Example: $y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$

$$W_1 = 1$$
$$W_2 = 1$$
$$W_3 = -3$$
$$W_4 = 11$$
$$W_5 = 38$$
$$W_6 = 249$$
$$W_7 = -2357$$

Example: $y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$

$$
\begin{array}{ll}
W_1 = 1 & P = (0,0) \\
W_2 = 1 & [2]P = (3,5) \\
W_3 = -3 & [3]P = \left(-\frac{11}{9}, \frac{28}{27}\right) \\
W_4 = 11 & [4]P = \left(\frac{114}{121}, -\frac{267}{1331}\right) \\
W_5 = 38 & [5]P = \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right) \\
W_6 = 249 & [6]P = \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right) \\
W_7 = -2357 & [7]P = \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right)
\end{array}
$$

Example: $y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$

$$
\begin{array}{ll}
W_1 = 1 & P = (0,0) \\
W_2 = 1 & [2]P = (3,5) \\
W_3 = -3 & [3]P = \left(-\frac{11}{9}, \frac{28}{27}\right) \\
W_4 = 11 & [4]P = \left(\frac{114}{121}, -\frac{267}{1331}\right) \\
W_5 = 38 & [5]P = \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right) \\
W_6 = 249 & [6]P = \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right) \\
W_7 = -2357 & [7]P = \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right)
\end{array}
$$

Example: $y^2 + y = x^3 + x^2 - 2x, P = (0, 0)$

$$
\begin{aligned}
W_1 &= 1 & P &= (0,0) \\
W_2 &= 1 & [2]P &= (3,5) \\
W_3 &= -3 & [3]P &= \left(-\frac{11}{3^2}, \frac{28}{3^3}\right) \\
W_4 &= 11 & [4]P &= \left(\frac{114}{11^2}, -\frac{267}{11^3}\right) \\
W_5 &= 38 & [5]P &= \left(-\frac{2739}{38^2}, -\frac{77033}{38^3}\right) \\
W_6 &= 249 & [6]P &= \left(\frac{89566}{249^2}, -\frac{31944320}{249^3}\right) \\
W_7 &= -2357 & [7]P &= \left(-\frac{2182983}{2357^2}, -\frac{20464084173}{2357^3}\right)
\end{aligned}
$$

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

$\uparrow$
Q
$P \rightarrow$

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	−55287	23921	1587077	−7159461
94	479	919	−2591	13751	68428	424345
−31	53	−33	−350	493	6627	48191
−5	8	−19	−41	−151	989	−1466
1	3	−1	−13	−36	181	−1535
1	1	2	−5	7	89	−149
0	1	1	−3	11	38	249

$\uparrow Q$

$P \rightarrow$

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	−55287	23921	1587077	−7159461
94	479	919	−2591	13751	68428	424345
−31	53	−33	−350	493	6627	48191
−5	8	−19	−41	−151	989	−1466
1	3	−1	−13	−36	181	−1535
1	1	2	−5	7	89	−149
0	1	1	−3	11	38	249

$\uparrow Q$

$P \rightarrow$

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	−55287	23921	1587077	−7159461
94	479	919	−2591	13751	68428	424345
−31	53	−33	−350	493	6627	48191
−5	8	−19	−41	−151	989	−1466
1	3	−1	−13	−36	181	−1535
1	1	2	−5	7	89	−149
0	1	1	−3	11	38	249

$\uparrow Q$

$P \rightarrow$

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

$\uparrow$
Q

$P \rightarrow$

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	−55287	23921	1587077	−7159461
94	479	919	−2591	13751	68428	424345
−31	53	−33	−350	493	6627	48191
−5	8	−19	−41	−151	989	−1466
1	3	−1	−13	−36	181	−1535
1	1	2	−5	7	89	−149
0	1	1	−3	11	38	249

$Q \uparrow$

$P \rightarrow$

Prime Divisors in an Elliptic Net

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
$\uparrow$	0	1	1	-3	11	38	249
Q							
	$P \rightarrow$						

Prime Divisors in an Elliptic Net

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

	4335	5959	12016	−55287	23921	1587077	−7159461
	94	479	919	−2591	13751	68428	424345
	−31	53	−33	−350	493	6627	48191
	−5	8	−19	−41	−151	989	−1466
	1	3	−1	−13	−36	181	−1535
	1	1	2	−5	7	89	−149
$\uparrow Q$	0	1	1	−3	11	38	249
	$P \rightarrow$						

Prime Divisors in an Elliptic Net

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	−55287	23921	1587077	−7159461
94	479	919	−2591	13751	68428	424345
−31	53	−33	−350	493	6627	48191
−5	8	−19	−41	−151	989	−1466
1	3	−1	−13	−36	181	−1535
1	1	2	−5	7	89	−149
0	1	1	−3	11	38	249

$Q \uparrow$

$P \rightarrow$

Prime Divisors in an Elliptic Net

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	−55287	23921	1587077	−7159461
94	479	919	−2591	13751	68428	424345
−31	53	−33	−350	493	6627	48191
−5	8	−19	−41	−151	989	−1466
1	3	−1	−13	−36	181	−1535
1	1	2	−5	7	89	−149
0	1	1	−3	11	38	249

$Q \uparrow$

$P \rightarrow$

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1
	$P \rightarrow$																			

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1
	$P \rightarrow$																			

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1
	$P \rightarrow$																			

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1
	$P \rightarrow$																			

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1
	$P \rightarrow$																			

$$\mathbf{r} = (3,1), \qquad a_r = 2, b_r = 2, c_r = 1$$

$$W(4,3) \equiv W(1,2)2^1 2^2 1^1 \equiv 3W(1,2) \mod 5$$

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$P \rightarrow$

$$\mathbf{r} = (9, 0), \qquad a_r = 4, b_r = 3, c_r = 2$$

$$W(11, 3) \equiv W(2, 3)4^2 3^3 2^1 \equiv 4W(2, 3) \mod 5$$

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$P \rightarrow$

$$\mathbf{r} = (9, 0), \qquad a_r = 4, b_r = 3, c_r = 2$$

$$W(11, 3) \equiv W(2, 3)4^2 3^3 2^1 \equiv 4W(2, 3) \mod 5$$

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$P \rightarrow$

$$\mathbf{r} = (9, 0), \qquad a_r = 4, b_r = 3, c_r = 2$$

$$W(11, 3) \equiv W(2, 3)4^2 3^3 2^1 \equiv 4W(2, 3) \mod 5$$

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$P \rightarrow$

$$\mathbf{r} = (9, 0), \qquad a_r = 4, b_r = 3, c_r = 2$$

$$W(11, 3) \equiv W(2, 3)4^2 3^3 2^1 \equiv 4W(2, 3) \mod 5$$