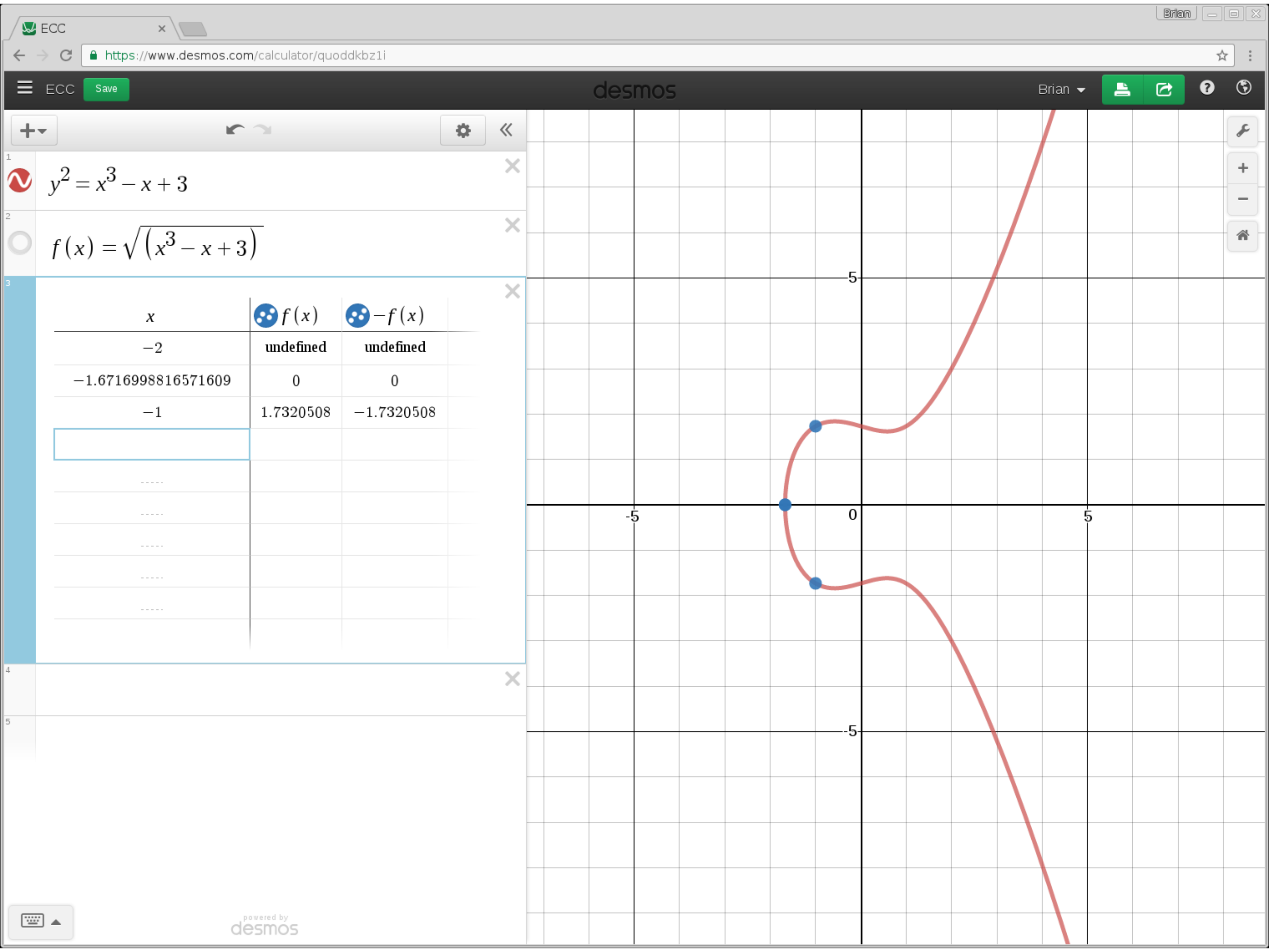

ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
$y^2 = x^3 - x + 3$
$f(x) = \sqrt{(x^3 - x + 3)}$
5
-10
-5
0
5
-5
powered by desmos


ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
1
$y^2 = x^3 - x + 3$
2
$f(x) = \sqrt{(x^3 - x + 3)}$
3
x
$f(x)$
4
5
5
-10
-5
0
5
-5
powered by desmos


ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
$y^2 = x^3 - x + 3$
$f(x) = \sqrt{(x^3 - x + 3)}$
x
$f(x)$
$-f(x)$
powered by desmos
5
-10
-5
0
5
-5


ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
1
$y^2 = x^3 - x + 3$
2
$f(x) = \sqrt{(x^3 - x + 3)}$
3
x
$f(x)$
$-f(x)$
-2
undefined
undefined
4
5
powered by desmos
5
-10
-5
0
5
-5


ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
$y^2 = x^3 - x + 3$
$f(x) = \sqrt{(x^3 - x + 3)}$
x | $f(x)$ | $-f(x)$
-2 | undefined | undefined
-1.6716998816571609 | 0 | 0
5
-5
0
-5
5
powered by desmos


ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
$y^2 = x^3 - x + 3$
$f(x) = \sqrt{(x^3 - x + 3)}$
x
f(x)
−f(x)
−2
undefined
undefined
−1.6716998816571609
0
0
−1
1.7320508
−1.7320508
5
-5
0
5
-5
powered by desmos

ECC

https://www.desmos.com/calculator/quoddkbz1i

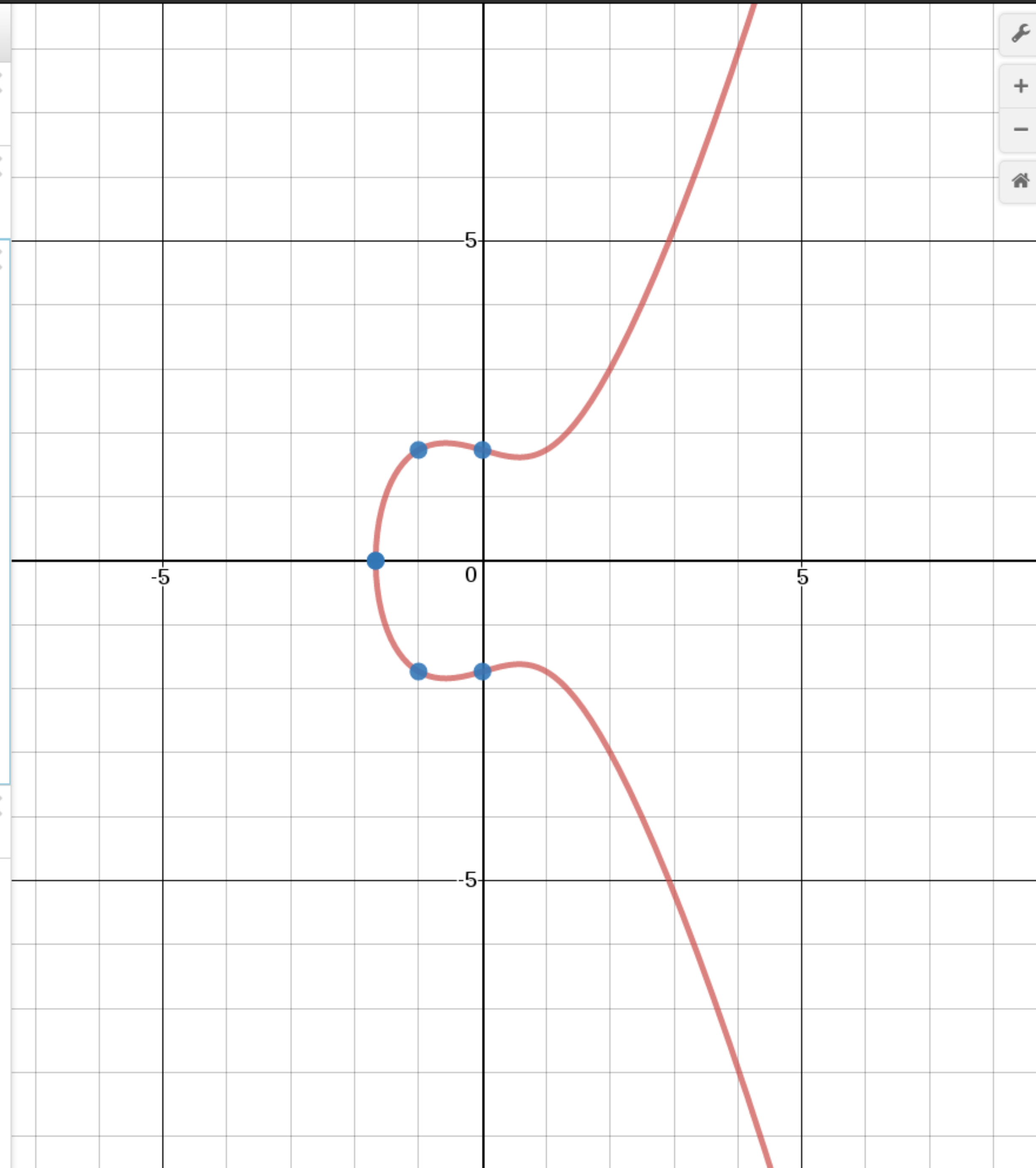
desmos

1. $y^2 = x^3 - x + 3$

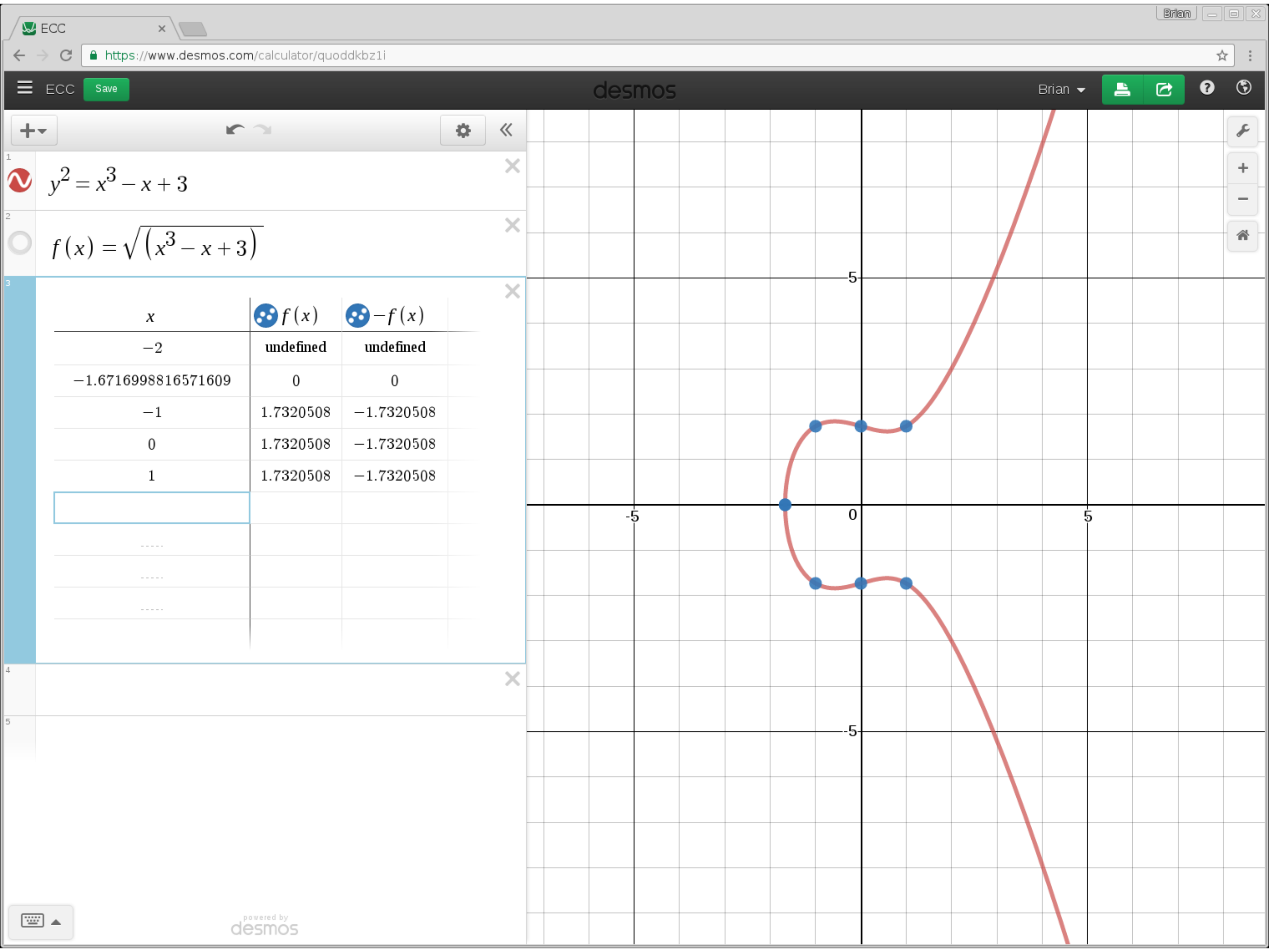
2. $f(x) = \sqrt{(x^3 - x + 3)}$

3.

x	$f(x)$	$-f(x)$
-2	undefined	undefined
-1.6716998816571609	0	0
-1	1.7320508	-1.7320508
0	1.7320508	-1.7320508



powered by desmos


ECC
https://www.desmos.com/calculator/quoddkbz1i
ECC
Save
desmos
Brian
$y^2 = x^3 - x + 3$
$f(x) = \sqrt{(x^3 - x + 3)}$
x | $f(x)$ | $-f(x)$
−2 | undefined | undefined
−1.6716998816571609 | 0 | 0
−1 | 1.7320508 | −1.7320508
0 | 1.7320508 | −1.7320508
1 | 1.7320508 | −1.7320508
5
-5
0
5
-5
powered by desmos

ECC

https://www.desmos.com/calculator/quoddkbz1i

ECC Save desmos Brian

1 $y^2 = x^3 - x + 3$

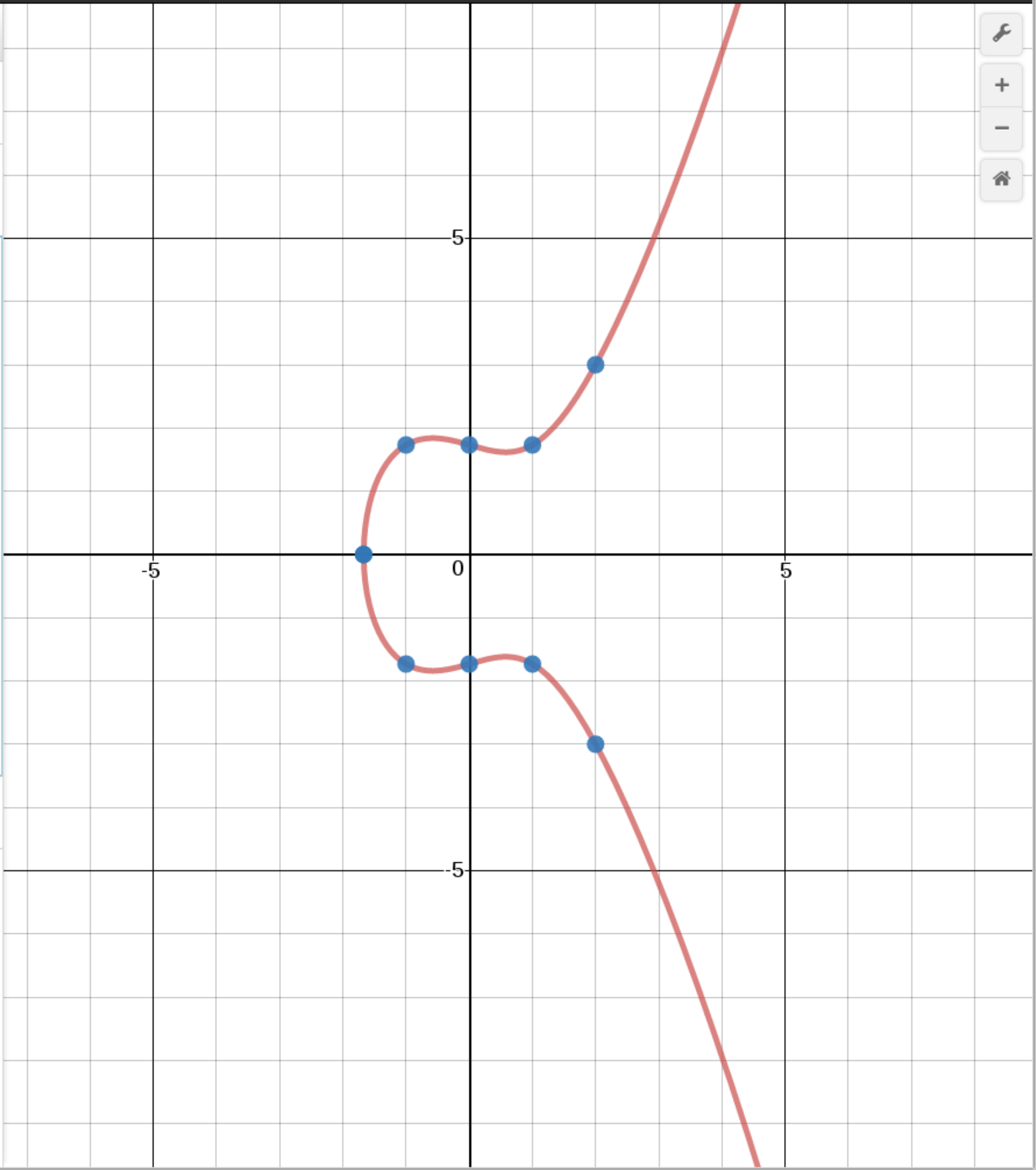
2 $f(x) = \sqrt{(x^3 - x + 3)}$

3

x	$f(x)$	$-f(x)$
−2	undefined	undefined
−1.6716998816571609	0	0
−1	1.7320508	−1.7320508
0	1.7320508	−1.7320508
1	1.7320508	−1.7320508
2	3	−3

4

5



powered by desmos

ECC

https://www.desmos.com/calculator/quoddkbz1i

ECC Save desmos Brian

1 $y^2 = x^3 - x + 3$

2 $f(x) = \sqrt{(x^3 - x + 3)}$

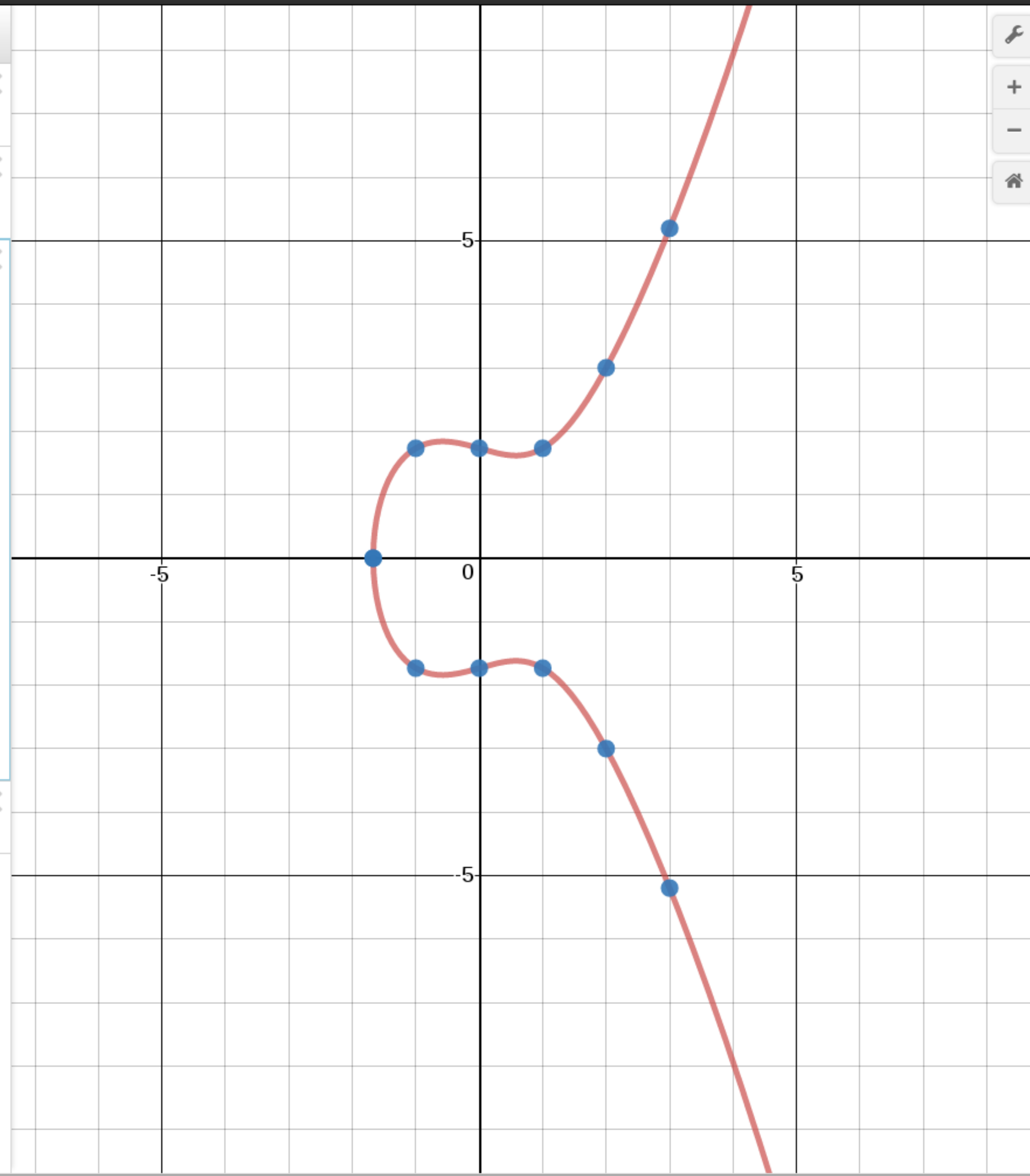
3

x	$f(x)$	$-f(x)$
−2	undefined	undefined
−1.6716998816571609	0	0
−1	1.7320508	−1.7320508
0	1.7320508	−1.7320508
1	1.7320508	−1.7320508
2	3	−3
3	5.1961524	−5.1961524

4

5

powered by desmos



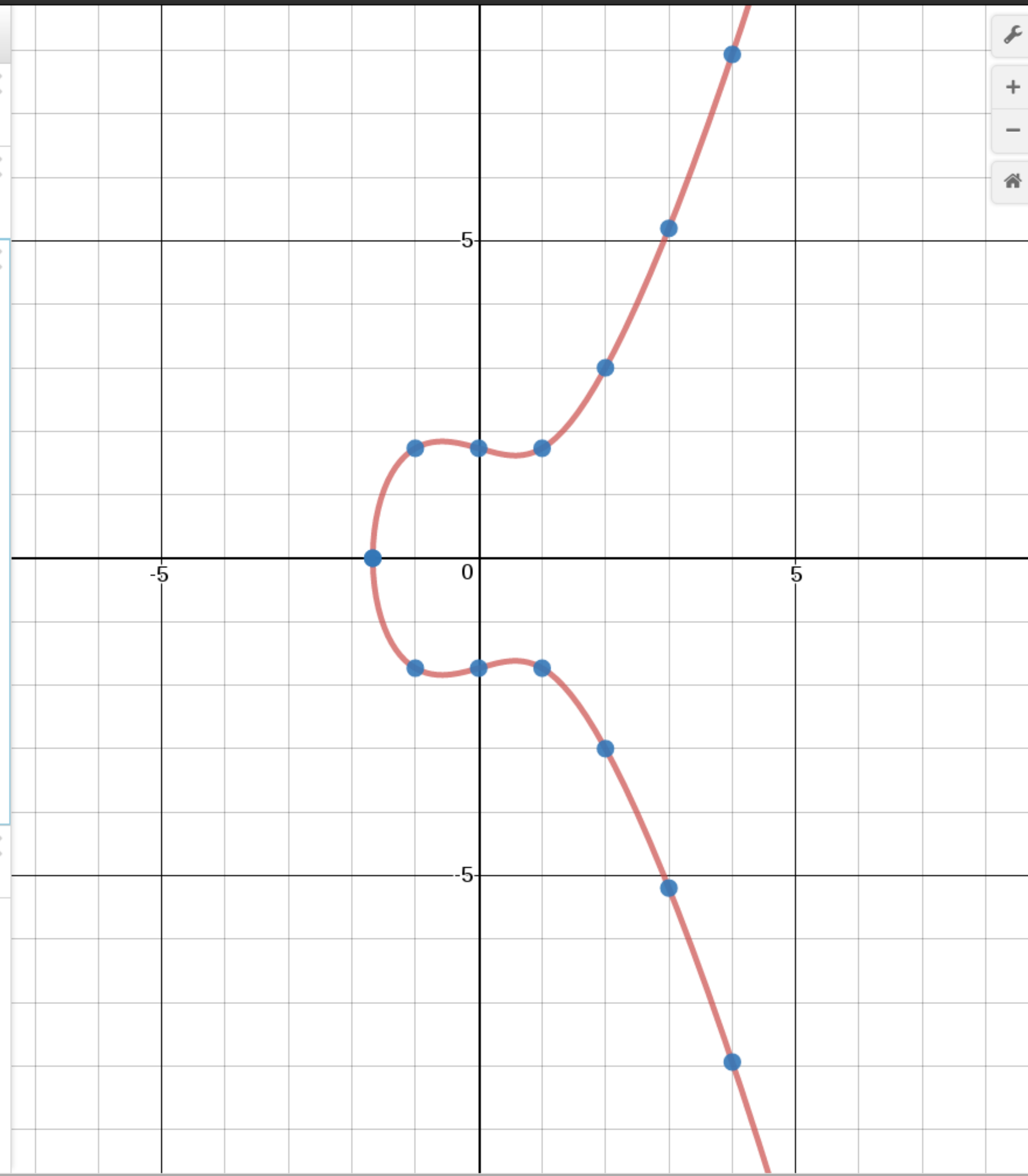
ECC

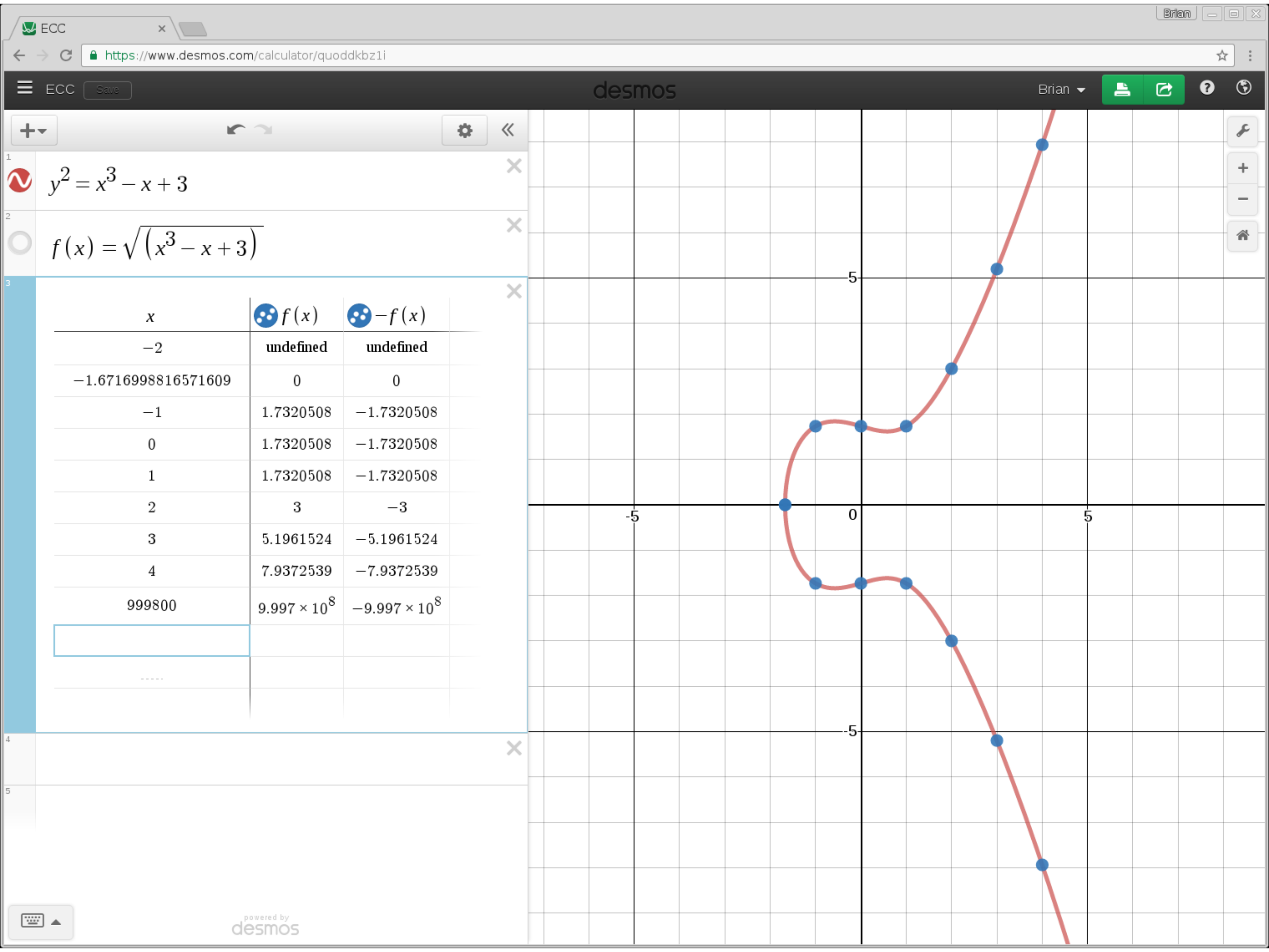
https://www.desmos.com/calculator/quoddkbz1i

$$y^2 = x^3 - x + 3$$

$$f(x) = \sqrt{(x^3 - x + 3)}$$

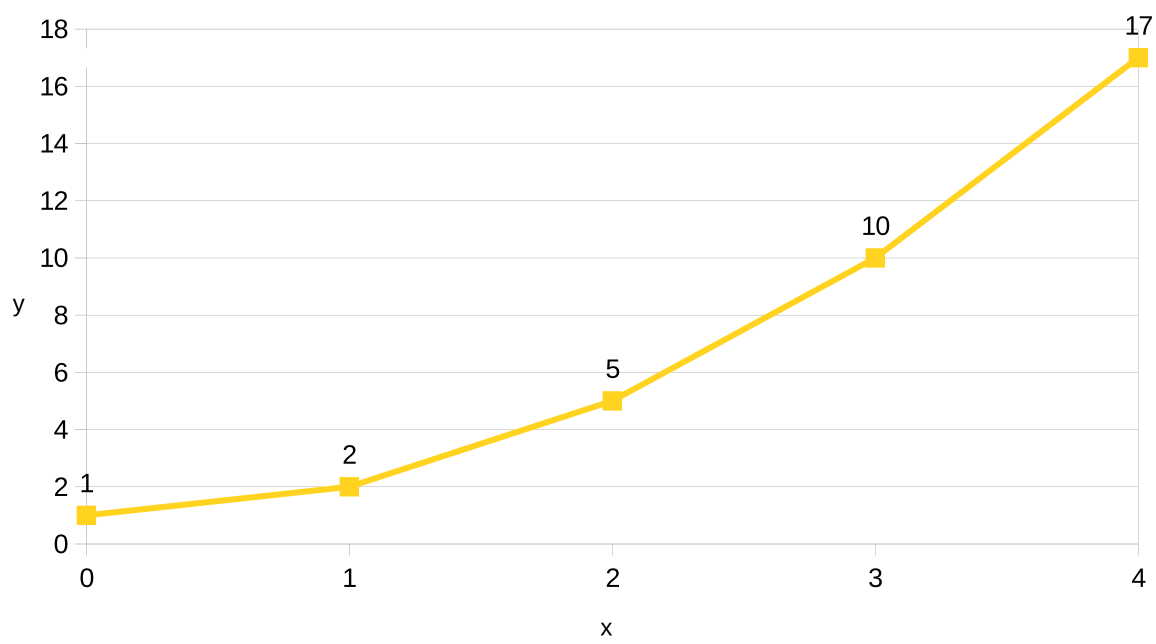
x	$f(x)$	$-f(x)$
-2	undefined	undefined
-1.6716998816571609	0	0
-1	1.7320508	-1.7320508
0	1.7320508	-1.7320508
1	1.7320508	-1.7320508
2	3	-3
3	5.1961524	-5.1961524
4	7.9372539	-7.9372539




ECC
https://www.desmos.com/calculator/quoddkbz1i
desmos
Brian
$y^2 = x^3 - x + 3$
$f(x) = \sqrt{(x^3 - x + 3)}$
x | f(x) | −f(x)
−2 | undefined | undefined
−1.6716998816571609 | 0 | 0
−1 | 1.7320508 | −1.7320508
0 | 1.7320508 | −1.7320508
1 | 1.7320508 | −1.7320508
2 | 3 | −3
3 | 5.1961524 | −5.1961524
4 | 7.9372539 | −7.9372539
999800 | 9.997 × 10^8 | −9.997 × 10^8
5
-5
0
-5
5
-5
powered by desmos

Graphing

x	x^2+1
0	0
1	2
2	5
3	10
4	17
5	26



Finite Fields

- Finite
  - There is an end
- Field
  - Football
  - Soccer
- Demo A

Benefits from Finite Fields

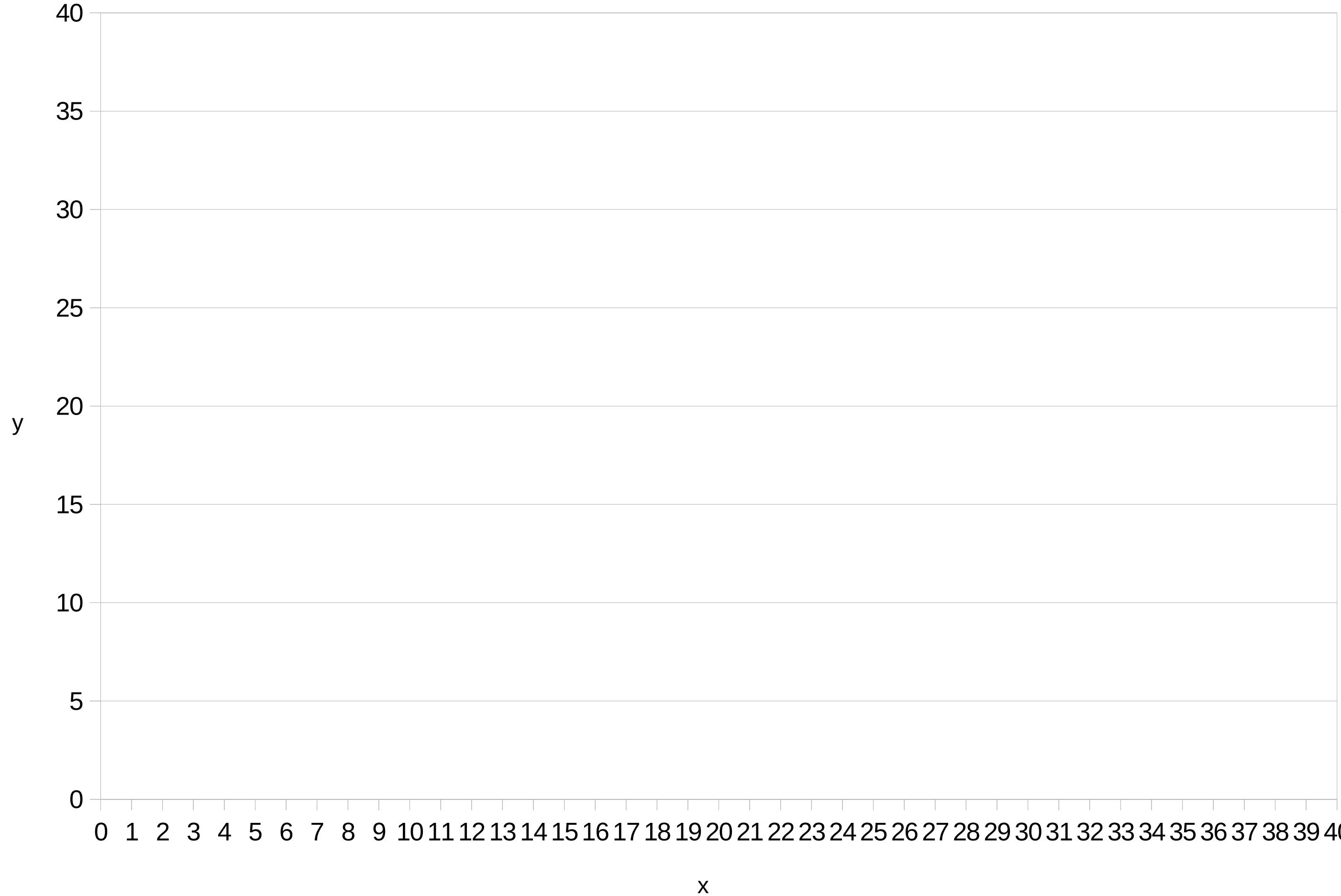
- computers are terrible at irrational numbers
- get to use whole numbers (integers)
- reduce the size of the problem
- Field is “closed”

Example Finite Field

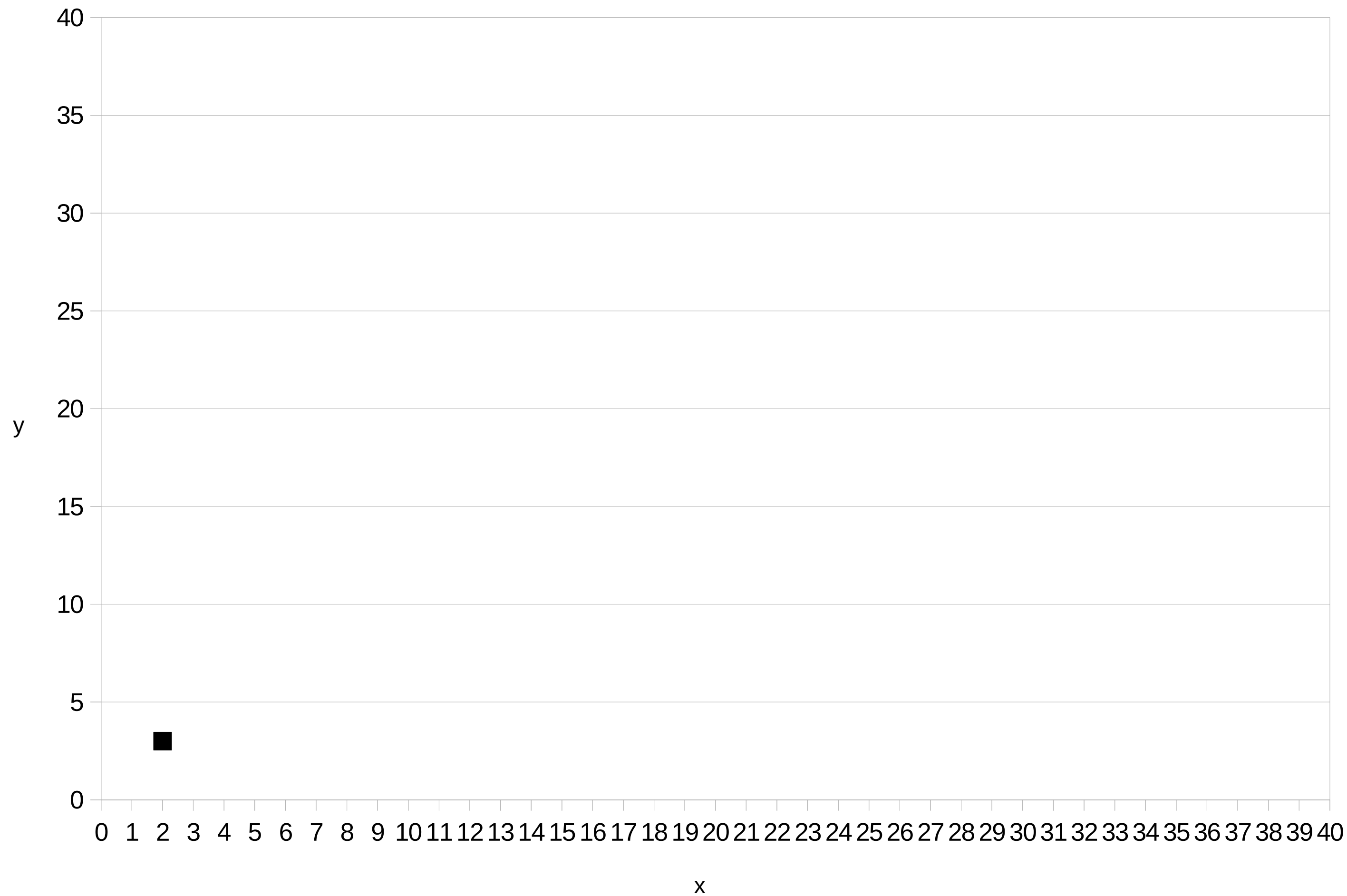
- Field size is 41
- x axis goes from 0 to 40
- y axis goes from 0 to 40

Graphing an EC on a Finite Field

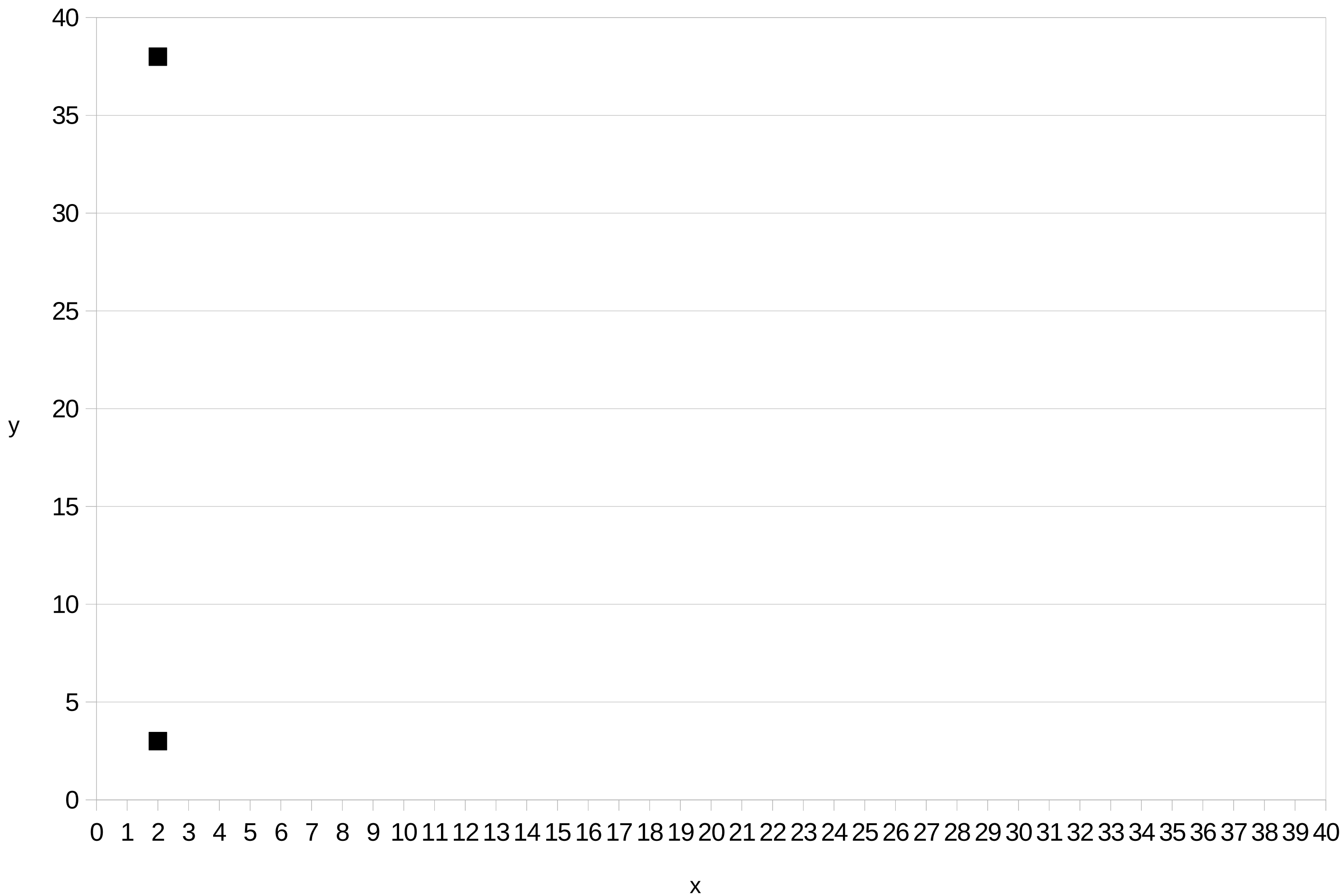
x	$y^2 \,(mod\,41) \equiv x^3 - x + 3 \,(mod\,41)$



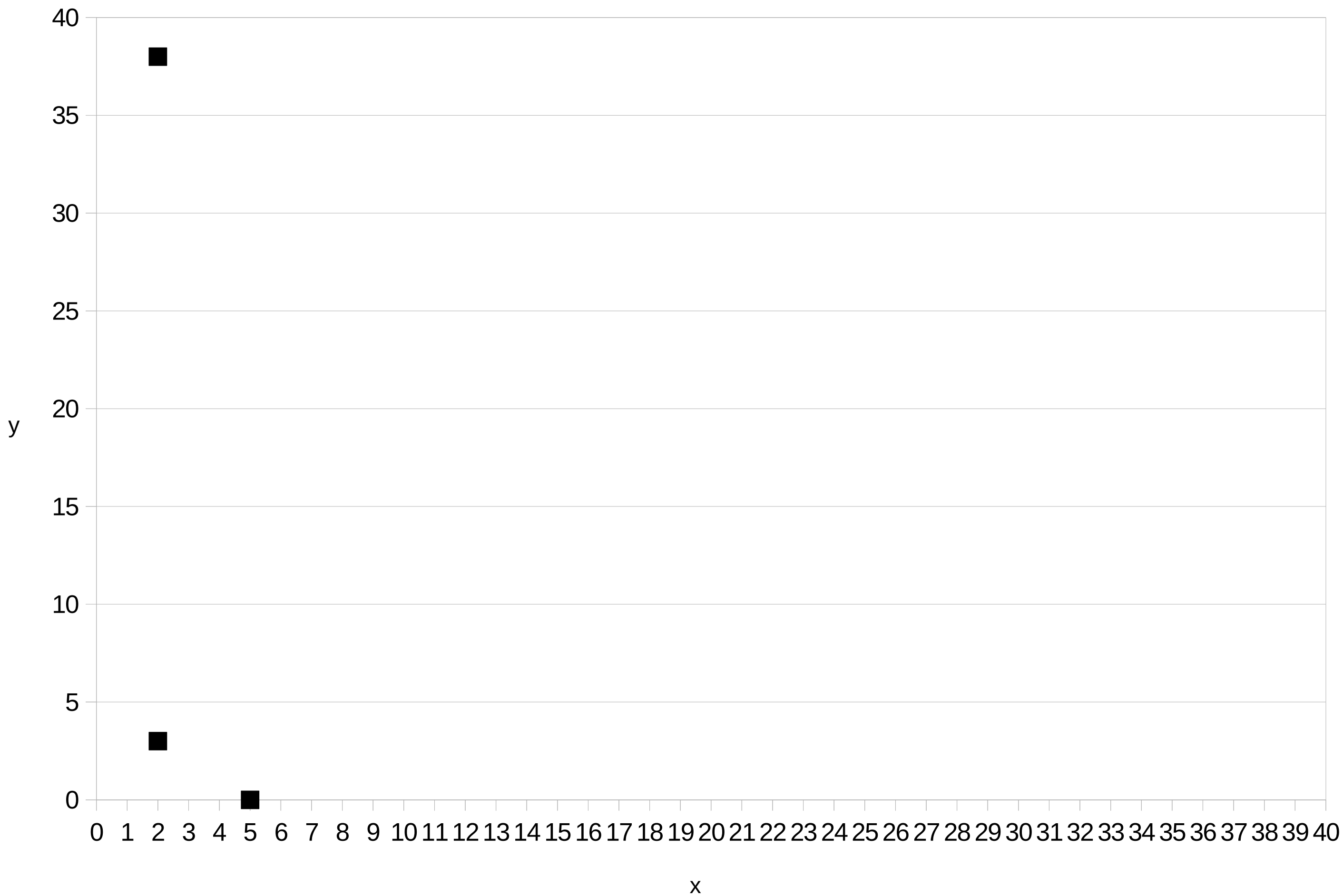
x	$y^2 (mod\, 41) \equiv x^3 - x + 3 \, (mod\, 41)$
2	3;



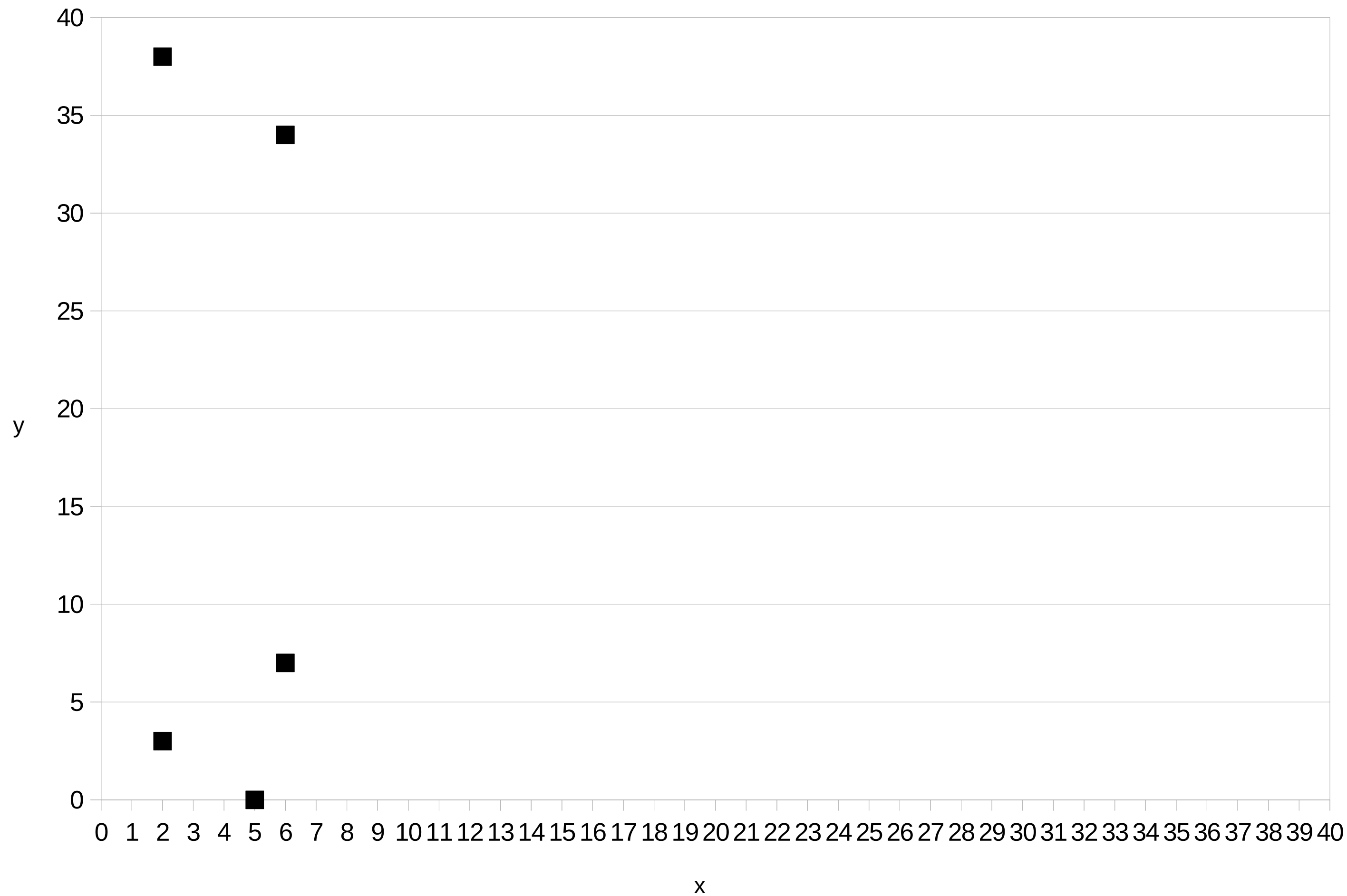
x	$y^2 (mod\ 41) \equiv x^3 - x + 3\ (mod\ 41)$
2	3; 38



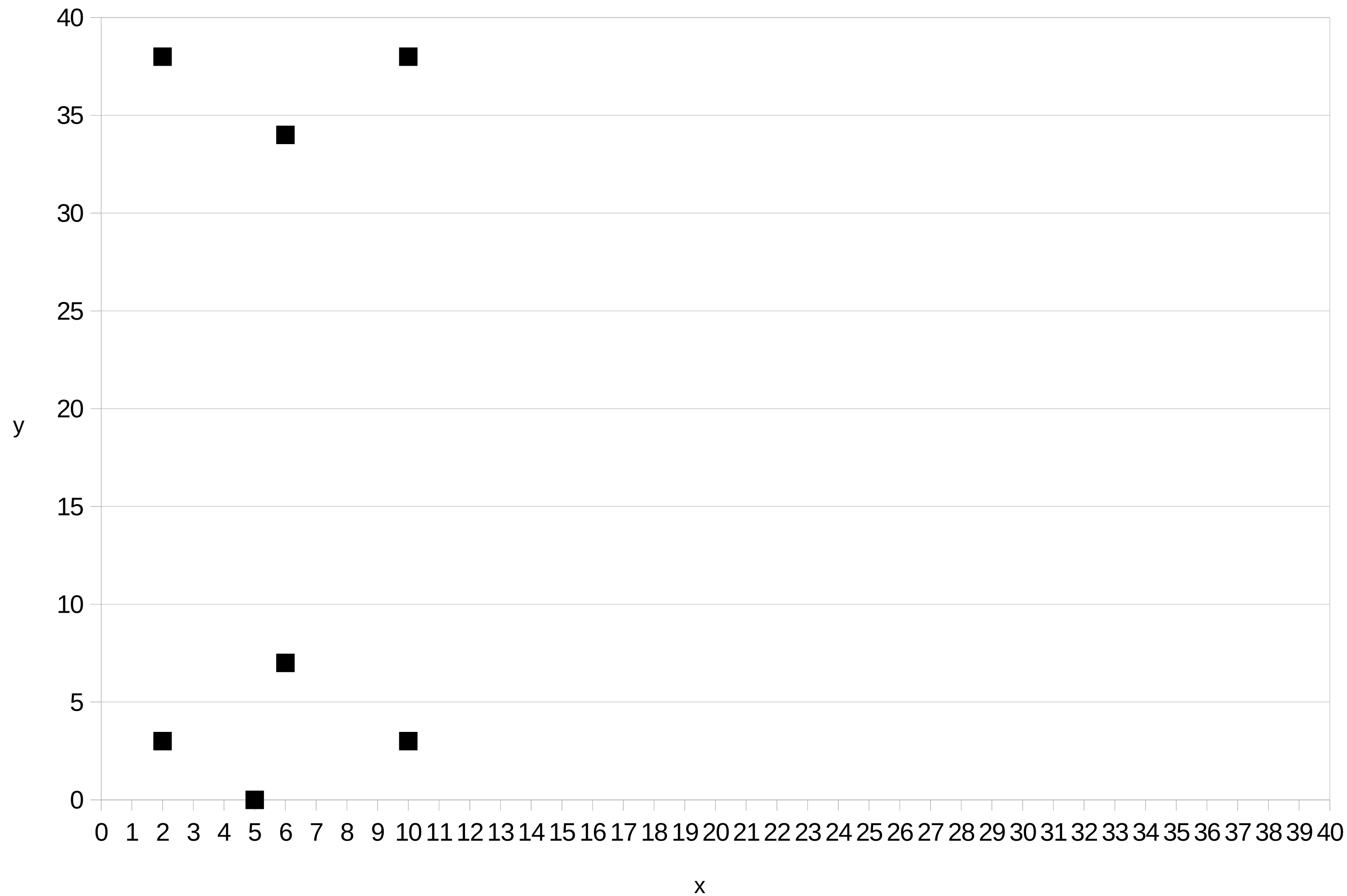
x	$y^2 \left(mod\, 41 \right) \equiv x^3 - x + 3 \left(mod\, 41 \right)$
2	3; 38
5	0



x	$y^2 (mod\, 41) \equiv x^3 - x + 3\, (mod\, 41)$
2	3; 38
5	0
6	7; 34



x	$y^2 (mod\ 41) \equiv x^3 - x + 3\ (mod\ 41)$
2	3; 38
5	0
6	7; 34
10	3; 38

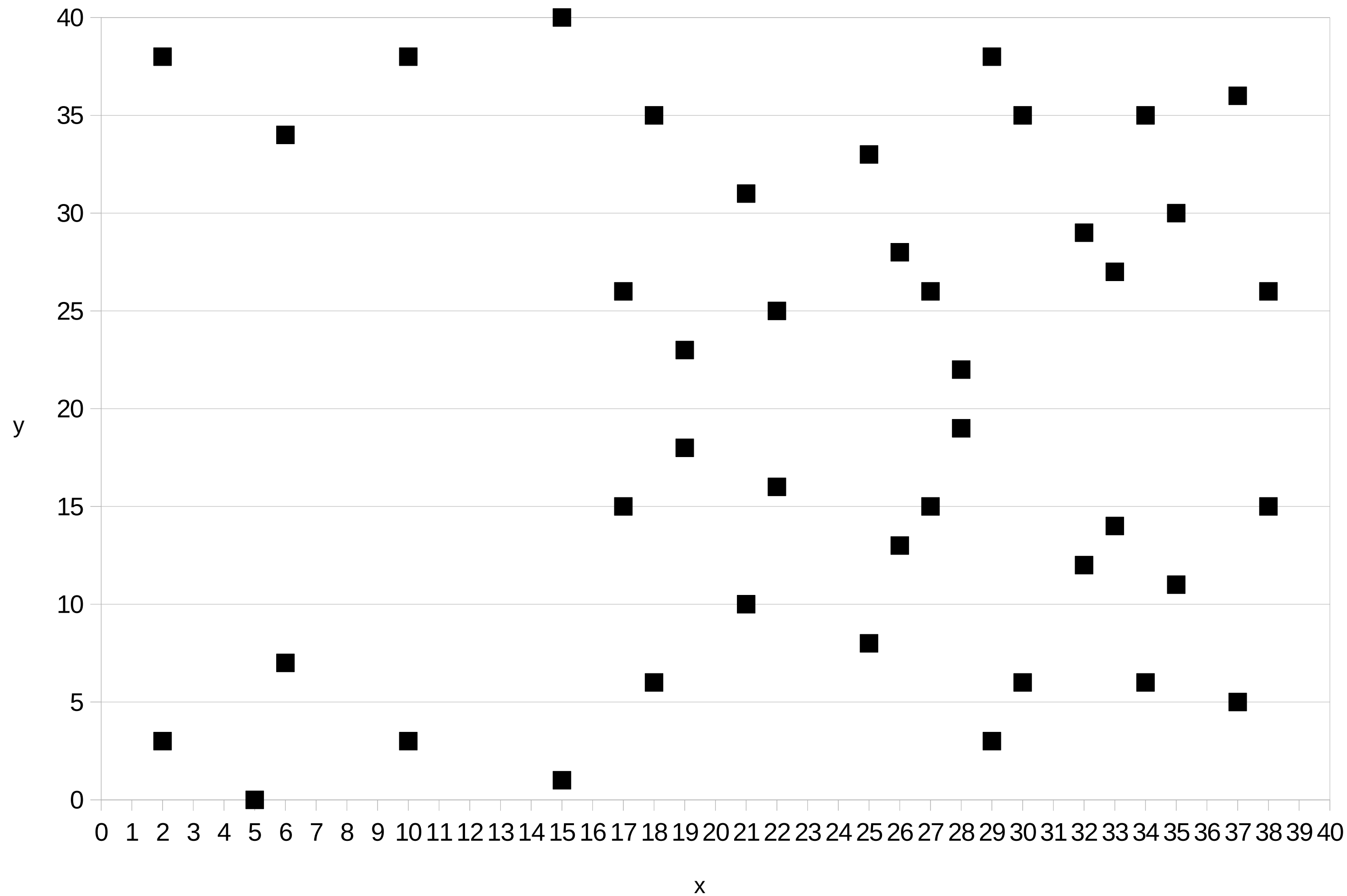


Fun with Certificates part II

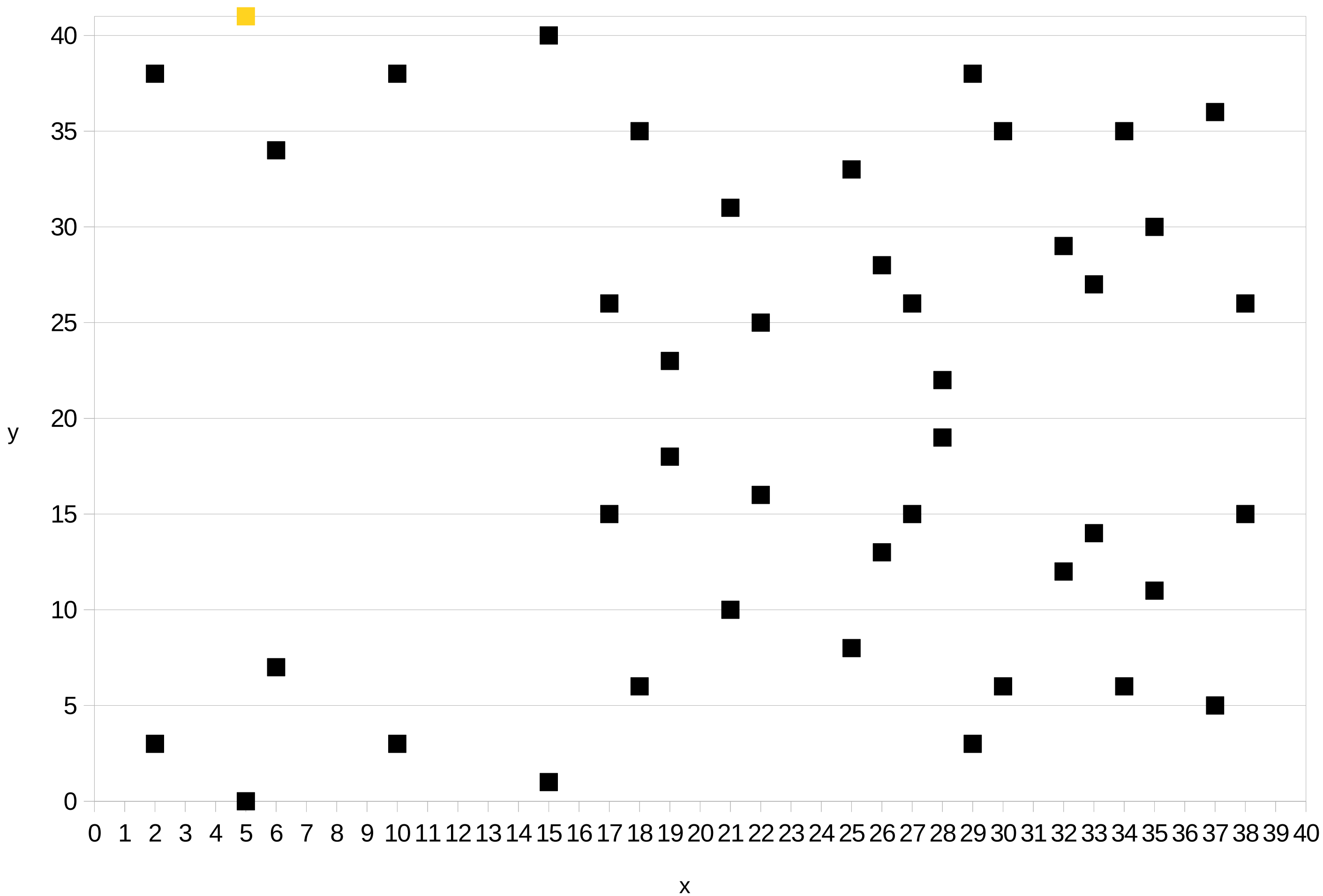
Elliptic Curve Cryptography

May 13, 2019

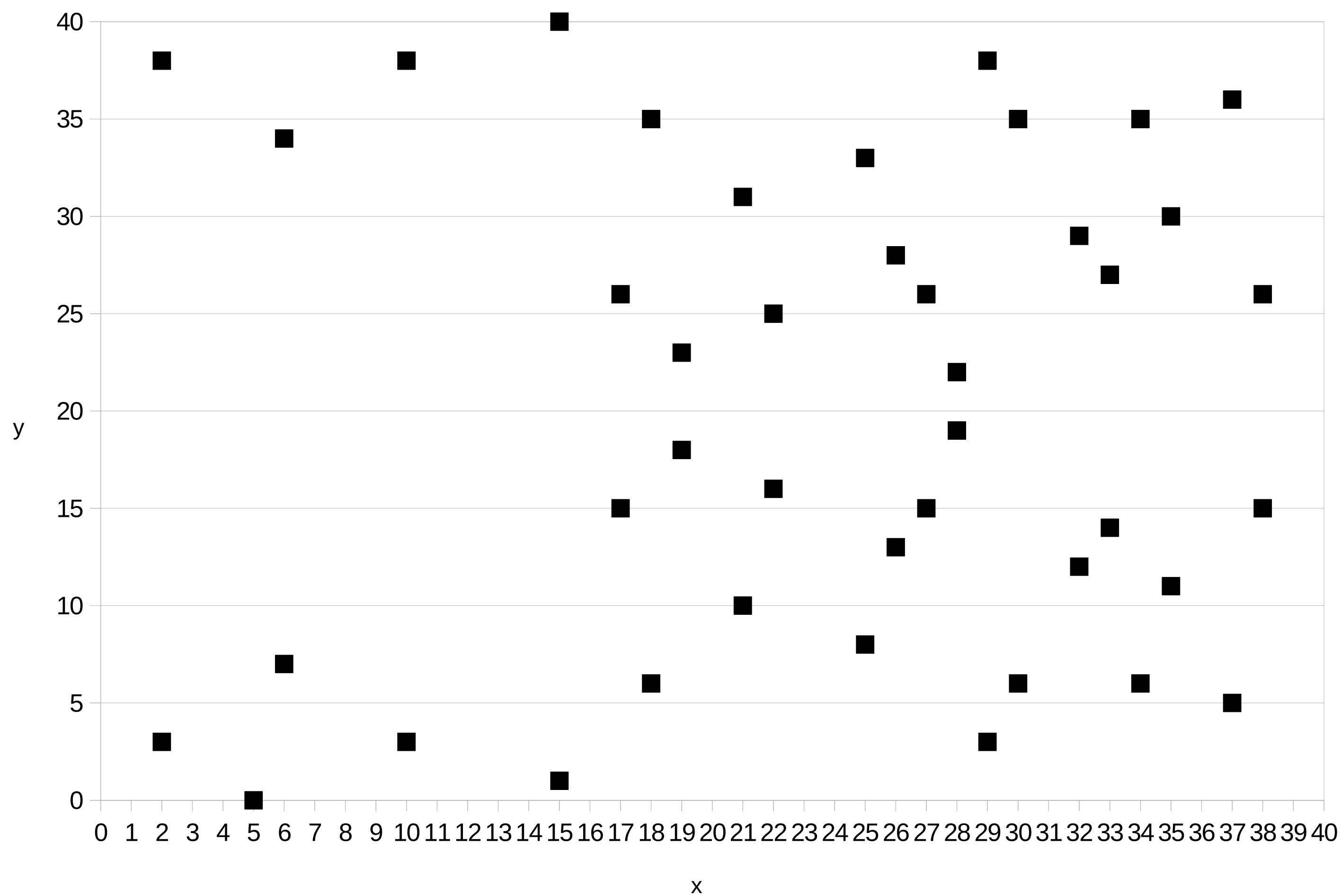
x	$y^2 (mod\, 41) \equiv x^3 - x + 3\, (mod\, 41)$
2	3; 38
5	0
6	7; 34
10	3; 38
15	1; 40
17	15; 26
18	6; 35
...	...



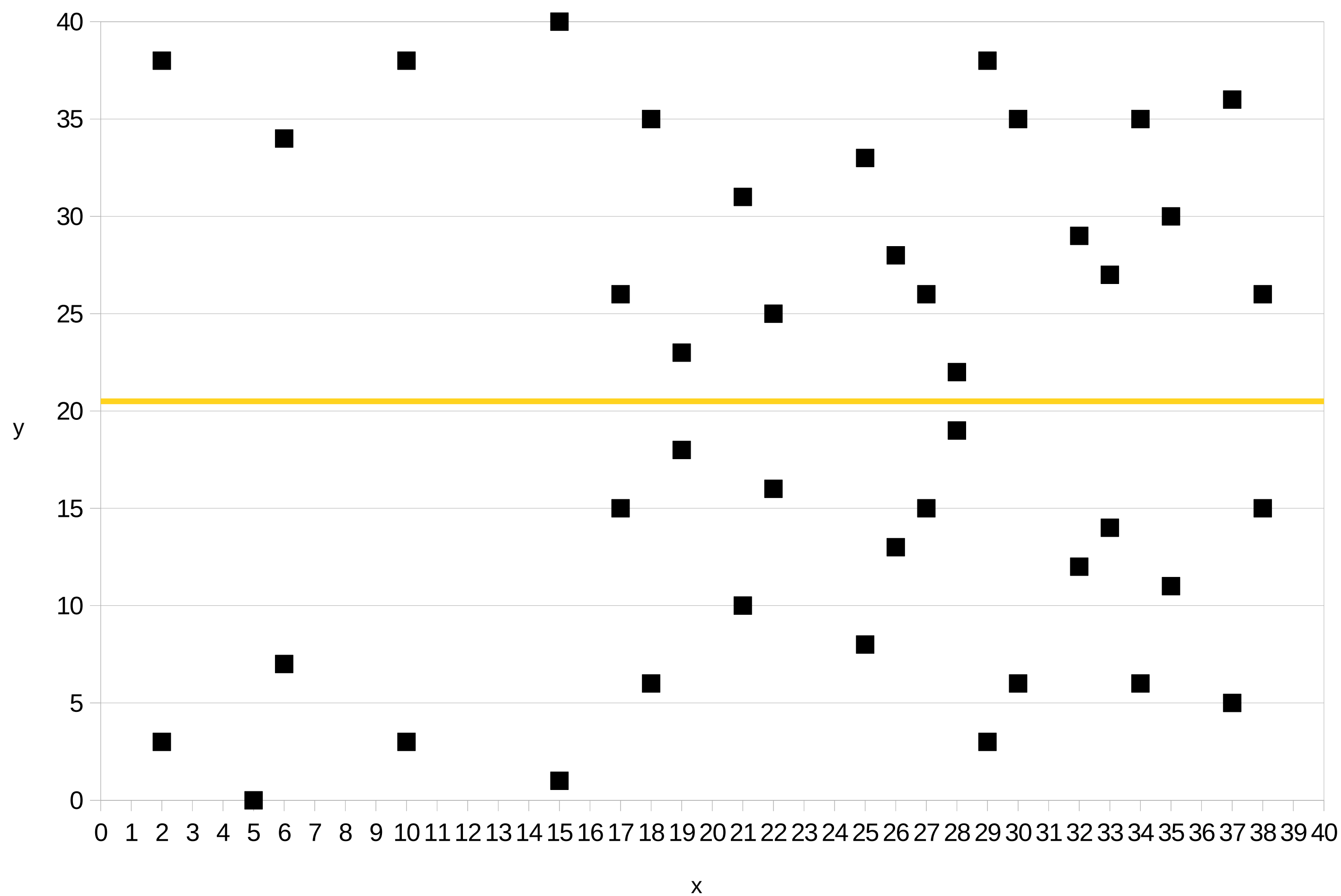
x	$y^2 \pmod{41} \equiv x^3 - x + 3 \pmod{41}$
2	3; 38
5	0; 41
6	7; 34
10	3; 38
15	1; 40
17	15; 26
18	6; 35
…	…



x	$y^2 \,(mod\, 41) \equiv x^3 - x + 3 \,(mod\, 41)$
2	3; 38
5	0
6	7; 34
10	3; 38
15	1; 40
17	15; 26
18	6; 35
...	...



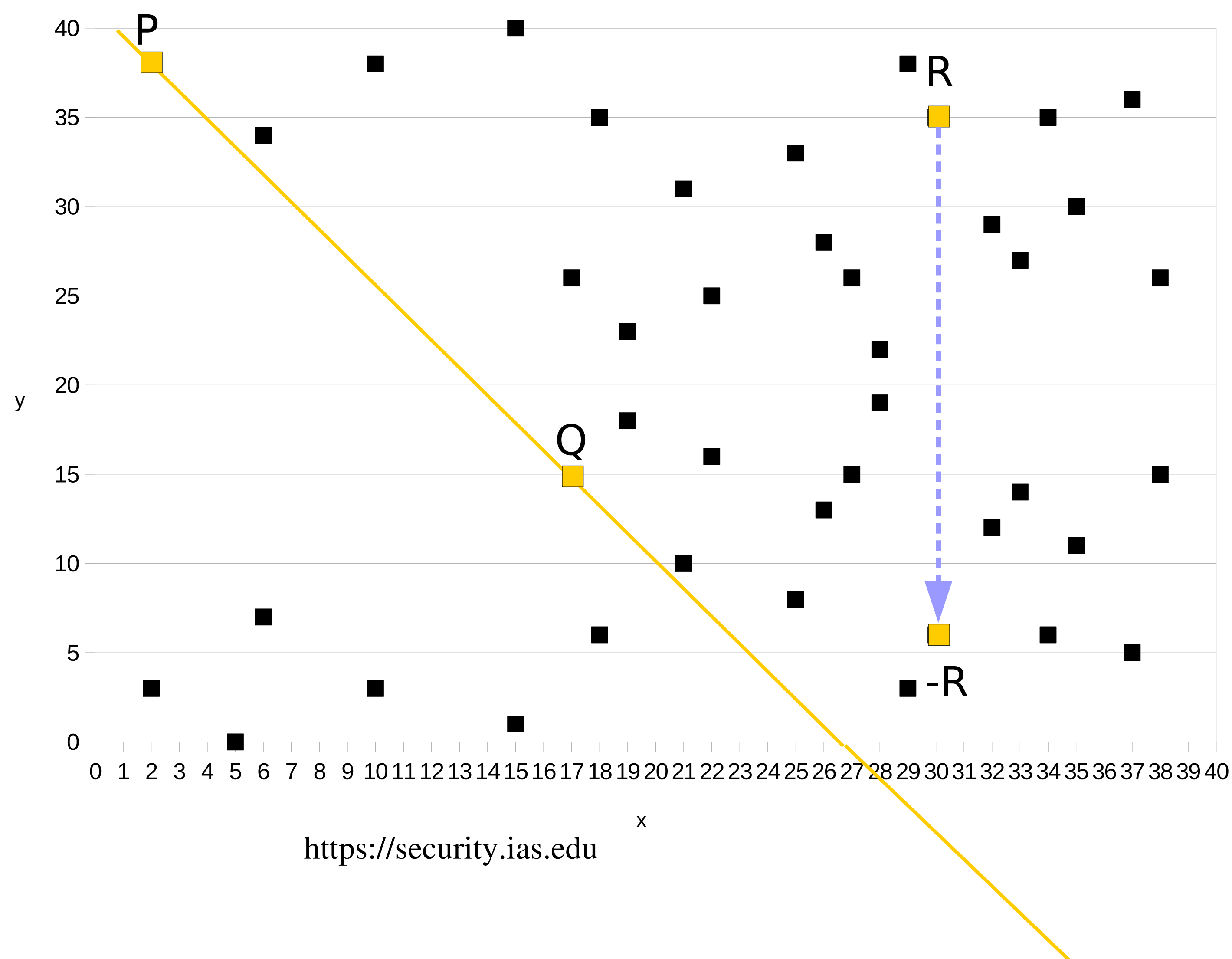
x	$y^2 (mod\, 41) \equiv x^3 - x + 3 \, (mod\, 41)$
2	3; 38
5	0
6	7; 34
10	3; 38
15	1; 40
17	15; 26
18	6; 35
…	…



Point Addition ⊕

- Draw a line between points P and Q
- Flip over at the sides, keep your slope
- When you hit the next point, flip to opposite side of the graph

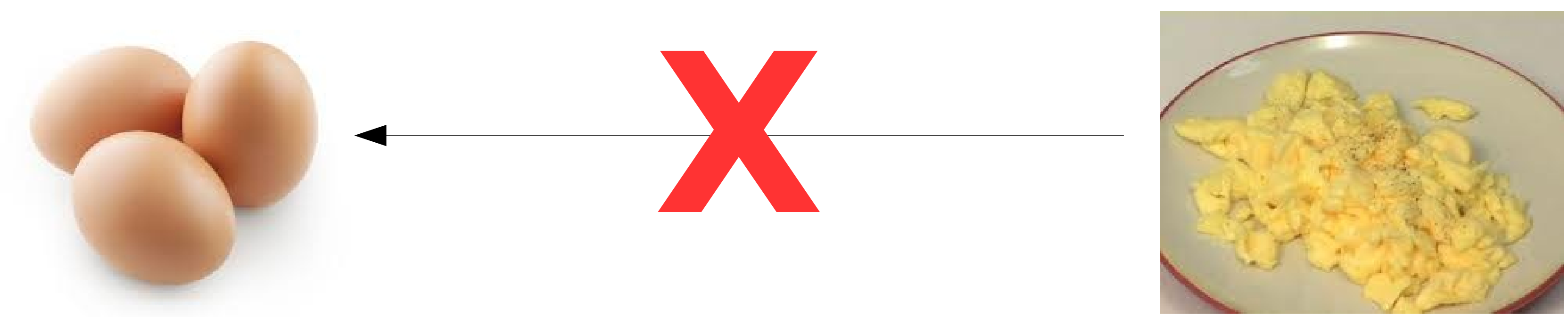
x	$y^2 \,(mod\, 41) \equiv x^3 - x + 3 \,(mod\, 41)$
2	3; 38
5	0
6	7; 34
10	3; 38
15	1; 40
17	15; 26
18	6; 35
…	…



P ⊕ Q ⊕ R = 0

P ⊕ Q = -R

One way function



One way function

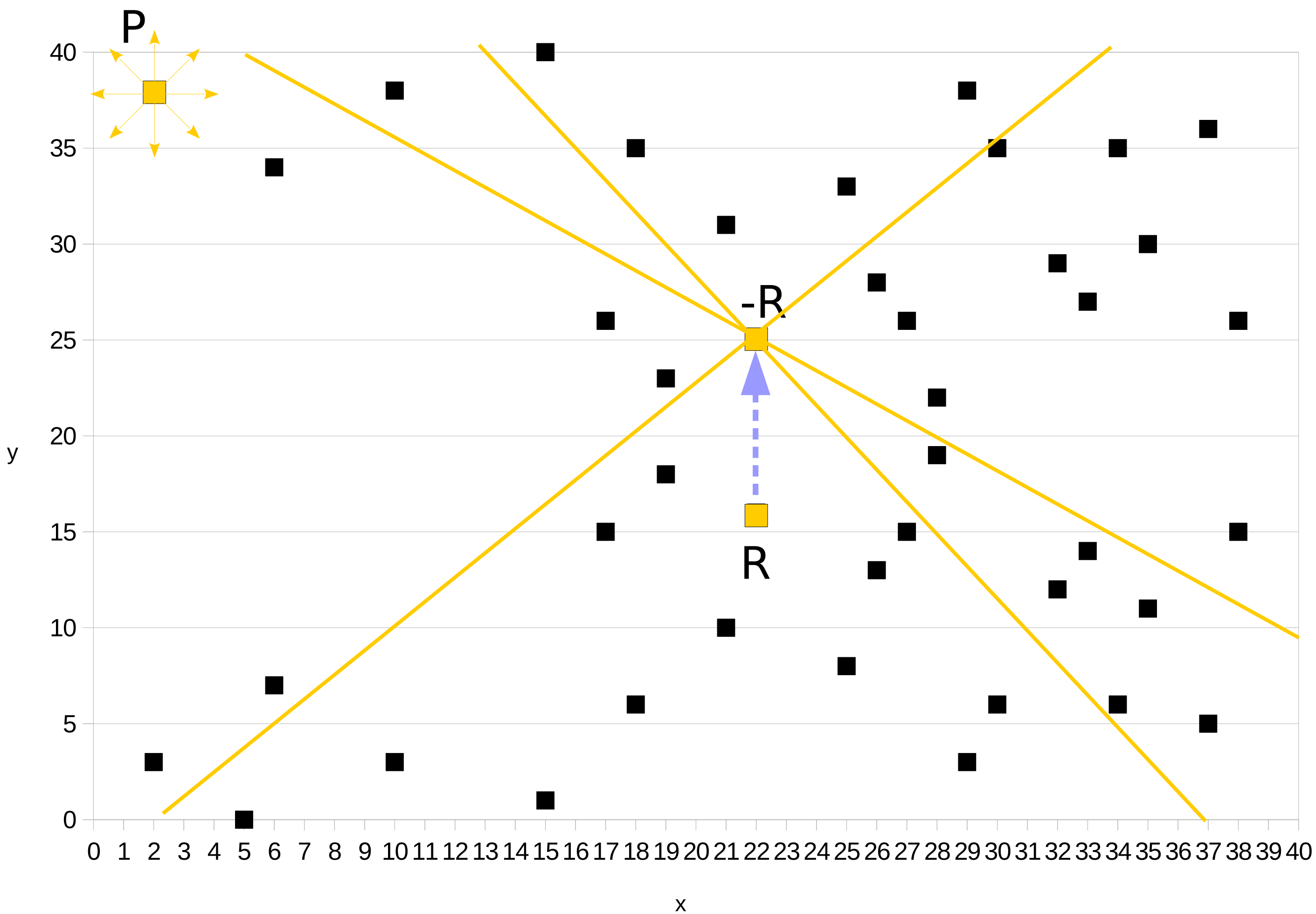
- Point addition ⊕ and multiplication ⊙ are easy
- Point subtraction ⊖ and division ⊘ are hard
- Given R, what are P & Q?

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

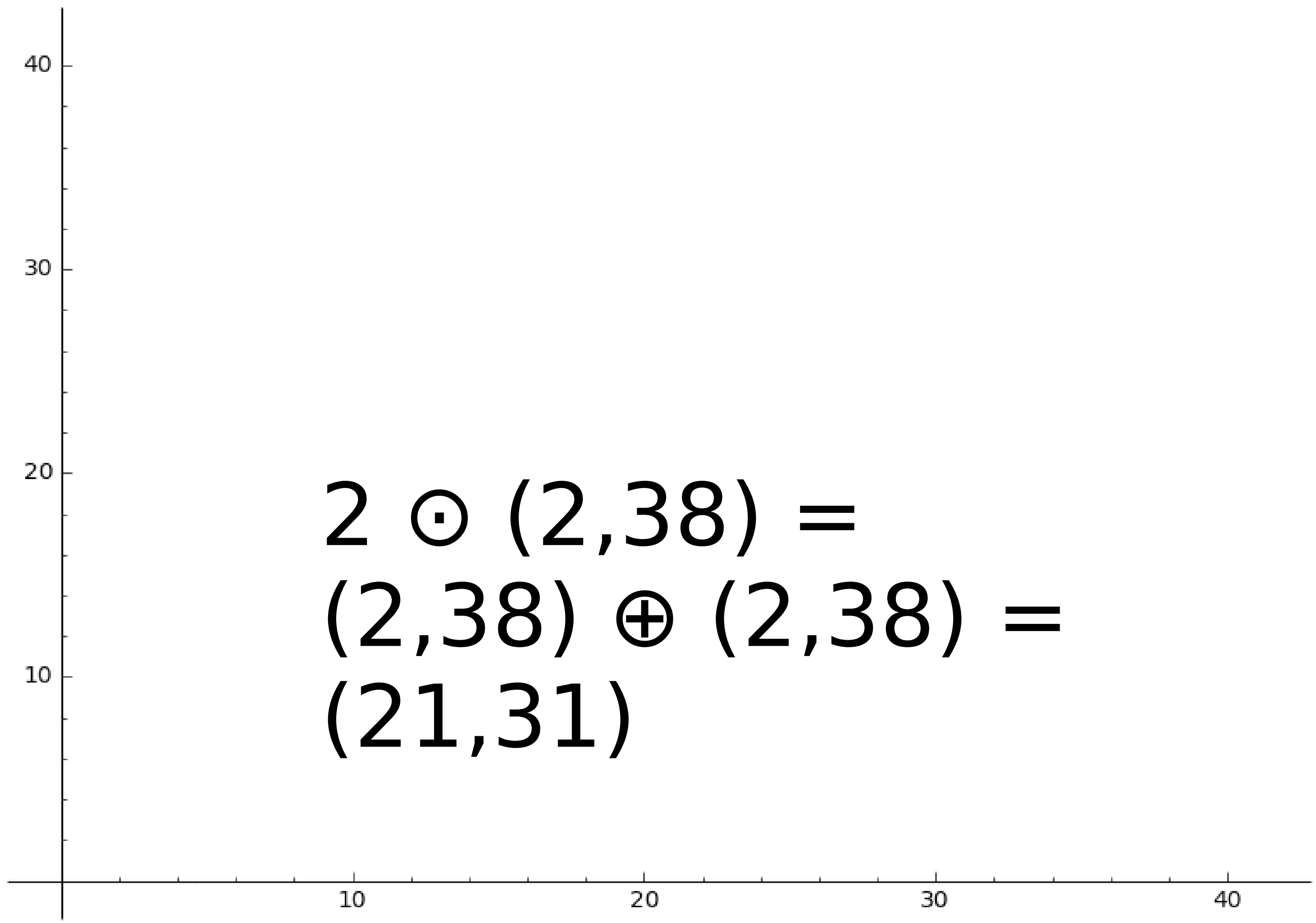
x	$y^2 (mod\ 41) \equiv x^3 - x + 3 (mod\ 41)$
2	3; 38
5	0
6	7; 34
10	3; 38
15	1; 40
17	15; 26
18	6; 35
…	…



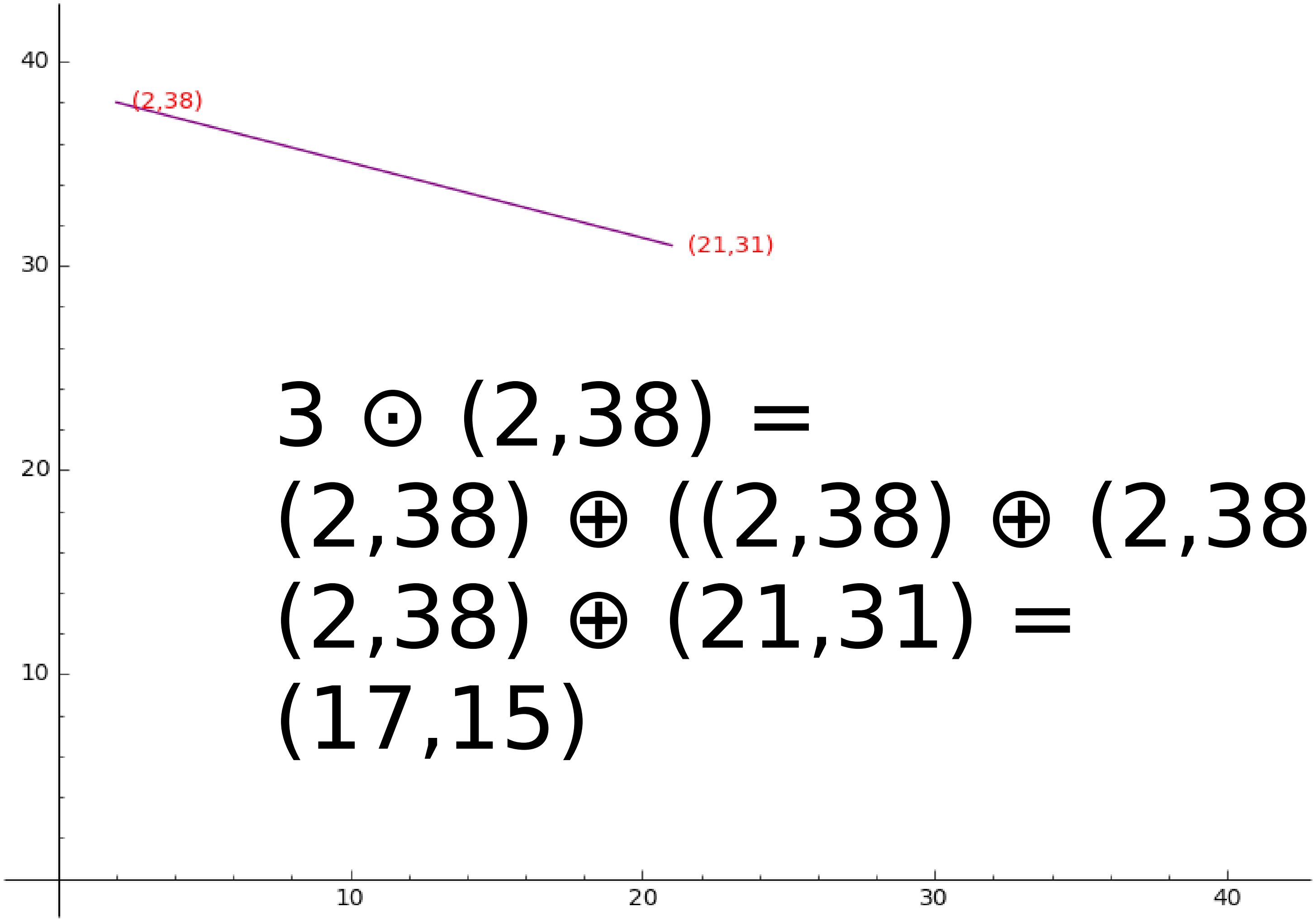
P + Q = -R

P + Q + R = 0

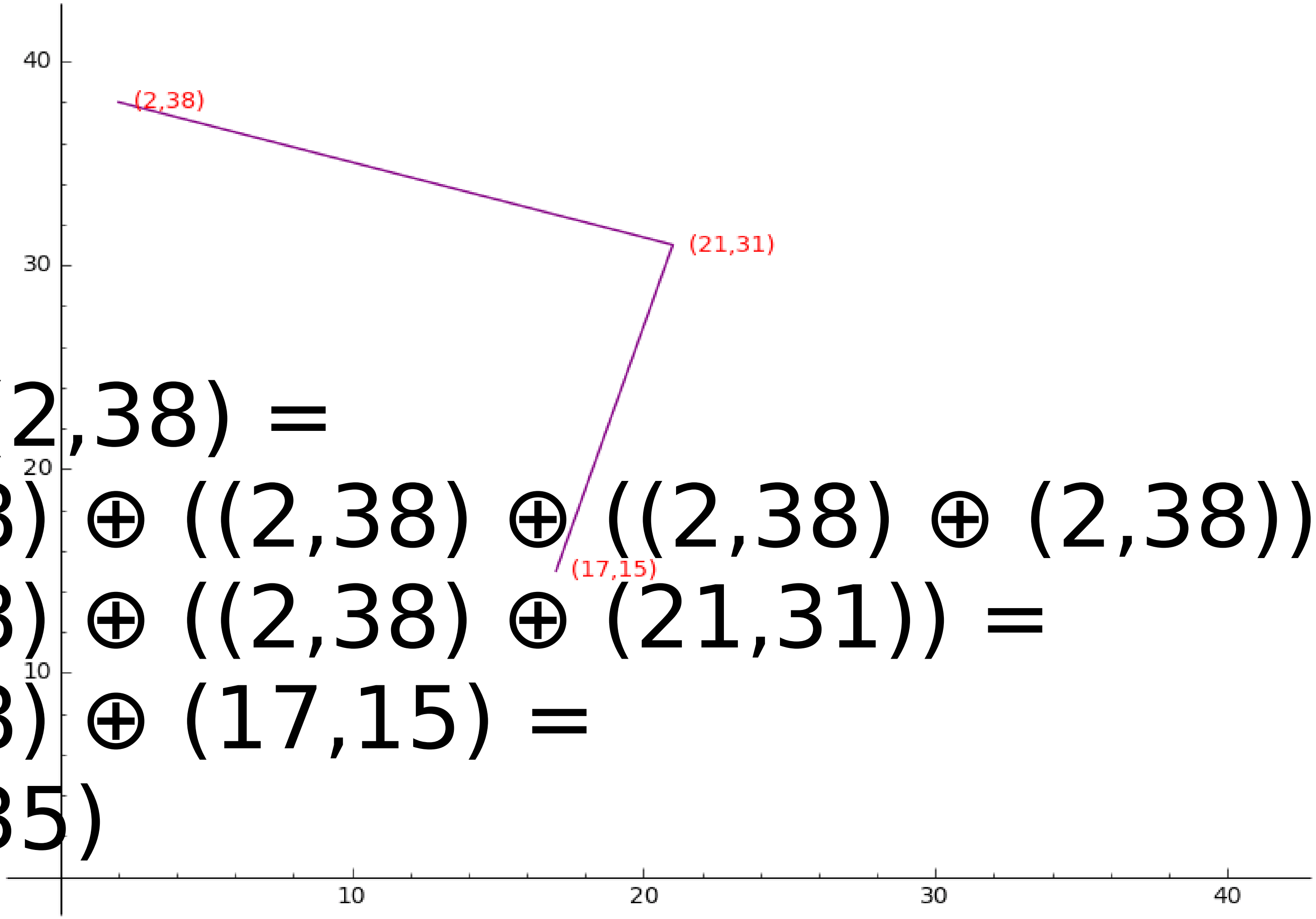
Point Multiplication ⊙



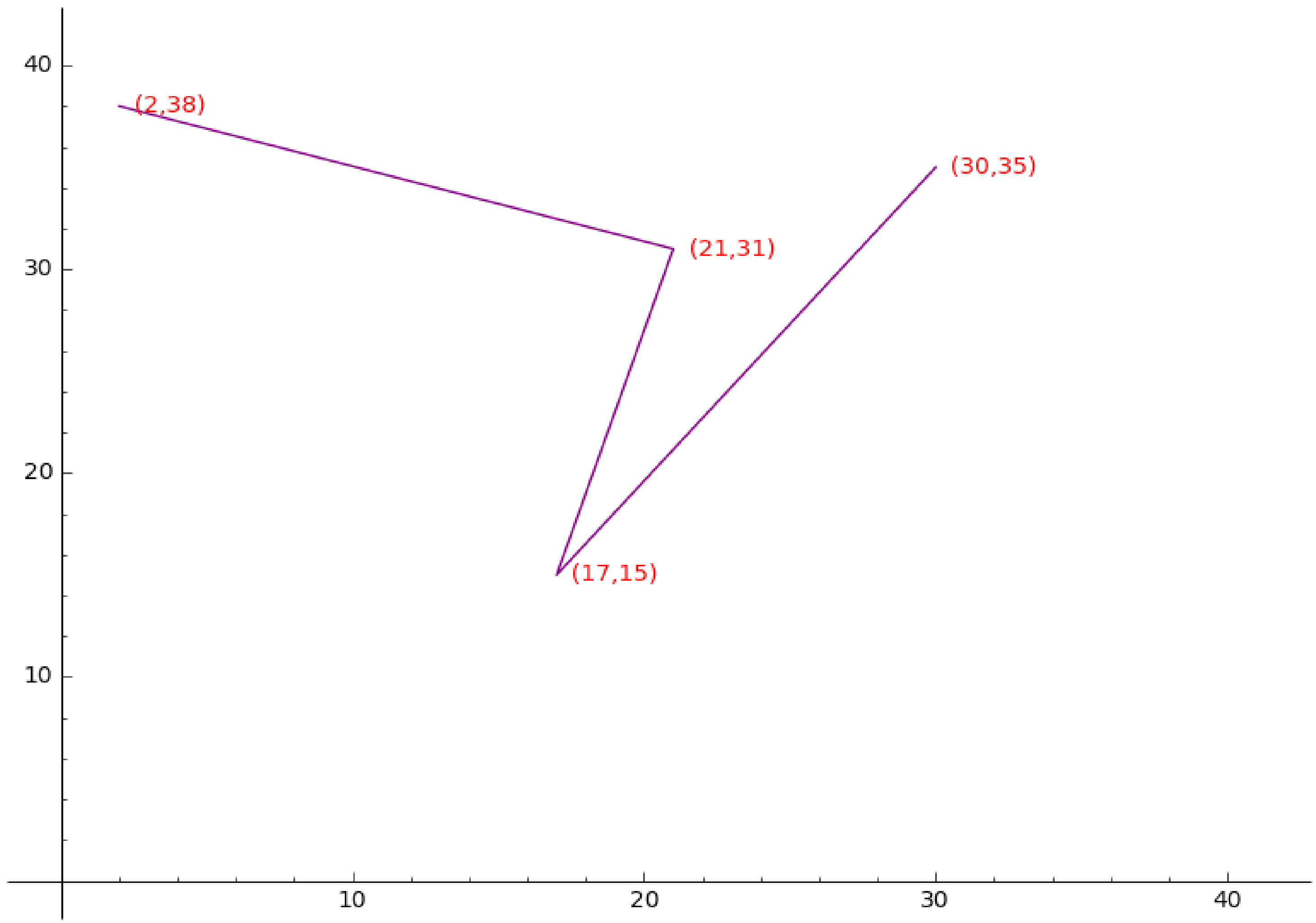
$$2 \odot (2,38) = (2,38) \oplus (2,38) = (21,31)$$

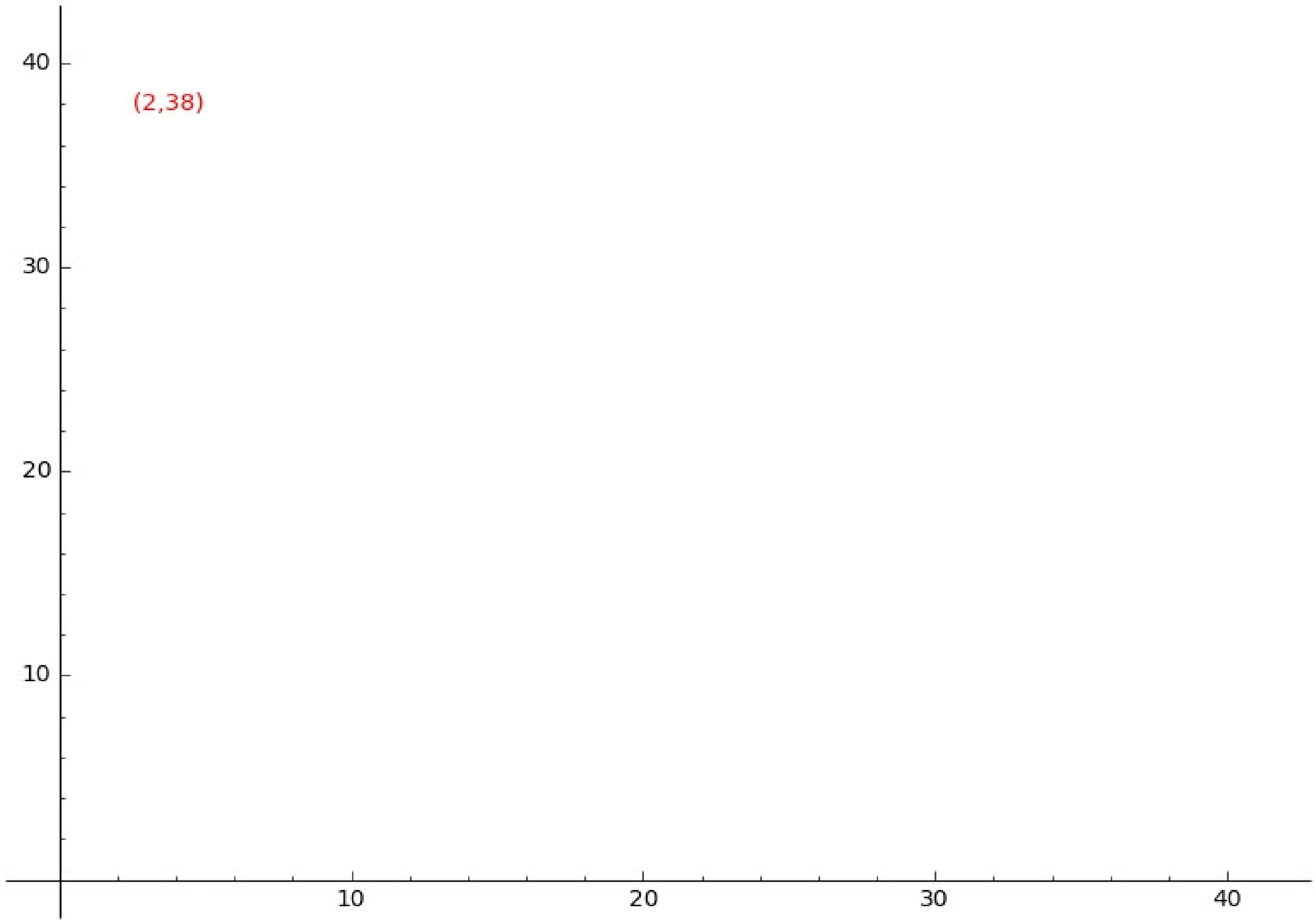


$3 \odot (2,38) =$
$(2,38) \oplus ((2,38) \oplus (2,38)) =$
$(2,38) \oplus (21,31) =$
$(17,15)$



$4 \odot (2,38) =$
$(2,38) \oplus ((2,38) \oplus ((2,38) \oplus (2,38))) =$
$(2,38) \oplus ((2,38) \oplus (21,31)) =$
$(2,38) \oplus (17,15) =$
$(30,35)$

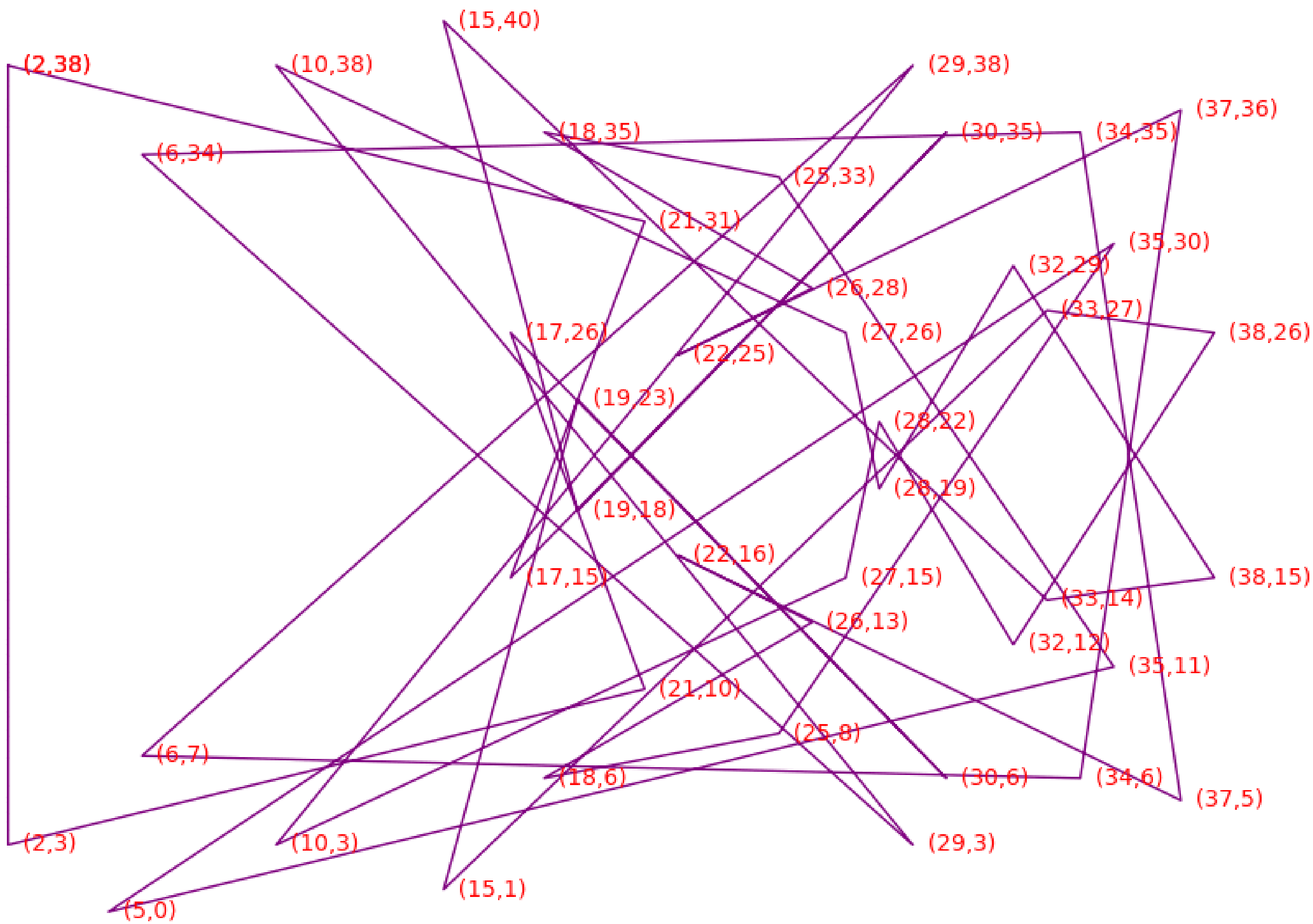

40
30
20
10
10
20
30
40
(2,38)
(30,35)
(21,31)
(17,15)


(2,38)
40
30
20
10
10
20
30
40

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

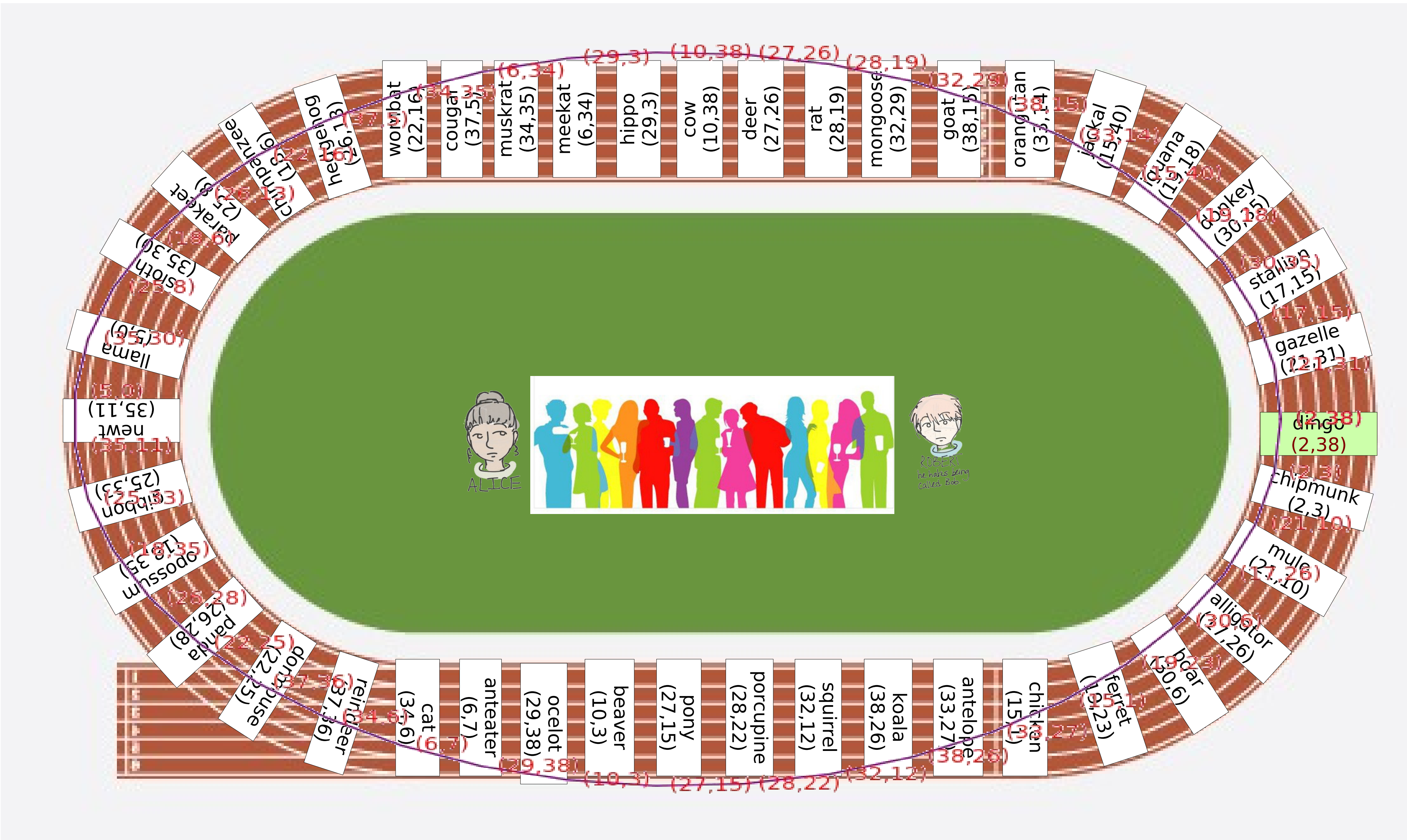


Network Security
Institute for Advanced Study

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019



And they lived happily ever after...

... until Dual_EC_DRBG

Dua ministic Randon EC_DRBG)

- Develope
- Approved
- RSA Secur
- Bruce Schne
- Edward Snowde ments revealing plot by NSA

Is ECC compromised then?

- No, but we have some trust issues.
- ANSI X9.62 (1999), IEEE P1363 (2000)?
- SEC 2 (2000), NIST FIPS 186-2 (2000)?
- ANSI X9.63 (2001), Brainpool (2005)?
- NSA Suite B (2005)?
- ANSSI FRP256V1 (2011)?

SafeCurves

- Choosing safe curves for elliptic-curve cryptography
- https://safecurves.cr.yp.to/

Million Dollar ECC curve

- Publicly verifiable randomness produced in February 2016 by many national lotteries
- http://cryptoexperts.github.io/million-dollar-curve/

And they lived happily ever after...

Hello? It's Eve here.
Did you forget about me?
I heard everything!

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019


ALICE
EVELYN
ROBERT
he hates being called Bob.

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

nkwwm

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

nkimmy Jimmy or(jq(Jimmy)

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

Jimmy orqql

Jimmy

Jimmy

Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019

Jimmy

Jimmy

(gddg)jg

Jimmy

Jimmy

ldg jg

Jimmy

Jimmy

(goteis)fs godg jg

Jimmy

tes fs got it

Jimmy

tes fs

got it

Jimmy

got it

Jimmy

RSA Certificates

- Subject (FQDN)
- Issuer (CA)
- Public Key
  - Modulus (n) product of two prime numbers
  - Public Exponent (e)
- x509 extensions
- Certificate Authority Signature

File Edit View Terminal Tabs Help

```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl x
509 -in fb.ias.edu.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 536270 (0x82ece)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness
CA-1
        Validity
            Not Before: Apr  9 20:45:24 2008 GMT
            Not After : Apr 10 20:45:24 2009 GMT
        Subject: C=US, O=fb.ias.edu, OU=GT63809955, OU=See www.rapidssl.com/reso
urces/cps (c)08, OU=Domain Control Validated - RapidSSL(R), CN=fb.ias.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b7:01:d0:51:16:4a:85:e6:2a:2f:2a:86:60:3a:
                    7b:51:eb:a7:52:f5:f2:09:8c:46:ab:2d:bf:11:4e:
                    a6:7d:f5:f5:b3:50:0d:4e:a5:48:23:fe:50:95:92:
                    63:25:03:54:46:35:4d:d8:c7:a2:0e:14:53:0e:0e:
                    3e:1e:3e:9d:19:f9:16:39:2e:00:f8:5d:92:ec:76:
                    ba:cb:8e:b3:86:b4:f9:ed:bd:1e:32:7a:bc:c7:cd:
                    f0:fb:c3:75:d7:34:1f:cb:1c:3a:cc:04:c9:4f:57:
                    d7:26:ef:75:27:22:49:66:5a:57:ef:47:cb:39:73:
                    70:bf:31:42:1d:40:70:9a:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encip
herment
            X509v3 Subject Key Identifier:
                2E:F0:33:FF:F0:DF:8D:88:A1:BD:A1:EA:B0:29:0B:81:E6:0D:25:0C
            X509v3 CRL Distribution Points:
                URI:http://crl.geotrust.com/crls/globalca1.crl

            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6
C

            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
    Signature Algorithm: md5WithRSAEncryption
        14:fa:0d:67:64:63:a4:58:47:f5:7f:73:1a:00:59:20:86:8a:
        f9:82:88:b5:6e:a2:82:6c:e3:8f:a0:bd:8b:f0:04:72:bb:49:
        7d:f6:4b:62:5a:1a:7e:7f:5b:43:d6:6e:27:f8:6d:50:2b:f7:
        ea:50:bd:94:f7:be:3f:3a:59:f6:a8:cd:66:f1:d7:9e:7d:43:
        6f:2c:a4:36:6a:eb:88:0f:4c:9b:ff:b6:cc:79:e4:ea:b2:9a:
        24:0f:93:75:5a:5e:42:a6:12:7e:2c:fa:20:25:46:fe:e3:bd:
        1b:e9:fa:52:5b:65:7b:a4:f1:e6:56:87:c1:34:5d:2a:49:e1:
        a4:26
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$
```

File Edit View Terminal Tabs Help

```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl x
509 -in fb.ias.edu.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 536270 (0x82ece)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness
CA-1
        Validity
            Not Before: Apr  9 20:45:24 2008 GMT
            Not After : Apr 10 20:45:24 2009 GMT
        Subject: C=US, O=fb.ias.edu, OU=GT63809955, OU=See www.rapidssl.com/reso
urces/cps (c)08, OU=Domain Control Validated - RapidSSL(R), CN=fb.ias.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b7:01:d0:51:16:4a:85:e6:2a:2f:2a:86:60:3a:
                    7b:51:eb:a7:52:f5:f2:09:8c:46:ab:2d:bf:11:4e:
                    a6:7d:f5:f5:b3:50:0d:4e:a5:48:23:fe:50:95:92:
                    63:25:03:54:46:35:4d:d8:c7:a2:0e:14:53:0e:0e:
                    3e:1e:3e:9d:19:f9:16:39:2e:00:f8:5d:92:ec:76:
                    ba:cb:8e:b3:86:b4:f9:ed:bd:1e:32:7a:bc:c7:cd:
                    f0:fb:c3:75:d7:34:1f:cb:1c:3a:cc:04:c9:4f:57:
                    d7:26:ef:75:27:22:49:66:5a:57:ef:47:cb:39:73:
                    70:bf:31:42:1d:40:70:9a:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encip
herment
            X509v3 Subject Key Identifier:
                2E:F0:33:FF:F0:DF:8D:88:A1:BD:A1:EA:B0:29:0B:81:E6:0D:25:0C
            X509v3 CRL Distribution Points:
                URI:http://crl.geotrust.com/crls/globalca1.crl

            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6
C

            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
    Signature Algorithm: md5WithRSAEncryption
        14:fa:0d:67:64:63:a4:58:47:f5:7f:73:1a:00:59:20:86:8a:
        f9:82:88:b5:6e:a2:82:6c:e3:8f:a0:bd:8b:f0:04:72:bb:49:
        7d:f6:4b:62:5a:1a:7e:7f:5b:43:d6:6e:27:f8:6d:50:2b:f7:
        ea:50:bd:94:f7:be:3f:3a:59:f6:a8:cd:66:f1:d7:9e:7d:43:
        6f:2c:a4:36:6a:eb:88:0f:4c:9b:ff:b6:cc:79:e4:ea:b2:9a:
        24:0f:93:75:5a:5e:42:a6:12:7e:2c:fa:20:25:46:fe:e3:bd:
        1b:e9:fa:52:5b:65:7b:a4:f1:e6:56:87:c1:34:5d:2a:49:e1:
        a4:26
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$
```

ECC Certificates

- Subject (FQDN)
- Issuer (CA)
- Public Key
  - Curve
  - Generator (start)
  - Public x,y coordinate
- x509 extensions
- Certificate Authority Signature

RSA

ep@epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates_part2_20170502 84x54

```
penssl x509 -text -noout -in fb.ias.edu.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 536270 (0x82ece)
    Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
        Validity
            Not Before: Apr  9 20:45:24 2008 GMT
            Not After : Apr 10 20:45:24 2009 GMT
        Subject: C=US, O=fb.ias.edu, OU=GT63809955, OU=See www.rapidssl.com/resource
s/cps (c)08, OU=Domain Control Validated - RapidSSL(R), CN=fb.ias.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b7:01:d0:51:16:4a:85:e6:2a:2f:2a:86:60:3a:
                    7b:51:eb:a7:52:f5:f2:09:8c:46:ab:2d:bf:11:4e:
                    a6:7d:f5:f5:b3:50:0d:4e:a5:48:23:fe:50:95:92:
                    63:25:03:54:46:35:4d:d8:c7:a2:0e:14:53:0e:0e:
                    3e:1e:3e:9d:19:f9:16:39:2e:00:f8:5d:92:ec:76:
                    ba:cb:8e:b3:86:b4:f9:ed:bd:1e:32:7a:bc:c7:cd:
                    f0:fb:c3:75:d7:34:1f:cb:1c:3a:cc:04:c9:4f:57:
                    d7:26:ef:75:27:22:49:66:5a:57:ef:47:cb:39:73:
                    70:bf:31:42:1d:40:70:9a:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherm
ent
            X509v3 Subject Key Identifier:
                2E:F0:33:FF:F0:DF:8D:88:A1:BD:A1:EA:B0:29:0B:81:E6:0D:25:0C
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.geotrust.com/crls/globalca1.crl

            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6C

            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
    Signature Algorithm: md5WithRSAEncryption
         14:fa:0d:67:64:63:a4:58:47:f5:7f:73:1a:00:59:20:86:8a:
         f9:82:88:b5:6e:a2:82:6c:e3:8f:a0:bd:8b:f0:04:72:bb:49:
         7d:f6:4b:62:5a:1a:7e:7f:5b:43:d6:6e:27:f8:6d:50:2b:f7:
         ea:50:bd:94:f7:be:3f:3a:59:f6:a8:cd:66:f1:d7:9e:7d:43:
         6f:2c:a4:36:6a:eb:88:0f:4c:9b:ff:b6:cc:79:e4:ea:b2:9a:
         24:0f:93:75:5a:5e:42:a6:12:7e:2c:fa:20:25:46:fe:e3:bd:
         1b:e9:fa:52:5b:65:7b:a4:f1:e6:56:87:c1:34:5d:2a:49:e1:
         a4:26
[2]epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates_part2_20170502$
```

ECC

ep@epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates_part2_20170502 84x54

```
        Version: 3 (0x2)
        Serial Number:
            d4:16:55:2c:dc:22:dd:cc
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=New Jersey, O=Institute for Advanced Study, CN=myfakesite.i
as.edu/emailAddress=bepstein@ias.edu
        Validity
            Not Before: Apr 30 22:17:09 2017 GMT
            Not After : Apr 30 22:17:09 2018 GMT
        Subject: C=US, ST=New Jersey, O=Institute for Advanced Study, CN=myfakesite.
ias.edu/emailAddress=bepstein@ias.edu
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:16:1a:c8:0f:7a:20:01:50:40:9e:84:a2:d7:fe:
                    85:87:0e:98:4f:e2:13:c9:a4:5d:96:33:46:9b:d9:
                    84:20:d5:5a:2c:89:59:17:bd:e2:7d:33:eb:35:4c:
                    bc:c9:08:70:9f:39:61:06:15:17:94:48:a9:0c:82:
                    0c:6c:fa:71:e5
                Field Type: prime-field
                Prime:
                    00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
                    ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:fe:ff:
                    ff:fc:2f
                A:    0
                B:    7 (0x7)
                Generator (uncompressed):
                    04:79:be:66:7e:f9:dc:bb:ac:55:a0:62:95:ce:87:
                    0b:07:02:9b:fc:db:2d:ce:28:d9:59:f2:81:5b:16:
                    f8:17:98:48:3a:da:77:26:a3:c4:65:5d:a4:fb:fc:
                    0e:11:08:a8:fd:17:b4:48:a6:85:54:19:9c:47:d0:
                    8f:fb:10:d4:b8
                Order:
                    00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
                    ff:fe:ba:ae:dc:e6:af:48:a0:3b:bf:d2:5e:8c:d0:
                    36:41:41
                Cofactor:  1 (0x1)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                06:41:4F:30:B6:5E:F0:93:6C:26:69:54:A2:0E:09:22:A8:3B:B8:09
            X509v3 Authority Key Identifier:
                keyid:06:41:4F:30:B6:5E:F0:93:6C:26:69:54:A2:0E:09:22:A8:3B:B8:09

    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:21:00:e8:48:02:68:1a:63:06:ee:d1:0d:e6:48:c4:
         41:8b:07:7a:08:4e:5a:96:e8:83:d0:08:9b:62:9b:9b:07:c2:
         05:02:20:21:59:67:5d:cc:54:ae:c8:63:54:e2:de:66:f3:7f:
         1c:b5:39:f9:70:ef:5d:e6:3e:78:24:84:6e:df:26:8b:5e
[2]epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates_part2_20170502$
```

RSA Private Keys

- Private Key
  - Modulus (n) product of two prime numbers (p*q)
  - Public Exponent (e)
  - Private Exponent (d)
  - Prime1 (p)
  - Prime2 (q)

File Edit View Terminal Tabs Help

```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl r
sa -in regular.key -text -noout
Private-Key: (512 bit)
modulus:
    00:c4:a4:bb:01:fb:af:06:5b:ce:11:1e:af:39:3c:
    24:21:af:12:c8:c5:ec:ac:bc:03:98:01:c5:e0:dd:
    b3:27:20:8d:64:a9:39:0d:4d:7a:03:6a:8e:a1:e3:
    86:b9:d7:5d:60:7c:40:1e:ea:51:3d:55:6e:f4:d1:
    76:63:92:81:b3
publicExponent: 65537 (0x10001)
privateExponent:
    00:c2:fb:f4:d2:ca:95:8a:60:8d:bc:3c:08:d3:5f:
    e7:13:df:5d:68:e7:98:fe:ce:8f:61:b2:a0:5b:90:
    79:8c:58:e5:e5:4e:a3:b3:f7:6f:f2:42:8f:cc:75:
    e4:07:6b:88:d0:9e:bc:5b:57:86:f3:59:ee:4e:15:
    98:ad:54:fe:c1
prime1:
    00:e1:55:70:0d:8d:eb:f5:68:3d:4a:d3:bc:0d:07:
    9d:5c:c4:fd:02:7d:69:ea:f7:f8:d5:01:5e:01:75:
    16:98:4f
prime2:
    00:df:67:bb:7b:79:39:19:8a:9f:0f:1d:84:ea:b0:
    8e:d7:4e:49:34:22:f3:a4:78:9a:35:22:0c:07:26:
    d7:c3:5d
exponent1:
    6b:c7:85:00:46:b8:ed:39:fd:cf:33:b5:87:f9:f3:
    6f:f3:1d:1d:ba:c5:15:c9:a4:30:a6:25:c3:c6:b0:
    97:0b
exponent2:
    00:94:84:31:6e:f4:37:b1:73:26:2a:b6:45:16:80:
    29:75:98:e5:b1:73:4a:e5:9c:07:68:2b:2a:33:d6:
    ee:b9:41
coefficient:
    00:9b:04:15:53:4e:49:10:1d:f0:76:48:bc:11:b5:
    c9:d8:0a:6a:dc:49:41:84:48:d4:d4:5b:8f:51:a0:
    42:60:d6
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$
```

ECC Private Keys

- Private Key
  - Private number (how many steps)
  - Public x,y coordinate
  - Public Generator (starting point)
  - Curve

RSA

```
[2]epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates
_part2_20170502$ openssl rsa -in regular.key -text -noout
Private-Key: (512 bit)
modulus:
    00:c4:a4:bb:01:fb:af:06:5b:ce:11:1e:af:39:3c:
    24:21:af:12:c8:c5:ec:ac:bc:03:98:01:c5:e0:dd:
    b3:27:20:8d:64:a9:39:0d:4d:7a:03:6a:8e:a1:e3:
    86:b9:d7:5d:60:7c:40:1e:ea:51:3d:55:6e:f4:d1:
    76:63:92:81:b3
publicExponent: 65537 (0x10001)
privateExponent:
    00:c2:fb:f4:d2:ca:95:8a:60:8d:bc:3c:08:d3:5f:
    e7:13:df:5d:68:e7:98:fe:ce:8f:61:b2:a0:5b:90:
    79:8c:58:e5:e5:4e:a3:b3:f7:6f:f2:42:8f:cc:75:
    e4:07:6b:88:d0:9e:bc:5b:57:86:f3:59:ee:4e:15:
    98:ad:54:fe:c1
prime1:
    00:e1:55:70:0d:8d:eb:f5:68:3d:4a:d3:bc:0d:07:
    9d:5c:c4:fd:02:7d:69:ea:f7:f8:d5:01:5e:01:75:
    16:98:4f
prime2:
    00:df:67:bb:7b:79:39:19:8a:9f:0f:1d:84:ea:b0:
    8e:d7:4e:49:34:22:f3:a4:78:9a:35:22:0c:07:26:
    d7:c3:5d
exponent1:
    6b:c7:85:00:46:b8:ed:39:fd:cf:33:b5:87:f9:f3:
    6f:f3:1d:1d:ba:c5:15:c9:a4:30:a6:25:c3:c6:b0:
    97:0b
exponent2:
    00:94:84:31:6e:f4:37:b1:73:26:2a:b6:45:16:80:
    29:75:98:e5:b1:73:4a:e5:9c:07:68:2b:2a:33:d6:
    ee:b9:41
coefficient:
    00:9b:04:15:53:4e:49:10:1d:f0:76:48:bc:11:b5:
    c9:d8:0a:6a:dc:49:41:84:48:d4:d4:5b:8f:51:a0:
    42:60:d6
[2]epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates
_part2_20170502$
```

ECC

```
[2]epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates
_part2_20170502$ openssl ec -in sample_ecc.key -text -noout
read EC key
Private-Key: (256 bit)
priv:
    5e:a1:bc:ba:2f:ee:5d:a9:85:21:19:56:09:d9:c6:
    09:66:59:93:fd:c6:7d:bc:51:ba:69:76:ba:2e:70:
    ac:30
pub:
    04:16:1a:c8:0f:7a:20:01:50:40:9e:84:a2:d7:fe:
    85:87:0e:98:4f:e2:13:c9:a4:5d:96:33:46:9b:d9:
    84:20:d5:5a:2c:89:59:17:bd:e2:7d:33:eb:35:4c:
    bc:c9:08:70:9f:39:61:06:15:17:94:48:a9:0c:82:
    0c:6c:fa:71:e5
Field Type: prime-field
Prime:
    00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:fe:ff:
    ff:fc:2f
A:    0
B:    7 (0x7)
Generator (uncompressed):
    04:79:be:66:7e:f9:dc:bb:ac:55:a0:62:95:ce:87:
    0b:07:02:9b:fc:db:2d:ce:28:d9:59:f2:81:5b:16:
    f8:17:98:48:3a:da:77:26:a3:c4:65:5d:a4:fb:fc:
    0e:11:08:a8:fd:17:b4:48:a6:85:54:19:9c:47:d0:
    8f:fb:10:d4:b8
Order:
    00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:fe:ba:ae:dc:e6:af:48:a0:3b:bf:d2:5e:8c:d0:
    36:41:41
Cofactor:  1 (0x1)
[2]epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates
[2]epmacpro:~/Dropbox/doc/ias/security_talks/fun_with_certificates
_part2_20170502$
```


ALICE


EVELYN

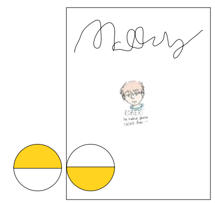

ROBERT
he hates being called Bob.

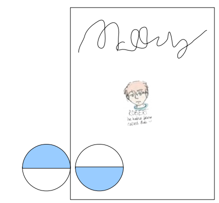

MALLORY

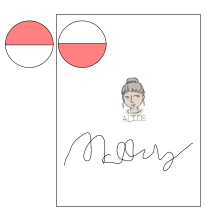
Fun with Certificates part II

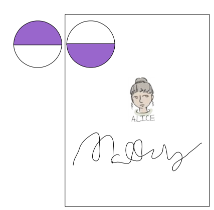
Elliptic Curve Cryptography

May 13, 2019





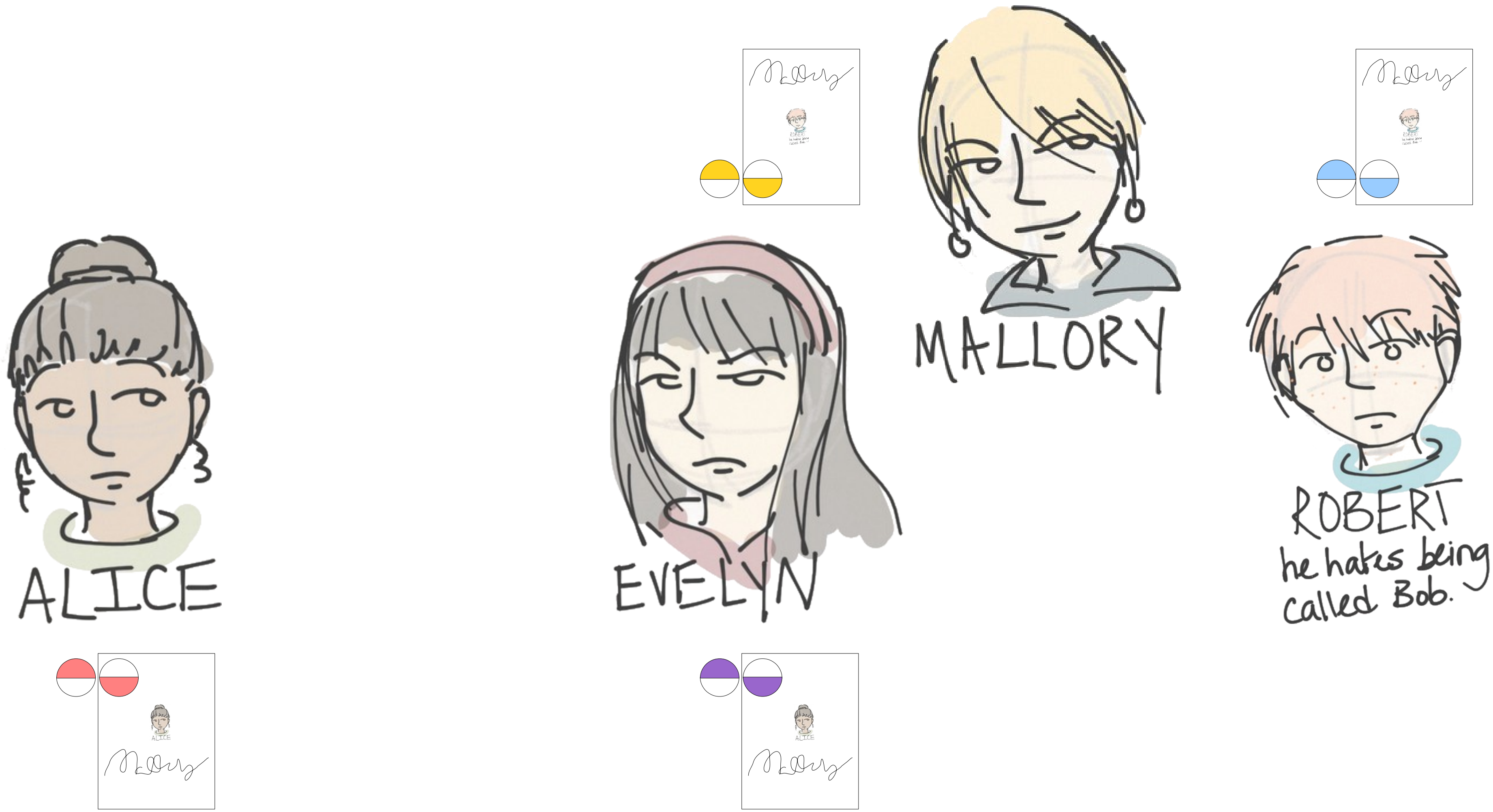




Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019



Trust

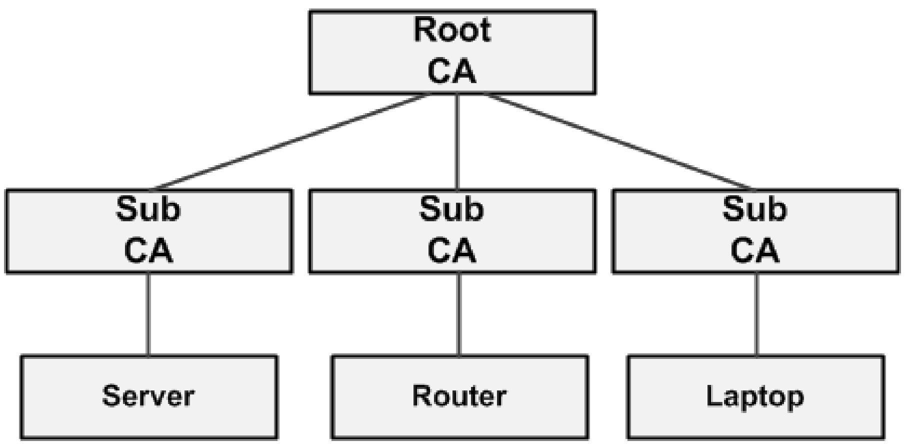
- Public Key Infrastructure (PKI)
    - Certificate Authority (CA) i.e. notary
    - Intermediate Certificate
    - Client Certificate
- Web of Trust

Fun with Certificates part II

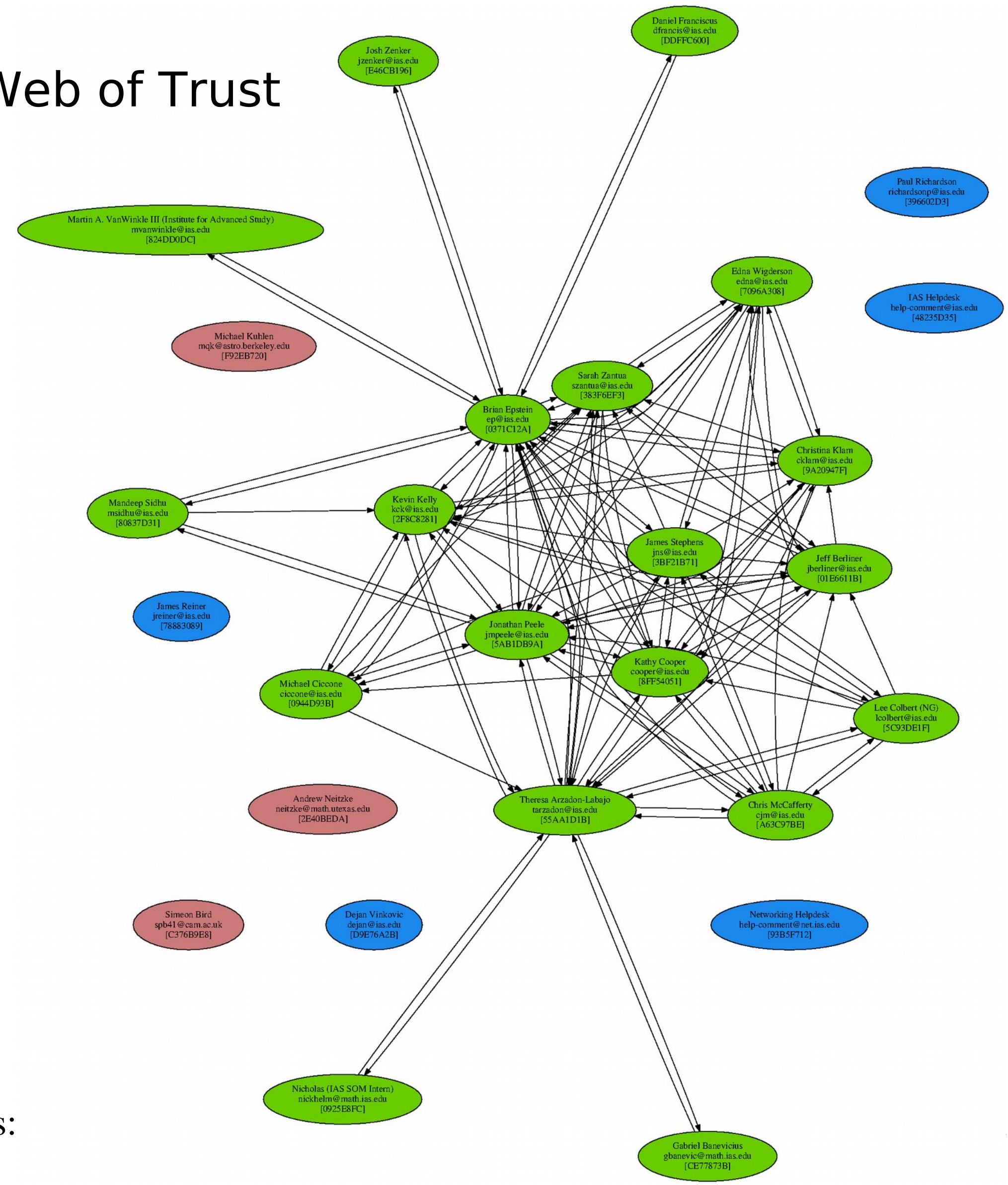
Elliptic Curve Cryptography

May 13, 2019

Public Key Infrastructure (PKI)



Web of Trust



https:

PKI

- Why do we trust CAs?
  - time consuming vetting process
  - regularly audited
  - $$$
  - bundled with product
  - certificate revocation

Structure

- Root CA
  - self signed
- Intermediate certificate
- Server certificate

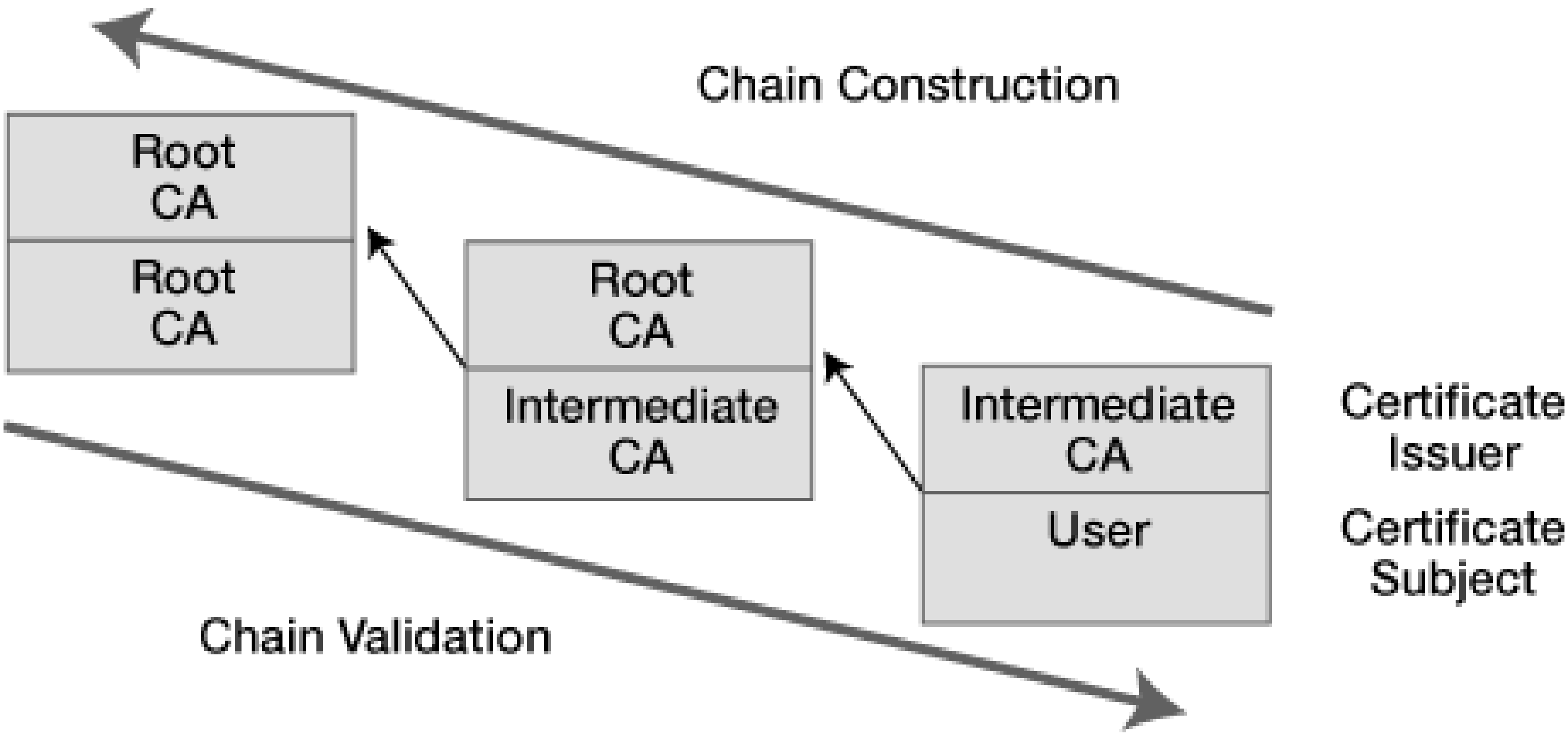


FIGURE 1: Certificate-chain-processing overview

Who provides the CA certificate, the client or the server?

The client.

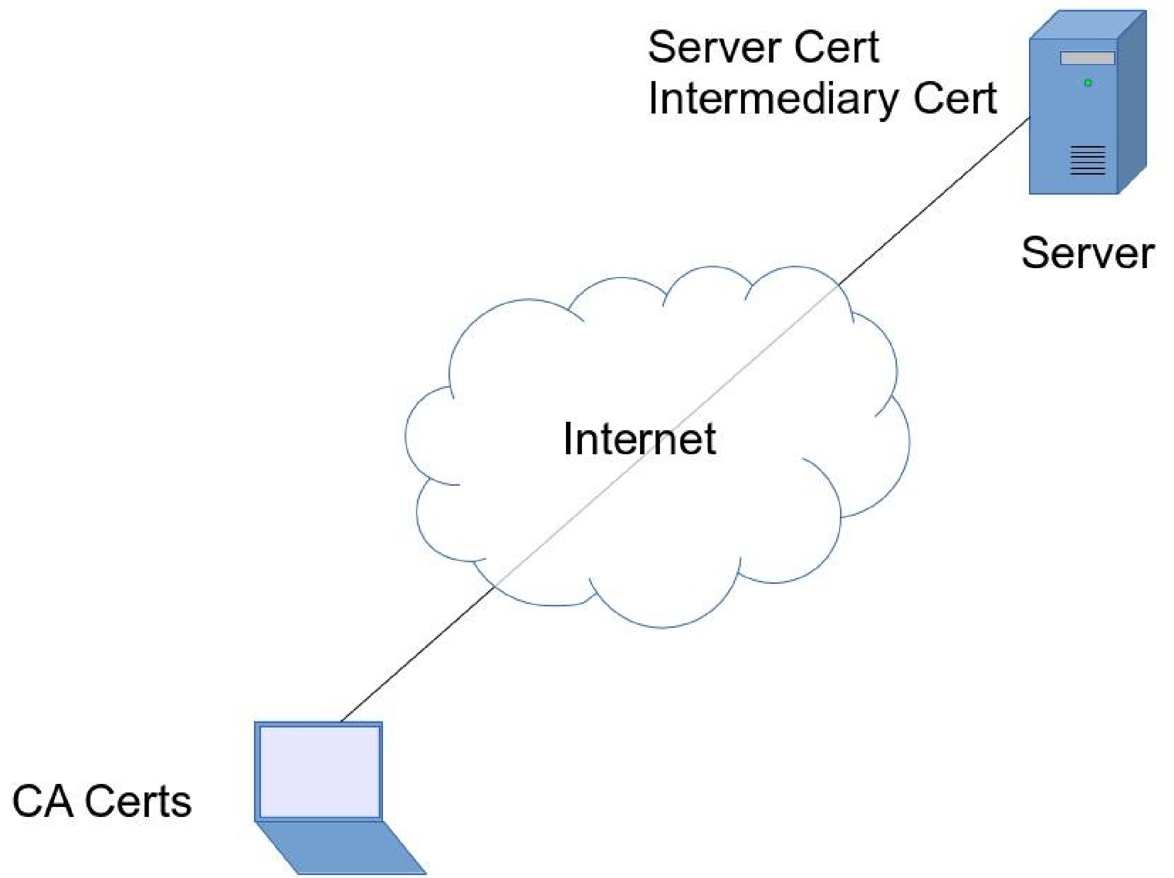
...the intermediate certificate?

The server. (or it should)

Fun with Certificates part II

Elliptic Curve Cryptography

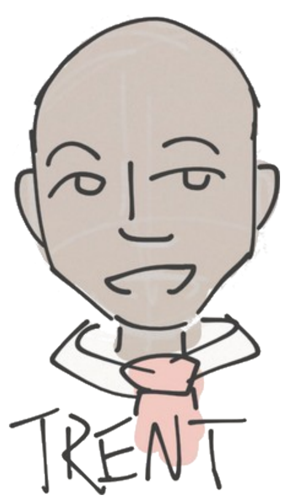
May 13, 2019



Fun with Certificates part II

Elliptic Curve Cryptography

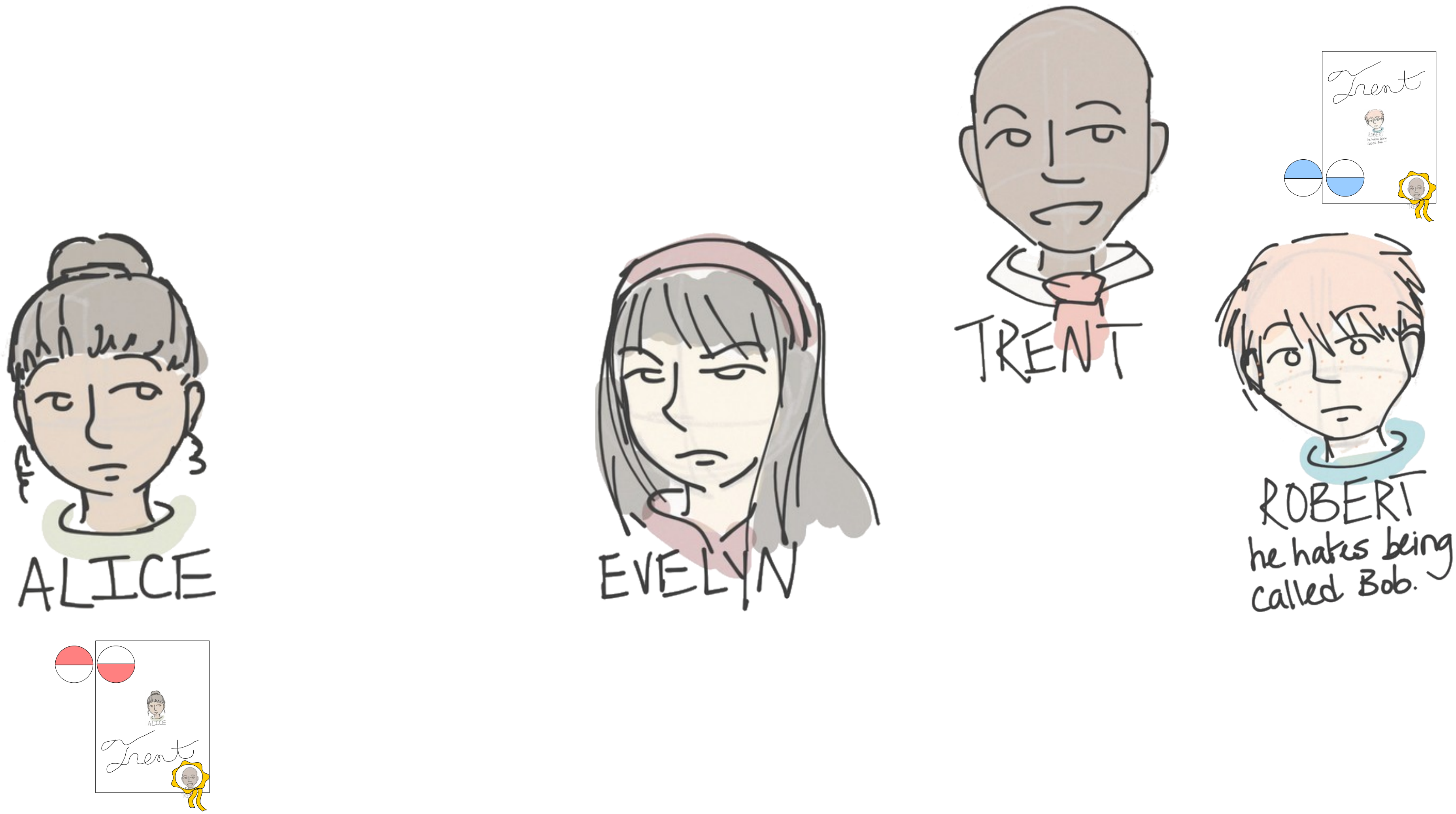
May 13, 2019



Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019



Getting Your Cert Signed

- Internal Certificate Authority
- Commercial Certificate Authority
    - Be a reseller ($12/yr, $119/yr wildcard)
- inCommon for .edu’s ($2k-$20k/yr)
    - https://www.incommon.org/certificates/

Semi-primes

41 * 43 = 1763 easy!

1739 = 47 * 37 difficult

1791904897 = 49943 * 35879 hard, I need a computer!

170122668341587273458646411386585043888873643113298660753168823105496218048396254258389541689798276387535036676575062116463749217204880781486238521463801806647717753763762209533452596
443765433132839199250997874070119227832756249288919712152428105344288137338378592441098310151010596800002333954751873349228763 *

143685366445138003711595402594806625836106895764255994658099545498390517894693472991085893832864915801761970155763201096759761623694012072299292478856561357050062892354466628960025947
611851554780658080196114743327960874693198902680721554877864174333388893106637708514607610834750473283277858418617695308935563 =

244441379412856453795116849112993656784238330464487793812387960841625360467978990192342054422182134999269912972292810247012789506480686777023328857303833579789770401844841211750799876
036943987423766956509508532778372224942810381358670228770832264798563958674474197721436059032452267170180693075044291999303273447847679173832832671061339171744722805614579081864158823
897380675873058252911444157228551578908838716486494665328138329218817328839427363142674827442717524564306490042394023133936383728794873948705684286205987215552936208360027477948962129
430697755765904346533242421364404794444891894641015313209968513198569

Really hard, I need a super computer and a couple of millennia!

Breaking semi-primes

- Brute force
- Sieve methods (slightly better)
- Rainbow table
    - What if we stored all 174 bit primes on micro-SD cards?

Let's store every 174 bit prime number!

100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001001101

11972621413014756705924586149611790497021399392059337

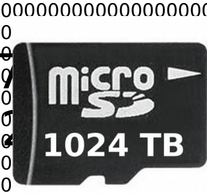
$\cong 1.2*10^{52}$

11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111101

1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001001
1011000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000010
1001011000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0101111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0001100001011000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000001101011111100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000011001111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000011100011011000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000100011111011000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000001001111101110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000001010001001110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000001010011100110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000001011100001110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000001100000111110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000001101110000110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000001110100000110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000001111000010 1..

2394524282602951341184917 … 3580994042798784118783

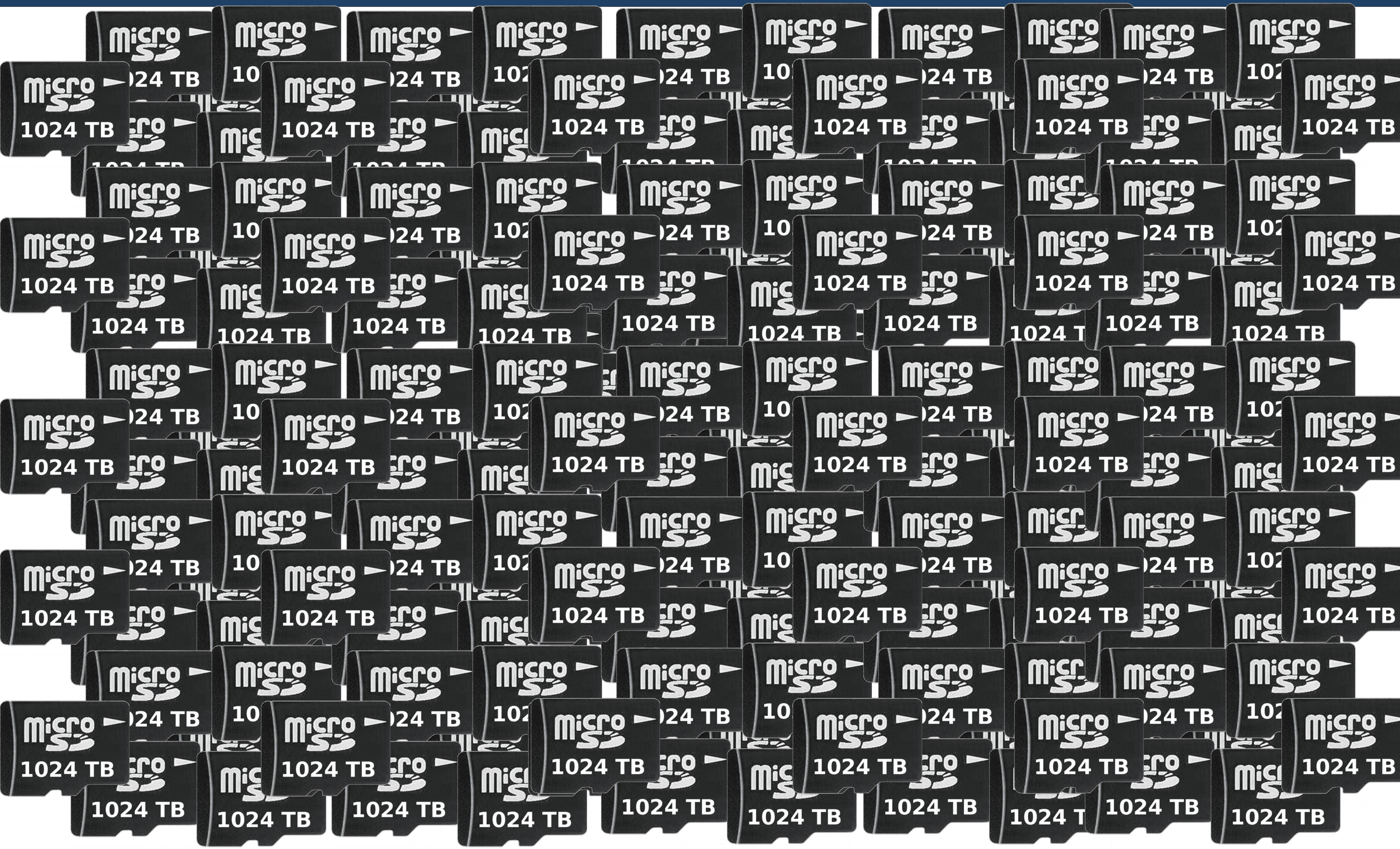
≅ …



Fun with Certificates part II

Elliptic Curve Cryptography

May 13, 2019



How many?

$\# \text{ primes} = \pi(x) = x/\ln(x)$

$x_1 = 1197262141301475670592458614961179049702139939205939 2$

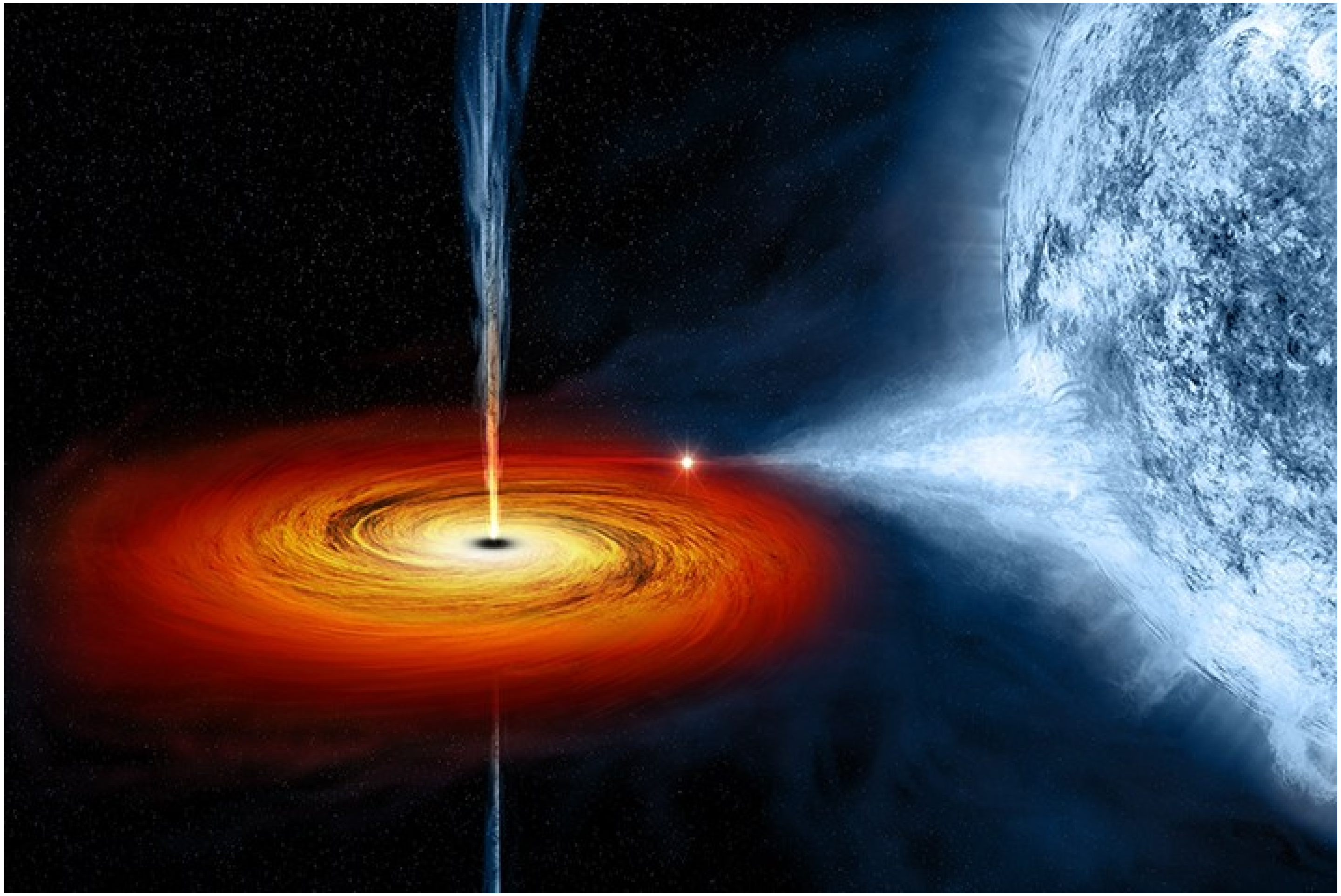
$x_2 = 2394524282602951341184917229922358099404279878411878 3$

$\pi(x_2) - \pi(x_1) \cong$ **$9.87*10^{49}$ primes**

$$9.87*10^{49} \text{ primes} \times \frac{174 \text{ bits}}{\text{prime}} \times \frac{1 \text{ byte}}{8 \text{ bits}} \times \frac{1 \text{ kb}}{1024 \text{ bytes}} \times \frac{1 \text{ mb}}{1024 \text{ kb}} \times \frac{1 \text{ gb}}{1024 \text{ mb}}$$

$$\times \frac{1 \text{ tb}}{1024 \text{ gb}} \times \frac{1 \text{ pb}}{1024 \text{ tb}} \times \frac{0.005 \text{ g}}{1\text{pb microsd}} \times \frac{1 \text{ kg}}{1000 \text{ g}} \times \frac{\text{solar mass}}{1.9891*10^{30} \text{ kg}} =$$

4.8 solar masses $\cong$???

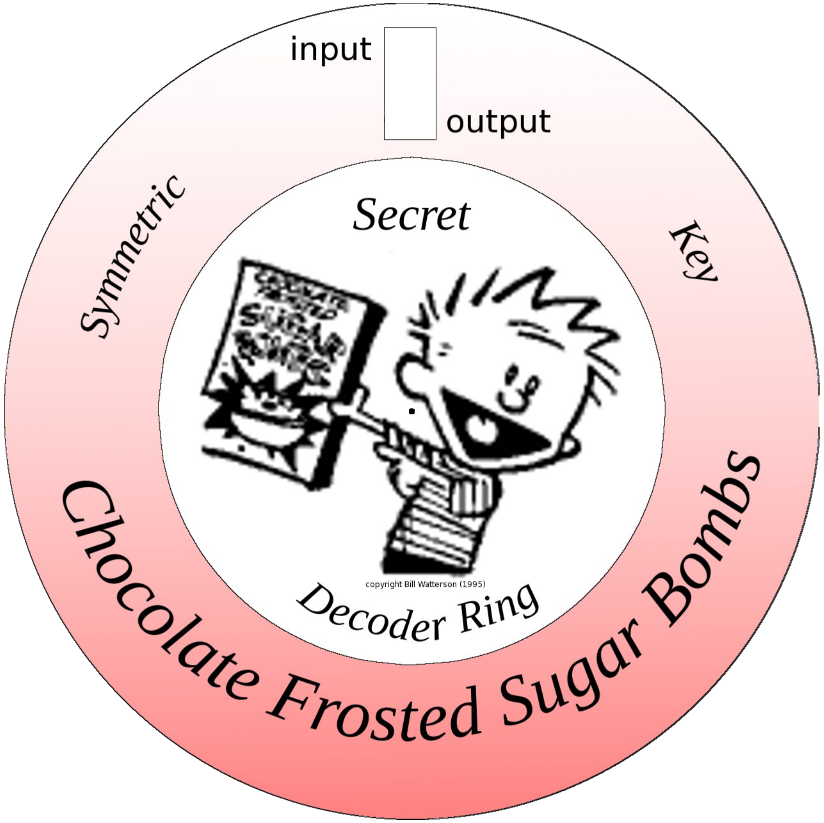



And finally, monsieur,
a wafer-thin mint.
micro SD
1024 TB
Mr. Creosote

Cert Lab

Wrap-up

- Cryptography
- RSA overview
- Explain why ECC came about
- ECC deep dive
- Safe Curves and Trust
- Certs


input
output
Symmetric
Secret
Key
copyright Bill Watterson (1995)
Decoder Ring
Chocolate Frosted Sugar Bombs

T
H
A
N
K
S