CHAPTER 20

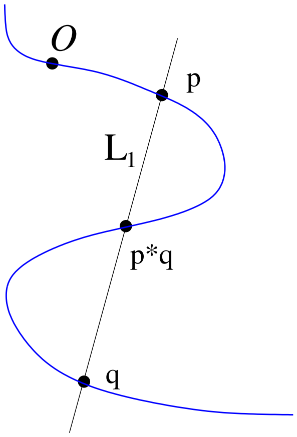
Group law on the nonsingular cubic

It is now high time for the “smooth” version of Chapter 17: group laws and addition theorems for elliptic curves. We start by introducing an algebro-geometrically defined binary operation on the points of a cubic curve, and prove that it coincides with addition on $\mathbb{C}/\Lambda_E$ under the Abel isomorphism. This gives one proof that the operation defines an abelian group, and we give another more natural one as well. From the fact that it makes Abel’s map into a homomorphism we will then derive functional equations for elliptic integrals.

20.1. Definition of the group law

Let $E \subset \mathbb{P}^2$ be a nonsingular cubic, which we shall not require to be in Weierstrass form, and fix a flex $\mathcal{O}$. Let p and q be points of E.

Step 1: Draw the line L_1 through p and q:

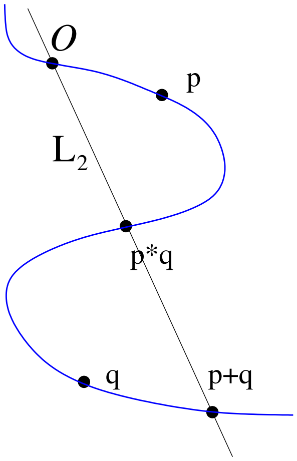


By Bézout, there is a third intersection point, which we shall denote $p * q$, so that

$$L_1 \cdot E = [p] + [q] + [p * q].$$

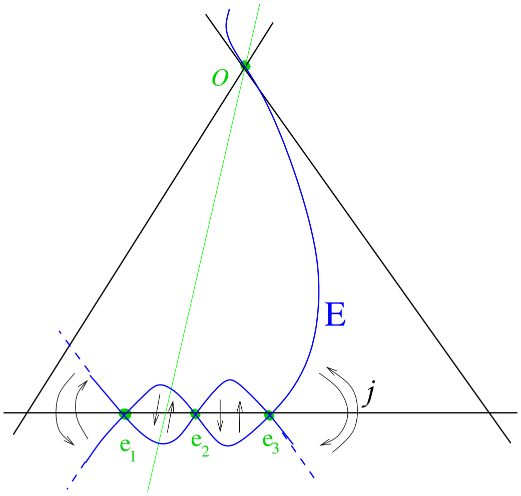
Note that the three points need not be distinct — any two, or all three, may coincide. This has the usual interpretation: a double-intersection means L_1 is tangent to E at that point; a triple-intersection means you have a flex.

Step 2: Draw the line L_2 through $\mathcal{O}$ and $p * q$:



The third intersection point is denoted $p + q$, with the same interpretations as above.

In the special case where E is in Weierstrass form, L_2 is a vertical line $\{X = x_0 Z\}$. So the map sending $p * q$ to $p + q$ is just the involution $\jmath : E \to E$ taking $(x, y) \mapsto (x, -y)$:



We have therefore constructed a binary operation

$$E \times E \to E$$
$$(p, q) \mapsto p + q$$

on the (set consisting of the) points of E. It is not yet clear that this defines a group. It *is* clear that it is commutative, so that *if* it defines a group, then that group is abelian.

20.2. Relation to the group structure on the 1-torus

Let $T : \mathbb{P}^2 \to \mathbb{P}^2$ be the projective transformation putting E into Weierstrass form (and taking $\mathcal{O}$ to $\mathcal{O}' := [0 : 0 : 1]$). Denote the binary operation defined on points of $E' := T(E)$ (via the method just described, with $\mathcal{O}'$ replacing $\mathcal{O}$) by $+'$. Since projectivities preserve lines, intersection multiplicities, and so forth, it is clear that $T(p) +' T(q) = T(p + q)$. So to show that "$+$" defines a group law for arbitrary E, it suffices to check this for Weierstrass cubics.

Hence we may assume E is in Weierstrass form (and $\mathcal{O} = [0:0:1]$). Take the Abel map

$$u : E \to \mathbb{C}/\Lambda_E$$

to be as in Chapter 19, with inverse $\mathcal{P}$. We know that "addition mod Λ_E" defines a group law on $\mathbb{C}/\Lambda_E$. The next result implies not only that our operation on E defines a group law, it says that u is an isomorphism of groups.

20.2.1. THEOREM. *The Abel map respects binary operations. That is, the equivalent formulas*

$$\mathcal{P}(u_1) + \mathcal{P}(u_2) = \mathcal{P}(u_1 + u_2) \tag{20.2.2}$$

$$u(p) + u(q) \equiv u(p + q) \ \textit{mod}\ \Lambda_E \tag{20.2.3}$$

hold.

PROOF. We will prove (20.2.3), in a manner reminiscent of the proof of Theorem 19.2.1. Writing F_{L_i} for the degree-1 homogeneous polynomial defining L_i, consider the meromorphic function

$$f := \left.\frac{F_{L_2}}{F_{L_1}}\right|_E \in \mathcal{K}(E)^*.$$

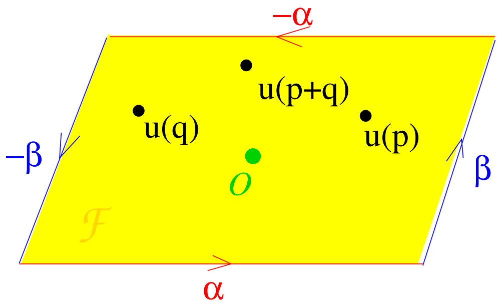
Reading its divisor off from the intersection points of the $\{L_i\}$ and E,

$$\begin{aligned}(f) &= [p+q] + [p*q] + [\mathcal{O}] - ([p] + [q] + [p*q]) \\ &= [p+q] - [p] - [q] + [\mathcal{O}].\end{aligned}$$

So for its pullback $\mathcal{P}^* f = f \circ \mathcal{P}$ to $\mathbb{C}/\Lambda_E$,

$$(\mathcal{P}^* f) = [u(p+q)] - [u(p)] - [u(q)] + [0].$$

Cut open $\mathbb{C}/\Lambda_E$ and put $\mathfrak{U} := \int_0^* du$ on the resulting fundamental region $\mathfrak{F}$:



Write $\mathfrak{U}(p)$ for $\mathfrak{U}(u(p))$ (and so on) for simplicity. By the residue theorem,

$$\mathfrak{U}(p+q) - \mathfrak{U}(p) - \mathfrak{U}(q)\ (+0) = \frac{1}{2\pi i}\oint_{\partial\mathfrak{F}} \mathfrak{U} \cdot \frac{d(\mathcal{P}^* f)}{\mathcal{P}^* f}$$

$$= \left\{-\frac{1}{2\pi i}\int_\alpha \mathrm{dlog}(\mathcal{P}^* f)\right\}\int_\beta du \ + \ \left\{\frac{1}{2\pi i}\int_\beta \mathrm{dlog}(\mathcal{P}^* f)\right\}\int_\alpha du.$$

Since both terms in braces are integers, the whole thing belongs to

$$\mathbb{Z}\left\langle \int_\alpha du, \int_\beta du \right\rangle = \Lambda_E.$$

Since $\mathfrak{U}(p), \mathfrak{U}(q), \mathfrak{U}(p+q)$ are lifts to $\mathbb{C}$ of $u(p), u(q), u(p+q)$, going modulo Λ_E we see that $u(p+q) - u(p) - u(q) \equiv 0$. □

We will generalize this argument in the next chapter to get Abel's theorem for E.

20.2.4. REMARK. For an arbitrary smooth cubic C, one still has (up to scale) a unique $\omega \in \Omega^1(C)$, which gives rise to an Abel isomorphism $u : C \to \mathbb{C}/\Lambda_{(C,\omega)}$. Property (20.2.3) still holds in this setting by more or less the same proof; this avoids passing through Weierstrass form.

20.3. A more algebro-geometric approach

Returning to the setup of §20.1, let us suppose that the coefficients of the homogeneous cubic polynomial defining E belong to some subfield $k \subset \mathbb{C}$. We shall say *E is defined over k*. If $K \subset \mathbb{C}$ is a field extension of k (e.g. k itself, or $\mathbb{C}$), then we can consider the *K-points of E*

$$E(K) := \{[Z : X : Y] \in E \mid Z, X, Y \in K\}.$$

20.3.1. PROPOSITION. *$E(K)$ is closed under "+", and is consequently a subgroup of E.*

PROOF. If $p, q \in E(K)$ then the line $L_1 = L_{pq}$ is defined over K, and so can be parametrized $\mathbb{P}^1 \overset{\cong}{\to} L_{pq}$ over K. This means that the formulas expressing $[Z{:}X{:}Y]$ as functions of $[T_0{:}T_1] \in \mathbb{P}^1$ involve coefficients in K. So the pullback of the homogeneous polynomial defining E is defined over K. Now this can be written

$$\textstyle\sum_{j=0}^{3} \beta_j Z_0^{3-j} Z_1^j = \prod_{i=1}^{3} (Z_1 - \alpha_i Z_0),$$

assuming without loss of generality that there are no Z_0 factors; and what we know is that the $\beta_j \in K$. At first glance that does not guarantee that the $\alpha_i \in K$. But in this case we know that two of them — say, α_1, α_2 — correspond to p, q and so *must* belong to K. Consequently $\alpha_3 \in K$ as well, and its image point $p * q$ is also defined over K. Repeat the argument for L_2 and the claim follows. □

20.3.2. REMARK. (a) In light of the above definition, the "correct" notation for the set of complex points of E, which we have heretofore denoted simply "E", is $E(\mathbb{C})$.

(b) As a $\mathbb{C}$-module, $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_E$ has rank 1, but as an abelian group (i.e. "$\mathbb{Z}$-module"), its rank is *infinite*. (Consider a bunch of $\mathbb{Q}$-linearly independent complex numbers modulo Λ_E — there is no bound on the size of the $\mathbb{Q}$-vector space you can generate in this fashion.) On the other hand, for the subgroup $E(\mathbb{Q})$, a famous theorem of MORDELL (1922) asserts that the rank (as an abelian group) is always finite. In Exercise (6) below, you will show computationally that the rank of $E(\mathbb{Q})$ in one example is at least 1.

Now the Abel map u is non-algebraic (i.e., transcendental); it should be seen as providing a link between the complex algebraic and the complex analytic. Such maps together with their inverses, which include multivariate abelian functions, modular and automorphic forms, and the "mirror map" in string theory, are very important in arithmetic algebraic geometry. While they do not preserve the field of definition, they have nevertheless been essential to the study of things like class field theory, the proof of Fermat's last theorem, and instanton numbers. Still, in light of the subgroup structures $E(K) \subset E(\mathbb{C})$, it is a bit sloppy to prove that "$+$" is a group law in a manner that only works over $\mathbb{C}$.

So we will now give the "fully algebraic" approach to this proof, by checking that

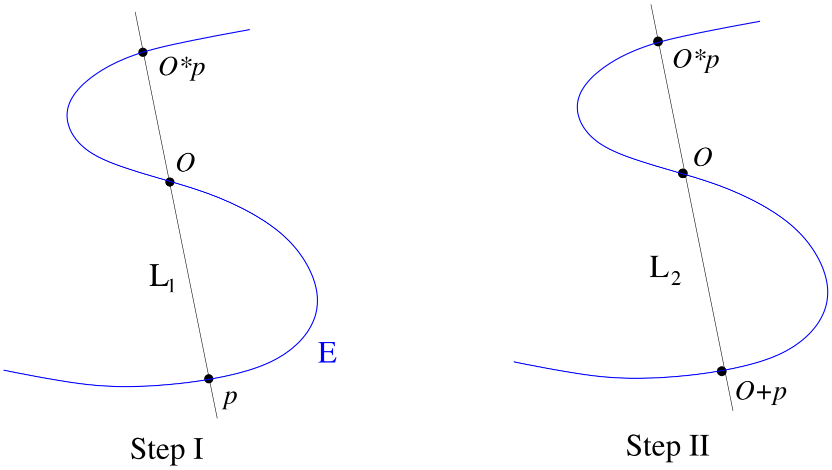
$$\mathcal{O} + p = p \quad (\forall\, p \in E), \tag{20.3.3}$$

$$(p * q) + (p + q) = \mathcal{O} \quad (\forall\, p, q \in E), \text{ and} \tag{20.3.4}$$

$$\text{the operation "}+\text{" is associative.} \tag{20.3.5}$$

Notice that (20.3.4) implies $(p * \mathcal{O}) + (p + \mathcal{O}) = \mathcal{O}$, and thus that $p * \mathcal{O} = -p$, so we indeed have inverses; (20.3.3) and (20.3.5) are the other two group axioms.

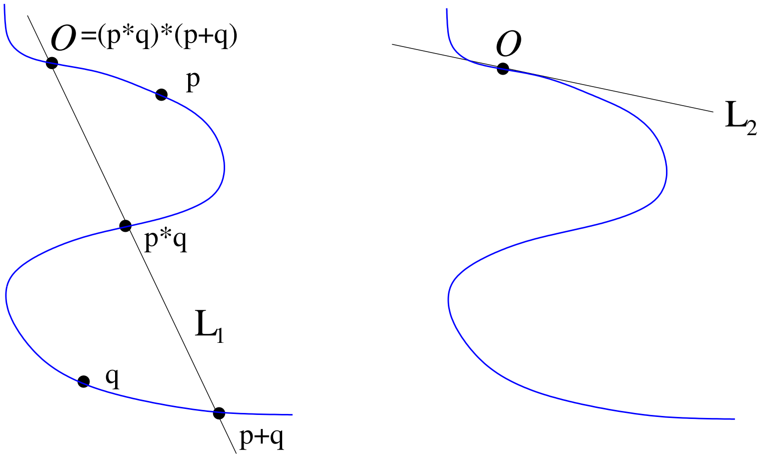
To verify (20.3.3), we have the pictorial depiction of the two-step process for adding $\mathcal{O}$ and p:



Step I

Step II

in which $L_1 = L_{\mathcal{O}p}$ and $L_2 = L_{\mathcal{O},\mathcal{O}*p} = L_1$!! Consequently the third intersection point $\mathcal{O} + p$ of L_2 with E, is none other than p. Property (20.3.4) isn't much harder; again, a picture:

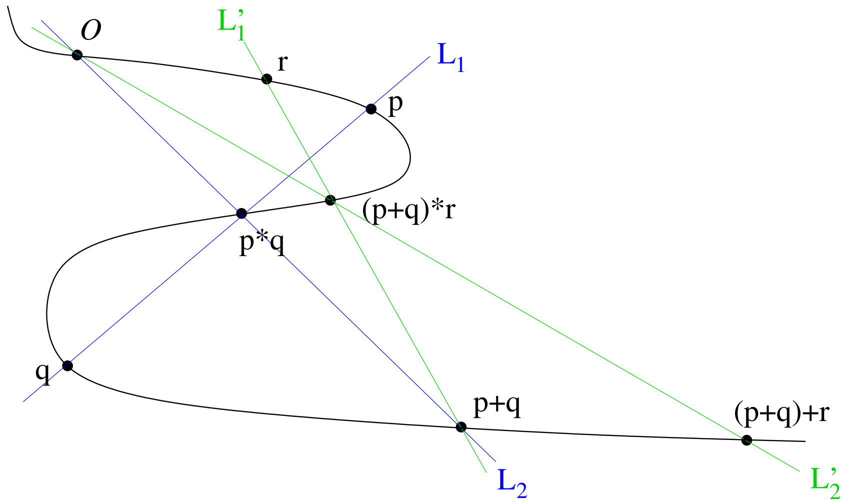


where $L_1 = L_{p*q,\,p+q}$. Since the line through $\mathcal{O}$ and $p * q$ intersects E in (and defines) $p + q$, it follows that L_1's third intersection point $(p * q) * (p + q)$ with E is just $\mathcal{O}$. Then

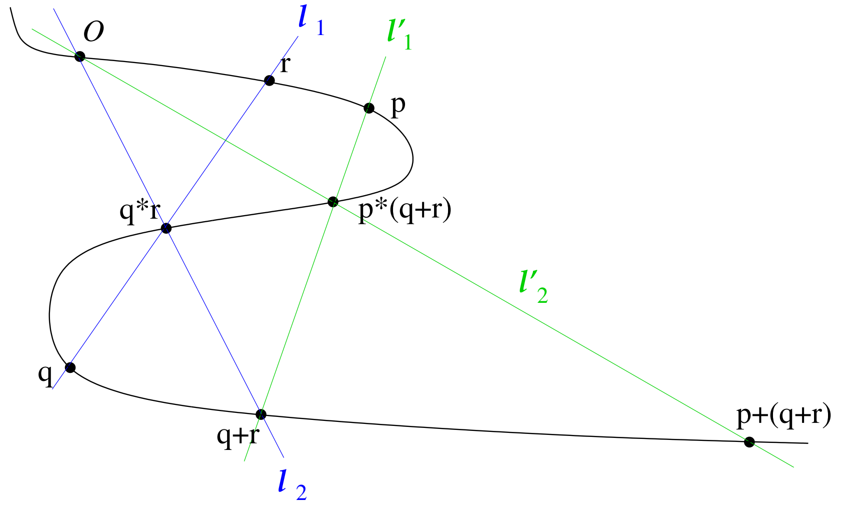
$$L_2 := L_{\mathcal{O},(p*q)*(p+q)} = L_{\mathcal{O},\mathcal{O}} = T_{\mathcal{O}}E,$$

and since $\mathcal{O}$ is a flex ($(T_{\mathcal{O}}E \cdot E)_{\mathcal{O}} = 3$), the third intersection point is again $\mathcal{O}$.

Finally we come to the associativity issue (20.3.5). Here I won't break the two steps up into two pictures. Instead, here is a depiction of $(p+q)+r$, where the blue lines compute $p+q$ and the green ones the addition of r to the result:



... and here is what $p+(q+r)$ looks like (blue lines for $q+r$, green for adding result to p):



We have to show $(p+q)+r = p+(q+r)$, or equivalently

$$(p+q)*r = p*(q+r).$$

Now look at the three cubics E, $C = L_1 \cup \ell_2 \cup L_1'$, and $D = \ell_1 \cup L_2 \cup \ell_1'$, with intersections

$$E \cdot C \;=\; [\mathcal{O}]+[p]+[q]+[r]+[p*q]+[p+q]+[q*r]+[q+r]+[(p+q)*r]$$

and

$$E \cdot D \;=\; [\mathcal{O}]+[p]+[q]+[r]+[p*q]+[p+q]+[q*r]+[q+r]+[p*(q+r)].$$

Argue à la §15.2: the ratio of the homogeneous polynomials defining C and D induces a meromorphic function on E with divisor

$$E \cdot C - E \cdot D \;=\; [(p+q)*r] - [p*(q+r)],$$

leading as usual to a contradiction *unless* these two points are the same.

20.4. Addition theorems

Now assume $E = \{y^2 = Q(x)\}$ (with $Q(x) = 4x^3 - g_2x - g_3$) is in Weierstrass form; we would like to unwind the statements (20.2.2) and (20.2.3) that $\mathcal{P}$ and u are group homomorphisms (hence isomorphisms), to produce something more computationally explicit.

We do this first for the Weierstrass map. Writing $p = \mathcal{P}(u_1) = (\wp(u_1), \wp'(u_1))$ and $q = \mathcal{P}(u_2) = (\wp(u_2), \wp'(u_2))$, we have

$$\begin{aligned} p*q &= \jmath(p+q) = \jmath(\mathcal{P}(u_1)+\mathcal{P}(u_2)) \\ &= \jmath(\mathcal{P}(u_1+u_2)) = \jmath(\wp(u_1+u_2), \wp'(u_1+u_2)) \\ &= (\wp(u_1+u_2), -\wp'(u_1+u_2)). \end{aligned}$$

Now p, q, and $p*q$ are collinear by construction — they lie on L_1 in the group law "process" for E. We may express this in projective coordinates by saying that

$$0 = \det \begin{pmatrix} 1 & 1 & 1 \\ \wp(u_1) & \wp(u_2) & \wp(u_1+u_2) \\ \wp'(u_1) & \wp'(u_2) & -\wp'(u_1+u_2) \end{pmatrix}. \tag{20.4.1}$$

This is the *first addition theorem*, and is the analogue for bi-periodic functions of the standard trigonometric angle-addition formulas. It really does express $\wp(u_1+u_2)$ in terms of $\wp(u_1)$ and $\wp(u_2)$, since $\wp'(\alpha) = \pm\sqrt{Q(\wp(\alpha))}$.

Let's actually compute the group law on E. Start by writing $y = ax+b$ for L_1 and substituting this into the equation of E to "intersect" them. This gives

$$0 = 4x^3 - g_2x - g_3 - (ax+b)^2 = 4(x-x(p))(x-x(q))(x-x(p+q))$$

since L_1 and E meet in p, q, $p*q$. (Note that $x(p+q) = x(p*q)$.)[1] From expanding these two expressions and comparing coefficients of x^2, one finds that

$$a^2 = 4(x(p)+x(q)+x(p+q));$$

and since a is the slope of L_1 it is obvious that

$$a = \frac{y(q)-y(p)}{x(q)-x(p)}.$$

Therefore we have

$$x(p+q) = \frac{1}{4}\left(\frac{y(q)-y(p)}{x(q)-x(p)}\right)^2 - x(p) - x(q). \tag{20.4.2}$$

Now $u(p) = \int_{\mathcal{O}}^{p} \frac{dx}{y} = \int_{\infty}^{x(p)} \frac{dx}{\sqrt{Q(x)}}$, similarly $u(q) = \int_{\infty}^{x(q)} \frac{dx}{\sqrt{Q(x)}}$ and $u(p+q) = \int_{\infty}^{x(p+q)} \frac{dx}{\sqrt{Q(x)}}$. Re-expressing

$$u(p)+u(q) \equiv u(p+q) \mod \Lambda_E$$

using all these formulas yields the *second addition theorem*:

(20.4.3)

$$\int_{\infty}^{x_1} \frac{dx}{\sqrt{Q(x)}} + \int_{\infty}^{x_2} \frac{dx}{\sqrt{Q(x)}} \underset{\Lambda_E}{\equiv} \int_{\infty}^{\left\{\frac{1}{4}\left(\frac{\sqrt{Q(x_2)}-\sqrt{Q(x_1)}}{x_2-x_1}\right)^2 - x_2 - x_1\right\}} \frac{dx}{\sqrt{Q(x)}}$$

which yields a nontrivial functional equation for the elliptic integral $\int_{\infty}^{*} \frac{dx}{\sqrt{Q(x)}}$.

* * *

[1] The dictionary we have in mind is: $x(p) = \wp(u_1)$, $y(p) = \wp'(u_1)$; $x(q) = \wp(u_2)$, $y(q) = \wp'(u_2)$; and $x(p+q) = \wp(u_1+u_2)$, $y(p+q) = \wp'(u_1+u_2)$.

The problems below (with the exception of the last one) take place on a nonsingular cubic $E := \{y^2 = 4x^3 - g_2x - g_3\} \subset \mathbb{P}^2$ *in Weierstrass form*, with base point $\mathcal{O} = [0{:}0{:}1]$, holomorphic form $\omega = \frac{dx}{y}|_E \in \Omega^1(E)$, and Abel map $u\colon E \to \mathbb{C}/\Lambda_E$, $u(p) = \int_{\mathcal{O}}^{p} \omega$ (recall that this is an isomorphism), with inverse $\mathcal{P}(u) = [1 : \wp(u) : \wp'(u)]$. I have written everything in affine form, which you can convert to projective coordinates if needed.

Exercises

(1) Show that the 2-torsion points on $\mathbb{C}/\Lambda_E$ correspond to the x-intercepts $\{(e_i, 0)\}_{i=1}^{3}$ and the point $\mathcal{O}$.

(2) Assume $g_2, g_3 \in \mathbb{Q}$. Given $p, q \in E(\mathbb{Q})$ (i.e. the x, y coordinates are rational), give another proof that $p + q \in E(\mathbb{Q})$, using the addition theorems.

(3) *For this and the following three problems take* $g_2 = -4$, $g_3 = 0$. Consider the complex analytic automorphism $A : E \to E$ sending $(x, y) \mapsto (-x, iy)$. In Exercise (1) of Chapter 13, you showed that $A^*\omega = i\omega$. (a) Find A^*u (i.e. compute $u \circ A$). (b) Prove that $i\Lambda_E = \Lambda_E$. (In fact, Λ_E is a "square" lattice — so this is a very special elliptic curve!)

(4) "Special case" of the 2nd addition theorem (or rather, what we did in §20.4 above doesn't exactly work in the case we'll do here, so you'll have to work it out from scratch): write $\wp(2u)$ in terms of $\wp(u)$, for E as in exercise (3), i.e. with equation $y^2 = 4x^3 + 4x$. [Hint: write $\wp'(u)$ and then the slope a of E at $(\wp(u), \wp'(u))$, in terms of $\wp(u)$. Write $y = ax + b$ for the line tangent to E at this point. Then factor $4x^3 + 4x - (ax + b)^2$ into linear factors (what are the roots?), multiply out both expressions, and compare coefficients of x^2.]

(5) Continuing the last problem, show that $(1, 2\sqrt{2})$ is a 4-torsion point. Use the "CM" (= Complex Multiplication) recalled in exercise (3) to get three more 4-torsion points. Can you use the group law to find them all? (If not, why?)

(6) This problem also depends on (4). Consider a point P of E with rational x-coordinate $x_0 = \frac{p}{2^a q}$, where the fraction is written in lowest terms, a is an odd natural number and p and q are odd integers. Show that P is of infinite order (in the group). [Hint: write (x_0, y_0) for this point, and let $(x_1, y_1) := 2(x_0, y_0)$ under the group law; if $x_0 = \wp(u)$, then $x_1 = \wp(2u)$. So rewriting your formula from (4) as a formula for x_1 in terms of x_0 and simplifying, show that x_1 is of the same form, but with larger a. Then suppose the starting point was an N-torsion point for some N and produce a contradiction via the pigeonhole principle.]

(7) This problem takes place on an arbitrary nonsingular cubic $E \subset \mathbb{P}^2$, with base point $\mathcal{O}$ = choice of flex in E, holomorphic form $\omega \in \Omega^1(E)$ with periods generating a lattice Λ_E, and Abel map $u : E \overset{\cong}{\to} \mathbb{C}/\Lambda_E$, $u(p) = \int_{\mathcal{O}}^{p} \omega$. Prove that the 3-torsion points on $\mathbb{C}/\Lambda$ correspond (under u) to the flexes on E.