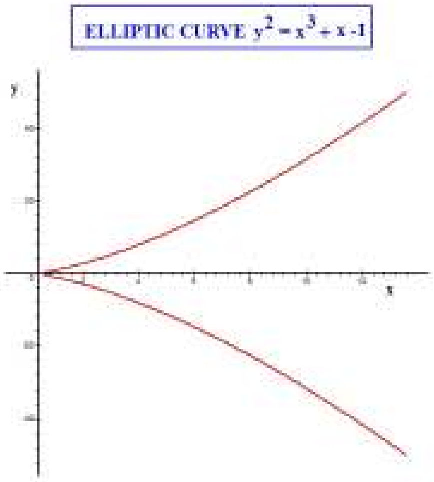
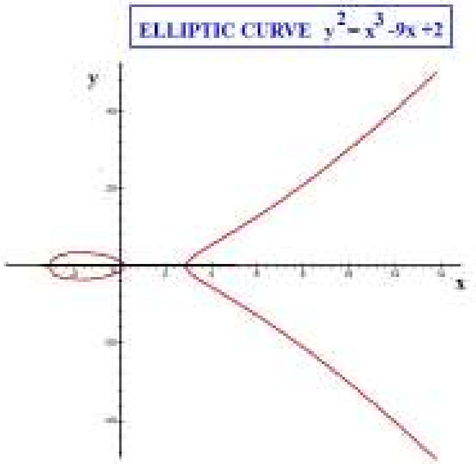
PROPERTIES OF ELLIPTIC CURVES AND THEIR USE IN FACTORING LARGE NUMBERS

A very important set of curves which has received considerably attention in recent years in connection with the factoring of large numbers are the elliptic curves-

$$y^2 = x^3 + ax + b$$

where a and b are integers. We will discuss here some of their properties and then show how they can be used to factor large numbers. Our starting point will be to look at several specific examples. We show you the cases of (1) a=-b=1 and (2) a=-9, b=2 below-





Note that the graphs are symmetric about the x axis and that the derivative becomes infinite at one or three distinct values of x. Also the curves go to ±∞ as x→+∞. The first and second derivatives of these curves are given by-

$$\frac{dy}{dx} = \frac{(3x^2 + a)}{2y} \quad and \quad \frac{d^2y}{dx^2} = \frac{[12xy^2 - (3x^2 + a)^2]}{4y^3}$$

For a>0, there are no points where the derivative is zero and inflection points are encountered when the numerator of the second derivative vanishes. The curves become singular when dy/dx=0/0 and thus when $3x^2=-a$ and y=0 simultaneously.

Next consider two neighboring points $P(x_1,y_1)$ and $Q(x_2,y_2)$ lying along the upper branch of the curve for x>0. If we draw a straight line through these points they will generally intersect the curve at a third point $R(x_3,y_3)$. The equation for this straight line will be-

$$y = sx + c = s(x - x_1) + y_1$$

where s is its slope

$$s = \frac{(y_2 - y_1)}{(x_2 - x_1)}$$

Of particular interest for number factoring is the limiting case where P and Q coincide. Under that condition s can be replaced by the derivative at P(x_1,y_1) and one finds on equating the straight line to the cubic we have at $x=x_3$ that-

$$[s(x\ \ -x_1)+y_1]^2 = x^3 + ax + b$$

This result may be rewritten as the cubic-

$$x^3 - s^2x^2 + (a - 2s(y_1 - sx_1)x + (b - (y_1 - sx_1)^2) = (x\ \ - x_1)^2(x - x_3)$$

Looking at just the coefficient of the x^2 term and setting it to zero (since an elliptic curve has no quadratic term), we find that-

$$x_3 = \left[\frac{(3x_1^2 + a)}{2y_1}\right]^2 - (2x_1)$$

since x_1=x_2 when P=Q. It also follows that-

$$y_3 = \left[\frac{(3x_1^2 + a)}{2y_1}\right](x_3 - x_1) + y_1$$

to yield a unique point R(x_3,y_3). For the case (1) above where a=1 and b=-1, we find R(2,3) if one takes P(1,1)=Q(1,1). For the case (2) where a=-9 and b=2, we find R(69/2, 571sqrt(2)/4) when P(3,sqrt(2))=Q(3,sqrt(2). We test this result by plugging into the cubic curve to find-

(571sqrt(2)/4)^2=(69/2)$^{3\ -}$9(69/2)+2=40755.12499..

which checks. In standard mathematical notation one calls R(x_3,y_3)=2P(x_1,y_1).

Another particularly interesting elliptic curve is-

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

It is rich in integer solutions starting with [x_1,y_1]=[3,4] followed by [6,14], [11,36],[18,76],etc. These points along the upper branch of the solution curve are easiest to determine by substituting subsequent values of x into the equation and then seeing which sum equals the square of an integer. We find that $x_{n+1}=x_n+(2n+1)$ for the integer solution pair[x_{n+1} ,y_{n+1}]. A little manipulation then predicts the very simple result-

$$x_n = 2 + n^2 \text{ , } y_n = n(n^2+3) \text{ , } n = 1,2,3,4,...$$

Thus the integer point [9803, 970596] is guaranteed to lie on the solution curve.

Next we demonstrate how one can use elliptic integrals to factor a number N. The idea behind this approach is due to H. Lenstra (An.of Math126,649-673,1987) and works as follows. Take the first elliptic curve mentioned above and choose the simple composite number N=333. We write-

$$y^2 = x^3 + x - 1(\text{mod}\, N) \; with \; N = 333$$

This elliptic curve has the simple integer point P(1,1) lying along it and we have already shown that another point is R(2,3). To get a point further out on the upper branch of the curve we must first do a bit of manipulation involving modular arithmetic. We note that the derivative of the curve at (2,3) is 13/6 and that this will not produce a larger value for a new x_3. To get an x_3 further out along the upper branch of the curve we must first manipulate the 13/6 derivative term by carrying out a Euclidian Algorithm on the numbers N=333 and 6. Calculating first the greatest common divisor (gcd), we have-

$$333 = 55 \cdot 6 + 3; \qquad 6 = 2 \cdot 3 + 0;$$

Looking at the remainder 3 in the first equation, we have the gcd(333,6)=3. So we see at once that 6 and 333 are both factored by 3 and hence-

$$333 = 3 \cdot 111$$

Furthermore we can break down the 111 by applying Euclid's Algorithm to 111 and 6. This produces the gcd(111,6)=3 so that both 6 and 111 are factored by 3. Thus we have the final result-

$$333 = 3 \cdot 3 \cdot 37 = 9 \cdot 37$$

Which factors our number N. In most cases the factoring is not quite as simple as this and one must work rather hard to actually find the inverse of a number M appearing in the denominator of the derivative of $y(x_3)$ to obtain larger values for x_3. Also one is free to change the a and bs in the elliptic equation. The work can become easier by an appropriate choice of a and b usually not known beforehand.

Next, consider factoring the number N=63=3·3·7 using the equation $y^2=x^3+8x-8$ which also has an integer point P(1,1). Here the derivative at P(1,1) is $dy(x_1)/dx=11/2$. One finds on applying the Euclid Algorithm between 2 and 63 that-

$$63 = 31\cdot 2 + 1;$$

So that gcd(63,2)=1 and on inverting-

$$1 = 1\cdot 63 - 31\cdot 2 \bmod(63)$$

The inverse of 2 then becomes -31+[integer · (63)]. One possibility for 2^{-1} is 32. Thus we can write-

$$x_3 = [11(32)]^2 - 2(1) = 123902$$
$$y_3 = [11(32)](123902 - 1) + 1 = 43613153$$

Notice that these two new large values are integers which contradicts the fact that the cubic $y^2=x^3+8x-8$ has only a limited number of integer points including (1,1), (2,4) , (6,16), (17,71) and (22,104) along the upper branch . This means that x_3 and y_3 must be approximations, but probably pretty good ones. Let's check. We find-

$$(y_3)^2 = 1902107114601409$$
$$x_3^{\ 3} + x_3 - 1 = 1902107028738016$$

So we indeed see close agreement but not an exact match.

Continuing on, we next look at the derivative at the new $y(x_3)$. It yields-

$$\frac{dy(x_3)}{dx} = \frac{23027558410}{43613153}$$

meaning that we have to be able to invert the denominator in the last expression to get the next x_3. It is s clear that 43613153 and 63 have 1 as its greatest common denominator since the first number is prime. So the process must be continued until a point is reached where the denominator of the derivative factors N=63. The factor will turn out to be 3, 7,or 21 in this case. Computer automation makes this elliptic curve method of factoring large numbers N one of the best presently available. However, the challenge still remains to find additional and superior methods for quickly factoring very large numbers of 100 digits or larger as required in cryptography.

Finally let us generate the differential equation which has $y^2=x^3+ax+b$ as a solution. We already have given the form of the first and second derivatives above. Differentiating the first derivative again one has-

$$\frac{d}{dx}\left[\frac{3x^2+a}{2y}\right]=\frac{3x}{y}-\frac{(3x^2+a)}{2y^2}\frac{dy}{dx}=\frac{[3x-(\frac{dy}{dx})^2]}{y}$$

So the governing second order non-linear equation for elliptic curves is-

$$y\frac{d^2y}{dx^2}=3x-\left[\frac{dy}{dx}\right]^2$$

Just to show that things work, take the simple solution $y=x^{(3/2)}$. Here-

$$x^{3/2}(\frac{3}{4\sqrt{x}})=3x-\frac{9x}{4}$$

August 2010