MIDTERM - MATH 104C SPRING 2012: SOLUTIONS

1. Let $E : y^2 = x^3 + qx$, with $q > 3$ a prime number.
   (a) Show that E has a torsion point $P \neq \infty$. What is its order, i.e. the smallest k such that $kP = \infty$?

Answer : The point $P = (0, 0)$ lies on E. It has vertical tangent line (check this via implicit differentiation, or geometrically, using the symmetry with respect to the x-axis). Hence the third intersection of the tangent with E is at the point ∞, by our definitions. It follows that $2P = \infty$, i.e. P has order 2.

   (b) Show that the group of torsion points of E together with ∞ is at most twice as big as the order of the point P in (a). *Hint* : You may assume the results of Problem 3 regardless whether you could do it or not).

Answer : It follows from a theorem in class that $(t + 1)|(N_p + 1)$, where t is the number of torsion points in $E(\mathbf{Q})$, provided that p does not divide the discriminant Δ. The latter is equal to $-4q^3$ in our case. Hence we can use $p = 3$. By Problem 3, $N_p = 3$. Hence $(t + 1)|(3 + 1) = 4$. Hence the group of torsion points together with the point ∞ has at most order 4.

Remark : It is also easy to see that this group can not be equal to $\mathbf{Z}_2 \times \mathbf{Z}_2$, as any point of order 2 would have to lie on the x-axis. In fact, with some additional work, one can show that there are no other torsion points besides (0,0).

2. Let $E : y^2 = x^3 + 3x$, and let $P = (1, 2)$.
   (a) Calculate the rational point $2P$. Is P a torsion point?

Answer : Using implicit differentiation, we get

$$\frac{dy}{dx} = \frac{3x^2 + 3}{2y} = \frac{6}{4} = \frac{3}{2},$$

where the last two equalities hold for the point $P = (1, 2)$. One deduces from this that the tangent line at $(1, 2)$ has the equation $y = \frac{3}{2}x + \frac{1}{2}$. We get from this that $x_1 + x_2 + x_3 = \frac{9}{4} - 0$, and hence $x_3 = \frac{1}{4}$ for the third intersection of the tangent line with E. Plugging this value for x_3 in the equation for the tangent line, we obtain $y_3 = \frac{7}{4}$. Hence $2P = (\frac{1}{4}, -\frac{7}{4})$.

As the coefficients of $2P$ are not integers, it can not be a torsion point. Hence also P can not be a torsion point (as any multiple of a torsion point would again be a torsion point).

   (b) Calculate $2P$ mod 43, i.e. as a point in $E(\mathbf{F}_{43})$.

Answer : We have $4 \cdot 11 = 44 = 1$ mod 43. Hence $4^{-1} = 11$ mod 43, $2^{-1} = 22$ mod 43, and $8^{-1} = 11 \cdot 22 = 27 = -16$ mod 43. One calculates from this that $2P = (11, (-7)(-16)) = (11, 26)$ mod 43.

   (c) Find k such that $kP = (\frac{A_k}{B_k^2}, \frac{C_k}{B_k^3})$ satisfies $43|B_k$. You may assume that kP can be written as stated, and you may assume the results of Problem 3 regardless whether you could do it or not.

Answer : We showed in one of our review exercises that the restriction $\overline{kP}$ mod 43 for the point kP is equal to ∞ (in the group $E(\mathbf{F}_{43}) \cup \{\infty\}$) if and only if $43|B_k$. (You should prove this for yourself, again, or ask me if you do not remember how we did it). Hence it suffices to find a k for which $\overline{kP} = \infty$ mod 43.

If $|G|$ is the order of the finite group G, then it follows that $|G|x$ is equal to the identity element of G, for any $x \in G$, by Lagrange's theorem. The group $E(\mathbf{F}_{43}) \cup \{\infty\}$ has $N_{43}+1$ elements. Again, by Problem 3, we have $N_{43} = 43$, as $43 \equiv 3$ mod 4, and 43 doe not divide the discrimant $\Delta = -4 \cdot 3^3$ of E. Hence we have $\overline{44P} = \infty$. It follows that 43 divides B_{44}, by the discussion in the first paragraph.

Remark : Of course, it could already happen for a smaller k that 43 divides B_k. What k could you choose for $p = 3$? Compare with your actual calculations.

3. Let $E : y^2 = x^3 + bx$, with $b \neq 0$, and let p be a prime number with $p \equiv 3$ mod 4. The goal is to prove that $N_p = p$, where N_p is the number of points on E mod p.
   (a) *(Extra Credit; only do it if you have plenty of time.)* Show that for any a with $(a, p) = 1$ either a or $-a$ is a quadratic residue.

Answer : (sketch) This can be fairly easily done if you are familiar with the Legendre symbol. The key point for this, and also for a direct solution, is the fact that -1 is not a quadratic residue mod p if $p \equiv 3$ mod 4. So if for a with $(a, p) = 1$ we had both $a \equiv b^2$ mod p and $-a \equiv c^2$ mod p, then we would have $(bc^{-1})^2 \equiv -1$ mod p, a contradiction. Hence at most one of a or $-a$ can be a quadratic residue. But as there are $(p-1)/2$ quadratic residues a with $(a, p) = 1$, exactly one of a or $-a$ must be a quadratic residue.

   (b) Show that $N_p = p$ (*Hint* : Let $f(x) = x^3 + bx$. Then $f(-x) = -f(x)$. Use this and part (a)).

Answer : We consider possible y values as pairs of numbers $\{f(x), f(-x) = -f(x)\}$ for $x = 1, 2, \ ... \ (p-1)/2$. If $f(x) \neq 0$ mod p, then exactly one of the two numbers is a quadratic residue by (a), and we get two solutions for that number, and 0 for the other number. If $f(x) = 0 = f(-x)$, then we get the two solutions $(x, 0)$ and $(-x, 0)$. Hence we get $2 \cdot \frac{p-1}{2} = p - 1$ solutions for the x-values $x = \pm 1, \pm 2, \ ... \ \pm \frac{p-1}{2}$. Finally, as $f(0) = 0$, we also get the solution $(0, 0)$ for $x = 0$. This finishes the proof.