Math 110 HW 5 solutions

June 9, 2013

1. Let E be the elliptic curve over the field $\mathbb{F}_5$ defined by the equation $y^2 = x^3 + 2x + 1$. On E, compute $2P$ where P is the point $(1, 2)$. How many points are in E?

   Recall $\mathbb{F}_5$ is just the integers mod 5.

   To find the points, if $x = 0$ then $y^2 \equiv 1$ so $y \equiv \pm 1 \equiv 1, 4 \pmod 5$. If $x = 1$ then $y^2 = 4$ so $y \equiv \pm 2 \equiv 2, 3 \pmod 5$. If $x = 2$ then $y^2 \equiv 3$ which has no solutions, if $x = 3$ then $y^2 \equiv 4$ as before, and if $x = 4$ then $y^2 \equiv 3$ which has no solutions.

   So the points of the curve are $(0, 1), (0, 4), (1, 2), (1, 3), (3, 2), (3, 3)$ which is six points, and the point at infinity makes it 7.

   Now at the point $(1, 2)$ we need the slope of the tangent line using implicit differentiation as in the book. We get $2ydy = 3x^2dx + 2dx$, so $dy/dx = \frac{3x^2+2}{2y}$. Substituting in $(1, 2)$ for (x, y) we have the numerator 0, denominator 2, so we get slope 0. Thus we are looking for another point with the same y-coordinate, that's the point $(3, 2)$. Reflecting across the y-axis we get $(3, -2)$ which on the list is $(3, 3)$.

2. Let p be an odd prime number. Suppose that $a \not\equiv 0 \pmod p$. Give a criterion for whether a is or is not a square modulo p according to the largest power of 2 which divides $\mathrm{ord}_p(a)$.

   Let $p - 1 = 2^k d$ where d is odd, so that 2^k is the largest power of 2 that divides $p - 1$. Then if a is a square, there is an element whose order is twice that of a. In that case the order of a must be at most $2^{k-1}d$, and must divide that, so the largest power of 2 that divides the order of a is $k - 1$.

   To show that this is a sufficient condition, suppose b is a primitive root mod p; that is, b has order $p - 1$. Then there is some i such that $b^i \equiv a \pmod p$. If i is even, then $b^{i/2}$ gives a square root of a. Suppose i is odd, and let $r = \mathrm{ord}_p(a)$. Then $p - 1$ divides ir because $b^{ir} \equiv a^r \equiv 1 \pmod p$. Thus 2^k divides r.

   So if 2^k does not divide r, then i is even, thus a has a square root. Another way of saying this is that a has a square root mod p if and only if the largest power of 2 dividing $\mathrm{ord}_p(a)$ is 2^{k-1}.

3. Working over the integers mod p, consider the nodal curve C defined by $y^2 = x^3$. Prove that any point on this curve is of the form (t^2, t^3) for some $t \in \mathbb{F}_p$.

   If $x = 0$ then $y = 0$ also and then $(x, y) = (t^2, t^3)$ with $t = 0$. So now we may assume that $x \neq 0$. Let $t = y/x$. Then $x = x^3/x^2 = y^2/x^2 = t^2$ and $y = tx = t \cdot t^2 = t^3$.

4. For nonzero distinct s, t, u, prove that three points $(s^2, s^3), (t^2, t^3)$, and (u^2, u^3) are collinear if and only if $1/s + 1/t + 1/u = 0$. (This shows that one does not get a new group from the curve C in the previous problem.)

   If the three points are collinear, since s, t, u are distinct, the x coordinates of each point are distinct as are the y coordinates. So the points all lie on a line $y = ax + b$ of nonzero, finite slope. Thus we have the equations

$$\begin{aligned} s^3 &= as^2 + b \\ t^3 &= at^2 + b \\ u^3 &= au^2 + b \end{aligned}$$

   So the points are the three distinct roots of a cubic $x^3 - ax^2 + b = 0$. Thus that cubic has the form $(x-s)(x-t)(x-u)$, which multiplying out gives us $x^3 - (s+t+u)x^2 + (st+tu+us)x + stu$. That tells us $a = s+t+u$ and $b = stu$, but the most relevant information is that $st+tu+us = 0$. Since stu is nonzero we can divide by it to obtain $1/s + 1/t + 1/u = 0$.

   Going the other way, if $1/s + 1/t + 1/u = 0$ then we set $a = s + t + u$ and $b = stu$ and thus obtain the line $y = ax + b$ which contains all three points.

5. Factor 35 using the elliptic curve method with the elliptic curve $y^2 = x^3 + 5x + 8$ and the point $(1, 28)$.

   First to check that the point is on the curve: $28^2 = 784 \equiv 14 \pmod{35}$, and $1 + 5 + 8 = 14$.

   The tangent line to $(1, 28)$ is found again using implicit differentiation: $2ydy = 3x^2dx + 5dx$, so $\frac{dy}{dx} = \frac{3x^2+5}{2y}$. Substitute in $(1, 28)$ and we have $8/56$. Unfortunately we cannot invert 56 mod 35, and to see why we calculate with the Euclidean algorithm that $gcd(56, 35) = gcd(35, 21) = gcd(21, 14) = gcd(14, 7) = 7$. Therefore 7 is a factor of 35, and dividing we get 5. We then verify that 5 and 7 are prime, so we have successfully factored 35.