

MATH 4450/6450
HOMEWORK 7 SOLUTIONS AND COMMENTS

Comments about the book problems: For Problem 21, I guess the point was that a user can figure out $\phi(n)$ because he knows that $de_{\text{User}} - 1$ is a multiple of $\phi(n)$. I'd want to be convinced that this could be done quickly, though.

Extra Problem 1: Let p be an odd prime, and $a \in \mathbb{F}_p^*$. Recall that an elliptic curve over \mathbb{F}_p is called *supersingular* if the number of \mathbb{F}_p -points on it equals $p + 1$. (Actually, this is not quite right when $p = 2$ or 3 , because 1 and $2p + 1$ fall inside the Hasse bound there as well; but at least for $p \geq 5$ this definition is correct). Let E be the elliptic curve over \mathbb{F}_p given by the equation $y^2 = x^3 + ax$.

(a) Suppose that $p \equiv 3 \pmod{4}$. Show that for any $x \in \mathbb{F}_p^*$, $x^2 \neq -a$, exactly one element of the set $\{x, -x\}$ is the x -coordinate of a point on E .

(b) Conclude that if $p \equiv 3 \pmod{4}$, E is supersingular. (Don't forget ∞ when you count points!)

(c) Now suppose that $p \equiv 1 \pmod{4}$. Let α be an element of \mathbb{F}_p such that $\alpha^2 \equiv -1 \pmod{p}$. (Why does this α exist?) Show that if $(x, y) \in E(\mathbb{F}_p)$, then $(-x, \alpha y) \in E(\mathbb{F}_p)$ as well.

(d) Conclude that if $p \equiv 1 \pmod{4}$ and $\left(\frac{a}{p}\right) = 1$, then $\#E(\mathbb{F}_p)$ is divisible by 4, so E can't be supersingular. (Hint: most of the points come in sets of four, because of part (c); then there are some special points where $y = 0$ that you haven't counted yet, and don't forget ∞ !)

Remark: It is true that E can't be supersingular in part (d) even if $\left(\frac{a}{p}\right) = -1$, but I don't know an elementary proof.

Solution: (a) Let $f(x) = x^3 + ax$. Then $f(-x) = -f(x)$. So exactly one of $f(x)$ and $f(-x)$ is a square (because -1 is not a square mod p , and $f(x) \neq 0$). So we can either solve $y^2 = f(x)$ or $y^2 = f(-x)$, but not both. \square

(b) Suppose $-a$ is not a square mod p . Then for every pair $\pm x$ of elements of \mathbb{F}_p^* , there are two points on the elliptic curve with x -coordinate equal to either x or $-x$, by part (a). So that gives $p - 1$ points on the curve. The only points we haven't counted are $(0, 0)$ and ∞ , so the total is $p + 1$.

Now suppose $-a$ is a square mod p . Then for every pair $\pm x$ of elements of \mathbb{F}_p^* whose square is not $-a$, we get two points on the elliptic curve with x -coordinate equal to either x or $-x$. That's $p - 3$ points on the curve. Next, if $x^2 \equiv -a \pmod{p}$, the only points with first coordinate equal to $\pm x$ are $(x, 0)$ and $(-x, 0)$. The only ones we haven't counted yet are $(0, 0)$ and ∞ , and again the total is $p + 1$. \square

(c) Clearly α exists because $\left(\frac{-1}{p}\right) = 1$. If $(x, y) \in E(\mathbb{F}_p)$, then $(-x)^3 + a(-x) = -(x^3 + ax) = -y^2 = (\alpha y)^2$, so $(-x, \alpha y) \in E(\mathbb{F}_p)$. \square

(d) We can partition all the non- ∞ points in $E(\mathbb{F}_p)$ into sets of the form

$$\{(x, y), (-x, \alpha y), (x, -y), (-x, -\alpha y)\}.$$

All of these sets have four elements, unless some of the four distinct-looking points in each set coincide. This can only happen if $y = 0$ (otherwise, all four of the y -coordinates are different). So we've got that $E(\mathbb{F}_p)$ is partitioned into a bunch of sets of order 4 each, plus ∞ , plus the points where $y = 0$. How many of those points are there? Well, since a is a square mod p , $x^3 + ax = 0$ has three solutions, namely $0, \pm\alpha\beta$, where $\beta^2 = a$. So there are three points with y -coordinate 0. Adding it up, we see that the number of points in $E(\mathbb{F}_p)$ is divisible by 4. \square

Extra Problem 2: Let E be the elliptic curve $y^2 = x^3 + 7$. We will show that there are no points (x, y) on E where x and y are both integers. So from now on, assume that $y^2 = x^3 + 7$ with x and y both integers.

(a) Show that x is odd.

(b) Show that there is a prime $p \equiv 3 \pmod{4}$ that divides $x^2 - 2x + 4$.

(c) Show that $p|y^2 + 1$. This gives a contradiction. (Why?)

Remark: In fact there are no *rational* solutions to the equation $y^2 = x^3 + 7$.

Solution: (a) If x is even, then $y^2 = x^3 + 7 \equiv 3 \pmod{4}$, which is impossible. \square

(b) Since x is odd, we can look at $x^2 - 2x + 4 \equiv 1 - 2 + 4 \equiv 3 \pmod{4}$. Since it is 3 mod 4, one of its prime divisors must be 3 mod 4. \square

(c) We have

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4),$$

and since p divides the right side, it divides the left side. This is a contradiction because we cannot have $y^2 \equiv -1 \pmod{p}$, since p is 3 mod 4. \square

Extra Problem 3: Let K be a field (of characteristic not equal to 2 or 3), and $a \in K^*$. Consider the curve C over K defined by the equation $X^3 + Y^3 = aZ^3$ in two-dimensional projective space. Let $O = (1: -1: 0) \in C$. Define an addition law on this curve by the familiar-looking rule that three points are deemed to sum to O if and only if they are collinear.

(a) To warm up, show that if $P = (b: c: d) \in C$, then the negative of P with respect to the above addition law is the point $(c: b: d) \in C$.

(b) Let E be the elliptic curve $y^2 = x^3 - 432a^2$. Consider the functions f and g defined by the following rules:

$$f(X: Y: Z) = \left(12a \frac{Z}{X+Y}, 36a \frac{X-Y}{X+Y} \right)$$

$$g(x, y) = (36a + y: 36a - y: 6x)$$

Show that f is a function from $C(K)$ to $E(K)$ (if we make the reasonable-looking convention that $f(O) = \infty$). Show that g is a function from $E(K)$ to $C(K)$ (if we make the reasonable-looking convention that $g(\infty) = O$). Show that f and g are inverses. (Remember that in projective space, scaling all the coordinates by the same constant doesn't change the point.)

(c) Consider the elliptic curve E_1 given by the equation $y^2 = x^3 - 432$ over \mathbb{Q} . Determine the set $E_1(\mathbb{Q})$. (You might want to assume some sort of "last theorem" or something...)

(d) Consider the curve C_9 in \mathbb{P}^2 given by the equation $X^3 + Y^3 = 9Z^3$. Certainly the point $P = (1: 2: 1)$ is on this curve. Find a rational point on C_9 which is not $(1: -1: 0)$, $(1: 2: 1)$, or $(2: 1: 1)$. (Hint: Consider $g(2f(P))$.)

Remarks: If you believe that f and g preserve collinearity (which is not hard to see from the formulas), then you can see that the addition law we've defined on C has all the properties of the addition law on E (it inherits them via the bijection g). Using this, it is not terribly difficult to write down the formulas for the sum of two points on C (or you can do it directly from the definitions, of course).

Solution: (a) Well, first suppose that $(b, c, d) \neq O$ and $b \neq c$. Then the line through $(1: -1: 0)$ and $(b: c: d)$ is $dX + dY - (b+c)Z = 0$. Clearly $(c: b: d)$ is the other point on C on this line. Now some computations (e.g. divide out by one of the variables and use implicit differentiation to find the slope of the tangent line) should convince you that the equation of the tangent line to C at $(b: c: d)$ is $b^2X + c^2Y = ad^2Z$, and if $b = c$ then of course $(1: -1: 0)$ is the third point on C on this line. Finally, for the case $(b: c: d) = O$, we need to show that the tangent line to C at O hits C only at O . This tangent line is $X + Y = 0$. Notice that $X + Y = 0$ implies that $Z = 0$, and there is only one point $(X: Y: Z)$ such that $X + Y = 0$ and $Z = 0$, namely O . (Remember that we're in projective space!) \square

(b) These are just computations. First of all, let's show that f is a function from $C(K)$ to $E(K)$. Suppose $X^3 + Y^3 = aZ^3$ and $(X : Y : Z) \neq O$. We have

$$\begin{aligned}
\left(12a \frac{Z}{X+Y}\right)^3 - 432a^2 &= 1728a^3 \frac{Z^3}{(X+Y)^3} - 432a^2 \\
&= 432a^2 \frac{4aZ^3 - (X+Y)^3}{(X+Y)^3} \\
&= 432a^2 \frac{4(X^3 + Y^3) - (X+Y)^3}{(X+Y)^3} \\
&= 432a^2 \frac{3(X^3 - X^2Y - XY^2 + Y^3)}{(X+Y)^3} \\
&= 1296a^2 \frac{(X+Y)(X-Y)^2}{(X+Y)^3} \\
&= 1296a^2 \frac{(X-Y)^2}{(X+Y)^2} = \left(36a \frac{X-Y}{X+Y}\right)^2
\end{aligned}$$

which shows that $f(X : Y : Z) \in E(K)$.

Next, let's show that g is a function from $E(K)$ to $C(K)$. Suppose $y^2 = x^3 - 432a^2$. We have

$$(36a + y)^3 + (36a - y)^3 = 2 \cdot 36^3 a^3 + 216ay^2 = 36^3 a^3 + 216a(x^3 - 432a^2) = 216ax^3 = a(6x)^3$$

which shows that $g(x, y) \in C(K)$.

Finally, one can compute

$$\begin{aligned}
g(f(X : Y : Z)) &= \left(\frac{72a}{X+Y}X : \frac{72a}{X+Y}Y : \frac{72a}{X+Y}Z\right) = (X : Y : Z) \\
f(g(x, y)) &= (x, y)
\end{aligned}$$

and of course $g(f(O)) = O$, $f(g(\infty)) = \infty$. \square

(c) Well, the function g given above defines a bijection from $E_1(\mathbb{Q})$ to $C_1(\mathbb{Q})$, where C_1 is given by the equation $X^3 + Y^3 = Z^3$. The only points on C_1 are the trivial points $(1 : -1 : 0)$, $(0 : 1 : 1)$, and $(1 : 0 : 1)$, by Fermat's last theorem ($n = 3$ case). Taking f of these three points yields

$$E_1(\mathbb{Q}) = \{\infty, (12, -36), (12, 36)\}. \quad \square$$

(d) We can easily calculate that $f(P) = (36, -108)$ on the curve E_9 defined by $y^2 = x^3 - 34992$. The tangent line to E_9 at this point has slope $3x^2/2y = -18$, so its equation is $y = -18x + 540$. Plugging this into the equation for the curve gives $x^3 - 324x^2 + 19440x - 326592 = 0$, and long-dividing by $(x - 36)^2$ yields $x - 252$. (If you believe your arithmetic, you can get 252 from just subtracting $324 - 36 - 36$.) If $x = 252$, then $y = -3996$. This is not quite $2f(P)$; it's $-2f(P)$. So

$$2f(P) = (252, 3996).$$

The point we're looking for is $g(252, 3996) = (4320 : -3672 : 1512) = (540 : -459 : 189)$. \square

Extra Problem 4: Let C be the curve in \mathbb{P}^3 given by the equations

$$\begin{aligned}u^2 + v^2 &= w^2 \\ u^2 - v^2 &= z^2\end{aligned}$$

Let E be the elliptic curve $y^2 = x^3 - 16x$.

(a) Show that the transformations

$$\begin{aligned}f(u : v : w : z) &= \left(\frac{4(w-z)}{2u-w-z}, \frac{16v}{2u-w-z} \right) \\ g(x, y) &= (16 + x^2 : 4y : x^2 + 8x - 16 : x^2 - 8x - 16)\end{aligned}$$

send $C(\mathbb{Q})$ to $E(\mathbb{Q})$ and $E(\mathbb{Q})$ to $C(\mathbb{Q})$, and that they are inverses. What point on $C(\mathbb{Q})$ corresponds to $\infty \in E(\mathbb{Q})$? Find three other points on $C(\mathbb{Q})$ and decide which rational points on $E(\mathbb{Q})$ they go to.

(b) (hard, I think—extra credit only) Determine $C(\mathbb{Q})$ (or $E(\mathbb{Q})$, which is equivalent by part (a).)

Solution: As in Problem 3, these are just computations. First let us show that f takes $C(\mathbb{Q})$ to $E(\mathbb{Q})$. Suppose $(u : v : w : z)$ satisfies the equations for C . Then

$$\begin{aligned}\left(\frac{4(w-z)}{2u-w-z} \right)^3 - 16 \frac{4(w-z)}{2u-w-z} &= \frac{4(w-z)}{2u-w-z} \left(\frac{4(w-z)}{2u-w-z} - 4 \right) \left(\frac{4(w-z)}{2u-w-z} + 4 \right) \\ &= \frac{4(w-z)}{2u-w-z} \cdot \frac{8(w-u)}{2u-w-z} \cdot \frac{8(u-z)}{2u-w-z} \\ &= \frac{256}{(2u-w-z)^3} (u^2(z-w) + u(w^2-z^2) - w^2z + wz^2) \\ &= \frac{256}{(2u-w-z)^3} (u^2(z-w) + u(2v^2) - (u^2+v^2)z + w(u^2-v^2)) \\ &= \frac{256}{(2u-w-z)^3} (2uv^2 - v^2z - wv^2) \\ &= \frac{256v^2}{(2u-w-z)^2} = \left(\frac{16v}{2u-w-z} \right)^2.\end{aligned}$$

Next let us show that g takes $E(\mathbb{Q})$ to $C(\mathbb{Q})$. Suppose $y^2 = x^3 - 16x$. Then

$$\begin{aligned}(16 + x^2)^2 + (4y)^2 &= x^4 + 32x^2 + 256 + 16y^2 = x^4 + 16x^3 + 32x^2 - 256x + 256 = (x^2 + 8x - 16)^2 \\ (16 + x^2)^2 - (4y)^2 &= x^4 + 32x^2 + 256 - 16y^2 = x^4 - 16x^3 + 32x^2 + 256x + 256 = (x^2 - 8x - 16)^2.\end{aligned}$$

Notice that the point that corresponds to ∞ is the point where $2u - w - z$ vanishes, which is $(1 : 0 : 1 : 1)$.

Finally, let's show that f and g are inverses. We compute

$$\begin{aligned}g(f(u : v : w : z)) &= \left(16 + \frac{16(w-z)^2}{(2u-w-z)^2} : \frac{64v}{2u-w-z} : \right. \\ &\quad \left. \frac{16(w-z)^2}{(2u-w-z)^2} + \frac{8(w-z)}{(2u-w-z)} - 16 : \frac{16(w-z)^2}{(2u-w-z)^2} - \frac{8(w-z)}{(2u-w-z)} - 16 \right)\end{aligned}$$

Now

$$(2u-w-z)^2 + (w-z)^2 = 4u^2 - 4u(w+z) + 2(w^2+z^2) = 4u^2 - 4u(w+z) + 4u^2 = 4u(2u-w-z),$$

so the first coordinate above is just $\frac{64u}{2u-w-z}$.

We can similarly work out the last two coordinates as $\frac{64w}{2u-w-z}$ and $\frac{64z}{2u-w-z}$. I've done enough already, I think.

And we also compute

$$f(g(x, y)) = \left(\frac{4(16x)}{64}, \frac{16(4y)}{64} \right) = (x, y)$$

as desired. \square

(b) Notice that $u^4 - v^4 = (wz)^2$, so $u^4 = (wz)^2 + v^4$. It is known that the equation $Z^4 = X^2 + Y^4$ has only trivial solutions (i.e. $X = 0$ or $Y = 0$). (Apparently this was the only proof Fermat ever published! See

<http://fermatslasttheorem.blogspot.com/2005/05/fermats-one-proof.html>

for one account. The method is sometimes called “proof by infinite descent”; notice that this is a stronger result than the $n = 4$ case of Fermat’s last theorem.) So this means that either $v = 0$ or $wz = 0$. So v or w or z is zero. If $v = 0$, we get $u^2 = w^2 = z^2$, which gives the four points $(1 : 0 : \pm 1 : \pm 1)$. (Not eight points, because we’re in projective space and multiplying all the coordinates by -1 doesn’t give new points!) If $w = 0$, we get no points over \mathbb{Q} because $u = v = 0$. If $z = 0$, we get $u^2 = v^2$, but then we get $2u^2 = w^2$, which has no nonzero rational solutions, so we get no new points.

Our conclusion, then, is that

$$C(\mathbb{Q}) = \{(1 : 0 : 1 : 1), (1 : 0 : 1 : -1), (1 : 0 : -1 : 1), (1 : 0 : -1 : -1)\}.$$

Taking f of these points gives

$$E(\mathbb{Q}) = \{\infty, (4, 0), (-4, 0), (0, 0)\}. \quad \square$$

Extra Problem 5: (a) Let X_1 and X_2 be two cubic curves. Suppose they intersect in points P_1, \dots, P_9 . Show that any cubic curve X_3 passing through P_1, \dots, P_8 also passes through P_9 . (Hint: use the Lemma I stated in class, just like I did to prove associativity of elliptic curve addition.)

(b) Prove the *Theorem of the mystic hexagon* (fancy name!): Let $ABCDEF$ be a hexagon inscribed in a conic. Let P be the intersection of \overline{AB} and \overline{DE} . Let Q be the point of intersection of \overline{BC} and \overline{EF} . Let R be the point of intersection of \overline{CD} and \overline{FA} . Then P, Q, R are collinear.

(Hint: use part (a)!)

Solution: (a) Be careful here. There is a point Q such that any cubic curve through P_1, \dots, P_8 also passes through Q , by the Lemma. First we show that $Q = P_9$. Well, X_1 and X_2 are both cubic curves passing through P_1, \dots, P_8 , so Q must be another point that's on both curves. The only possibility is P_9 , so $Q = P_9$. Now then, any cubic curve X_3 passing through P_1, \dots, P_8 also passes through $Q = P_9$, by the Lemma. \square

(b) Let X_1 be the union of the three lines $\overline{AB}, \overline{CD}, \overline{EF}$. Let X_2 be the union of the three lines $\overline{BC}, \overline{DE}, \overline{FA}$. Let X_3 be the union of the conic and the line \overline{PQ} .

Now X_1 and X_2 are cubic curves intersecting in the points $A, B, C, D, E, F, P, Q, R$. And X_3 passes through A, B, C, D, E, F, P, Q . So X_3 passes through R , by part (a). Now certainly R can't be on the conic, because if it were, we'd have that the intersection of the conic and, say, the line \overline{CD} would have three points C, D, R on it, which would contradict Bézout. So R is on the line \overline{PQ} . \square