Math 502

Maple Routines for Cubic Curves

due Tuesday, April 15, 2008

The cubic curve routines for *Maple* may be found at

`http://www.albany.edu/~hammond/maple/ellc` .

`winitell`

For these routines a cubic curve is represented by its vector of ten coefficients. For reasons connected with the usual numbering of the coefficients of a cubic curve in Weierstrass normal form the vector of coefficients is stored as an array with index values in the interval $[-3, 6]$. Of course such an array may be introduced explicitly using the *Maple* function `array`. The function `winitell` is provided here for convenience in entering a cubic curve in Weierstrass form. It takes as argument a list with 6 entries which are the coefficients $a_0, a_1, a_2, a_3, a_4, a_6$. (The automatic value $a_5 = 1$ serves behind the scenes in the 10 slot array as the coefficient of y^2.) There is an optional second argument, a prime number p, that is used to indicate the field of coefficients, for handling arithmetic mod p.

`affelleq`

If E is (the coefficient array for) a cubic curve in Weierstrass form, then `affelleq(E)` returns its affine equation relative to coordinates X, Y. (These coordinate symbols are used globally by this collection of routines.)

Example:

```
E:=winitell([1,0,0,0,-25,0]): affelleq(E);
                                      2    3
                                     Y  = X  - 25 X
```

`isoncurve`

If E is a cubic curve and P a point given either in affine form (a pair) or homogeneous form (a triple), the function `isoncurve` may be called with E as first argument and P as second argument to determine "true" or "false" for the question of whether P lies on E. An optional third argument p, a prime, indicates the question should be considered for arithmetic mod p.

Example:

```
F:=winitell([1,0,0,0,5,19]): affelleq(F);
                                 2    3
                                Y  = X  + 5 X + 19

isoncurve(F,[-2,1]); isoncurve(F,[2,-1]);
                                true
                                false
```

`negell`

If E is a cubic curve and P a point on E, then the function `negell` may be called with E as first argument and P as second argument (and with a prime p as optional third argument) to find the negative of P relative to the arithmetic on E. Note that this type of negative of a point is different from the negative of a point in vector arithmetic.

Example:

```
negell(F,[-2,1]);
                                [-2,-1]
```

```
negell(F,[2,-1]);
                                    negell: Point is not on curve
```

`powell`

The function `powell` may be used to find an integer multiple of a point relative to the arithmetic on E, i.e.,

$$nP \;=\; \underbrace{P + \ldots + P}_{n \text{ times}} \quad .$$

Note that this type of scalar multiple is different from the scalar multiple of a point in vector arithmetic. Call `powell` with the curve as first argument, the integer multiplier as second argument, and the point as third argument. (An optional fourth argument p, a prime, indicates computation mod p.)

Example:

```
powell(F, 3, [-2,1]);
                                         -153306  83099195
                                        [-------, --------]
                                          97969   30664297
```

Note the entry of denominators. It is the rule rather than the exception when working with rational coefficients and coordinates. Of course, denominators should not appear in computations modulo a prime p.

Example:

```
powell(F, 3, [-2,1], 7);
                                        [2, 3]

isoncurve(F, [2,3]); isoncurve(F, [2,3], 7);
                                        false
                                        true
```

`addell`

Use `addell` to add points of a cubic curve E relative to the arithmetic of points on the curve. Call `addell` with the curve as first argument, the points to be added as second and third arguments, and a prime p, if wanted, as optional fourth argument.

Example:

```
 isoncurve(F,[5,13]);
                                        true

addell(F,[-2,1],[5,13]);
                                            -3  -1483
                                           [--, -----]
                                            49   343
```

Get used to seeing denominators. Note also that is it not an easy matter to come up with examples of points on E having rational coordinates, much less integer coordinates.

But now explain what is happening here:

```
addell(F,[-2,1],[5,13],7);
                                           [0, 1, 0]
```

There are 3 coordinates, because the point of F in question is not a point of the affine plane. It is, in fact, the triple of homogeneous coordinates for the unique point of F on the line at infinity — the origin for the arithmetic on F. This computation means, therefore, that $(5, 13)$ is the negative relative to the arithmetic on F when coefficients and coordinates are integers mod 7. Note that this is consistent with the fact that $(-2, -1)$ is the negative of $(-2, 1)$ when coefficients and coordinates are rational since one has

$$5 \equiv\, -2 \pmod 7 \;\text{ and }\; 13 \equiv\, -1 \pmod 7 \quad .$$