PARI and Elliptic Curves

Jared Guissmo E. Asuncion

July 25, 2017

PARI/GP is a free software system for number theory. It has three components:

- `libpari`, the PARI library
  - written in C
  - consists of fast special purpose routines
- the gp interpreter
  - simpler to use than C
  - easy to use for quick calculations
  - slower in general
- the gp2c compiler

We can work with

- integers (`t_INT`)
```
? 1 + 1
% 2
```
- real numbers (`t_REAL`)
```
? sqrt(2)
% 1.4142135623730950488
```
- integers mod N (`t_INTMOD`)
```
? Mod(5, 7)^4
% Mod(2, 7)
```
- fractions (`t_FRAC`)
```
? 23/69
% 1/3
```
- complex numbers (`t_COMPLEX`)
```
? (3 + 4*I)*(3 - 4*I)
% 25
```
- vectors (`t_VEC`)
```
? 3 * [23, 140]
% [69, 140]
```

PARI tries to guess the domain in which you are working.

```
? 2 * Mod(7, 11)
% Mod(3, 11)

? Mod(7, 11) * 2
% Mod(3, 11)

? Mod(7, 11) * 2
% Mod(3, 11)

? Mod(7, 10) + Mod(2, 15)
% Mod(4, 5)
```

ellinit

We can define an elliptic curve by feeding a vector to the `ellinit` command.

- for the short Weierstrass form: `[a4, a6]` defines an elliptic curve $y^2 = x^3 + a_4x + a_6$.
- for the long Weierstrass form: `[a1, a2, a3, a4, a6]` defines an elliptic curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

```
? E = ellinit([0, 1])
% [0, 0, 0, 0, 1, 0, 0, 4, 0, 0, -864,[+++]

? E.a1
% 0

? E.a6
% 1
```

```
? E = ellinit([0, 1])
% [0, 0, 0, 0, 1, 0, 0, 4, 0, 0, -864,[+++]

? E.a1
% 0

? E.a6
% 1

? E.disc
% 432
```

```
? E = ellinit([0, 1])
% [0, 0, 0, 0, 1, 0, 0, 4, 0, 0, -864,[+++]

? E.a1
% 0

? E.a6
% 1

? E.disc
% 432

? E.j
% 0
```

```
? E = ellinit([Mod(0, 5), Mod(1, 5)])
% [Mod(0, 5), Mod(0, 5), Mod(0, 5), Mo[+++]

? E.a1
% Mod(0, 5)

? E.a6
% Mod(1, 5)

? E.disc
% Mod(3, 5)

? E.j
% Mod(0, 5)
```

elliptic curve from j-invariant

What if we want an elliptic curve with a particular j-invariant?

Solution 1

Solution 2

elliptic curve from j-invariant

What if we want an elliptic curve with a particular j-invariant?

Solution 1

Make a function that returns an appropriate vector.

Solution 2

elliptic curve from j-invariant

What if we want an elliptic curve with a particular j-invariant?

Solution 1

Make a function that returns an appropriate vector.

The elliptic curve

$$Y^2 + XY = X^3 + \frac{36}{1728 - j}X + \frac{1}{1728 - j}$$

has j-invariant j.

Solution 2

How to declare functions in GP?

Way 1

```
funcname = (x, y) -> do_stuff
```

Example:

```
? way1 = j -> [1, 0, 0, 36/(1728  - j), 1/(1728  - j)]
% (j)->[1,0,0,36/(1728-j),1/(1728-j)]
```

How to declare functions in GP?

Way 1

```
funcname = (x, y) -> do_stuff
```

Example:

```
? way1 = j -> [1, 0, 0, 36/(1728  - j), 1/(1728  - j)]
% (j)->[1,0,0,36/(1728-j),1/(1728-j)]
```

Way 2

```
funcname(x, y) = { do_stuff }
```

Example:

```
? way2(j) = {
  return([1, 0, 0, 36/(1728  - j), 1/(1728  - j)]);
}
```

How to declare functions in GP?

Way 1

```
funcname = (x, y) -> do_stuff
```

Example:

```
? way1 = j -> [1, 0, 0, 36/(1728  - j), 1/(1728  - j)]
% (j)->[1,0,0,36/(1728-j),1/(1728-j)]
```

Way 2

```
funcname(x, y) = { do_stuff }
```

Example:

```
? way2(j) = {
  return([1, 0, 0, 36/(1728  - j), 1/(1728  - j)]);
}
```

Notice that the curly braces allow you to type “multiline” commands.

Looks good.

```
? evecfromj = j -> [1, 0, 0, 36/(1728  - j), 1/(1728  - j)]
% (j)->[1, 0, 0, 36/(1728-j), 1/(1728-j)]

? E = ellinit(evecfromj(3))
% [1, 0, 0, 12/575, 1/1725, 1, 24/575, 4/1725, 143/991[+++]

? E.j
% 3
```

Oh no!

```
? evecfromj = j -> [1, 0, 0, 36/(1728  - j), 1/(1728  - j)]
% (j)->[1, 0, 0, 36/(1728-j), 1/(1728-j)]

? E = ellinit(evecfromj(1728))
  ***   at top-level: E=ellinit(evecfromj(1728))
  ***                           ^-----------------
  ***   in function evecfromj: [1,0,0,36/(1728-j),1/(1728-j
  ***                                   ^------------------
  *** _/_: impossible inverse in dvmdii: 0.
  ***   Break loop: type 'break' to go back to GP prompt
break>
```

We need `if` statements to handle other cases! How do we make `if` statements?

We need `if` statements to handle other cases! How do we make `if` statements?

Just ask!

- You can use `?` to ask for a short explanation on how a function is used.
- You can use `??` to ask for a long explanation on how a function is used.
- You can use `???` to list relevant functions based on a query.

We need `if` statements to handle other cases! How do we make `if` statements?

Just ask!

- You can use `?` to ask for a short explanation on how a function is used.
- You can use `??` to ask for a long explanation on how a function is used.
- You can use `???` to list relevant functions based on a query.

```
? ?if
% if(a,{seq1},{seq2}): if a is nonzero, seq1 is evaluated,
otherwise seq2. seq1 and seq2 are optional, and if seq2 is
omitted, the preceding comma can be omitted also.
```

```
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  return([1, 0, 0, 36/(1728  - j), 1/(1728  - j)]);
}
```

```
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  return([1, 0, 0, 36/(1728  - j), 1/(1728  - j)]);
}

? ellinit(evecfromj(0)).j
% 0

? ellinit(evecfromj(1728)).j
% 1728

? ellinit(evecfromj(420)).j
% 420
```

```
? a4 = 1234567890;
? a6 = 9876543210;
```

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  a4 = 36/(1728 - j);
  a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
```

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  a4 = 36/(1728 - j);
  a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
? evecfromj(420);
```

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  a4 = 36/(1728 - j);
  a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
? evecfromj(420);
? a4
```

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  a4 = 36/(1728 - j);
  a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
? evecfromj(420);
? a4
% 3/109
```

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  a4 = 36/(1728 - j);
  a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
? evecfromj(420);
? a4
% 3/109
? a6
```

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  a4 = 36/(1728 - j);
  a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
? evecfromj(420);
? a4
% 3/109
? a6
% 1/1308
```

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  a4 = 36/(1728 - j);
  a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
? evecfromj(420);
? a4
% 3/109
? a6
% 1/1308
```

local variables

Use the function `my` to declare **local** variables within a function.

```
? a4 = 1234567890;
? a6 = 9876543210;
? evecfromj(j) = {
  if(j == 0, return([0, 0, 0, 0, 1]));
  if(j == 1728, return([0, 0, 0, 1, 0]));
  my(a4 = 36/(1728 - j));
  my(a6 = 0); a6 = 1/(1728  - j);
  return([1, 0, 0, a4, a6]);
}
? evecfromj(420);
? a4
% 1234567890
? a6
% 9876543210
```

local variables

Use the function `my` to declare **local** variables within a function.

elliptic curve from j-invariant

What if we want an elliptic curve with a particular j-invariant?

Solution 1

Make a function that returns an appropriate vector.

The elliptic curve

$$Y^2 + XY = X^3 + \frac{36}{1728 - j}X + \frac{1}{1728 - j}$$

has j-invariant j.

Solution 2

elliptic curve from j-invariant

What if we want an elliptic curve with a particular j-invariant?

Solution 1

Make a function that returns an appropriate vector.

The elliptic curve

$$Y^2 + XY = X^3 + \frac{36}{1728 - j}X + \frac{1}{1728 - j}$$

has j-invariant j.

Solution 2

Use `ellfromj` function.

```
? ???j-invariant
```

```
? ???j-invariant

? ???$j$-invariant
ellfromj          ellinit           ellissupersingular ellj
ellminimaltwist   ellmodulareqn     weber

See also:
  All domains
```

```
? ???j-invariant

? ???$j$-invariant
ellfromj            ellinit             ellissupersingular ellj
ellminimaltwist     ellmodulareqn       weber

See also:
  All domains

? ellfromj(420)
% [0, 0, 0, 1648080, 1437125760]
```

```
? ???j-invariant

? ???$j$-invariant
ellfromj            ellinit             ellissupersingular ellj
ellminimaltwist     ellmodulareqn       weber

See also:
  All domains

? ellfromj(420)
% [0, 0, 0, 1648080, 1437125760]

? ellfromj(Mod(5,7))
% [0, 0, 0, Mod(1, 7), Mod(3, 7)]
```

```
? ???j-invariant

? ???$j$-invariant
ellfromj            ellinit             ellissupersingular ellj
ellminimaltwist     ellmodulareqn       weber

See also:
  All domains

? ellfromj(420)
% [0, 0, 0, 1648080, 1437125760]

? ellfromj(Mod(5,7))
% [0, 0, 0, Mod(1, 7), Mod(3, 7)]

? ellfromj(Mod(0,2))
% [0, 0, Mod(1, 2), 0, 0]
```

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
Note that $P = (2, 1) \in E$.

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
Note that $P = (2, 1) \in E$. And note that $3P = (1, 1) \in E$.

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
Note that $P = (2, 1) \in E$. And note that $3P = (1, 1) \in E$.

```
? E = ellinit([Mod(3,5),Mod(2,5)]);
? P = [Mod(2, 5), Mod(1, 5)];
```

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
Note that $P = (2, 1) \in E$. And note that $3P = (1, 1) \in E$.

```
? E = ellinit([Mod(3,5),Mod(2,5)]);
? P = [Mod(2, 5), Mod(1, 5)];

? 3*P
% [Mod(1, 5), Mod(3, 5)]
```

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
Note that $P = (2, 1) \in E$. And note that $3P = (1, 1) \in E$.

```
? E = ellinit([Mod(3,5),Mod(2,5)]);
? P = [Mod(2, 5), Mod(1, 5)];

? 3*P
% [Mod(1, 5), Mod(3, 5)]  <--------- WRONG
```

Points on an elliptic curve

Points on an elliptic curve are represented by vectors.

- The point at infinity is represented `[0]`.
- Any other affine point is represented `[x, y]`.

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
Note that $P = (2, 1) \in E$. And note that $3P = (1, 1) \in E$.

```
? E = ellinit([Mod(3,5),Mod(2,5)]);
? P = [Mod(2, 5), Mod(1, 5)];

? 3*P
% [Mod(1, 5), Mod(3, 5)]  <---------- WRONG

? ellmul(E,P,3)
% [Mod(1, 5), Mod(1, 5)]
```

for and print

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.

for and print

Consider $E: Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
This curve has exactly five points, one of them is $P = (2, 1)$.

for and print

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
This curve has exactly five points, one of them is $P = (2, 1)$.
Hence, the group is cyclic of order 5.

for and print

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
This curve has exactly five points, one of them is $P = (2, 1)$.
Hence, the group is cyclic of order 5.
Let print all five multiples of P (i.e. all points of E).

`for` and `print`

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
This curve has exactly five points, one of them is $P = (2, 1)$.
Hence, the group is cyclic of order 5.
Let print all five multiples of P (i.e. all points of E).

```
? E = ellinit([Mod(3,5),Mod(2,5)]);
? P = [Mod(2, 5), Mod(1, 5)];
```

for and print

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
This curve has exactly five points, one of them is $P = (2, 1)$.
Hence, the group is cyclic of order 5.
Let print all five multiples of P (i.e. all points of E).

```
? E = ellinit([Mod(3,5),Mod(2,5)]);
? P = [Mod(2, 5), Mod(1, 5)];

? for(i=1, 5, print(i,"P = ",ellmul(E, P, i)));
```

for and print

Consider $E : Y^2 = X^3 + 3X + 2$ in $\mathbb{F}_5$.
This curve has exactly five points, one of them is $P = (2, 1)$.
Hence, the group is cyclic of order 5.
Let print all five multiples of P (i.e. all points of E).

```
? E = ellinit([Mod(3,5),Mod(2,5)]);
? P = [Mod(2, 5), Mod(1, 5)];

? for(i=1, 5, print(i,"P = ",ellmul(E, P, i)));
1P = [Mod(2, 5), Mod(1, 5)]
2P = [Mod(1, 5), Mod(4, 5)]
3P = [Mod(1, 5), Mod(1, 5)]
4P = [Mod(2, 5), Mod(4, 5)]
5P = [0]
```

`vector` and `apply`

Consider $E : Y^2 = X^3 + 2$ in $\mathbb{F}_7$.

vector and apply

Consider $E : Y^2 = X^3 + 2$ in $\mathbb{F}_7$.

$$E(\mathbb{F}_p) \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \langle P \rangle \times \langle Q \rangle = \langle (3,6) \rangle \times \langle (5,6) \rangle.$$

vector and apply

Consider $E: Y^2 = X^3 + 2$ in $\mathbb{F}_7$.

$$E(\mathbb{F}_p) \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \langle P \rangle \times \langle Q \rangle = \langle (3,6) \rangle \times \langle (5,6) \rangle.$$

```
? E = ellinit([Mod(0,7),Mod(2,7)]);
? P = [Mod(3, 7), Mod(6, 7)];
? Q = [Mod(5, 7), Mod(6, 7)];
```

vector and apply

Consider $E : Y^2 = X^3 + 2$ in $\mathbb{F}_7$.

$$E(\mathbb{F}_p) \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \langle P \rangle \times \langle Q \rangle = \langle (3,6) \rangle \times \langle (5,6) \rangle.$$

```
? E = ellinit([Mod(0,7),Mod(2,7)]);
? P = [Mod(3, 7), Mod(6, 7)];
? Q = [Mod(5, 7), Mod(6, 7)];

? S = vector(3, i, ellmul(E, P, i))
% [[Mod(3, 7), Mod(6, 7)], [Mod(3, 7), Mod(1, 7)], [0]]
```

vector and apply

Consider $E : Y^2 = X^3 + 2$ in $\mathbb{F}_7$.

$$E(\mathbb{F}_p) \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \langle P \rangle \times \langle Q \rangle = \langle (3,6) \rangle \times \langle (5,6) \rangle.$$

```
? E = ellinit([Mod(0,7),Mod(2,7)]);
? P = [Mod(3, 7), Mod(6, 7)];
? Q = [Mod(5, 7), Mod(6, 7)];

? S = vector(3, i, ellmul(E, P, i))
% [[Mod(3, 7), Mod(6, 7)], [Mod(3, 7), Mod(1, 7)], [0]]

? T = apply(x->elladd(E,x,Q),S)
% [[Mod(6, 7), Mod(1, 7)], [Mod(0, 7), Mod(3, 7)], [Mo[+++]
```

vector and apply

Consider $E : Y^2 = X^3 + 2$ in $\mathbb{F}_7$.

$$E(\mathbb{F}_p) \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \langle P \rangle \times \langle Q \rangle = \langle (3,6) \rangle \times \langle (5,6) \rangle.$$

```
? E = ellinit([Mod(0,7),Mod(2,7)]);
? P = [Mod(3, 7), Mod(6, 7)];
? Q = [Mod(5, 7), Mod(6, 7)];

? S = vector(3, i, ellmul(E, P, i))
% [[Mod(3, 7), Mod(6, 7)], [Mod(3, 7), Mod(1, 7)], [0]]

? T = apply(x->elladd(E,x,Q),S)
% [[Mod(6, 7), Mod(1, 7)], [Mod(0, 7), Mod(3, 7)], [Mo[+++]

? U = apply(x->elladd(E,x,Q),T)
% [[Mod(0, 7), Mod(4, 7)], [Mod(6, 7), Mod(6, 7)], [Mo[+++]
```

and []

- `#v` returns the length of the vector `v`.
- `v[i]` returns the `i`th component of `v`.

and []

- #v returns the length of the vector v.
- v[i] returns the ith component of v.

```
? v = primes([2,100])
% [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]
```

and []

- #v returns the length of the vector v.
- v[i] returns the ith component of v.

```
? v = primes([2,100])
% [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]

? #v
% 15
```

and []

- `#v` returns the length of the vector `v`.
- `v[i]` returns the ith component of `v`.

```
? v = primes([2,100])
% [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]

? #v
% 15

? v[7]
% 17
```

external files

Use the `read` function to execute commands from a file.

You can also use the shorthand `\r file.gp` to execute `file.gp`.

external files

Use the `read` function to execute commands from a file.
You can also use the shorthand `\r file.gp` to execute `file.gp`.

~/dummy.gp

```
for(i=1, 3, print(i));
favoritenumber = 2;
```

external files

Use the `read` function to execute commands from a file.
You can also use the shorthand `\r file.gp` to execute `file.gp`.

~/dummy.gp

```
for(i=1, 3, print(i));
favoritenumber = 2;
```

```
? read("~/dummy.gp");
1
2
3
% 2
? favoritenumber^favoritenumber
% 4
```

Exercise

Make a function `ellmodcount` that returns the number of (nonsingular) elliptic curves modulo p, given a prime $p \geq 5$.

Hint: `ellinit` returns `[]` if the elliptic curve is singular.

Exercise

Make a function `ellmodcount` that returns the number of (nonsingular) elliptic curves modulo p, given a prime $p \geq 5$.

Hint: `ellinit` returns `[]` if the elliptic curve is singular.

```
? ellmodcount(5)
% 20

? ellmodcount(7)
% 42

? ellmodcount(101)
% 10100
```

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field.

Hilbert class field

The Hilbert class field H_K is the maximal abelian unramified extension of K.

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field.

Hilbert class field

The Hilbert class field H_K is the maximal abelian unramified extension of K.

Let L be a field extension of K.

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field.

Hilbert class field

The Hilbert class field H_K is the maximal abelian unramified extension of K.

Let L be a field extension of K.

unramified prime

A prime $\mathfrak{p} \in \mathcal{O}_K$ is said to be unramified if its prime decomposition in $\mathcal{O}_L$ is squarefree, that is,

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g$$

where the $\mathfrak{P}_i$ are distinct.

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field.

Hilbert class field

The Hilbert class field H_K is the maximal abelian unramified extension of K.

Let L be a field extension of K.

unramified prime

A prime $\mathfrak{p} \in \mathcal{O}_K$ is said to be unramified if its prime decomposition in $\mathcal{O}_L$ is squarefree, that is,

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g$$

where the $\mathfrak{P}_i$ are distinct.

unramified extension

An extension L/K is unramified if all prime ideals in $\mathcal{O}_K$ are unramified.

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field.

Hilbert class field

The Hilbert class field H_K is the maximal abelian unramified extension of K.

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field.

Hilbert class field

The Hilbert class field H_K is the maximal abelian unramified extension of K.

abelian extension

An extension L/K is abelian if it is Galois with abelian Galois group.

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field.

Hilbert class field

The Hilbert class field H_K is the maximal abelian unramified extension of K.

abelian extension

An extension L/K is abelian if it is Galois with abelian Galois group.

Class field theory tells us that H_K exists and unique and there exists a map, called the Artin map, which induces an isomorphism between

$$\mathrm{Cl}(\mathcal{O}_K) = \frac{\mathcal{I}(\mathcal{O}_K)}{\mathcal{P}(\mathcal{O}_K)} \cong \mathrm{Gal}\left(\frac{H_K}{K}\right).$$

Recall that a lattice of full rank Λ is an additive subgroup of $\mathbb{C}$ with a $\mathbb{Z}$-basis ω_1 and ω_2. We write $\Lambda = [\omega_1, \omega_2] = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Recall that a lattice of full rank Λ is an additive subgroup of $\mathbb{C}$ with a $\mathbb{Z}$-basis ω_1 and ω_2. We write $\Lambda = [\omega_1, \omega_2] = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

j-invariant of a lattice

$$j(\Lambda) = 1728 \cdot \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3^2(\Lambda)}$$

Recall that a lattice of full rank Λ is an additive subgroup of $\mathbb{C}$ with a $\mathbb{Z}$-basis ω_1 and ω_2. We write $\Lambda = [\omega_1, \omega_2] = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

j-invariant of a lattice

$$j(\Lambda) = 1728 \cdot \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3^2(\Lambda)}$$

j-invariant of a complex number

Let $\Lambda = [\tau_1, \tau_2]$. We define

$$j\left(\frac{\tau_1}{\tau_2}\right) := j(\Lambda).$$

Recall that a lattice of full rank Λ is an additive subgroup of $\mathbb{C}$ with a $\mathbb{Z}$-basis ω_1 and ω_2. We write $\Lambda = [\omega_1, \omega_2] = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

j-invariant of a lattice

$$j(\Lambda) = 1728 \cdot \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3^2(\Lambda)}$$

j-invariant of a complex number

Let $\Lambda = [\tau_1, \tau_2]$. We define

$$j\left(\frac{\tau_1}{\tau_2}\right) := j(\Lambda).$$

j-invariant of an ideal class

Let $\mathfrak{p} \in \mathrm{Cl}(\mathcal{O}_K)$. Take $I = [\alpha_1, \alpha_2]$ to be a representative of $\mathfrak{p}$. We define

$$j(\mathfrak{p}) := j(I)$$

Theorem

For every ideal class $\mathfrak{k} \in \mathrm{Cl}(\mathcal{O}_K)$, *we have*

$$H_K = K(j(\mathfrak{k})).$$

Theorem

For every ideal class $\mathfrak{k} \in \mathrm{Cl}(\mathcal{O}_K)$, *we have*

$$H_K = K(j(\mathfrak{k})).$$

Moreover, there exists an isomorphism via the following well-defined map

$$\sigma : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Gal}(H_K/K)$$
$$\mathfrak{k} \to \sigma_{\mathfrak{k}}.$$

such that if $\mathfrak{p}$ *is a representative of* $\mathfrak{k}$, *then* $\sigma_{\mathfrak{k}} := x^{N(\mathfrak{p})}$ *is the Frobenius automoprhism associated with* $\mathfrak{p}$.

Theorem

For every ideal class $\mathfrak{k} \in \mathrm{Cl}(\mathcal{O}_K)$, *we have*

$$H_K = K(j(\mathfrak{k})).$$

Moreover, there exists an isomorphism via the following well-defined map

$$\sigma : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Gal}(H_K/K)$$
$$\mathfrak{k} \to \sigma_{\mathfrak{k}}.$$

such that if $\mathfrak{p}$ *is a representative of* $\mathfrak{k}$, *then* $\sigma_{\mathfrak{k}} := x^{N(\mathfrak{p})}$ *is the Frobenius automoprhism associated with* $\mathfrak{p}$. *Furthermore,*

$$j(\mathfrak{k})^{\sigma_{\mathfrak{h}}} = j(\mathfrak{k}\mathfrak{h}^{-1}) \quad \text{and} \quad \overline{j(\mathfrak{h})} = j(\mathfrak{h}^{-1})$$

for all $\mathfrak{h} \in \mathrm{Cl}(\mathcal{O}_K)$

Hilbert class polynomial

We define the Hilbert class polynomial to be

$$h_K(X) = \prod_{\sigma \in \mathrm{Gal}(H_K/K)} (X - x^{\sigma}) = \prod_{\mathfrak{h} \in \mathrm{Cl}(\mathcal{O}_K)} (X - x^{\sigma_{\mathfrak{h}}})$$

for some fixed $\mathfrak{k}$.

Hilbert class polynomial

We define the Hilbert class polynomial to be

$$h_K(X) = \prod_{\sigma \in \mathrm{Gal}(H_K/K)} (X - x^{\sigma}) = \prod_{\mathfrak{h} \in \mathrm{Cl}(\mathcal{O}_K)} (X - x^{\sigma_{\mathfrak{h}}})$$

for some fixed $\mathfrak{k}$.

$$\mathrm{Cl}(-D) \xleftrightarrow{\sim} \mathrm{Cl}(\mathcal{O}_K) \xleftrightarrow{\sim} \mathrm{Gal}(H_K/K) \overset{\sim}{\leftrightarrow} \text{roots of } h_K$$

$$[A, B, C] \overset{\Theta}{\mapsto} [(A, (-B + \sqrt{-D})/2] \xmapsto{\sigma} \sigma_{\mathfrak{h}^{-1}} \xmapsto{x^{-}} x^{\sigma}$$

```
? [X,Y]=quadclassunit(-231).gen
% [Qfb(2, 1, 29), Qfb(7, 7, 10)]
```

```
? [X,Y]=quadclassunit(-231).gen
% [Qfb(2, 1, 29), Qfb(7, 7, 10)]

? QfbA=Q->Vec(Q)[1];
? QfbB=Q->Vec(Q)[2];
? QfbC=Q->Vec(Q)[3];
? QfbD=Q->QfbB(Q)^2-4*QfbA(Q)*QfbC(Q);
? QfbCmp=Q->(-QfbB(Q)+sqrt(QfbD(Q)))/(2*QfbA(Q));
```

```
? xxx = vector(6,i,X^i)
% [Qfb(2, 1, 29), Qfb(4, -3, 15), Qfb(8, 5, 8), Qfb(4, 3, 1
5), Qfb(2, -1, 29), Qfb(1, 1, 58)]
? yyy = vector(6,i,X^i*Y)
% [Qfb(5, -3, 12), Qfb(6, 3, 10), Qfb(3, 3, 20), Qfb(6, -3,
 10), Qfb(5, 3, 12), Qfb(7, 7, 10)]
```

```
? xxx = vector(6,i,X^i)
% [Qfb(2, 1, 29), Qfb(4, -3, 15), Qfb(8, 5, 8), Qfb(4, 3, 1
5), Qfb(2, -1, 29), Qfb(1, 1, 58)]
? yyy = vector(6,i,X^i*Y)
% [Qfb(5, -3, 12), Qfb(6, 3, 10), Qfb(3, 3, 20), Qfb(6, -3,
 10), Qfb(5, 3, 12), Qfb(7, 7, 10)]

? \p 100
   realprecision = 115 significant digits (100 digits)
```

```
? xxx = vector(6,i,X^i)
% [Qfb(2, 1, 29), Qfb(4, -3, 15), Qfb(8, 5, 8), Qfb(4, 3, 1
5), Qfb(2, -1, 29), Qfb(1, 1, 58)]
? yyy = vector(6,i,X^i*Y)
% [Qfb(5, -3, 12), Qfb(6, 3, 10), Qfb(3, 3, 20), Qfb(6, -3,
 10), Qfb(5, 3, 12), Qfb(7, 7, 10)]

? \p 100
   realprecision = 115 significant digits (100 digits)

? zzz = concat(apply(QfbCmp,xxx), apply(QfbCmp,yyy))
% [-1/4 + 3.79967103839266590791718605150991125939558161542
5559079199140596300910970513859227578017904 1[+++]
```

```
? xxx = vector(6,i,X^i)
% [Qfb(2, 1, 29), Qfb(4, -3, 15), Qfb(8, 5, 8), Qfb(4, 3, 1
5), Qfb(2, -1, 29), Qfb(1, 1, 58)]
? yyy = vector(6,i,X^i*Y)
% [Qfb(5, -3, 12), Qfb(6, 3, 10), Qfb(3, 3, 20), Qfb(6, -3,
 10), Qfb(5, 3, 12), Qfb(7, 7, 10)]

? \p 100
   realprecision = 115 significant digits (100 digits)

? zzz = concat(apply(QfbCmp,xxx), apply(QfbCmp,yyy))
% [-1/4 + 3.79967103839266590791718605150991125939558161542
5559079199140596300910970513859227578017904 1[+++]
? www = apply(ellj, zzz)
% [743.99999999999999605917520891104873430051279069283273328
5235149707970628547736236964763562242811604 8[+++]
```

```
? cp = prod(i=1,12,x-www[i])
% x^12 + (5454127280310031673 82.0000000000000000000000000
00000000000000000000000000000000000000000000000[+++]
```

```
? cp = prod(i=1,12,x-www[i])
% x^12 + (545412728031003167382.000000000000000000000000000
00000000000000000000000000000000000000000000[+++]

? cp = round(cp)
% x^12 + 545412728031003167382*x^11 + 457521468949021321664
3494701*x^10 + 29747504488688449508638516757[+++]
```

```
? cp = prod(i=1,12,x-www[i])
% x^12 + (545412728031003167382.0000000000000000000000000
000000000000000000000000000000000000000000000[+++]

? cp = round(cp)
% x^12 + 545412728031003167382*x^11 + 457521468949021321664
3494701*x^10 + 29747504488688449508638516757[+++]

? pc = polclass(-231)
  *** polclass: Warning: increasing stack size to 16000000.
time = 56 ms.
% x^12 + 545412728031003167382*x^11 + 457521468949021321664
3494701*x^10 + 29747504488688449508638516757[+++]
```

```
? cp = prod(i=1,12,x-www[i])
% x^12 + (545412728031003167382.0000000000000000000000000000
00000000000000000000000000000000000000000000000[+++]

? cp = round(cp)
% x^12 + 545412728031003167382*x^11 + 457521468949021321664
3494701*x^10 + 29747504488688449508638516757[+++]

? pc = polclass(-231)
  *** polclass: Warning: increasing stack size to 16000000.
time = 56 ms.
% x^12 + 545412728031003167382*x^11 + 457521468949021321664
3494701*x^10 + 29747504488688449508638516757[+++]

? pc == cp
% 1
```

Let R be an integral domain with field of fractions K. A fractional R-ideal I is a non-zero R-submodule of K such that $xI \subset R$ for some $x \in K^*$.

ideal class group

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field. Let $\mathcal{O}_K$ be the ring of algebraic integers of K. We define the ideal class group of K to be

$$\mathrm{Cl}(\mathcal{O}_K) = \frac{\mathcal{I}(\mathcal{O}_K)}{\mathcal{P}(\mathcal{O}_K)} = \frac{\text{fractional ideals of } \mathcal{O}_K}{\text{principal fractional ideals of } \mathcal{O}_K}.$$

Proposition

Let $N \in \mathbb{N}$ and E be an elliptic curve modulo N. If there exist $m, q \in \mathbb{Z}$ and a point $P \in E$ such that

- q is a prime factor of m
- $q > (N^{1/4} + 1)^2$
- $mP = 0$
- $(m/q)P \neq 0$

then N is prime.

Proposition

Let $N \in \mathbb{N}$ and E be an elliptic curve modulo N. If there exist $m, q \in \mathbb{Z}$ and a point $P \in E$ such that

- q is a prime factor of m
- $q > (N^{1/4} + 1)^2$
- $mP = 0$
- $(m/q)P \neq 0$

then N is prime.

Proof: Let $N > 1$ be composite and p be its smallest prime divisor. Consider $\psi : E(\mathbb{Z}/N\mathbb{Z}) \to E(\mathbb{Z}/p\mathbb{Z})$. Since $mP = 0$ and $(m/q)P \neq 0$, then $\psi(mP) = m\psi(P) = 0$ and $\psi((m/q)P) = (m/q)\psi(P) \neq 0$. Since q is prime, it must divide the order of $\psi(P)$. Thus, $q \leq |E(\mathbb{Z}/p\mathbb{Z})|$. By Hasse's theroem, $q < (\sqrt{p} + 1)^2$. Since $p \leq \sqrt{N}$, we get $q < (\sqrt[4]{N} + 1)^2$. Contradiction.

Atkin-Morain Elliptic Curve Primality Proving

Input: an integer N

Output: a primality certificate or FAIL

- Find m and q.
- Find E and P such that $mP = \infty$ and $\frac{m}{q}P \neq \infty$.

How to find E.

- Find a discriminant D such that
  - $U^2 + |D|V^2 = 4N$ has an integer solution (U, V).
  - $m = N + 1 \pm U$ can be decomposed to $m = qs$ where s is a product of small primes
- Find an elliptic curve E modulo N with j-invariant j, where j is a root of the Hilbert class polynomial $H_D(x)$. If this curve does not have m points, take its quadratic twist.

Let's install `cornacchia2`, part of the C functions in PARI.

Let's install `cornacchia2`, part of the C functions in PARI.

```
? install(cornacchia2, "lGGD&D&")
```

Let's install `cornacchia2`, part of the C functions in PARI.

```
? install(cornacchia2, "lGGD&D&")
? N = 21854044248854244363087690318894335471973824853839;
? D = -307;
```

Let's install `cornacchia2`, part of the C functions in PARI.

```
? install(cornacchia2, "lGGD&D&")
? N = 21854044248854244363087690318894335471973824853839;
? D = -307;
? cornacchia2(abs(307), N, &U, &V);
```

Let's install `cornacchia2`, part of the C functions in PARI.

```
? install(cornacchia2, "lGGD&D&")
? N = 2185404424885424436308769031889433547197382485383 9;
? D = -307;
? cornacchia2(abs(307), N, &U, &V);
? m = N + 1 - U;
```

Let's install `cornacchia2`, part of the C functions in PARI.

```
? install(cornacchia2, "lGGD&D&")
? N = 2185404424885424436308769031889433547197382485383 9;
? D = -307;
? cornacchia2(abs(307), N, &U, &V);
? m = N + 1 - U;
? factor(m)
```

Let's install cornacchia2, part of the C functions in PARI.

```
? install(cornacchia2, "lGGD&D&")
? N = 21854044248854244363087690318894335471973824853839;
? D = -307;
? cornacchia2(abs(307), N, &U, &V);
? m = N + 1 - U;
? factor(m)
%
[                                        2 2]

[                                      347 1]

[15744988651912279800495451661444919178173088091 1]
```

Let's install cornacchia2, part of the C functions in PARI.

```
? install(cornacchia2, "lGGD&D&")
? N = 218540442488542443630876903188943354719738248538839;
? D = -307;
? cornacchia2(abs(307), N, &U, &V);
? m = N + 1 - U;
? factor(m)
%
[                                            2 2]

[                                          347 1]

[157449886519122798004954516614449191781730880911]
? q = 157449886519122798004954516614449191781730880911;
```

Let's find the j-invariant.

Let's find the *j*-invariant.

```
? pc = polclass(-307)
% x^3 + 805016812009981390848000*x^2 - 5083646425734146
162688000000*x + 8987619631060626702336000000000
```

Let's find the *j*-invariant.

```
? pc = polclass(-307)
% x^3 + 805016812009981390848000*x^2 - 5083646425734146
162688000000*x + 8987619631060626702336000000000

? rts = polrootsmod(pc, N)
% [Mod(2930370407138978366426453308494489185559337508342, 2185404424885424436308769031889433547197382485383 9),
 Mod(8927666903536288701686175688305102895600954861147,
  2185404424885424436308769031889433547197382485383 9),
  Mod(9996006938178977294975060517077931380832141636350
  , 2185404424885424436308769031889433547197382485383 9)
  ]~
```

Let's find the elliptic curve.

Let's find the elliptic curve.

Let's find the elliptic curve.

```
? E = ellinit(ellfromj(rts[1]));
```

Let's find the elliptic curve.

```
? E = ellinit(ellfromj(rts[1]));
? P = random(E);
```

Let's find the elliptic curve.

```
? E = ellinit(ellfromj(rts[1]));
? P = random(E);
% [Mod(471949867302613863199424950158738220040087295242
9, 21854044248854244363087690318894335471973824853839),
 Mod(16436948036515590607739997036396948331082598678058
, 21854044248854244363087690318894335471973824853839)]
```

Let's find the elliptic curve.

```
? E = ellinit(ellfromj(rts[1]));
? P = random(E);
% [Mod(47194986730261386319942495015873822004008729524
9, 218540442488542443630876903188943354719738248538839),
 Mod(164369480365155906077399970363969483310825986780 58
, 218540442488542443630876903188943354719738248538839)]
? mP = ellmul(E,P,m);
```

Let's find the elliptic curve.

```
? E = ellinit(ellfromj(rts[1]));
? P = random(E);
% [Mod(47194986730261386319942495015873822004008729524 2
9, 2185404424885424436308769031889433547197382485383 9),
 Mod(1643694803651559060773999703639694833108259867805 8
, 2185404424885424436308769031889433547197382485383 9)]
? mP = ellmul(E,P,m);
% [Mod(150167756983247895435042449135068510038102327014
04, 21854044248854244363087690318894335471973824853839)
, Mod(17982172423262072546372509725056869399501033857 18
5, 21854044248854244363087690318894335471973824853839)]
```

Let's do the twist.

Let's do the twist.

```
? Et = ellinit(elltwist(E));
```

Let's do the twist.

```
? Et = ellinit(elltwist(E));
? P = random(Et)
```

Let's do the twist.

```
? Et = ellinit(elltwist(E));
? P = random(Et)
% [Mod(93622367598200817702681539188234499850192935359４
1, 21854044248854244363087690318894335471973824853839),
 Mod(81221413871268865850873081768791227940325861410８2,
  21854044248854244363087690318894335471973824853839)]
```

Let's do the twist.

```
? Et = ellinit(elltwist(E));
? P = random(Et)
% [Mod(936223675982008177026815391882344998501929353594
1, 21854044248854244363087690318894335471973824853839),
 Mod(81221413871268865850873081768791227940325861410 82,
  21854044248854244363087690318894335471973824853839)]
? mP = ellmul(Et,P,m)
```

Let's do the twist.

```
? Et = ellinit(elltwist(E));
? P = random(Et)
% [Mod(93622367598200817702681539188234499850192935359 4
1, 2185404424885424436308769031889433547197382485383 9),
 Mod(81221413871268865850873081768791227940325861410 82,
  2185404424885424436308769031889433547197382485383 9)]
? mP = ellmul(Et,P,m)
% [0]
? sP = ellmul(Et,P,m/q)
```

Let's do the twist.

```
? Et = ellinit(elltwist(E));
? P = random(Et)
% [Mod(936223675982008177026815391882344998501929353594
1, 2185404424885424436308769031889433547197382485383 9),
 Mod(812214138712688658508730817687912279403258614108 2,
  2185404424885424436308769031889433547197382485383 9)]
? mP = ellmul(Et,P,m)
% [0]
? sP = ellmul(Et,P,m/q)
% [Mod(658043150183461232595703969431679868788684412422
7, 2185404424885424436308769031889433547197382485383 9),
 Mod(232098536873506501679423118946061150726809350730 2,
  2185404424885424436308769031889433547197382485383 9)]
```