

Solutions to Math 42 Homework Assignment

Exercise 46.2 Exercise 44.2(c) says that the elliptic curve $E : y^2 = x^3 - x$ has a torsion collection $\{(0, 0), (1, 0), (-1, 0)\}$ containing three points.

- (a) Find the number of points on E modulo p for $p = 2, 3, 5, 7, 11$. Which ones satisfy $N_p \equiv 3 \pmod{4}$?
- (b) Find the solutions to E modulo 11, other than the solutions in the torsion collection, and group them into bundles of four solutions each by drawing lines through the points in the torsion collection.

Solution. (a) $N_2 = 2$, $N_3 = 3$, $N_5 = 7$, $N_7 = 7$, $N_{11} = 11$, $N_{13} = 7$, $N_{17} = 15$. All satisfy $N_p \equiv 3 \pmod{4}$ except for N_2 .

(b) Starting with the solution $(4, 4)$ to E modulo 11, we find new points by drawing lines through $(4, 4)$ and points in the torsion collection:

The line through $(4, 4)$ and $(0, 0)$ gives $(8, 8)$.
The line through $(4, 4)$ and $(1, 0)$ gives $(9, 7)$.
The line through $(4, 4)$ and $(-1, 0)$ gives $(6, 10)$.

Next we plug in value for x until we find another solution, say $(6, 1)$. Then we draw lines through $(6, 1)$ and the points in the torsion collection to find the remaining solutions,

The line through $(6, 1)$ and $(0, 0)$ gives $(9, 7)$.
The line through $(6, 1)$ and $(1, 0)$ gives $(8, 8)$.
The line through $(6, 1)$ and $(-1, 0)$ gives $(4, 7)$.

So the set of 11 solutions to E modulo 11 is made up of the three points

$$\{(0, 0), (1, 0), (-1, 0)\}$$

in the torsion packet together with the two bundles of four points each

$$\{(4, 4), (8, 8), (9, 7), (6, 10)\} \quad \text{and} \quad \{(6, 1), (9, 7), (8, 8), (4, 7)\}.$$

Exercise 47.1 In this exercise you will look for further patterns in the coefficients of the product Θ described in the Modularity Theorem for E_3 . If we write Θ as a sum,

$$\Theta = c_1T + c_2T^2 + c_3T^3 + c_4T^4 + c_5T^5 + \dots,$$

the Modularity Theorem says that for primes $p \geq 3$ the p^{th} coefficient c_p is equal to the p -defect a_p of E_3 . Use the following table, which lists the c_n coefficients of Θ for all $n \leq 100$, to formulate conjectures.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
c_n	1	-2	-1	2	1	2	-2	0	-2	-2	1	-2	4	4	-1	-4	-2
n	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
c_n	4	0	2	2	-2	-1	0	-4	-8	5	-4	0	2	7	8	-1	4
n	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
c_n	-2	-4	3	0	-4	0	-8	-4	-6	2	-2	2	8	4	-3	8	2
n	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
c_n	8	-6	-10	1	0	0	0	5	-2	12	-14	4	-8	4	2	-7	-4
n	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
c_n	1	4	-3	0	4	-6	4	0	-2	8	-10	-4	1	16	-6	4	-2
n	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100		
c_n	12	0	0	15	4	-8	-2	-7	-16	0	-8	-7	6	-2	-8		

- (a) Find a relationship between c_m , c_n , and c_{mn} when $\gcd(m, n) = 1$.
- (b) Find a relationship between c_p and c_{p^2} for primes p . To assist you, here are the values of c_{p^2} for $p \leq 37$.

$$\begin{aligned}
 c_{2^2} &= 2, & c_{3^2} &= -2, & c_{5^2} &= -4, & c_{7^2} &= -3, \\
 c_{11^2} &= 1, & c_{13^2} &= 3, & c_{17^2} &= -13, & c_{19^2} &= -19, \\
 c_{23^2} &= -22, & c_{29^2} &= -29, & c_{31^2} &= 18, & c_{37^2} &= -28
 \end{aligned}$$

(*Hint.* The prime $p = 11$ is a bad prime for E_3 , so you may want to treat c_{11^2} as experimental error and ignore it!)

Solution. (a) If $\gcd(m, n) = 1$, then $c_{mn} = c_m c_n$.

(b) Comparing c_p to c_{p^2} doesn't yield a pattern, but a pattern emerges if one compares c_p^2 with c_{p^2} , namely

$$c_p^2 = c_{p^2} + p.$$

This holds for all p except for $p = 11$.