What follows is a prettied-up posting to the Usenet newsgroup `sci.math` from some years ago.

```
Path: honte.uleth.ca!news.ucalgary.ca!...(Usenet path truncated)
From: rusin@washington.math.niu.edu (Dave Rusin)
Newsgroups: sci.math
Subject: Re: Elliptic curves equations
Date: 18 Jan 1995 17:20:43 GMT
Organization: Northern Illinois University, Math
Lines: 34
Message-ID: <3fjilb$np7@mp.cs.niu.edu>
References: <3fj9qb$nu0@lute.gcr.com>
NNTP-Posting-Host: washington.math.niu.edu
```

In article `<3fj9qb$nu0@lute.gcr.com>`, Mark W Winstead `<mwwinst@gcr.com>` wrote:

```
>I am looking for the precise definition of an elliptic curve.  Also, as
>some of you know, you can define a group off an elliptic curve.  I would
>also like to have the equations for adding two points on an elliptic
>curve to get their sum.
```

Come now, this one's too fun just to look up. Given two points A and B on the curve, draw the line through them. It meets the curve in one more point C on the curve. Then the group law is defined by $A+B+C=0$. (If $A=B$ you use the tangent line through A instead). Do this intelligently and it's not so bad. If the curve sits in the affine plane over a field, the line in question is the set of points of the form $tA+(1-t)B$. Now if the elliptic curve is the solution to a cubic polynomial f, the third point C is found by asking that $f(tA+(1-t)B)=0$. This is a cubic polynomial in t, and you already know it has roots 0 and 1, so there's not much left to compute: $f(tA+(1-t)B)=t(t-1)(dt+f)$. Then C is $(-f/d)A+(1+f/d)B$.

You might try this on curves in the simple form

$$f=-y^2+x^3+Mx+N;$$

here the origin is the point at infinity, so you find that the negative of (x,y) in the group is the point $(x,-y)$. Writing $A=(x_1,y_1)$ and $B=(x_2,y_2)$ you should get the coordinates of $C=-(A+B)$ to be

$$x_3=-(x_1+x_2)+m^2, \qquad y_3=y_1+m(x_3-x_1),$$

where $m=(y_2-y_1)/(x_2-x_1)$ if A and B are distinct, and $m=(3x_1^2+M)/(2y_1)$ if $A=B$.

Inasmuch as the highly-rated Elliptic Curve Method for factoring large integers relies heavily on repeating this calculation over and over (and over and over), it is highly desirable to do the computations with as few machine cycles as possible. Quite a bit of work has been done in this direction during the 1980's and early 1990's. Montgomery has, I think, taken this work to the limit.

dave