Elliptic curves, Factorization and Primality Testing

Notes for talks given at London South bank University

7, 14 & 21 November 2007

Tony Forbes

ADF34C 3.3.3A

PLANE CURVES, AFFINE AND PROJECTIVE

Let $\mathbb{K}$ be a field, such as $\mathbb{C}$ or a finite field $\mathbb{F}_p$, p prime. We are going to consider curves in $\mathbb{K}^2$ defined by $F(x,y)=0$, where $F(x,y)$ is a polynomial in x,y with coefficients in some subfield of $\mathbb{K}$ (usually $\mathbb{Q}$ or $\mathbb{F}_p$), and $x,y\in\mathbb{K}$.

We extend the affine plane $\mathbb{K}^2$ to the projective plane. Points are equivalence classes of triples (X,Y,Z) with $X,Y,Z\in\mathbb{K}$ not all zero, and two triples are equivalent, $(X,Y,Z)\sim(X',Y',Z')$ iff $X'=tX$, $Y'=tY$, $Z'=tZ$ for some non-zero t.

If $Z\neq 0$, we can identify the triple (X,Y,Z) with $(X/Z,Y/Z)$ in $\mathbb{K}^2$. The triples $(X,Y,0)$ correspond to 'points at infinity'. One can think of these points as directions in $\mathbb{K}^2$.

Now we can define a projective $\mathbb{K}$ curve using projective coordinates, $F(x,y,z)=0$, where $F(x,y,z)$ is a homogeneous polynomial in x,y,z with $x,y,z\in\mathbb{K}$ and coefficients in some subfield of $\mathbb{K}$.

Having said all that, we will most of the time just talk about curves in an affine plane, referring to any new points that arise in the projective plane as *points at infinity*.

Theorem 1 *Let $\mathcal{C}: F(x,y)=0$ be an affine curve in $\mathbb{C}^2$ and let $P=(A,B)$ be a point on $\mathcal{C}$. Suppose $\dfrac{\partial F}{\partial x}(A,B)$ and $\dfrac{\partial F}{\partial y}(A,B)$ are not both zero. Then the tangent line to $\mathcal{C}$ at P is given by*

$$\frac{\partial F}{\partial x}(A,B)\,(x-A)+\frac{\partial F}{\partial y}(A,B)\,(y-B)=0.$$

Proof. This is elementary calculus. □

We call P a *singular* point of the curve $F(x,y)=0$ if

$$\frac{\partial F}{\partial x}(P)=\frac{\partial F}{\partial y}(P)=0.$$

For example, both $\mathcal{C}_1: y^2=x^3+x^2$ and $\mathcal{C}_2: y^2=x^3$ have a singular points at $(0,0)$. In the region $x\in[-1,1]$, $\mathcal{C}_1$ looks vaguely like $\propto$ with two distinct tangents at $(0,0)$, and $\mathcal{C}_2$ looks like $\prec$ with a cusp at $(0,0)$.

We call a point *non-singular* if it is not singular. We call a curve *non-singular* if it has no singular points. Quite often we will restrict our attention to non-singular curves, especially if we want to draw tangents.

Theorem 2 (Bézout) *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be projective $\mathbb{C}$ curves. Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ have no common components. Then the number of points common to both $\mathcal{C}_1$ and $\mathcal{C}_2$, with each point counted with appropriate multiplicity, is given by $(\deg\mathcal{C}_1)(\deg\mathcal{C}_2)$.*

Proof. See [4, Appendix A, Sections 3,4]. This reference has a more rigorous statement of Bézout's theorem as well as a proper explanation of 'appropriate multiplicity'. □

Exercise for reader: The cubics $\mathcal{C}_1:(y-1)(y-2)(y-3)=0$ and $\mathcal{C}_2:(y+1)(y+2)(y+3)=0$ are triples of straight lines parallel to the x-axis. Show that $\mathcal{C}_1$ meets $\mathcal{C}_2$ at infinity with multiplicity 9.

CUBIC CURVES WITH RATIONAL COEFFICIENTS

The most general cubic in two variables $x, y \in \mathbb{C}$ is

$$a_1x^3 + a_2y^3 + a_3x^2y + a_4xy^2 + a_5x^2 + a_6y^2 + a_7xy + a_8x + a_9y + a_{10} = 0$$

We shall insist that the a_i are rational and at least one of a_1, a_2, a_3, a_4 is non-zero. Such a curve is *singular* at (X, Y) if

$$\frac{\partial F}{\partial x}(X, Y) = \frac{\partial F}{\partial y}(X, Y) = 0.$$

Alternatively we projectivize with a third variable, $z \in \mathbb{C}$, and make the polynomial homogeneous

$$F(x, y, z) = a_1x^3+a_2y^3+a_3x^2y+a_4xy^2+a_5x^2z+a_6y^2z+a_7xyz+a_8xz^2+a_9yz^2+a_{10}z^3 = 0.$$

Putting $z = 1$ recovers the original coordinates. Such a curve is *singular* at (X, Y, Z) if

$$\frac{\partial F}{\partial x}(X, Y, Z) = \frac{\partial F}{\partial y}(X, Y, Z) = \frac{\partial F}{\partial z}(X, Y, Z) = 0.$$

This is consistent with the affine definition. Indeed, one can prove that

$$\frac{\partial F}{\partial x}(X, Y, 1) = \frac{\partial F}{\partial y}(X, Y, 1) = 0 \ \Rightarrow \ \frac{\partial F}{\partial z}(X, Y, 1) = 0.$$

Let $\mathbb{K}$, $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$, be a field. A $\mathbb{K}$-*point* is a point whose coordinates are in $\mathbb{K}$.

Theorem 3 *Let $\mathcal{C}$ be a cubic curve with rational coefficients.*
Suppose P_1 and P_2 are two points on $\mathcal{C}$. Then the line $\mathcal{L}$ joining P_1 and P_2 meets $\mathcal{C}$ again at P_3, say. Moreover, if P_1, P_2 are $\mathbb{K}$-points, then so is P_3.
The tangent to $\mathcal{C}$ at a $\mathbb{K}$-point meets $\mathcal{C}$ again at a $\mathbb{K}$-point.

Proof. The equation that determines the x coordinates of the intersection of $\mathcal{C}$ and $\mathcal{L}$ is a cubic in x with rational coefficients and two $\mathbb{K}$-point roots. Hence the third root must also be a $\mathbb{K}$-point. Similarly for the y coordinate. Similarly for the single point and tangent case. □

Being a cubic seems to be essential here. Also it is possible that $P_1 = P_2 = P_3$. You can have a tangent meeting the cubic in three points, as with $y = x^3$ where the tangent at $(0, 0)$ meets the cubic three times at $(0, 0)$.

Example. Take the cubic $y^2 = x^3 - 2$. This has a rational point at $P_1 = (3, 5)$. By differentiating $y = \sqrt{x^3 - 2}$ to get $\dfrac{dy}{dx} = \dfrac{3x^2/2}{\sqrt{x^3 - 2}}$ we see that the slope of the cubic at P_1 is $27/10$. So $\mathcal{L}$, the line tangent to the cubic at P_1, has equation $y = 27x/10 - 31/10$. Plugging this in the cubic gives

$$\left(\frac{27x}{10} - \frac{31}{10}\right)^2 = x^3 - 2,$$

which simplifies to

$$100x^3 - 729x^2 + 1674x - 1161 = 0,$$

which factorizes as $(100x - 1161/9)(x-3)(x-3) = 0$. Hence $\mathcal{L}$ meets the cubic again at $(129/100, -383/1000)$.

Bachet's formula (16??). The example generalizes to any cubic of the form $y^2 = x^3 + c$. If (X, Y) is a point on the cubic, then so is

$$\left(\frac{X^4 - 8cX}{4Y^2}, \frac{-X^6 - 20cX^3 + 8c^2}{8Y^3} \right).$$

Theorem 4 *Suppose $\mathcal{C}$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are cubic curves with no common components. Suppose $\mathcal{C}$ goes through eight of the nine intersection points (counted with appropriate multiplicities) of $\mathcal{C}_1$ and $\mathcal{C}_2$. Then $\mathcal{C}$ also goes through the ninth intersection point.*

Proof. A cubic curve is defined by 10 coefficients. But one of them is redundant because we can divide through by it. Hence the linear space spanned by the coefficients of possible cubics is 9-dimensional. So the linear space spanned by the coefficients of possible cubics that go through 8 given points is 1-dimensional.

Suppose $F_1(x, y) = 0$ and $F_2(x, y) = 0$ define the curves $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. Now consider the cubics obtained by taking linear combinations: $\lambda_1 F_1 + \lambda_2 F_2 = 0$ with λ_1, λ_2 not both zero. These cubics pass through the eight intersection points

Because the cubics that go through the eight intersection points form a 1-dimensional space, and because $\lambda_1 F_1 + \lambda_2 F_2$ is a 1-dimensional space, *all* such cubics, including $\mathcal{C}$, must be of the form $\lambda_1 F_1 + \lambda_2 F_2 = 0$.

But then, since F_1 and F_2 are both zero at the ninth point, $\mathcal{C}$ also passes through the ninth point. □

THE CUBIC CURVE GROUP

Let $\mathbb{K}$ be a field, $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$. Take a non-singular cubic curve $\mathcal{C}$ with rational coefficients. Choose a $\mathbb{K}$-point O (O can be at infinity).

Define binary operations $*$ and $+$ on the $\mathbb{K}$-points of $\mathcal{C}$ as follows.

Take two $\mathbb{K}$-points on $\mathcal{C}$. Consider the line $\mathcal{L}$ defined by P and Q. If $P = Q$, this is the tangent to $\mathcal{C}$ at P; if $P \neq Q$, this is the line that passes through P and Q. Then $P * Q$ is the third point of $\mathcal{C}$ that intersects $\mathcal{L}$, and

$$P + Q = (P * Q) * O.$$

If P is a point of inflexion, then $P * P = P$.

Theorem 5 *Let $\mathcal{C}$ be a non-singular projective cubic curve with rational coefficients. The $\mathbb{K}$-points of $\mathcal{C}$ together with the operation $+$ is an Abelian group.*

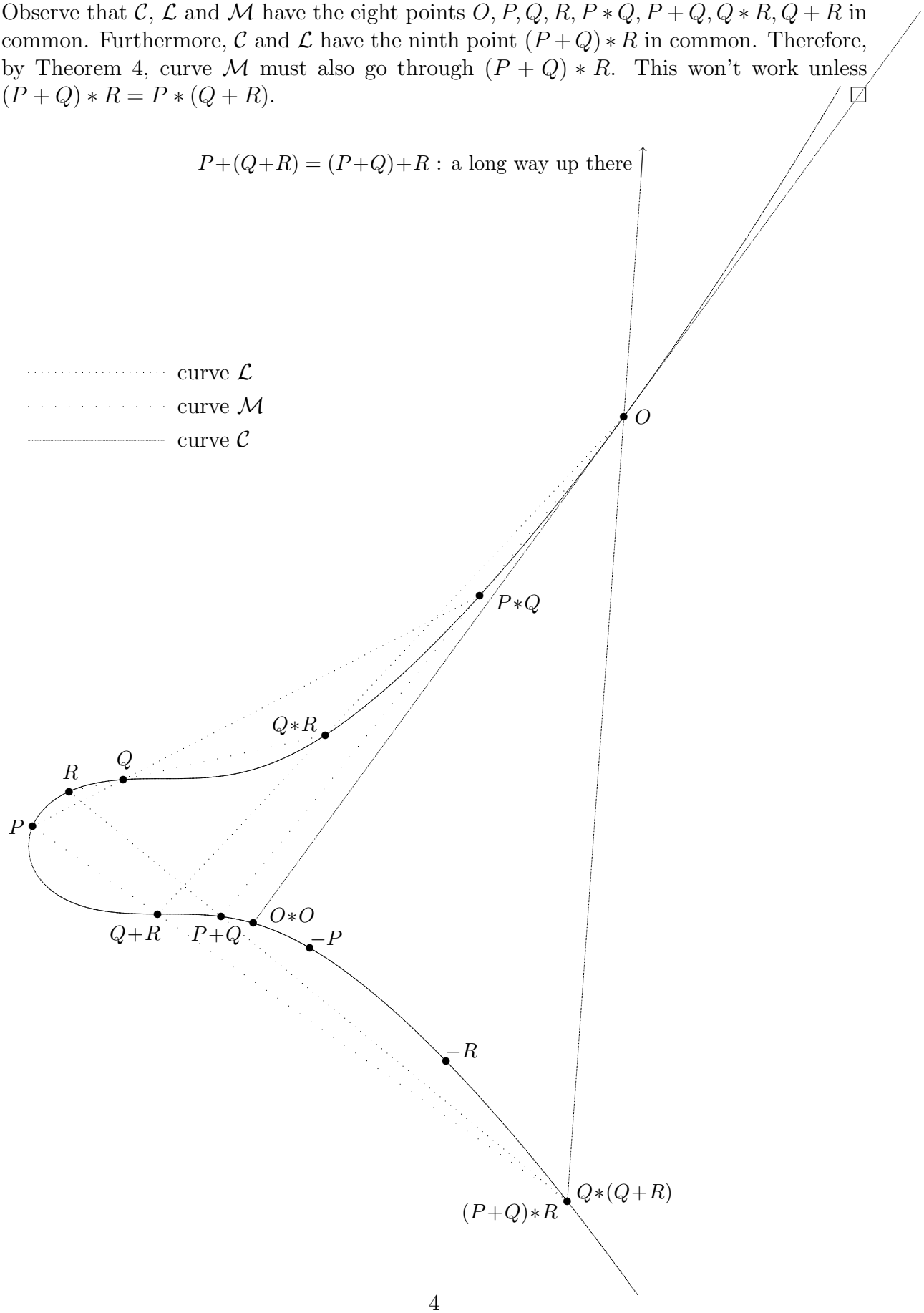
Proof. Closure follows from Theorem 3, it is clear that O is the identity, and it is obvious that the operation $+$ is commutative.

Define $-P = P * (O * O)$. Then $P + (-P) = (P * (-P)) * O = (O * O) * O = O$, and one can also prove that $-P$ is the only point that has this property.

Associativity. Let P, Q and R be distinct $\mathbb{K}$-points on $\mathcal{C}$. We wish to prove that $(P + Q) + R = P + (Q + R)$. It suffices to prove that $(P + Q) * R = P * (Q + R)$.

Let $\mathcal{L}_1$ denote the line containing the points $P, Q, P * Q$.
Let $\mathcal{M}_1$ denote the line containing the points $O, P * Q, P + Q$.
Let $\mathcal{L}_2$ denote the line containing the points $R, P + Q, (P + Q) * R$.

Let $\mathcal{M}_2$ denote the line containing the points $Q, R, Q * R$.
Let $\mathcal{L}_3$ denote the line containing the points $O, Q * R, Q + R$.
Let $\mathcal{M}_3$ denote the line containing the points $P, Q + R, P * (Q + R)$.
Let $\mathcal{L}$ denote the cubic defined by the triple of lines $\mathcal{L}_1$, $\mathcal{L}_2$, $\mathcal{L}_3$.
Let $\mathcal{M}$ denote the cubic defined by the triple of lines $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$.
Observe that $\mathcal{C}$, $\mathcal{L}$ and $\mathcal{M}$ have the eight points $O, P, Q, R, P * Q, P + Q, Q * R, Q + R$ in common. Furthermore, $\mathcal{C}$ and $\mathcal{L}$ have the ninth point $(P + Q) * R$ in common. Therefore, by Theorem 4, curve $\mathcal{M}$ must also go through $(P + Q) * R$. This won't work unless $(P + Q) * R = P * (Q + R)$. □



WEIERSTRASS NORMAL FORM

A function is *rational* if it is the ratio of two polynomial functions. A *birational map* is a function ϕ : (projective complex plane) $\to$ (projective complex plane) such that ϕ is a rational function with a rational function inverse ϕ^{-1} defined at least nearly everywhere.

Given a projective cubic curve $\mathcal{C}$, it is possible to find a birational map that transforms it into *Weierstrass normal form*:

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3.$$

(And with a further linear transformation you can get rid of the x^2 term as well.) This curve has a single point with $z = 0$, equivalent to $(0, 1, 0)$; so for simplicity one can think of the affine curve

$$y^2 = x^3 + ax^2 + bx + c,$$

together with *the* point at infinity, which is in the direction of the y-axis.

A non-singular cubic in Weierstrass normal form is called an *elliptic curve*. With the curve in this form life becomes much easier, especially for performing computations.

Let $\mathcal{C}$ be the cubic defined by $F(x, y) = y^2 - f(x) = 0$, where $f(x) = x^3 + ax^2 + bx + c$. Then

$$\frac{\partial F}{\partial x} = -f'(x), \qquad \frac{\partial F}{\partial y} = 2y.$$

Now $\mathcal{C}$ is singular at (x, y) iff both derivatives are zero. Equivalently, $y = 0$ and x is a root of both $f(x)$ and $f'(x)$. This is equivalent to $f(x)$ having a double root at x. Thus we have a simple criterion: $\mathcal{C}$ is non-singular iff the discriminant $\Delta f(x)$ is non-zero. The discriminant can be computed:

$$\Delta f(x) = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2,$$

where α, β, γ are the roots of $f(x)$ in its splitting field.

Example. $u^3 + v^3 = k$, $k \neq 0$. Put

$$u = \frac{36k + y}{6x}, \quad v = \frac{36k - y}{6x}.$$

Then the cubic becomes

$$y^2 = x^3 - 432k^2$$

and its discriminant is non-zero. The inverse transformation is

$$x = \frac{12k}{u + v}, \quad y = 36k\,\frac{u - v}{u + v}.$$

The Weierstrass elliptic function. Given complex numbers ω_1, ω_2, such that $\omega_1/\omega_2 \notin \mathbb{R}$, we define the lattice

$$\mathbb{L} = \mathbb{L}(\omega_1, \omega_2) = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$$

and the doubly periodic function

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \mathbb{L}\setminus 0} \left(\frac{1}{(z + \omega)^2} - \frac{1}{\omega^2} \right).$$

Then $\wp(z)$ has periods ω_1 and ω_2. The series converges absolutely and hence $\wp(z)$ has a double pole at 0. Let

$$g_2 = 60 \sum_{\omega \in \mathbb{L}\setminus 0} \frac{1}{\omega^4}, \qquad g_3 = 140 \sum_{\omega \in \mathbb{L}\setminus 0} \frac{1}{\omega^6}.$$

Then $\wp$ satisfies the differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

So the map ψ defined by

$$\psi : z \mapsto \begin{cases} (\wp(z), \wp'(z), 1), & \text{if } z \notin \mathbb{L}, \\ (0, 1, 0), & \text{if } z \in \mathbb{L}, \end{cases}$$

gives an isomorphism between the torus $\mathbb{C}/\mathbb{L}$ and the elliptic curve $y^2 = 4x^3 - g_2x - g_3$ with discriminant $\Delta = 16(g_2^3 - 27g_3^2)$. Moreover, there is the addition formula

$$\wp(z_1 + z_2) = \begin{cases} -\wp(z_1) - \wp(z_2) + \dfrac{1}{4}\left(\dfrac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2, & \text{if } z_1 \neq z_2, \\ -2\wp(z_1) + \dfrac{1}{4}\left(\dfrac{\wp''(z_1)}{\wp(z_1)}\right)^2, & \text{if } z_1 = z_2. \end{cases}$$

from which one can derive the addition formulae for the corresponding elliptic curve group.

THE ELLIPTIC CURVE GROUP

Given points P and Q on an elliptic curve with $O = \infty$, we shall obtain an explicit formula for $P + Q$. Let the curve be $y^2 = x^3 + ax^2 + bx + c$ and let P_1, P_2 be points on it.

Write $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1 * P_2 = (x_3, -y_3)$, and note the minus sign. Then because O is a long long way away in the y direction, we have $P_1 + P_2 = (x_3, y_3)$.

Assume $P_1 \neq P_2$. The line joining P_1, P_2 is

$$y = \lambda x + \mu, \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \mu = y_1 - \lambda x_1.$$

To get (x_3, y_3), the point where the line meets the curve, substitute $y = \lambda x + \mu$ to get

$$(\lambda x + \mu)^2 - x^3 - ax^2 - bx - c = -(x - x_1)(x - x_2)(x - x_3) = 0$$

and equate coefficients of x^2 to get

$$\lambda^2 - a = x_1 + x_2 + x_3.$$

Hence

$$x_3 = \lambda^2 - a - x_1 - x_2, \qquad y_3 = -\lambda x_3 - \mu,$$

or

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 - a - x_1 - x_2, -\lambda x_3 - \mu).$$

If $y_1 \neq y_2$, then $(x_1, y_1) + (x_1, y_2) = O$ because now $\lambda = \infty$.

If $x_1 = x_2$, then we use for λ the slope of the tangent at (x_1, y_1):

$$\lambda = \frac{dy}{dx}(x_1, y_1) = \frac{3x_1^2 + 2ax_1 + b}{2y_1}.$$

As usual with Abelian groups, we write $2X$ for $X+X$, and in general mX for $(m-1)X+X$.

Observe that for any point on the curve of the form $(x_1, 0)$, the tangent at $(x_1, 0)$ is vertical; so $2(x_1, 0) = O$. Thus points of order 2 (if any) occur at the roots of $x^3 + ax^2 + bx + c$. If all three points are present, they together with O form the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The x coordinates of points of order 3 are roots of

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

(Compute the x coordinate of $2(x, y)$ and equate to x, the x coordinate of $-(x, y)$.) If these roots are distinct and if the corresponding $\pm y$ values are distinct, and if all eight points are on the curve, then together with O they form a group of order 9, namely $\mathbb{Z}_3 \times \mathbb{Z}_3$. On a real curve the points of order 3 occur at the points of inflexion.

Theorem 6 (Mordell) *The group of rational points on an elliptic curve with rational coefficients is the finitely generated Abelian group $\mathcal{T} \times \mathbb{Z}^r$, where $\mathcal{T}$ is the finite subgroup consisting of rational points of finite order and r is a non-negative integer.*

The number r is called the *rank* of the group, and $\mathcal{T}$ is called the *torsion subgroup.*

Theorem 7 (Mazur) *The torsion subgroup of Theorem 6 can only be isomorphic to one of the following 15 groups:*

$$\mathbb{Z}_m, \quad m = 1, 2, \ldots, 9, 10, 12, \quad \textit{or} \quad \mathbb{Z}_2 \times \mathbb{Z}_{2m}, \quad m = 1, 2, 3, 4.$$

Hence the order of the torsion subgroup can never exceed 16.

Theorem 8 (Lutz–Nagell) *If the coefficients a, b, c of an elliptic curve are integers, and if (x, y) is a rational point of finite order, then x and y are integers, and either $y = 0$ or $y^2 | \Delta$. Furthermore, if p is an odd prime that does not divide the discriminant of the curve, then the reduction map restricted to the torsion subgroup is one-one.*

Example. Consider the curve $y^2 = x^3 - 36x$. The points of order 2 are at the roots of the cubic, $(0, 0), (\pm 6, 0)$. So there is a subgroup $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Also one can show that $(-2, 8)$ has order greater than 16; so the group has rank at least 1. In fact the torsion subgroup is actually isomorphic to $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and the rank of the group really is 1.

So we now know that the order of the torsion group is small. But all known ranks are small, too, the largest (as at November 2007) being 28.

Open problem. Is there an upper bound on the rank of the group of rational points on an elliptic curve?

However, we do have the following upper bound for the rank, which depends only on the factors of the discriminant (see [3, Proposition 4.19]).

Let the zeros of $x^3 + ax^2 + bx + c$ be α, β and γ, so that the discriminant of the curve is $(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$. Let π_1 denote the number of primes that divide exactly one of $\alpha - \beta$, $\alpha - \gamma$ and $\beta - \gamma$. Let π_2 denote the number of primes that divide two, and hence all three of $\alpha - \beta$, $\alpha - \gamma$ and $\beta - \gamma$. Then if a, b and c are integers and r is the rank of the curve, we have

$$r \leq \pi_1 + 2\pi_2 - 1.$$

A list of record-breaking ranks of elliptic curves as at November 2007 [Dujella, http://web.math.hr/∼duje/tors/tors.html]:

$\mathcal{T}$	rank	who and when
$\{O\}$	28	Elkies (2006)
$\mathbb{Z}_2$	18	Elkies (2006)
$\mathbb{Z}_3$	13	Eroshkin (2007)
$\mathbb{Z}_4$	12	Elkies (2006)
$\mathbb{Z}_2 \times \mathbb{Z}_2$	14	Elkies (2005)
$\mathbb{Z}_5$	6	Dujella–Lecacheux (2001)
$\mathbb{Z}_6$	7	Dujella (2001,2006), Eroshkin (2007)
$\mathbb{Z}_7$	5	Dujella–Kulesz (2001), Elkies (2006)
$\mathbb{Z}_8$	6	Elkies (2006)
$\mathbb{Z}_2 \times \mathbb{Z}_4$	8	Elkies (2005)
$\mathbb{Z}_9$	3	Dujella (2001), MacLeod (2004), Eroshkin (2006), Eroshkin–Dujella (2007)
$\mathbb{Z}_{10}$	4	Dujella (2005), Elkies (2006)
$\mathbb{Z}_{12}$	3	Dujella (2001,2005,2006), Rathbun (2003,2006)
$\mathbb{Z}_2 \times \mathbb{Z}_6$	6	Elkies (2006)
$\mathbb{Z}_2 \times \mathbb{Z}_8$	3	Connell (2000), Dujella (2000,1,6), Campbell–Goins (2003), Rathbun (2003,6)

And here, for example, is the rank 14 curve with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_2$ (Elkies, 2005):

$$\begin{aligned} y^2 &= x^3 + x^2 - 1268052845566467493359390830758088982868000060 41\, x \\ &\quad + 643793313699399778366415146783051122430039276438015681484514903112995 9. \end{aligned}$$

Discriminant:

$2^8 \cdot 3^6 \cdot 5^2 \cdot 7^4 \cdot 11^4 \cdot 19^2 \cdot 31^2 \cdot 41^2 \cdot 59^2 \cdot 61^2 \cdot 67^2 \cdot 89^2 \cdot 107^2 \cdot 137^2 \cdot 173^2 \cdot 199^2 \cdot 241^2 \cdot 263^2 \cdot 347^2 \cdot 383^2 \cdot 421^2 \cdot 607^2 \cdot 613^2 \cdot 821^2 \cdot 1103^2 \cdot 1621^2 \cdot 4127^2 \cdot 6491^2 \cdot 21319^2 \cdot 22639^2$.

Four torsion points:

O,
$(-37918794306490795215 2101, 0)$,
$(51870834651609429682821, 0)$,
$(32731710841329852246 9279, 0)$.

Fourteen independent points of infinite order:

$(-81970142887190856673101, 12759864611101256666082696860554 3800)$,
$(-18984134573496121015547 1, 15384728439871635104858358484778 0100)$,
$(-16997876756220820658564 1, 15192425661742654875596221925415 3720)$,
$(33014620114926581780241 9, 23631234300896247709645396196927880)$,
$(33932177644287702305715, 46628563736499124960967519990139912)$,
$(50406420344642537872966 71, 11288943893314536628860892480063576320)$,
$(87003996297663795182542 5, 74478588611457705242485790489768 1972)$,
$(-94766107666974777578601, 13267900528207075300269916676185 8600)$,
$(36383241902220788682821, 43272482685006943024094711026446000)$,
$(32732815198161991848891 9, 14660301361870663029888023088298 80)$,
$(-35195310533062185489054, 86433024924668666503453219833567375)$,
$(87550004905649373826135107 69/64, 81918650872038320813050162701061611971 4345/512)$,
$(-21492190599047486336174 1, 15415452421896437456989522564607 8920)$,
$(-30638181710700171821444 1, 12856423014463601265074979598946 8680)$.

THE ELLIPTIC CURVE GROUP MODULO p

It is possible to do everything modulo p for an odd prime p. Now an elliptic curve is the set of points (x, y) such that

$$y^2 \equiv x^3 + ax^2 + bx + c \pmod{p}$$

for some a, b, c satisfying

$$-4ca^3 + a^2b^2 + 18abc - 4b^3 - 27c^2 \not\equiv 0 \pmod{p},$$

together with the 'point at infinity', O, or $(0, 1, 0)$ in projective coordinates.

Although the geometric interpretation is lost, the formula for $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ works just as before. We agree that $y_1 \neq y_2 \Rightarrow (x_1, y_1) + (x_1, y_2) = O$ and $2(x, 0) = O$ for points (x_1, y_1), (x_1, y_2) and $(x, 0)$ on the curve.

Of course one needs to prove that this structure forms an Abelian group. As before, associativity is difficult. Unfortunately our existing Theorem 5 won't work. However, we can at length prove that associativity holds by applying the formulae. This tedious exercise is left to the reader!

So the construction of the group works exactly as it does in $\mathbb{C}$, even though what we have to define addition in the $\mathbb{F}_p$ case are just some meaningless expressions. Personally I find this utterly amazing!

Example

$$y^2 = x^3 + x + 1, \quad p = 5.$$

The points on the curve are $\{O, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}$.

The discriminant is $-4 - 27 = 4 \pmod{p}$.

Let $P = (0, 1)$. Then $2P = (4, 2)$, $3P = P + 2P = (0, 1) + (4, 2) = (2, 1)$, $4P = 2(2P) = 2(4, 2) = (3, 4)$, $6P = 2(3P) = 2(2, 1) = (2, 4)$ and $9P = 6P + 3P = (2, 4) - (2, 1) = O$. The rest follows by negation.

P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$
$(0, 1)$	$(4, 2)$	$(2, 1)$	$(3, 4)$	$(3, 1)$	$(2, 4)$	$(4, 3)$	$(0, 4)$	O

The group is $\mathbb{Z}_9$.

Theorem 9 (Special case of Weil's theorem) *Suppose θ is the quadratic character: $\theta(x) = 1$ if x is a non-zero square modulo p, $\theta(x) = -1$ if x is not a square modulo p, $\theta(0) = 0$. Suppose $f(x) \in \mathbb{F}_p[x]$ is a cubic with distinct roots in its splitting field, and suppose $f(x)$ is not a constant multiple of a square. Then*

$$\left| \sum_{x \in \mathbb{F}_p} \theta(f(x)) \right| \leq 2\sqrt{p}.$$

Proof. See [5], pages 1–80 for a proof of Weil's theorem. □

Theorem 10 (Hasse) *Let $\mathcal{C}$ be an elliptic curve modulo p. Then $|\mathcal{C}|$, the number of points of $\mathcal{C}$, satisfies*

$$p + 1 - 2\sqrt{p} \leq |\mathcal{C}| \leq p + 1 + 2\sqrt{p}.$$

Proof. Let the curve be given by $y^2 = f(x)$, where $f(x)$ is a cubic with three distinct roots in its splitting field. Then we have, remembering to count the point at infinity,

$$|\mathcal{C}| = 1 + \sum_{x=0}^{p-1}(1 + \theta(f(x))) = p + 1 + \sum_{x=0}^{p-1}\theta(f(x)).$$

Now use Theorem 9. □

INTEGER FACTORIZATION: POLLARD $p-1$ METHOD

Given a positive integer N, we want to find a non-trivial factor of N.

First see if N is a probable prime. If it is we don't attempt to factorize N; instead we look for a primality proof. The simplest probable-primality test is based on *Fermat's little theorem*:

$$2^N \equiv 2 \pmod{n}. \qquad (*)$$

Hence if $2^N \not\equiv 2 \pmod{N}$, then we can conclude that N is composite. Conversely, if we compute $2^N \bmod N$ and the answer is 2, although we cannot prove anything, it turns out nevertheless that N is quite likely to be prime. Composite numbers that satisfy (*) are known as *pseudoprimes to the base* 2. Although comparatively rare, they do exist—341, for example—and therefore as a primality test (*) can sometimes give an erroneous result.

The $p-1$ method (John Pollard, 1974). Suppose N has a prime factor p. Compute

$$M = 2^{1000000!} \bmod N.$$

Now suppose $p-1$ divides 1000000!, which will happen if $p-1$ is a product of primes less than 1000000 with not too many duplicates. Then $M \equiv 1 \pmod{p}$. Hence p divides $g = \gcd(M-1, N)$ and g will be greater than 1 and a factor of N. If we are unlucky, g will be N itself and we will have gained nothing. But most of the time g will be a non-trivial divisor of N, which is precisely what we want.

There is nothing special about 1000000!. In practice, one computes $M_1 = 2^1$, $M_2 = M_1^2$, $M_3 = M_2^3$, ..., doing the gcd test every few hundred iterations.

As a test, the $p-1$ method takes only a few seconds to find the prime factors 1659431 and 1325815267337711173 of $10^{53} - 1$. (This explains why in encryption methods involving the RSA scheme you should avoid primes p where $p-1$ or (for other reasons) $p+1$ is a product of small primes.) In fact we have

$$\begin{aligned} 1659431 - 1 &= 2 \cdot 5 \cdot 31 \cdot 53 \cdot 101, \\ 1325815267337711173 - 1 &= 2^2 \cdot 3^2 \cdot 11 \cdot 53 \cdot 1279 \cdot 1553 \cdot 3557 \cdot 8941. \end{aligned}$$

The other factors are 3^2 and 107, and the cofactor 47198858799491425660200071 is prime.

The obvious drawback with the $p-1$ method is that it works only for divisors p of N where $p-1$ is the product of small primes. Unfortunately this doesn't happen very often.

The $p-1$ method is so called because the computations to find that prime factor p are taking place in a group of order $p-1$, namely the multiplicative group modulo p. If $p-1$ is not a product of small primes, perhaps we can find some group of order q, say, in which to perform the same computations, where q *is* a product of small primes. This is the basis of the elliptic curve method.

INTEGER FACTORIZATION: ELLIPTIC CURVES (H. W. Lenstra, 1987)

Given a positive integer N, we want to find a non-trivial factor of N.

We create an elliptic curve of the form

$$y^2 = x^3 + bx + c$$

by choosing b and c at random subject to $\gcd(4b^3 + 27c^2, N) = 1$. This last condition makes sure that $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ for any prime factor p of N.

Denote the group by $E(b, c; p)$, where p is a prime factor of N. Group addition $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ is as follows.

(i) If $y_1 \neq 0$, then $(x_1, y_1) + (x_1, -y_1) = O$;

(ii) $(x_1, 0) + (x_1, 0) = O$;

(iii) In all other cases,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{if } x_1 \neq x_2, \qquad \lambda = \frac{3x_1 + b}{2y_1} \quad \text{if } x_1 = x_2,$$

$$(x_1, y_1) + (x_2, y_2) \;=\; (\lambda^2 - x_1 - x_2,\ \lambda(x_1 - x_3) - y_1).$$

What we would like to do now is compute $M_1 = A$, $M_2 = 2M_1$, $M_3 = 3M_2$, ... in $E(b, c, p)$ for some starting point A on the curve. Unfortunately we can't work directly in this group because we don't know what p is.

So we work modulo N. We pretend that N is prime, we work as if $E(b, c; N)$ is a group, and we can imagine the computations reduced modulo p for the unknown divisor p of N. We compute $M_1 = A$, $M_2 = 2M_1$, $M_3 = 3M_2$, ... in $E(b, c; N)$. However, the computation of λ involves determining the multiplicative inverse of d, say, where $d = x_2 - x_1$ or $d = 2y_1$. Assuming $d \not\equiv 0 \pmod{N}$, for the inverse of d to exist we must have $\gcd(d, N) = 1$. So we need to make this test each time we compute λ. If $\gcd(d, N) = 1$, we proceed with the computations. On the other hand, if we find that $\gcd(d, N) > 1$, we stop the process because we have actually succeeded in finding a non-trivial factor of N.

If we have computed M_j as far some largish number, say $M_{1000000} = (1000000!)A$, and the gcd test has failed to produce a factor, we give up and start again with a new elliptic curve chosen at random. And if this doesn't work we choose another curve. And so on.

The method works when N has a prime factor p for which $|E(b, c; p)|$ has only small prime factors. We know from Theorem 10,

$$p + 1 - 2\sqrt{p} \leq |E(b, c; p)| \leq p + 1 + 2\sqrt{p}.$$

It is known that all these values occur. Indeed, we have the following result.

Theorem 11 (Waterhouse, 1969) *Given a prime $p > 3$ and any q in the range $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$, there exists b, c such that $|E(b, c; p)| = q$.*

Furthermore, the orders of the $E(b, c; p)$ seem to be reasonably uniformly distributed throughout the allowed interval.

Calculating jX is performed 'Russian agricultural community' style, so it can be done with just doubling and adding X. Start with $Y = O$ and expand j in binary. Then scan the sequence of binary digits left to right. If you see a 1, double Y and add X. If you see a 0, just double Y. For example, 21 is 10101 in binary; so $21X$ gets computed as $2(2(2(2(X)) + X)) + X$. In general the number of doublings is $\lfloor \log_2 j \rfloor$ and the number of $+ X$ operations is about half of that.

In the usual implementation of the elliptic curve method there are two stages, determined by two parameters, r and s. Let $q_1, q_2, \ldots, q_\sigma$ be the sequence of primes between r and s. In the first stage we compute M_r, as before. In the second stage we compute $S_1 = q_1 M_r$ followed by $S_2 = q_2 M_r = (q_2 - q_1)M_r + S_1$, $S_3 = q_3 M_r = (q_3 - q_2)M_r + S_2$, $\ldots$, $S_\sigma = q_\sigma M_r = (q_\sigma - q_{\sigma-1})M_r + S_\sigma$.

This works if $|E(b, c; p)|$ divides $r!q$ for some prime q in the interval $[r, s]$. Because the differences $q_{i+1} - q_i$ are small and often duplicated, the second stage goes quite quickly. Typical values of the parameters might be something like $r = 10000000, s = 1000000000$. Because of excessive duplication of small primes in $k!$ when k is large it is grossly wasteful to compute M_j in the simple manner that I have indicated. It is better to compute $M_j = p_j^{\alpha_j} M_{j-1}$, where p_j is the jth prime and the α_j are smallish numbers chosen with some care.

Ten factors found by elliptic curves (information supplied by Paul Zimmerman) [http://www.loria.fr/∼zimmerma/records/top100.html]:

	factor	from	when	who
67	444434979215670990789575255179863190894618060876873794628023807888 1	$10^{381}+1$	Aug 2006	B. Dodson
66	709601635082267320966424084955776789770864725643996885415676682297	$3^{466}+1$	Apr 2005	B. Dodson
65	652575267726449487647992128877025733918877152359815303437035067 31	$78^{129}-1$	May 2007	A. Bhargava/S. Pelissier
64	434467305871495447776131479343739290067288544536110390554895093 3	$10^{311}-1$	Sep 2005	K. Aoki/T. Shimoyama
63	516469933130631687266967194982169414626403685360388146231581267	$3^{533}+1$	Nov 2005	A. Kruppa
62	3106915037887379089520804689577136094946329354641210595144942 9	$2^{2034}+1$	Apr 2005	B. Dodson
62	1090227947018883491577649342728342046007427895751873028517091 3	$761^{68}+1$	Oct 2007	R. Hooft
61	845244690710948240607535422620066647006561114102225534469755 7	$77^{103}-1$	Jan 2007	CWI
61	781919897344868678956873258393150732185255488033133848503606 9	$61^{141}+1$	Apr 2007	A. Bhargava/S. Pelissier
61	204881518021551346338833557607121416822907767785864180923108 1	$2^{905}+1$	Sep 2006	B. Dodson

PRIMALITY TESTING: ELLIPTIC CURVES

Given a prime number, N, prove that N really is prime.

Much of this section is based on [1, Chapter 9].

In elementary number theory we have the following useful result.

Theorem 12 (Pocklington) *Suppose $N - 1$ is partially factorizable, say $N - 1 = FR$, where F is even, R is odd, $\gcd(F, R) = 1$ and F is completely factorized into primes. Suppose also that for each prime factor p of F there is a number a such that $a^{N-1} \equiv 1 \pmod N$ and $\gcd(a^{(N-1)/p} - 1, N) = 1$. Then any prime factor q of N must satisfy $q \equiv 1 \pmod F$.*

If N satisfies the conditions of Pocklington's theorem and $F > \sqrt{N}$ then we can conclude that N is prime. (With a bit more work, and a few extra conditions, you can prove the primality of N if $F > \sqrt[3]{N}$; see [2], for example.) As a primality test this works fine except that in general it is not possible to factorize $N - 1$ sufficiently. So, as with integer factorization, we use elliptic curves and a simplified analogue of Theorem 12.

Theorem 13 ([1, Section 9.2]) *Let $N > 1$ be an integer coprime to 6. Suppose that there there is a point P on the elliptic curve $y^2 = x^3 + bx + c$, where $gcd(4b^3 + 27c^2, N) = 1$, an integer m, and a prime divisor q of m satisfying the following conditions:*

(i) $q > (\sqrt[4]{N} + 1)^2$;

(ii) $mP = O$;

(iii) $(m/q)P \neq O$;

where all computations have been performed successfully in $E(b, c; N)$. Then N is prime.

Proof. Whilst performing computations in $E(b, c; N)$ for this theorem we are pretending that N is prime. As with factorization, everything works fine except possibly division during the computation of λ. But if a division fails, then N must be composite.

Suppose the conditions of the theorem hold for N and suppose N has a prime divisor $p < \sqrt{N}$. Then the computations in $E(b, c; N)$ that we performed modulo N can be reduced modulo p.

Now $E(b, c; p)$ is a legitimate elliptic curve group. Hence the point P in $E(b, c; p)$ has order which is a divisor of m but not a divisor of m/q. But since q is prime, q must divide the order of P in $E(b, c; p)$. So using Theorem 10 we have

$$q \le |E(b, c; p)| \le p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 < (\sqrt[4]{N} + 1)^2,$$

a contradiction. □

Theorem 13 is the basis of the *Goldwasser–Kilian test*. But there are two serious problems that need addressing.

The first is in the computation of m for Theorem 13. It turns out that to obtain a suitable m we may assume that N is prime and use $m = |E(b, c; N)|$, the order of the elliptic group modulo N. Computation of $|E(b, c; N)|$ is difficult, but it is feasible for N of a few thousand digits. Cohen's book [1] describes the Goldwasser–Kilian algorithm, which was fashionable in 1995, but since then enormous progress has been made. If one chooses the parameters on the elliptic curve carefully, then the computation of $|E(b, c; N)|$ can be speeded up considerably.

Again, it looks like we are assuming what we want to prove, namely that N is prime. But so long as the m which results actually works in Theroem 13 nobody is going to care where it came from. If $m = |E(b, c; N)|$ fails condition (ii) of Theorem 13, then N must be composite.

The second problem is that of finding a suitable prime factor q of m. If N has thousands of digits, the task of factorizing $m = |E(b, c; N)|$ is usually hopeless. In practice, what happens is that you look for an elliptic curve where $|E(b, c; N)|$ factorizes completely into a few small primes plus one big factor, q, $(\sqrt[4]{N} + 1)^2 < q < N$, where a simple test such as the converse of Fermat's little theorem indicates that q is a probable prime. We then pretend that q really is prime and use it in Theorem 13.

But now we have opened up a gaping hole in the logic. Theorem 13 is not a valid primality proof unless q is a true, proven prime. The only known way to get around this difficulty is to use Theorem 13 with q in place of N to prove that q is prime. But that creates another probable prime, q', a divisor of $|E(b', c'; q)|$, say, whose primality needs to be established beyond all doubt. And so on. Thus we need to perform a whole sequence of tests using Theorem 13 with smaller and smaller values of q until we reach a stage where the primality of q can be proved by elementary means.

In the Primo implementation [http://www.ellipsa.net/public/primo/record.html], the primality proof of the 7993-digit number

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot \cdots \cdot 18517 + 39317$$

required 1084 iterations of Theorem 13 and about 8.3 months of serious computing.

To give some indication of what can be achieved, we present a selection of large primes that have been verified by modern versions of the elliptic curve method [Chris Caldwell: http://primes.utm.edu/top20/page.php?id=27].

prime	digits	when	who
$((((((2521008887^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$	20562	Jun 2006	Morain, FastECPP
$2638^{4405}+4405^{2638}$	15071	Jul 2004	Wirth, Kleinjung, Franke, Morain, FastECPP
$(2^{42737}+1)/3$	12865	Aug 2007	Morain
$1234^{3265}+3265^{1234}$	10094	Aug 2005	Morain, FastECPP
$2739^{2930}+2930^{2739}$	10073	Jan 2005	Morain, FastECPP
$2072644824759\cdot 2^{33333}+5$	10047	Nov 2008	Morain, FastECPP [*M500* **226**]
$648^{3571}+3571^{648}$	10041	Dec 2003	Morain
$10^{9999}+33603$	10000	Aug 2003	Wirth, Kleinjung, Franke, FastECPP
$2658^{2659}+2659^{2658}$	9106	Aug 2005	Morain, FastECPP
$13^{8148}+2716^{2197}$	9077	Jan 2005	Morain

References

[1] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer–Verlag 1995.

[2] ADF, Large prime quadruplets, *Math. Gazette*, November 2000.

[3] Anthony W. Knapp, *Elliptic Curves*, Princeton University press, 1994.

[4] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer–Verlag, 1994.

[5] Wolfgang M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, *Lecture Notes in Mathematics* **536**, Springer–Verlag, 1976.