

Forms of Distinct Odd Primes in Elliptic Curve

$$y^2 = x^3 - pqx$$

Shin-Wook Kim

Deokjin-gu, Songcheon, 54823
I-Park Apt
Jeonju, Jeonbuk, Korea

This article is distributed under the Creative Commons by-nc-nd Attribution License.
Copyright © 2026 Hikari Ltd.

Abstract

If odd primes p and q are such that $p \equiv 3 \pmod{16}$ and $q \equiv 15 \pmod{16}$ or $p \equiv 11 \pmod{16}$ and $q \equiv 7 \pmod{16}$ in $E_{-pq}: y^2 = x^3 - pqx$ then, rank 2 can be deduced ([2] and [4]). It is trivial that we pursue primes p and q as complex as possible. The primes of the forms $p = ()u^4 + ()v^4 + ()w^4 + ()u^2v^2 + ()u^2w^2 + ()v^2w^2$ and $q = ()'u^4 + ()'v^4 + ()'w^4 + ()'u^2v^2 + ()'u^2w^2 + ()'v^2w^2$ in [5] was the beginning taking more numbers of terms than $p = Hu^4 + Iv^2v^2 + Kv^4$ and $q = H'u^4 + I'u^2v^2 + K'v^4$. In [10], the primes p and q are composed of 22 variables and 253 terms where variables are A and B and C and D and E and F and G and H and I and J and K and L and O and P and Q and R and S and T and U and V and W and Z . In this article, we add more variables to [10].

Mathematics Subject Classification: 11A41, 11G05

Keywords: Distinct primes, elliptic curve

1 Introduction

In [6], the primes p and q as $p = ()c^4 + ()d^2 + ()f^2 + ()g^2 + ()h^2 + ()i^2 + ()j^2 + ()k^2 + ()l^2 + ()s^2 + ()t^2 + ()u^2 + ()v^2 + ()w^2 + ()z^2 + ()c^2d + ()c^2f + ()c^2g + ()c^2h + ()c^2i + ()c^2j + ()c^2k + ()c^2l$

$() \cdot c^2s + ()c^2t + ()c^2u + ()c^2v + ()c^2w + ()c^2z + ()df + ()dg + ()dh + ()di + ()dj + ()dk + ()dl + ()ds + ()dt + ()du + ()dv + ()dw + ()dz + ()fg + ()fh + ()fi + ()fj + ()fk + ()fl + ()fs + ()ft + ()fu + ()fv + ()fw + ()fz + ()gh + ()gi + ()gj + ()gk + ()gl + ()gs + ()gt + ()gu + ()gv + ()gw + ()gz + ()hi + ()hj + ()hk + ()hl + ()hs + ()ht + ()hu + ()hv + ()hw + ()hz + ()ij + ()ik + ()il + ()is + ()it + ()iu + ()iv + ()iw + ()iz + ()jk + ()jl + ()js + ()jt + ()ju + ()jv + ()jw + ()jz + ()kl + ()ks + ()kt + ()ku + ()kv + ()kw + ()kz + ()ls + ()lt + ()lu + ()lv + ()lw + ()lz + ()st + ()su + ()sv + ()sw + ()sz + ()tu + ()tv + ()tw + ()tz + ()uv + ()uz + ()vw + ()vz + ()wz$ and $q = \{ \}c^4 + \{ \}d^2 + \{ \}f^2 + \{ \}g^2 + \{ \}h^2 + \{ \}i^2 + \{ \}j^2 + \{ \}k^2 + \{ \}l^2 + \{ \}s^2 + \{ \}t^2 + \{ \}u^2 + \{ \}v^2 + \{ \}w^2 + \{ \}z^2 + \{ \}c^2d + \{ \}c^2f + \{ \}c^2g + \{ \}c^2h + \{ \}c^2i + \{ \}c^2j + \{ \}c^2k + \{ \}c^2l + \{ \}c^2s + \{ \}c^2t + \{ \}c^2u + \{ \}c^2v + \{ \}c^2w + \{ \}c^2z + \{ \}df + \{ \}dg + \{ \}dh + \{ \}di + \{ \}dj + \{ \}dk + \{ \}dl + \{ \}ds + \{ \}dt + \{ \}du + \{ \}dv + \{ \}dw + \{ \}dz + \{ \}fg + \{ \}fh + \{ \}fi + \{ \}fj + \{ \}fk + \{ \}fl + \{ \}fs + \{ \}ft + \{ \}fu + \{ \}fv + \{ \}fw + \{ \}fz + \{ \}gh + \{ \}gi + \{ \}gj + \{ \}gk + \{ \}gl + \{ \}gs + \{ \}gt + \{ \}gu + \{ \}gv + \{ \}gw + \{ \}gz + \{ \}hi + \{ \}hj + \{ \}hk + \{ \}hl + \{ \}hs + \{ \}ht + \{ \}hu + \{ \}hv + \{ \}hw + \{ \}hz + \{ \}ij + \{ \}ik + \{ \}il + \{ \}is + \{ \}it + \{ \}iu + \{ \}iv + \{ \}iw + \{ \}iz + \{ \}jk + \{ \}jl + \{ \}js + \{ \}jt + \{ \}ju + \{ \}jv + \{ \}jw + \{ \}jz + \{ \}kl + \{ \}ks + \{ \}kt + \{ \}ku + \{ \}kv + \{ \}kw + \{ \}kz + \{ \}ls + \{ \}lt + \{ \}lu + \{ \}lv + \{ \}lw + \{ \}lz + \{ \}st + \{ \}su + \{ \}sv + \{ \}sw + \{ \}sz + \{ \}tu + \{ \}tv + \{ \}tw + \{ \}tz + \{ \}uv + \{ \}uz + \{ \}vw + \{ \}vz + \{ \}wz$ were treated in elliptic curve $E_{-pq}: y^2 = x^3 - pqx$ that derives rank 2. In [7] and [8] and [9] similar primes were also considered. Furthermore, in [10] more complex forms of primes were regarded. The variables are A and B and C and D and E and F and G and H and I and J and K and L and O and P and Q and R and S and T and U and V and W and Z and resultantly compared with [6], [7], [8], [9] the numbers of variables and terms are changed from 15 into 22 and 120 into 253 respectively. Henceforth, in view of numbers of terms, the terms $R^2, S^2, T^2, U^2, V^2, W^2, Z^2$ and $14AR, 14AS, 14AT, 14AU, 14AV, 14AW, 14AZ$ and $2BR, 2BS, 2BT, 2BU, 2BV, 2BW, 2BZ$ and $2CR, 2CS, 2CT, 2CU, 2CV, 2CW, 2CZ$ and $2DR, 2DS, 2DT, 2DU, 2DV, 2DW, 2DZ$ and $2ER, 2ES, 2ET, 2EU, 2EV, 2EW, 2EZ$ and $2FR, 2FS, 2FT, 2FU, 2FV, 2FW, 2FZ$ and $2GR, 2GS, 2GT, 2GU, 2GV, 2GW, 2GZ$ and $2HR, 2HS, 2HT, 2HU, 2HV, 2HW, 2HZ$ and $2IR, 2IS, 2IT, 2IU, 2IV, 2IW, 2IZ$ and $2JR, 2JS, 2JT, 2JU, 2JV, 2JW, 2JZ$ and $2KR, 2KS, 2KT, 2KU, 2KV, 2KW, 2KZ$ and $2LR, 2LS, 2LT, 2LU, 2LV, 2LW, 2LZ$ and $2OR, 2OS, 2OT, 2OU, 2OV, 2OW, 2OZ$ and $2PR, 2PS, 2PT, 2PU, 2PV, 2PW, 2PZ$ are added as new ones. Moreover, the terms $2QR, 2QS, 2QT, 2QU, 2QV, 2QW, 2QZ$ and $2RS, 2RT, 2RU, 2RV, 2RW, 2RZ$ and $2ST, 2SU, 2SV, 2SW, 2SZ$ and $2TU, 2TV, 2TW, 2TZ$ and $2UV, 2UW, 2UZ$ and $2VW, 2VZ$ and $2WZ$ are added as new ones. It is clear that we pursue more complex primis p and q . It is matched to progression in systematization of rank in elliptic curve $y^2 = x^3 + Apx$. Namely, as we obtaining distinct primes p

and q with more terms and more variables it contributes abstraction of rank in $y^2 = x^3 - pqx$. Our treatment is done under the hypothesis that resultant is gotten as a square form. Thus, the primes are also induced closely correlated to square forms. The form of prime as $p = 163t^4 - 4t^3u - 8tu^3 + 8t^2u^2 + 4u^4 \dots \dots \left(\frac{H}{f} \right)$ is educed in $E_{-2p}: y^2 = x^3 - 2px$. Outwardly, this form is little involved to square. And in curve $y^2 = x^3 - pqx$ with rank 2 it is not simple to take primes p and q as $\left(\frac{H}{f} \right)$ since there are two relating equations 3) $N^2 = pM^4 - qe^4$ for Γ and 5) $N^2 = 2pM^4 + 2qe^4$ for $\bar{\Gamma}$ which are necessary to search the solutions([2], [4]). In detail, in E_{-2p} it only needs to take into account prime p related to term $-2M^4$ whereas in E_{-pq} it requires to regard two primes p and q . We also needed to note about case of $M = t + u$. That is, if this holds then, M^4 is gotten as $t^4 + 4t^3u + 4tu^3 + 6t^2u^2 + u^4$, hence if primes p and q should be involved to this value then, finding the solutions of relating equations became complex. Thus, it is usual that the integer M is gotten as one variable with $e = 1$ then, searching the primes is done readily. Therefore, considering distinct odd primes p and q is done under the assumption that $M = e = 1$ became main tendency. But there is left probability that M can be monomial or polynomial. Now our investigation is an extension of [10]. We add more variables to existing things for attaining rank 2 in E_{-pq} . We choose X and Y as new variables. From these two things, more terms will be appeared in non-square parts in distinct primes. We appoint that primes p and q are the forms $p \equiv 3(\text{mod } 16)$ and $q \equiv 15(\text{mod } 16)$ or $p \equiv 11(\text{mod } 16)$ and $q \equiv 7(\text{mod } 16)$. Due to [2] and [4], it is enough that we regard solutions of two relating equations 3) $N^2 = pM^4 - qe^4$ for Γ and 5) $N^2 = 2pM^4 + 2qe^4$ for $\bar{\Gamma}$. In this paper, we approach to rank of elliptic curve $y^2 = x^3 - pqx$ where primes p and q are composed of more numbers of variables and terms than [10]. Now $r4.4$ is in [4] and $w.i.A.B.C.D.E.F.G.H.I.J.K.L.O.P.Q.R.S.T.U.V.W.X.Y.Z.1$ denotes that with integers A and B and C and D and E and F and G and H and I and J and K and L and O and P and Q and R and S and T and U and V and W and X and Y and Z and $(A, B, C, D, E, F, G, H, I, J, K, L, O, P, Q, R, S, T, U, V, W, X, Y, Z) = 1$.

2 Decision of Primes

As in previous section, we access to primes p and q with more numbers of terms than [10]. Two variables X and Y will be added. Now we consider the primes.

Theorem 2.1. Let distinct primes p and q be the forms $p = 11A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + O^2 + P^2 + Q^2 + R^2 + S^2 + T^2 + U^2 + V^2 + W^2 + X^2 + Y^2 + Z^2 + 6AB + 6AC + 6AD + 6AE + 6AF + 6AG + 6AH + 6AI + 6AJ + 6AK + 6AL + 6AO + 6AP + 6AQ + 6AR + 6AS + 6AT + 6AU + 6AV + 6AW + 6AX + 6AY + 6AZ + 2BC + 2BD + 2BE + 2BF + 2B$

$$\begin{aligned}
& \cdot G + 2BH + 2BI + 2BJ + 2BK + 2BL + 2BO + 2BP + 2BQ + 2BR + 2BS + 2 \\
& \cdot BT + 2BU + 2BV + 2BW + 2BX + 2BY + 2BZ + 2CD + 2CE + 2CF + 2CG \\
& + 2CH + 2CI + 2CJ + 2CK + 2CL + 2CO + 2CP + 2CQ + 2CR + 2CS + 2CT + \\
& 2CU + 2CV + 2CW + 2CX + 2CY + 2CZ + 2DE + 2DF + 2DG + 2DH + 2DI \\
& + 2DJ + 2DK + 2DL + 2DO + 2DP + 2DQ + 2DR + 2DS + 2DT + 2DU + 2D \\
& \cdot V + 2DW + 2DX + 2DY + 2DZ + 2EF + 2EG + 2EH + 2EI + 2EJ + 2EK + \\
& 2EL + 2EO + 2EP + 2EQ + 2ER + 2ES + 2ET + 2EU + 2EV + 2EW + 2EX \\
& + 2EY + 2EZ + 2FG + 2FH + 2FI + 2FJ + 2FK + 2FL + 2FO + 2FP + 2FQ \\
& + 2FR + 2FS + 2FT + 2FU + 2FV + 2FW + 2FX + 2FY + 2FZ + 2GH + 2GI \\
& + 2GJ + 2GK + 2GL + 2GO + 2GP + 2GQ + 2GR + 2GS + 2GT + 2GU + 2GV \\
& + 2GW + 2GX + 2GY + 2GZ + 2HI + 2HJ + 2HK + 2HL + 2HO + 2HP + 2H \\
& \cdot Q + 2HR + 2HS + 2HT + 2HU + 2HV + 2HW + 2HX + 2HY + 2HZ + 2IJ + \\
& 2IK + 2IL + 2IO + 2IP + 2IQ + 2IR + 2IS + 2IT + 2IU + 2IV + 2IW + 2IX \\
& + 2IY + 2IZ + 2JK + 2JL + 2JO + 2JP + 2JQ + 2JR + 2JS + 2JT + 2JU + 2JV \\
& + 2JW + 2JX + 2JY + 2JZ + 2KL + 2KO + 2KP + 2KQ + 2KR + 2KS + 2KT \\
& + 2KU + 2KV + 2KW + 2KX + 2KY + 2KZ + 2LO + 2LP + 2LQ + 2LR + 2L \\
& \cdot S + 2LT + 2LU + 2LV + 2LW + 2LX + 2LY + 2LZ + 2OP + 2OQ + 2OR + 2 \\
& \cdot OS + 2OT + 2OU + 2OV + 2OW + 2OX + 2OY + 2OZ + 2PQ + 2PR + 2PS \\
& + 2PT + 2PU + 2PV + 2PW + 2PX + 2PY + 2PZ + 2QR + 2QS + 2QT + 2Q \\
& \cdot U + 2QV + 2QW + 2QX + 2QY + 2QZ + 2RS + 2RT + 2RU + 2RV + 2RW \\
& + 2RX + 2RY + 2RZ + 2ST + 2SU + 2SV + 2SW + 2SX + 2SY + 2SZ + 2TU \\
& + 2TV + 2TW + 2TX + 2TY + 2TZ + 2UV + 2UW + 2UX + 2UY + 2UZ + 2V \\
& \cdot W + 2VX + 2VY + 2VZ + 2WX + 2WY + 2WZ + 2XY + 2XZ + 2YZ \text{ and } q = \\
& 7A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + O^2 + P^2 + \\
& Q^2 + R^2 + S^2 + T^2 + U^2 + V^2 + W^2 + X^2 + Y^2 + Z^2 + 6AB + 6AC + 6AD + \\
& 6AE + 6AF + 6AG + 6AH + 6AI + 6AJ + 6AK + 6AL + 6AO + 6AP + 6AQ + \\
& 6AR + 6AS + 6AT + 6AU + 6AV + 6AW + 6AX + 6AY + 6AZ + 2BC + 2BD \\
& + 2BE + 2BF + 2BG + 2BH + 2BI + 2BJ + 2BK + 2BL + 2BO + 2BP + 2BQ \\
& + 2BR + 2BS + 2BT + 2BU + 2BV + 2BW + 2BX + 2BY + 2BZ + 2CD + 2C \\
& \cdot E + 2CF + 2CG + 2CH + 2CI + 2CJ + 2CK + 2CL + 2CO + 2CP + 2CQ + 2 \\
& \cdot CR + 2CS + 2CT + 2CU + 2CV + 2CW + 2CX + 2CY + 2CZ + 2DE + 2DF + \\
& 2DG + 2DH + 2DI + 2DJ + 2DK + 2DL + 2DO + 2DP + 2DQ + 2DR + 2DS \\
& + 2DT + 2DU + 2DV + 2DW + 2DX + 2DY + 2DZ + 2EF + 2EG + 2EH + 2 \\
& \cdot EI + 2EJ + 2EK + 2EL + 2EO + 2EP + 2EQ + 2ER + 2ES + 2ET + 2EU + \\
& 2EV + 2EW + 2EX + 2EY + 2EZ + 2FG + 2FH + 2FI + 2FJ + 2FK + 2FL + \\
& 2FO + 2FP + 2FQ + 2FR + 2FS + 2FT + 2FU + 2FV + 2FW + 2FX + 2FY \\
& + 2FZ + 2GH + 2GI + 2GJ + 2GK + 2GL + 2GO + 2GP + 2GQ + 2GR + 2GS \\
& + 2GT + 2GU + 2GV + 2GW + 2GX + 2GY + 2GZ + 2HI + 2HJ + 2HK + 2HL \\
& + 2HO + 2HP + 2HQ + 2HR + 2HS + 2HT + 2HU + 2HV + 2HW + 2HX + 2 \\
& \cdot HY + 2HZ + 2IJ + 2IK + 2IL + 2IO + 2IP + 2IQ + 2IR + 2IS + 2IT + 2IU \\
& + 2IV + 2IW + 2IX + 2IY + 2IZ + 2JK + 2JL + 2JO + 2JP + 2JQ + 2JR + 2J \\
& \cdot S + 2JT + 2JU + 2JV + 2JW + 2JX + 2JY + 2JZ + 2KL + 2KO + 2KP + 2K \\
& \cdot Q + 2KR + 2KS + 2KT + 2KU + 2KV + 2KW + 2KX + 2KY + 2KZ + 2LO \\
& + 2LP + 2LQ + 2LR + 2LS + 2LT + 2LU + 2LV + 2LW + 2LX + 2LY + 2LZ +
\end{aligned}$$

+2OP + 2OQ + 2OR + 2OS + 2OT + 2OU + 2OV + 2OW + 2OX + 2OY + 2O
 · Z + 2PQ + 2PR + 2PS + 2PT + 2PU + 2PV + 2PW + 2PX + 2PY + 2PZ +
 2QR + 2QS + 2QT + 2QU + 2QV + 2QW + 2QX + 2QY + 2QZ + 2RS + 2RT
 +2RU + 2RV + 2RW + 2RX + 2RY + 2RZ + 2ST + 2SU + 2SV + 2SW + 2S
 · X + 2SY + 2SZ + 2TU + 2TV + 2TW + 2TX + 2TY + 2TZ + 2UV + 2UW +
 2UX + 2UY + 2UZ + 2VW + 2VX + 2VY + 2VZ + 2WX + 2WY + 2WZ + 2X
 · Y + 2XZ + 2YZ w.i. A. B. C. D. E. F. G. H. I. J. K. L. O. P. Q. R. S. T. U. V. W. X. Y.
 · Z. 1 and $p \equiv 11(\text{mod } 16)$ and $q \equiv 7(\text{mod } 16)$ in $E_{-pq} : y^2 = x^3 - pqx$ then,
 the consequence

$$\text{rank}(E_{-(11A^2+\dots+Z^2+6AB+\dots+6AZ+2BC+\dots+2YZ)}(7A^2+\dots+Z^2+6AB+\dots+6AZ+2BC+\dots+2YZ))(Q)) \\ = 2.$$

is given.

Proof. Equation 3) for Γ is $N^2 = (11A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + O^2 + P^2 + Q^2 + R^2 + S^2 + T^2 + U^2 + V^2 + W^2 + X^2 + Y^2 + Z^2 + 6AB + 6AC + 6AD + 6AE + 6AF + 6AG + 6AH + 6AI + 6AJ + 6A \cdot K + 6AL + 6AO + 6AP + 6AQ + 6AR + 6AS + 6AT + 6AU + 6AV + 6AW + 6AX + 6AY + 6AZ + 2BC + 2BD + 2BE + 2BF + 2BG + 2BH + 2BI + 2BJ + 2BK + 2BL + 2BO + 2BP + 2BQ + 2BR + 2BS + 2BT + 2BU + 2BV + 2BW + 2BX + 2BY + 2BZ + 2CD + 2CE + 2CF + 2CG + 2CH + 2CI + 2CJ + 2CK + 2CL + 2CO + 2CP + 2CQ + 2CR + 2CS + 2CT + 2CU + 2CV + 2CW + 2CX + 2CY + 2CZ + 2DE + 2DF + 2DG + 2DH + 2DI + 2DJ + 2DK + 2DL + 2DO + 2DP + 2DQ + 2DR + 2DS + 2DT + 2DU + 2DV + 2DW + 2DX + 2DY + 2 \cdot DZ + 2EF + 2EG + 2EH + 2EI + 2EJ + 2EK + 2EL + 2EO + 2EP + 2EQ + 2ER + 2ES + 2ET + 2EU + 2EV + 2EW + 2EX + 2EY + 2EZ + 2FG + 2FH + 2FI + 2FJ + 2FK + 2FL + 2FO + 2FP + 2FQ + 2FR + 2FS + 2FT + 2FU + 2FV + 2FW + 2FX + 2FY + 2FZ + 2GH + 2GI + 2GJ + 2GK + 2GL + 2GO + 2GP + 2GQ + 2GR + 2GS + 2GT + 2GU + 2GV + 2GW + 2GX + 2GY + 2G \cdot Z + 2HI + 2HJ + 2HK + 2HL + 2HO + 2HP + 2HQ + 2HR + 2HS + 2HT + 2HU + 2HV + 2HW + 2HX + 2HY + 2HZ + 2IJ + 2IK + 2IL + 2IO + 2IP + 2IQ + 2IR + 2IS + 2IT + 2IU + 2IV + 2IW + 2IX + 2IY + 2IZ + 2JK + 2JL + 2JO + 2JP + 2JQ + 2JR + 2JS + 2JT + 2JU + 2JV + 2JW + 2JX + 2JY + 2J \cdot Z + 2KL + 2KO + 2KP + 2KQ + 2KR + 2KS + 2KT + 2KU + 2KV + 2KW + 2KX + 2KY + 2KZ + 2LO + 2LP + 2LQ + 2LR + 2LS + 2LT + 2LU + 2LV + 2LW + 2LX + 2LY + 2LZ + 2OP + 2OQ + 2OR + 2OS + 2OT + 2OU + 2OV + 2OW + 2OX + 2OY + 2OZ + 2PQ + 2PR + 2PS + 2PT + 2PU + 2PV + 2P \cdot W + 2PX + 2PY + 2PZ + 2QR + 2QS + 2QT + 2QU + 2QV + 2QW + 2QX + 2QY + 2QZ + 2RS + 2RT + 2RU + 2RV + 2RW + 2RX + 2RY + 2RZ + 2ST + 2SU + 2SV + 2SW + 2SX + 2SY + 2SZ + 2TU + 2TV + 2TW + 2TX + 2TY + 2TZ + 2UV + 2UW + 2UX + 2UY + 2UZ + 2VW + 2VX + 2VY + 2VZ + 2 \cdot WX + 2WY + 2WZ + 2XY + 2XZ + 2YZ)M^4 - (7A^2 + B^2 + C^2 + D^2 + E^2 +$

$F^2 + G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + O^2 + P^2 + Q^2 + R^2 + S^2 + T^2 + U^2 + V^2$
 $+W^2 + X^2 + Y^2 + Z^2 + 6AB + 6AC + 6AD + 6AE + 6AF + 6AG + 6AH + 6A$
 $\cdot I + 6AJ + 6AK + 6AL + 6AO + 6AP + 6AQ + 6AR + 6AS + 6AT + 6AU + 6$
 $\cdot AV + 6AW + 6AX + 6AY + 6AZ + 2BC + 2BD + 2BE + 2BF + 2BG + 2BH$
 $+2BI + 2BJ + 2BK + 2BL + 2BO + 2BP + 2BQ + 2BR + 2BS + 2BT + 2BU$
 $+2BV + 2BW + 2BX + 2BY + 2BZ + 2CD + 2CE + 2CF + 2CG + 2CH + 2CI$
 $+2CJ + 2CK + 2CL + 2CO + 2CP + 2CQ + 2CR + 2CS + 2CT + 2CU + 2CV$
 $+2CW + 2CX + 2CY + 2CZ + 2DE + 2DF + 2DG + 2DH + 2DI + 2DJ + 2D$
 $\cdot K + 2DL + 2DO + 2DP + 2DQ + 2DR + 2DS + 2DT + 2DU + 2DV + 2DW$
 $+2DX + 2DY + 2DZ + 2EF + 2EG + 2EH + 2EI + 2EJ + 2EK + 2EL + 2EO$
 $+2EP + 2EQ + 2ER + 2ES + 2ET + 2EU + 2EV + 2EW + 2EX + 2EY + 2E$
 $\cdot Z + 2FG + 2FH + 2FI + 2FJ + 2FK + 2FL + 2FO + 2FP + 2FQ + 2FR + 2$
 $\cdot FS + 2FT + 2FU + 2FV + 2FW + 2FX + 2FY + 2FZ + 2GH + 2GI + 2GJ +$
 $2GK + 2GL + 2GO + 2GP + 2GQ + 2GR + 2GS + 2GT + 2GU + 2GV + 2GW$
 $+2GX + 2GY + 2GZ + 2HI + 2HJ + 2HK + 2HL + 2HO + 2HP + 2HQ + 2H$
 $\cdot R + 2HS + 2HT + 2HU + 2HV + 2HW + 2HX + 2HY + 2HZ + 2IJ + 2IK +$
 $2IL + 2IO + 2IP + 2IQ + 2IR + 2IS + 2IT + 2IU + 2IV + 2IW + 2IX + 2IY$
 $+2IZ + 2JK + 2JL + 2JO + 2JP + 2JQ + 2JR + 2JS + 2JT + 2JU + 2JV + 2J$
 $\cdot W + 2JX + 2JY + 2JZ + 2KL + 2KO + 2KP + 2KQ + 2KR + 2KS + 2KT + 2$
 $\cdot KU + 2KV + 2KW + 2KX + 2KY + 2KZ + 2LO + 2LP + 2LQ + 2LR + 2LS$
 $+2LT + 2LU + 2LV + 2LW + 2LX + 2LY + 2LZ + 2OP + 2OQ + 2OR + 2OS$
 $+2OT + 2OU + 2OV + 2OW + 2OX + 2OY + 2OZ + 2PQ + 2PR + 2PS + 2P$
 $\cdot T + 2PU + 2PV + 2PW + 2PX + 2PY + 2PZ + 2QR + 2QS + 2QT + 2QU +$
 $2QV + 2QW + 2QX + 2QY + 2QZ + 2RS + 2RT + 2RU + 2RV + 2RW + 2RX$
 $+2RY + 2RZ + 2ST + 2SU + 2SV + 2SW + 2SX + 2SY + 2SZ + 2TU + 2TV$
 $+2TW + 2TX + 2TY + 2TZ + 2UV + 2UW + 2UX + 2UY + 2UZ + 2VW + 2$
 $\cdot VX + 2VY + 2VZ + 2WX + 2WY + 2WZ + 2XY + 2XZ + 2YZ)e^4$. Now we
 have the triple $(1, 1, 2A)$ as the solution of this equation, thus we have that
 $\#\alpha(\Gamma) = 4$. Next, equation 5) for $\bar{\Gamma}$ is $N^2 = 2(11A^2 + B^2 + C^2 + D^2 + E^2 + F^2$
 $+G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + O^2 + P^2 + Q^2 + R^2 + S^2 + T^2 + U^2 + V^2 +$
 $W^2 + X^2 + Y^2 + Z^2 + 6AB + 6AC + 6AD + 6AE + 6AF + 6AG + 6AH + 6AI$
 $+6AJ + 6AK + 6AL + 6AO + 6AP + 6AQ + 6AR + 6AS + 6AT + 6AU + 6AV$
 $+6AW + 6AX + 6AY + 6AZ + 2BC + 2BD + 2BE + 2BF + 2BG + 2BH + 2B$
 $\cdot I + 2BJ + 2BK + 2BL + 2BO + 2BP + 2BQ + 2BR + 2BS + 2BT + 2BU + 2$
 $\cdot BV + 2BW + 2BX + 2BY + 2BZ + 2CD + 2CE + 2CF + 2CG + 2CH + 2CI$
 $+2CJ + 2CK + 2CL + 2CO + 2CP + 2CQ + 2CR + 2CS + 2CT + 2CU + 2CV$
 $+2CW + 2CX + 2CY + 2CZ + 2DE + 2DF + 2DG + 2DH + 2DI + 2DJ + 2D$
 $\cdot K + 2DL + 2DO + 2DP + 2DQ + 2DR + 2DS + 2DT + 2DU + 2DV + 2DW$
 $+2DX + 2DY + 2DZ + 2EF + 2EG + 2EH + 2EI + 2EJ + 2EK + 2EL + 2EO$
 $+2EP + 2EQ + 2ER + 2ES + 2ET + 2EU + 2EV + 2EW + 2EX + 2EY + 2E$
 $\cdot Z + 2FG + 2FH + 2FI + 2FJ + 2FK + 2FL + 2FO + 2FP + 2FQ + 2FR + 2$
 $\cdot FS + 2FT + 2FU + 2FV + 2FW + 2FX + 2FY + 2FZ + 2GH + 2GI + 2GJ +$
 $2GK + 2GL + 2GO + 2GP + 2GQ + 2GR + 2GS + 2GT + 2GU + 2GV + 2GW$
 $+2GX + 2GY + 2GZ + 2HI + 2HJ + 2HK + 2HL + 2HO + 2HP + 2HQ + 2H$

$\cdot R + 2HS + 2HT + 2HU + 2HV + 2HW + 2HX + 2HY + 2HZ + 2IJ + 2IK + 2IL + 2IO + 2IP + 2IQ + 2IR + 2IS + 2IT + 2IU + 2IV + 2IW + 2IX + 2IY + 2IZ + 2JK + 2JL + 2JO + 2JP + 2JQ + 2JR + 2JS + 2JT + 2JU + 2JV + 2JW + 2JX + 2JY + 2JZ + 2KL + 2KO + 2KP + 2KQ + 2KR + 2KS + 2KT + 2KU + 2KV + 2KW + 2KX + 2KY + 2KZ + 2LO + 2LP + 2LQ + 2LR + 2LS + 2LT + 2LU + 2LV + 2LW + 2LX + 2LY + 2LZ + 2OP + 2OQ + 2OR + 2OS + 2OT + 2OU + 2OV + 2OW + 2OX + 2OY + 2OZ + 2PQ + 2PR + 2PS + 2PT + 2PU + 2PV + 2PW + 2PX + 2PY + 2PZ + 2QR + 2QS + 2QT + 2QU + 2QV + 2QW + 2QX + 2QY + 2QZ + 2RS + 2RT + 2RU + 2RV + 2RW + 2RX + 2RY + 2RZ + 2ST + 2SU + 2SV + 2SW + 2SX + 2SY + 2SZ + 2TU + 2TV + 2TW + 2TX + 2TY + 2TZ + 2UV + 2UW + 2UX + 2UY + 2UZ + 2VW + 2VX + 2VY + 2VZ + 2WX + 2WY + 2WZ + 2XY + 2XZ + 2YZ)M^4 + 2(7A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + O^2 + P^2 + Q^2 + R^2 + S^2 + T^2 + U^2 + V^2 + W^2 + X^2 + Y^2 + Z^2 + 6AB + 6AC + 6AD + 6AE + 6AF + 6AG + 6AH + 6AI + 6AJ + 6AK + 6AL + 6AO + 6AP + 6AQ + 6AR + 6AS + 6AT + 6AU + 6AV + 6AW + 6AX + 6AY + 6AZ + 2BC + 2BD + 2BE + 2BF + 2BG + 2BH + 2BI + 2BJ + 2BK + 2BL + 2BO + 2BP + 2BQ + 2BR + 2BS + 2BT + 2BU + 2BV + 2BW + 2BX + 2BY + 2BZ + 2CD + 2CE + 2CF + 2CG + 2CH + 2CI + 2CJ + 2CK + 2CL + 2CO + 2CP + 2CQ + 2CR + 2CS + 2CT + 2CU + 2CV + 2CW + 2CX + 2CY + 2CZ + 2DE + 2DF + 2DG + 2DH + 2DI + 2DJ + 2DK + 2DL + 2DO + 2DP + 2DQ + 2DR + 2DS + 2DT + 2DU + 2DV + 2DW + 2DX + 2DY + 2DZ + 2EF + 2EG + 2EH + 2EI + 2EJ + 2EK + 2EL + 2EO + 2EP + 2EQ + 2ER + 2ES + 2ET + 2EU + 2EV + 2EW + 2EX + 2EY + 2EZ + 2FG + 2FH + 2FI + 2FJ + 2FK + 2FL + 2FO + 2FP + 2FQ + 2FR + 2FS + 2FT + 2FU + 2FV + 2FW + 2FX + 2FY + 2FZ + 2GH + 2GI + 2GJ + 2GK + 2GL + 2GO + 2GP + 2GQ + 2GR + 2GS + 2GT + 2GU + 2GV + 2GW + 2GX + 2GY + 2GZ + 2HI + 2HJ + 2HK + 2HL + 2HO + 2HP + 2HQ + 2HR + 2HS + 2HT + 2HU + 2HV + 2HW + 2HX + 2HY + 2HZ + 2IJ + 2IK + 2IL + 2IO + 2IP + 2IQ + 2IR + 2IS + 2IT + 2IU + 2IV + 2IW + 2IX + 2IY + 2IZ + 2JK + 2JL + 2JO + 2JP + 2JQ + 2JR + 2JS + 2JT + 2JU + 2JV + 2JW + 2JX + 2JY + 2JZ + 2KL + 2KO + 2KP + 2KQ + 2KR + 2KS + 2KT + 2KU + 2KV + 2KW + 2KX + 2KY + 2KZ + 2LO + 2LP + 2LQ + 2LR + 2LS + 2LT + 2LU + 2LV + 2LW + 2LX + 2LY + 2LZ + 2OP + 2OQ + 2OR + 2OS + 2OT + 2OU + 2OV + 2OW + 2OX + 2OY + 2OZ + 2PQ + 2PR + 2PS + 2PT + 2PU + 2PV + 2PW + 2PX + 2PY + 2PZ + 2QR + 2QS + 2QT + 2QU + 2QV + 2QW + 2QX + 2QY + 2QZ + 2RS + 2RT + 2RU + 2RV + 2RW + 2RX + 2RY + 2RZ + 2ST + 2SU + 2SV + 2SW + 2SX + 2SY + 2SZ + 2TU + 2TV + 2TW + 2TX + 2TY + 2TZ + 2UV + 2UW + 2UX + 2UY + 2UZ + 2VW + 2VX + 2VY + 2VZ + 2WX + 2WY + 2WZ + 2XY + 2XZ + 2YZ)e^4. The terms $22A^2$ and $14A^2$ exists in coefficients of M^4 and e^4 . Therefore, we can regard the square $36A^2$. There are square terms from $2B^2$ to $2Z^2$. Thus, it is possible to consider squares $4B^2$ and $4C^2$ and $4D^2$ and $4E^2$ and $4F^2$ and $4G^2$ and $4H^2$ and $4I^2$ and $4J^2$ and $4K^2$ and $4L^2$ and $4O^2$ and $4P^2$ and $4Q^2$ and $4R^2$ and $4S^2$ and $4T^2$ and $4U^2$ and $4V^2$ and $4W^2$ and $4X^2$ and $4Y^2$ and$

$4Z^2$. Next, there are common terms $12AB, 12AC, 12AD, 12AE, 12AF, 12AG, 12AH, 12AI, 12AJ, 12AK, 12AL, 12AO, 12AP, 12AQ, 12AR, 12AS, 12AT, 12AU, 12AV, 12AW, 12AX, 12AY, 12AZ$ in coefficients of M^4 and e^4 . Accordingly, we can anticipate appearance of terms $24AB, 24AC, 24AD, 24AE, 24AF, 24AG, 24AH, 24AI, 24AJ, 24AK, 24AL, 24AO, 24AP, 24AQ, 24AR, 24AS, 24AT, 24AU, 24AV, 24AW, 24AX, 24AY, 24AZ$. In both coefficients of M^4 and e^4 remaining terms are from $4BC$ to $4YZ$. Now in determining the components of integer N we can treat first one as $6A$ because of square $36A^2$. And others are $2B$ and $2C$ and $2D$ and $2E$ and $2F$ and $2G$ and $2H$ and $2I$ and $2J$ and $2K$ and $2L$ and $2O$ and $2P$ and $2Q$ and $2R$ and $2S$ and $2T$ and $2U$ and $2V$ and $2W$ and $2X$ and $2Y$ and $2Z$. Then, squares from $4B^2$ to $4Z^2$ can be derived and moreover by multiplication from $2B$ to $2Z$ in each pair left terms can be induced. And under the assumption of $M = e = 1$ this treatment can be given. Consequently, we got the solution of equation as $(1, 1, 6A + 2B + 2C + 2D + 2E + 2F + 2G + 2H + 2I + 2J + 2K + 2L + 2O + 2P + 2Q + 2R + 2S + 2T + 2U + 2V + 2W + 2X + 2Y + 2Z)$. On that account, we attain the conclusion $\#\bar{\alpha}(\bar{\Gamma}) = 4$. And it gives that $r4.4$. Consequently, the proof became completed. \square

We attained primes p and q where numbers of variables and terms are 24 and 300 respectively. The coefficients of A^2 are 11 and 7 respectively. And that of AB and AC and AD and AE and AF and AG and AH and AI and AJ and AK and AL and AO and AP and AQ and AR and AS and AT and AU and AV and AW and AX and AY and AZ are all 6. And there are common terms from $2BC$ to $2YZ$. But the crucial terms that decides the forms of primes are from $6AB$ to $6AZ$. Due to coefficients 6 in these terms the integer N of solution of equation for $\bar{\Gamma}$ is given as $6A + 2B + 2C + 2D + 2E + 2F + 2G + 2H + 2I + 2J + 2K + 2L + 2O + 2P + 2Q + 2R + 2S + 2T + 2U + 2V + 2W + 2X + 2Y + 2Z$ where the coefficient of resultant from AB to AZ are 24. Compared with the consequences in [6] and [7] and [8] and [9] the numbers of variables and terms are increased. In those the degree of first term was 4 and other variables' degree was 2. Meanwhile in above, degrees of squares are 2. Thus, non-square part's degree is 1 for each variable. Namely, there is no term of degree 2. It is different from the results in [6] and [7] and [8] and [9]. Furthermore, compared with [10], there increased numbers of variables from 22 to 24 and thus that of terms are changed from 253 to 300. Now the numbers 24 and 300 are not a maximal value of numbers in variables and terms. In [6] the forms of primes were derived from breaking precedent forms of primes. Namely, in [5], the degree of variable in square part is 4 and that of non-square part is 2(in each variable). Whereas in [6], the degree of square of first component 4 but others are 2. And it induces new forms $2c^2d$ and $2c^2f$ and $2c^2g$ and $2c^2h$ and $2c^2i$ and $2c^2j$ and $2c^2k$ and $2c^2l$ and $2c^2s$ and $2c^2t$ and $2c^2u$ and $2c^2v$ and $2c^2w$ and $2c^2z$ and at last it were involved to appearance of terms from $2df$ to $2wz$. Non-square terms from $2c^2d$ to $2c^2z$ and $2df$ to $2wz$ are different from $20u^2v^2$ and $20u^2w^2$ and $8v^2w^2$ (It is similar in [7] and [8] and

[9] S. W. Kim, Forms of primes in elliptic curve $y^2 = x^3 - pqx$, *Int. J. of Algebra*, **18** (2024), 155-166. <https://doi.org/10.12988/ija.2024.91917>

[10] S. W. Kim, Consequence of rank in curve $y^2 = x^3 - pqx$, *Int. J. of Algebra*, **20** (2026), 81-87. <https://doi.org/10.12988/ija.2026.92009>

[11] S. W. Kim, Elliptic curve $y^2 = x^3 + pqx$ with distinct odd primes, *Int. J. of Algebra*, **20** (2026), 71-80. <https://doi.org/10.12988/ija.2026.92008>

Received: March 5, 2026; Published: April 7, 2026