18.704 Fall 2004 Homework 8 Solutions

All references are to the textbook “Rational Points on Elliptic Curves” by Silverman and Tate, Springer Verlag, 1992. Problems marked (*) are more challenging exercises that are optional but not required.

1. A nonsingular projective conic with at least one point over the field \( \mathbb{F}_p \) has exactly \( p + 1 \) projective points; the reason is that one can project onto a line as is argued on page 109 of the text. In this problem we see that the same is not true for singular conics. Let \( p \neq 2 \) be a prime, and let \( C \) be the conic given by the homogeneous equation \( C : aX^2 + bXY + cY^2 = dZ^2 \) where \( a, b, c, d \in \mathbb{F}_p \) and \( a, b, d \neq 0 \). Let \( \#C(\mathbb{F}_p) \) be the number of points on \( C \) in projective space over \( \mathbb{F}_p \).

(a) Note that \( C \) is the given by the vanishing of \( F(X, Y, Z) = aX^2 + bXY + cY^2 − dZ^2 \) in \( \mathbb{P}^2 \). Recall that \( C \) is nonsingular at a point as long as not all partial derivatives of \( F \) vanish there. Show that \( C \) is nonsingular if and only if \( b^2 = 4ac \).

(b) Assume that \( C \) is singular. Then do Exercise 4.1(b) from the text. For \( p = 3 \), find choices of \( a, b, c, d \) for which each possibility occurs.

Solution. (a) The partial derivatives are \( \frac{\partial F}{\partial X} = 2aX + bY \), \( \frac{\partial F}{\partial Y} = bX + 2cY \), and \( \frac{\partial F}{\partial Z} = −2dZ \). If all of these are zero at a point, then (since we assume \( d \neq 0 \) and \( p \neq 2 \)), \( Z = 0 \). Then \( aX^2 + bXY + cY^2 = 0 \) and \( 2aX + bY = 0 \), so \( Y = −2ab^{-1}X \), so \( aX^2 + 2aX^2 + 4ca^2b^{-2}X^2 = 0 \). If \( X = 0 \), and then \( Y = 0 \), but \( [0, 0, 0] \) is not a point in projective space, so this is a contradiction. Thus \( −a + 4ca^2b^{-2} = 0 \), so \( 4ca^2 − ab^2 = 0 \) and so (since \( a \neq 0 \)) \( 4ca − b^2 = 0 \). The converse is similar.

(b) Since \( C \) is singular, by part (a) we have \( b^2 − 4ac = 0 \). The reason this is special is that the left hand side of our equation factors:

\[
aX^2 + bXY + cY^2 = (2aX − bY)(2aX − bY) = dZ^2.
\]

First we count the points at infinity. So if \( Z = 0 \), then \( 2aX = bY \). So \( [b, −2a, 0] \) is a point at infinity, and since scalar multiples give the same point of projective space, this is the only point at infinity.

Now we may assume \( Z = 1 \) and look for affine points \((x, y)\) with \((2ax − by)^2 = d \). If \( d \) is not a square in \( \mathbb{F}_p \), then this has no solutions. So in this case the
point at infinity is the only solution and \( \#C(F_p) = 1 \). Otherwise, \( d \) is a nonzero square in \( F_p \), say \( d = c^2 \). Then \( 2ax - by = \pm c \). Since we assume \( b \neq 0 \), for each possible choice of \( x \), we get the two solutions \( y = b^{-1}(2ax \pm e) \). Since \( x \) can vary over the \( p \) elements of \( F_p \), we get \( 2p \) affine points this way (note that the two elements \( 2ax \pm e \) are always distinct, otherwise \( 2e = 0 \) and since \( p \neq 2, e = 0 \), a contradiction.) Adding in the point at infinity, we get \( 2p + 1 \) points total on \( C \).

When \( p = 3 \), we get both possibilities by choosing \( d = 1 \) (a square) and \( d = 2 \) (not a square). So (for example) \( C : X^2 + 2XY + Y^2 = Z^2 \) has 7 solutions in \( F_3 \), but \( C : X^2 + 2XY + Y^2 = 2Z^2 \) has 1 solution in \( F_3 \).

2. (a) Let \( C \) be the projective curve \( x^3 + y^3 + z^3 = 0 \) which is the subject of Gauss’s theorem. Calculate \( \#C(F_p) \) for \( p = 307 \) (you don’t need a computer; see the suggestions on page 118.)

(b) Let \( p \) be a prime with \( p \equiv 2(\text{mod} \ 3) \), and let \( c \in F_p \). Prove that the curve \( C : y^2 = x^3 + c \) satisfies \( \#C(F_p) = p + 1 \).

Solution. (a) By the result of Gauss’s Theorem, \( \#C(F_p) \) is equal to \( p + 1 + A \), where \( 4p = A^2 + 27B^2 \) and \( A \) is congruent to 1 mod 3. So we need to find \( A \) and \( B \) where \( p = 307 \). As discussed on page 118, \( p + 1 + A \) is always divisible by 9. So \( A \equiv 7(\text{mod} \ 9) \). We try \( A = 7, 16, 23, \ldots \). If \( A = 7 \), then \( 27B^2 = 1079 \), but 1079 is not a multiple of 27. Trying \( A = 16 \), then \( 27B^2 = 972 \), and \( B^2 = 36 \) and \( B = 6 \) so we’re done: \( 4(307) = 16^2 + 27(6)^2 \). So \( \#C(F_p) = 308 + 16 = 324 \).

(b) As we saw in the proof of Gauss’s Theorem, for a prime \( p \) which is not congruent to 1 mod 3, every element of \( F_p \) has a unique cube root. Therefore as \( x \) varies over the elements in \( F_p \), \( x^3 + c \) varies over all of the elements of \( F_p \). Now if \( p = 2 \) then the result can be checked directly, so assume from now on that \( p \) is an odd prime. Then if \( x^3 + c \) is a nonzero square in \( F_p \) then there will be two points of the form \((x, y)\) on \( C \); if \( x^3 + c = 0 \) then there is one corresponding point \((x, 0)\) on \( C \); and if \( x^3 + c \) is not a square then there are no points on \( C \) with that \( x \)-coordinate. Now since \( p \) is odd, exactly \( 1/2 \) of the elements of \( F_p^* \) are squares. So we get \( 2(1/2)(p - 1) + 1 = p \) points on the curve in the affine plane. Throwing in the point at infinity \( O \), we get \( p + 1 \) points on \( C \).

3. In this exercise we work over \( \mathbb{Q} \), and revisit points of finite order again using reduction modulo \( p \) as a tool. The equation we are interested in is

\[
C : y^2 = x^3 + bx \quad \text{for some nonzero} \ b \in \mathbb{Z}.
\]

Let \( \Phi \subset C(\mathbb{Q}) \) be the subgroup consisting of all rational points of finite order on \( C \).

(a) In Exercise 4.8, p. 142, it is shown that if \( p \) is any prime number such that \( p \equiv 3 \ (\text{mod} \ 4) \), and \( b \) is not equal to 0 in \( F_p^\times \), then the curve \( C : y^2 = x^3 + bx \)
satisfies \( \#C(\mathbb{F}_p) = p + 1 \). Assume this without proof, and use it to show that the order of the group \( \Phi \) is 2 or 4.

(b) Recall from section III.4 that the multiplication by 2 map on \( C \) is decomposed as a composition \( \psi \circ \phi \) where \( \phi : C \rightarrow \overline{C} \) and \( \psi : \overline{C} \rightarrow C \) are given by explicit formulas on p. 79. Use these formulas to show that there exists a rational point \( P \in C \) such that \( 2P = (0, 0) \) if and only if \( b = 4d^4 \) for some integer \( d \).

(c) Show that the group structure of \( \Phi \) is given precisely by the following table:

\[
\Phi = \begin{cases} 
\mathbb{Z}/4\mathbb{Z} & \text{if } b = 4d^4 \text{ for some } d \in \mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } -b \text{ is a square} \\
\mathbb{Z}/2\mathbb{Z} & \text{otherwise.}
\end{cases}
\]

Solution. By exercise 4.8 which we were asked to quote, it follows that \( C(\mathbb{F}_p) = p + 1 \) for all \( p \) which are congruent to 3 mod 4 and which do not divide \( b \). Then by the reduction mod \( p \) theorem in Section IV.3, we see that \( N = |\Phi| \) divides \( p + 1 \) for all primes \( p \equiv 3(\text{mod } 4) \) such that \( p > b \). Rephrasing, we have that every prime greater than \( b \) which is congruent to 3 mod 4 is also congruent to \(-1 \mod N \). I hope your intuition told you this is not likely to happen if \( N \) is not equal to 1, 2, or 4.

To actually prove what we want, we can quote a famous theorem (Sorry not to warn you about this.) Dirichlet proved in the 1800’s that every arithmetic progression \( \{an + b|n \in \mathbb{N}\} \), where \( a \) and \( b \) are positive integers with \( \gcd(a, b) = 1 \), contains infinitely many prime numbers. So we see that if \( N \geq 5 \), then there are infinitely many primes in the progression \( \{4Nn + 3|n \geq 1\} \), and these are all primes which are congruent to 3 mod 4, but congruent to \( 3 \neq -1(\text{mod } N) \). This is a contradiction to what we showed above. So \( N \leq 4 \). But now \( N = 3 \) and \( N = 1 \) are no good, since we know that \( \Phi \) has the point \((0, 0)\) of order 2. So \( N = 2 \) or 4.

(b). Let \( \overline{C} \) be the curve \( y^2 = x^3 - 4bx \), and let \( \phi : C \rightarrow \overline{C} \) and \( \psi : \overline{C} \rightarrow C \) be the maps given in Section III.4. Suppose \( P \in C \) is a point such that \( 2P = (0, 0) \). Suppose \( Q = (w, z) \in \overline{C} \) such that \( \psi(Q) = (0, 0) \). Examining the formula for \( \psi \), we see that this implies that \( Q = (w, 0) \) for some nonzero \( w \) such that \( w^2 = 4b \). So \( b \) is a square; write \( b = f^2 \) for some integer \( f \geq 1 \). Now we also must have a point \( P = (x, y) \in C \) such that \( \phi(P) = Q = (w, 0) \). Examining the formula for \( \phi \), we see that if \( y = 0 \) then \( \phi(P) \in \{T, O\} \). So \( y \neq 0 \), and this implies by the formula that \( w \) is a perfect square, say \( w = e^2 \). Then \( w^2 = e^4 = 4b \). So \( 16b = 4e^4 \) and then writing \( e = 2d \), we have \( b = 4d^4 \) as required. Conversely, if \( b = 4d^4 \) for some integer \( d \) then one may check that setting \( P = (2d^2, 4d^3) \), we have \( 2P = (0, 0) \).

(c). By Part (a), we have \(|\Phi| = 2 \) or \(|\Phi| = 4 \).
Suppose that \( \Phi \) contains 4 points of order dividing 2. We know the points of order 2 are exactly those points with 0 y-coordinate, and there exists such a rational point other than \((0, 0)\) if and only if \(0 = x(x^2 + b)\) has a nonzero solution for \(x\), i.e. \(-b = d^2\) is a square. In this case we get \( \Phi = \{(\pm d, 0), (0, 0), \mathcal{O}\} \), and since every point has order dividing 2, we must have \( \Phi \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \). This is line 2 of the table.

So we may assume now that the only rational points of order dividing 2 on \(C\) are \((0, 0)\) and \( \mathcal{O} \). Suppose however that still \(|\Phi| = 4\). Then \( \Phi \) must be cyclic of order 4, and there is some rational point \(Q\) with \( \Phi = \{Q, (0, 0), 3Q, \mathcal{O}\} \) where \(Q\) has order 4. In particular, \(2Q = (0, 0)\), and by part (b), such a \(Q\) exists if and only if \(b = 4d^4\) for some \(d\). In this case \( \Phi \cong \mathbb{Z}/4\mathbb{Z} \) and this is line 1 of the table.

Finally, we have the case where \(|\Phi| = 2\). So in this case we must have \( \Phi = \{\mathcal{O}, (0, 0)\} \) and \( \Phi \cong \mathbb{Z}/2\mathbb{Z} \). This happens for all other choices of \(b\), and is line 3 of the table.