Elliptic curves: theory and applications (B. Conrad, 9/12/2010)

I. Exercises on conics in the plane (These are related to the first hour.)

I.1. Let C be the unit circle $\{u^2+v^2=1\}$ in the plane. For the lines $L_t=\{v=t(u+1)\}$ with varying slope t through the "base point" $P=(-1,0)$, the intersection $L_t\cap C$ consists of P and

$$P_t=\left(\frac{t^2-1}{t^2+1},\frac{2t}{t^2+1}\right);$$

draw a picture for yourself. This *parametric formula* for the circle (with parameter t) is superior to the parameterization $\theta\mapsto(\cos\theta,\sin\theta)$ for studying rationality properties of points on the circle, as we will see.

(i) If $w^2+aw+b=0$ is a quadratic polynomial with a known root r, give an easy formula for the other root using only addition and subtraction with r,a,b, no "quadratic formula".

(ii) Using (i), do the algebra to justify the above description of $L_t\cap C$. What happens if you formally set $t=\infty$ in the formula for P_t, and why is this geometrically reasonable (so we let $P_\infty=P$)?

(iii) For $t\in\mathbf{R}\cup\{\infty\}$, explain without extensive computations why $t\in\mathbf{Q}\cup\{\infty\}$ if and only if P_t has coordinates in $\mathbf{Q}$. By then setting $t=n/m$ for relatively prime positive integers m and n, express the condition that P_t lies in the first quadrant in terms of inequalities on n and m, and then deduce by clearing denominators that every *primitive* Pythagorean triple has the form

$$(n^2-m^2,2nm,n^2+m^2)$$

with n and m not both odd. What happens if we allow n or m (or both) to be ≤ 0?

(iv) Work out parametric formulas analogous to P_t when using the base point $(1,0)$, as well as for $3u^2+2v^2=5$ with the base point $(1,1)$ (formally allowing ∞ as a parameter, corresponding to $(1,-1)$). Deduce that this ellipse has *infinitely many* rational points, and relate the slope of the tangent line at the base point to the case $t=\infty$ in (ii).

I.2. Using the base point $(3/5,4/5)$ on the unit circle, adapt the method in I.1(ii) to obtain the following crazy-looking parameterization of *rational* nonzero solutions to $x^2+y^2=z^2$:

$$(3m^2-8mn-3n^2,-4m^2-6mn+4n^2,5(m^2+n^2))$$

with $m,n\in\mathbf{Q}$. For which $m,n\in\mathbf{Z}$ is this triple "primitive"? Whereas the choice of base point is not too significant for the study of $\mathbf{Q}$-points, it makes a *huge* difference in the study of integrality questions.

I.3. For integers a,b,m with $m>0$, we say $a\equiv b \bmod m$ (read "a is *congruent* to b modulo m") when $a-b$ is divisible by m (equivalently, a and b leave the same remainder upon division by m).

(i) If $a\equiv b\bmod m$ and $a'\equiv b'\bmod m$ then $a+b\equiv a'+b'\bmod m$ and $ab\equiv a'b'\bmod m$. Test this with some numerical examples, and show that if p is prime and $ab\equiv ac\bmod p$ with $a\not\equiv 0\bmod p$ then $b\equiv c\bmod p$ (cancellation!) but find a counterexample modulo 15. We say a is a *square* modulo m if $x^2\equiv a\bmod m$ has a solution. Find the squares modulo 3, 5, 7, 8, 9.

(ii) Prove that $u^2+v^2=3$ has *no* solutions in $\mathbf{Q}$. (Hint: clear denominators and work modulo 3 with a hypothetical "primitive" $\mathbf{Z}$ solution to $x^2+y^2=3z^2$.)

($*$) (iii) For each of the following, discuss (non-zero) solutions in $\mathbf{Q}$ and $\mathbf{Z}$, or show that none exist: $x^2-2y^2=z^2$, $2z^2+2y^2=3z^2$, $7x^2-23y^2=15z^2$, $7x^2+23y^2=15z^2$. Can you generalize?

I.4. Use the method of I.1(iv) to parameterize $\mathbf{Q}$-points on the hyperbola $u^2-7v^2=1$. If you know about Pell's equation, does your $\mathbf{Q}$-parameterization help at all in the study of $\mathbf{Z}$-points?

I.5. (i) In I.1, explain why $t=\tan(\theta/2)$ if $x=\cos\theta$ and $y=\sin\theta$.

($**$) (ii) Use (i) and I.1 to discover a trigonometric substitution that yields the identity

$$\int\sec(\theta)\mathrm{d}\theta=\log\left(\frac{1+\tan(\theta/2)}{1-\tan(\theta/2)}\right).$$

Similarly compute $\int \mathrm{d}\theta/(1+\sin(\theta))$ and $\int \mathrm{d}\theta/(3+5\sin(\theta))$. (This is the method of "Weierstrass substitution". It converts "any" trigonometric integral into an integral of a rational function, which is computable in theory via partial fractions and computable in practice in very special cases.)

II. Exercises on elliptic curves (These rest on material from the second hour.)

II.1. The elliptic curve $y^2 = x^3 - 25x$ has $(0, 0)$, $(\pm 5, 0)$, and $(-4, 6)$ as some of its $\mathbf{Q}$-points.

(i) By considering where $x^3 - 25x \geq 0$, draw a rough sketch of the solution locus E in $\mathbf{R}^2$.

(ii) If you draw a typical line through $P = (-4, 6)$, in how many other points does it meet E? What goes wrong if we try the rational parameterization method for degree-2 curves to higher-degree curves?

(iii) Determine where E meets the line joining P to each of the above other $\mathbf{Q}$-points; relate this to solving a cubic in x with $\mathbf{Q}$-coefficients and *two* known $\mathbf{Q}$ solutions (no cubic formula needed!).

(iv) The tangent line to E at P is $y = (23/12)x + 41/3$; prove this if you know calculus. Compute where this line meets the curve, and observe that you are led to a cubic equation in x with a *double root* at $x = -4$. By thinking of a tangent line as a "limit" of secant lines through a point, why should we get a double root?

II.2. The rational right triangle $(3/2, 20/3, 41/6)$ with area 6 gives rise to the rational point $(-4, 6)$ on $y^2 = x^3 - 36x$. But in terms of algebra, we can change signs on the numbers $3/2$, $20/3$, and $41/6$ and get *more* such rational points!

(i) Using sign changes, discover the following additional rational points: $(-4, -6)$ and $(25/4, \pm 75/8)$. Graph the picture of these points on the cubic curve.

(ii) Join such pairs not on the same vertical line and find yet more rational points on the curve. Going backwards, produce more impressive rational right triangles with area 6!

II.3. The curve $y^2 = x^3 - 49x$ has the rational point $(25, 120)$. Check it.

(i) Using the formulas, discover the "triangle" $(-24/5, -35/12, 337/60)$. What point on the elliptic curve corresponds to the genuine triangle $(24/5, 35/12, 337/60)$?

(ii) Now you have two points on the curve not on the same vertical line. Compute where their secant line meets the curve, and discover another triangle with area 7. Can you continue the process?

II.4. Fermat proved 1 is not a congruent number by relating it to his "last theorem" for exponent 4:

(i) Suppose there is a rational right triangle with area 1. Scaling by the common denominator of the side lengths, get positive *integers* a, b, c, d with $a^2 + b^2 = c^2$ and $ab/2 = d^2$. Prove that $g := \gcd(a, b)$ divides c and d also, so divide throughout by g to get to the case $g = 1$.

(ii) Using that $ab = 2d^2$ and $g = 1$, prove a and b have opposite parity. Deduce c is odd and $\gcd(b, c) = 1$. Swapping labels if necessary, arrange a is even and b is odd. Prove $a = 2k^2$ and $b = \ell^2$ with positive integers k and ℓ with ℓ odd.

(iii) Since $c^2 = a^2 + b^2 = 4k^4 + b^2$, deduce $\frac{c+b}{2} \cdot \frac{c-b}{2} = k^4$. But prove $\gcd((c + b)/2, (c - b)/2) = 1$, and conclude $(c + b)/2 = r^4$ and $(c - b)/2 = s^4$ with integers r and s.

(iv) Prove $b = r^4 - s^4$, so $\ell^2 = r^4 - s^4$. Get a point on $v^2 = u^4 + 1$ with $u, v \in \mathbf{Q} - \{0\}$, which we saw is ruled out by the "elliptic curve" interpretation of Fermat's method (though his infinite descent method can also be directly adapted to $X^4 - Y^4 = Z^2$; try for yourself!).

(**) II.5. Consider the congruence $y^2 \equiv x^3 - n^2x \bmod p$ for a prime $p \nmid 2n$.

(i) Prove that the squaring map on the nonzero classes modulo p is a 2-to-1 map, so there are exactly $(p - 1)/2$ nonzero squares modulo p.

(ii) If $p \equiv 3 \bmod 4$, it is a general fact that -1 is *not* a square modulo p. Using this, prove that the number of solutions to the cubic congruence is $3 + 2((p - 3)/2) = p$ for such p.

(iii) If we include an additional "point at infinity", then the solution locus to the congruence (together with this extra point) has a natural group structure by using this extra point as the identity and the secant/tangent method (defined purely algebraically!) as the composition law. In this sense, the solution locus modulo p is a finite group of order $p + 1$ when $p \equiv 3 \bmod 4$.

If you are familiar with elementary finite group theory, deduce that if the set of $\mathbf{Q}$-points is *finite* then together with an additional "point at infinity" its order must divide $p + 1$ for *all* large primes $p \equiv 3 \bmod 4$. ("Large" to avoid denominators in this hypothetical finite group of $\mathbf{Q}$-points.) Varying such p and using Dirichlet's deep theorem that every arithmetic progression of integers $\{a + nb\}_{n \geq 0}$ (with $b \neq 0$) contains infinitely many primes, prove that the group of $\mathbf{Q}$-points (with ∞) has order at most 4. So any $\mathbf{Q}$-point on $y^2 = x^3 - n^2x$ apart from the three with $y = 0$ *must* have infinite order in the group law of the elliptic curve!