Geometry and Arithmetic

Alex Tao

10 June 2008

1 Rational Points on Conics

We begin by stating a few definitions:
A *rational number* is a quotient of two integers and the whole set of rational numbers is denoted by $\mathbb{Q}$.
A point in the (x, y) plan is called a *rational point* if x and y can be written as rational numbers.
A line is a *rational line* if the equation of the line can be written as

$$ax + by + c = 0$$

with a, b, $c \in \mathbb{Q}$.
Similarly, a conic

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

is *rational* if the coefficients are rational numbers.

It is easily seen that if we have two rational lines that intersect, the intersection point is a rational point. If we now consider intersection points of a rational line and a rational conic, a simple example demonstrates that the intersection point is not, in general, rational:

$$\text{A line} \qquad x - y + 1 = 0 \qquad \text{and a conic} \qquad y - x^2 = 0$$

has intersection at $y = -3/2 \pm \sqrt{5}/2$. The intersection points are solutions to a quadratic equation produced from a line and a conic. If this quadratic equation has rational solutions then the intersection points are rational points. We know that if one solutions is irrational, then the other solutions is also irrational since the sum of the solutions is the rational coefficient of the middle term in the quadratic equation.

We could use the simple properties above to decribe all rational points on a conic, *provided that we have already found one rational point on it.* Let $\mathcal{O}$ be our initial rational point on the conic C. Take any rational line L_1 not containing $\mathcal{O}$ and project the conic onto L_1 from $\mathcal{O}$. By projecting some point $a \in C$, we mean that we insert the line, L_2, defined by $\mathcal{O}$ and a and see where it crosses L_1. We could repeat this process for every point in C. To project $\mathcal{O}$ itself onto L_1 we will need to use the tangent of the conic at $\mathcal{O}$. If we draw a line L_2 from $\mathcal{O}$ onto a point Q on L_1, we will define a point P which intersects the conic. Assuming that we are on the projective plane, the unique point $\mathcal{O}'$ making L_2 parallel to L_1 will produce an intersection at infinity.
If L_2 is a rational line, it's intersection with L_1, Q, will be a rational point. Conversely, if Q is a rational point, then L_2 is a rational line. If L_2 is a rational line and intersects the conic at $\mathcal{O}$ and P, $\mathcal{O}$ being a rational point by assumption implies that P is also a rational point. We have the following relation:

$$Q \text{ is rational} \quad \Longleftrightarrow \quad L_2 \text{ is rational} \quad \Longleftrightarrow \quad P \text{ is rational}$$

So finding rational points P on the conic is equivalent to finding rational points Q on L_1. This problem is now much simplified because finding rational points on a line is much easier than on a conic.

Now let's try this concretely on the unit circle $x^2 + y^2 = 1$. Let our initial rational point be $(-1, 0)$ and we project the circle on the line $x = 0$ from $(-1, 0)$. Call the projection line L and let L intersect the the y-axis at $(0, t)$ and the the circle at (x, y). Using the parameter t, L is defined as $y = t(1 + x)$. The intersections yield the relation

$$1 - x^2 = y^2 = t^2(1 + x)^2.$$

Cancelling out a factor of $(1 + x)$ on both sides with some rearranging gives the circle parametrisation of the circle

$$x = \frac{1 - t^2}{1 + t^2}, \qquad y = \frac{2t}{1 + t^2}$$

Now it is clear that (x, y) on the circle is rational iff t is rational.

These results can be used to solve the elementary problem of finding *Pythagorean Triplets* satisfying the lengths of the sides of a right angle triangle. By Pythagoras, the lengths of the sides X, Y, Z, satisfies the equation

$$X^2 + Y^2 = Z^2.$$

If there does not exist a common factor between the integers X, Y, Z, we will call the right angle triangle *primitive*. Further more, if any pair of X, Y, Z has a some prime common factor p, then p evidently divides the third integer. Now assume we are working with a primitive right angle triangle. Rewriting the equation gives

$$\frac{X^2}{Z^2} + \frac{Y^2}{Z^2} = 1$$

Let $x = X/Z$ and $y = Y/Z$ then we have $x^2 + y^2 = 1$ for rational pair of x and y. This is the exact problem from the last example.

Claim that X and Y cannot both be even or odd.
If X and Y were both even then they have a common factor of 2. Contradiction. If X and Y were both odd, then the fact that an odd number squares is congruent to 1 modulo 4 implies that Z^2 is 2 modulo 4. But any integer squared is either 0 or 1 modulo 4. Contradiction. WLOG, let X be odd and Y be even.

Using our previous formulas for rational points on a circle and writing rational number t as $t = m/n$ for some intergers m and n. Then

$$\frac{X}{Z} = x = \frac{n^2 - m^2}{n^2 + m^2}, \qquad \frac{Y}{Z} = y = \frac{2mn}{n^2 + m^2}$$

Since X/Z and Y/Z are in their lowest fraction terms, then there exists an integer λ such that

$$\lambda Z = n^2 + m^2, \qquad \lambda Y = 2mn, \qquad \lambda X = n^2 - m^2$$

We will show $\lambda = 1$. Since λ divides both $n^2 + m^2$ and $n^2 - m^2$ and their sum and difference $2n^2$ and $2m^2$. It follows that λ divides 2 so λ is either 1 or 2. Suppose $\lambda = 2$, then $\lambda X = n^2 - m^2$ is divisible by 2 but not divisible by 4 since X is odd. Hence $n^2 - m^2 \equiv 2$ modulo 4 but n^2 and m^2 are either 0 or 1 mod 4. Contradiction.
So $\lambda = 1$.

Using our final relations

$$Z = n^2 + m^2, \qquad Y = 2mn, \qquad X = n^2 - m^2,$$

we can now find our Pythagorean triples by putting in arbitrary coprime integers for m and n.

The expressions derived above are related to trigonometry, namely:

$$\cos\theta = x = \frac{n^2 - m^2}{n^2 + m^2}, \qquad \sin\theta = y = \frac{2mn}{n^2 + m^2}$$

So problems involving cosine and sine functions can often be simplified by solving the problem algebraically by introducing the parameter t.

Now, there may be conics where no there are no rational points on it at all. Take the circle

$$x^2 + y^2 = 3.$$

We may start to look for rational points on it, but in fact there are none. In other words, there are no two rational numbers whose squares sum up to 3.

Suppose there were two rational numbers $x = X/Z$ and $y = Y/Z$ which satisfy the above condition so that we can write the equation

$$X^2 + Y^2 = 3Z^2$$

and assume there are no common factors among X, Y, and Z.
Claim that 3 does not divide X or Y.
If 3 divides X then 3 divides the LHS of $3Z^2 - X^2 = Y^2$ and so 3 divides Y. Also, it would mean 9 divides $3Z^2$ so 3 divides Z. This contradicts with the fact that there are no common factors. Similarly, 3 does not divide Y.
It follows that

$$X \equiv \pm 1 (\text{mod } 3), \qquad Y \equiv \pm 1 (\text{mod } 3), \qquad \text{and so } X^2 \equiv Y^2 \equiv 1 (\text{mod } 3)$$

But now we have

$$(\text{mod } 3)\ 0 \equiv 3Z^2 = X^2 + Y^2 \equiv 1 + 1 \equiv 2\ (\text{mod } 3)$$

Contradiction. So no such two rational numbers x and y exists.

There exists a general test with finite steps for us to conclude whether there exists a rational on a rational conic. The theorem is due to Legendre and states that for the simple case

$$aX^2 + bY^2 = cZ^2$$

has integer solutions if and only if the integers are coprime to some prime m such that

$$aX^2 + bY^2 \equiv cZ^2\ (\text{mod m}).$$

Another formulation of the theorem is by Hasse, which states: "A homogeneous quadratic equation in several variables is solvable by integers, not all zero, if and only if it is solvable in real numbers and p-adic numbers for each prime p". We will not concern ourselves with these theorems here. We have discussed up to a satisfactory level of rational points on conics and move onto cubic curves.

2 The Geometry of Cubic Curves

The general form of a cubic is the following:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

We say that the cubic is a *rational cubic* if the coefficients of the equation are rational numbers. One famous example is to find rational solutions to the equation

$$x^3 + y^3 = 1,$$

this is equivalent to finding integer solutions of it's homogenised form

$$X^3 + Y^3 = Z^3.$$

Dealing with cubic curves is in general much more complicated than just projecting conics onto a line since each projection would give two more points on the cubic. There is though, a similar principle that if two rational point are found on the cubic, a rational line defined by the two points will intersect the cubic for the third time at a *rational* point. This relies on the fact that intersection between a rational cubic and a rational line is the solution of a rational cubic.

Let our two rational points be P and Q, and denote our third intersection point generated by the line through P and Q by $P*Q$. If we have only found one point, P say, then the tangent line of the cubic at P meets the cubic *twice* at P and the other intersection point will be our third intersection. Using this method, if we have a few rational point at hand, we can generate a lot more rational points. In fact, a theorem by Mordell (1912) states that only a finite number of rational points is needed in order for us to obtain the *complete* set of rational points on a non-singular rational cubic. A proof will be given in later sets of notes. In general, there is no known method in finite steps to determine whether or not a cubic curve has a rational point; as opposed to Hasse's Theorem for conics, there is no analogue for cubic curves.

By using the above generating method, one might question whether there is some kind of underlying algebraic structure. It certainly isn't a group since there is no identity element. We could though, twist things a little and construct a group out. The group is going to be commutative so by the standard notation, denote the group law by $+$. Starting off with a rational point $\mathcal{O}$, the law is defined by:

Adding P and Q means putting a line through $P * Q$ and $\mathcal{O}$ and take the third intersection of the line to be $P + Q$. That is, $P + Q = \mathcal{O} * (P * Q)$.

Commutativity says that $P + Q = Q + P$, which is clearly true by observing geometrically. Claim that $\mathcal{O}$ is the identity element.
$P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O})$. In words, to find P plus $\mathcal{O}$, we firstly find the third intersection $\mathcal{O} * P$ so that $\mathcal{O}$, P and $\mathcal{O} * P$ lie on the same line. Now if we take $\mathcal{O} * P$ and $\mathcal{O} * P$ to find the third point, it is exactly P.

The group must also have an inverse for every element Q, $-Q$ so that $Q + (-Q) = \mathcal{O}$. To show this, draw a tangent line from $\mathcal{O}$ and call the third intersection of the line with the cubic S. Use the line defined by Q and S to and find $Q * S$. Claim that $Q * S$ is our $-Q$. $Q + (Q * S) = \mathcal{O} * (Q * (Q * S)) = \mathcal{O} * S = \mathcal{O}$ since $\mathcal{O}$ on the cubic meets the tangent line twice. $SoQ * S = -Q$.

To show that the group is associative, we need the the Cayley-Bacharach Theorem for cubic curves discussed in the projective geometry notes. Associativity says that if we have 3 points P, Q and R on the cubic curve, then $P + Q) + R = P + (Q + R)$. Diagrams will not be inserted here but it is recommended that the reader should follow along by drawing up their own one. To get $P + Q$ we need to find $P * Q$ and use the line defined by $P * Q$ and $\mathcal{O}$ to find the third intersection point. Repeating the procedure, we find $(P+Q)+R$ by firstly finding $(P+Q)*R$ then finding the third point from the line defined by $\mathcal{O}$ and $(P+Q)*R$. To show that $P+Q)+R = P+(Q+R)$, it suffices to show that $P + Q) * R = P * (Q + R)$.
To find $P * (Q + R)$, firstly find $Q * R$ and find the third intersection of the line defined by $\mathcal{O}$ and $Q * R$, then find the third intersection from the line defined by P and $Q + R$. We need to show that $P + Q) * R = P * (Q + R)$.

We form two more cubics C_1 and C_2 by taking the union of the lines defined by the pairs

$$[\mathcal{O}, Q + R], \qquad [P, P * Q], \qquad \text{and} \qquad [R, (P + Q) * R]$$

and

$$[\mathcal{O}, P + Q], \qquad [R, Q * R], \qquad \text{and} \qquad [P, P * (Q + R)].$$

There are 9 points under consideration, namely, $\mathcal{O}$, P, Q, R, $P*Q$, $P+Q$, $Q * R$, $Q + R$ and the intersection point of the two lines $[R, (P + Q) * R]$ and $[P, P * (Q + R)]$. Since our original cubic, C, already crosses the eight points $\mathcal{O}$, P, Q, R, $P*Q$, $P+Q$, $Q*R$, $Q+R$, by the Cayley-Bacharach theorem, it must also cross the ninth point. So the intersection between $[R, (P+Q) * R]$ and $[P, P * (Q + R)]$ lies on C and we have $P + Q) * R = P * (Q + R)$.

There is nothing sacred about the choice of $\mathcal{O}$ and we could as well take another point $\mathcal{O}'$ and we could generate a group with the same algebraic

structure. It is also important to note that the number of times a line meets the cubic (or its multiplicity of intersection) affects the the third point of intersection. For instance, if the line through P and Q is a tangent at P, then $P * Q = P$. So one should take care of all cases in a general manner and count multiplicities correctly. We can now restate a Mordell's Theorem using the notion of the group law on cubics:

Mordell's Theorem

If a non-singular plane cubic curve has a rational point, then the group of rational points is finitely generated.

This simpler form uses minimal amount of group theory and much more accessible to the general reader.

3 Weierstrass Normal Form

We know that equations can be changed under coordinate transformations. One important occurence under *projective transformation*, a tranformation on the projective plane, changes cubics with at least one rational point into *Weierstrass normal form*. We will use the name Weierstrass form from now on and it takes the form

$$y^2 = 4x^3 - g_2x - g_3$$

or another general form

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

To put cubics on the projective plane into Weierstrass form, we need to choose a special set of X, Y and Z axes. Starting off with the rational point $\mathcal{O}$ on the cubic, we let the tangent to $\mathcal{O}$ be the Z axis. The Z axis will intersect the cubic at a third point P and we take the tangent at P to be the X axis. The Y axis is any line other than the Z axis going through $\mathcal{O}$. Finally, taking $x = X/Z$ and $y = Y/Z$ enables us, after some simple algebraic manipulations, to obtain y^2 as come cubic in x. To eliminate the x^2 term, we need to take an appropriate α such that replacing x by $x - \alpha$ does the job. Throughout the whole transformation, we should note that each step does not introduce any irrational factors and so the rational points in the original cubic remains untouched in the new equation. We will

not dwelve into the transformation anymore and will work with cubics of Weierstrass form from now.

An elliptic curve is a curve satisfying the cubic of normal form

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

with complex distinct roots. If we have an elliptic curve with at least one singular point and we want to find all the rational points on it, we could reduce the problem to a conic-like problem by taking the singular point as our initial point of projection $\mathcal{O}$. We now concentrate on non-singular elliptic curves.

4 Explicit Formulas for the Group Law

Consider the homogenised equation of the Weierstrass form a general cubic

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

and the line at infinity

$$Z = 0.$$

By looking at the intersection of the cubic with the line at infinity, we can find out how many points of the cubic lies at infinity. Substituting $Z = 0$ in the cubic, we obtain $X^3 = 0$ which has three repeated roots at $X = 0$. The lines corresponding to $X = 0$ are lines of constant x which means the only point at infinity of the cubic is the intersection of the vertical lines at infinity. Since it is a triple root for the intersection, the situation must be the line is tangent to the cubic at an inflection point, which we will call $\mathcal{O}$. If we regard $\mathcal{O}$ as a rational point, we can use the group law as we did above.

Adding two points P and Q is simplified in Weierstrass form. To find $P + Q$ we draw a line through P and Q and find the third intersection point $P * Q$. We now draw the line through $\mathcal{O}$ and $P * Q$ to find the third intersection $P + Q$. The point But any line crossing $\mathcal{O}$ will be a vertical line and so $P * Q$ will be directly "above" or "below" $P + Q$. Furthermore, since in Weierstrass form the cubic is symmetric about the x-axis, $P + Q$ is exactly the reflection point $P * Q$ about the x-axis. As before we also need an identity and this will be $\mathcal{O}$. The inverse of a point P is $-P$ and they are the pair of reflected point about the x-axis, so if $P = (x, y)$ then $-P = (x, -y)$. Also, $\mathcal{O} = -\mathcal{O}$.

With these simplifications, it is natural to develop some formulas to enable us to compute the addition of points quickly. Let us introduce some new notations:

$$P_1 = (x_1, y_1), \qquad P_2 = (x_2, y_2) \qquad P_1 * P_2 = (x_3, y_3) \qquad P_1 + P_2 = (x_3, -y_3).$$

Given two points P_1 and P_2 we can find a formula for the line going through them. The line will have equation

$$y = \lambda x + \nu, \qquad \text{where } \nu = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Substituting in the line equation into the cubic equation yields the third intersection point. Eliminating y gives a cubic equation in x which will factorise into $(x - x_1)(x - x_2)(x - x_3)$. Equating appropriate terms of x extracts the formulas

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

Now we only need to plug in the coordinates of the known points to find the third intersection. If our initial two points are repeated points with multiplicity of two then it is easily solved by taking the tangent, found using implicit differentiation, of the curve as the line. The computation we are facing with is finding $2P$ and the actual formula for λ will be

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}$$

After some algebraic manipulation we end up with the *duplication formula* for the x coordinate

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

There is also an equivalent relation for the y coordinate, $y(2P)$.