Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 20, 2014, No. 5, 1–10

A note on the Diophantine equations $x_1^k + x_2^k + x_3^k + x_4^k = 2y_1^k + 2y_2^k, k = 3, 6$

Farzali Izadi[1], **Foad Khoshnam**[2] **and Arman Shamsi Zargar**[3]

[1] Department of Pure Mathematics, Azarbaijan Shahid Madani University
Tabriz 53751-71379, Iran
e-mail: farzali.izadi@azaruniv.edu

[2] Department of Pure Mathematics, Azarbaijan Shahid Madani University
Tabriz 53751-71379, Iran
e-mail: khoshnam@azaruniv.edu

[3] Department of Pure Mathematics, Azarbaijan Shahid Madani University
Tabriz 53751-71379, Iran
e-mail: shzargar.arman@azaruniv.edu

Abstract: It is shown that infinitely many primitive solutions on the Diophantine equations of the title can be found on employing the theory of elliptic curves, which makes it possible to naturally find larger solutions in a matter of minutes.
Keywords: Diophantine equation, Elliptic curve.
AMS Classification: 11D25, 11G05.

1 Introduction

The study of primitive solutions to the Diophantine equations of the form

$$\sum_{i=1}^{m} x_i^k = \ell \sum_{j=1}^{n} y_j^k \tag{1}$$

has attracted interest since antiquity for various values of (m, n, k, ℓ). For example, for (m, n, k, ℓ) $= (3, 3, 6, 1)$ and $(2, 5, 6, 1)$, the solutions of the equation (1) have been known vastly in the literature. See, for example [1, 2, 3, 4, 5, 6, 7, 9, 10, 11].

In the following we discuss the method used to find new primitive solutions of the equation (1) with $(m, n, k, \ell) = (4, 2, 3, 2)$ and $(4, 2, 6, 2)$, i.e.,

$$x_1^3+x_2^3+x_3^3+x_4^3=2y_1^3+2y_2^3, \tag{2}$$

and

$$x_1^6+x_2^6+x_6^6+x_4^6=2y_1^6+2y_2^6, \tag{3}$$

which is based on the theory of elliptic curves, and leads to an infinite number of primitive solutions.

2 Method

Our method uses birational transformations to relate the equations (2) and (3) to positive rank elliptic curves. For our next results, recall that the shape of Weierstrass curve requires that an element P be representable in the form $P=(A/B^2, C/B^3)$, where A, B and C are integers, with B coprime to AC.

In the following theorem, we show an infinitude of primitive solutions to (2).

Theorem 2.1. *Given a and c so that the elliptic curve*

$$\mathcal{C}: y^2=x^3+27c^2(2c-a)^2x+27(2c-a)^3(a^3-2c^3),$$

with $x=3b(2c-a)$, $y=9d(2c-a)^2$ is of positive rank. Let $G=(A/B^2, C/B^3)$ be a rational point on the elliptic curve $\mathcal{C}$. Next let

$$\begin{aligned}
x_1 &= 36aB^3c^2-36a^2B^3c+9a^3B^3-C,\\
x_2 &= 36aB^3c^2-36a^2B^3c+9a^3B^3+C,\\
x_3 &= 6BAc-3BAa-36B^3c^3+36aB^3c^2-9a^2B^3c,\\
x_4 &= 6BAc-3BAa+36B^3c^3-36aB^3c^2+9a^2B^3c,\\
y_1 &= 36B^3c^3-36aB^3c^2+9a^2B^3c-C,\\
y_2 &= 36B^3c^3-36aB^3c^2+9a^2B^3c+C.
\end{aligned}$$

Then $(x_1, x_2, x_3, x_4, y_1, y_2)$ is an integral solution to (2).

Proof. Put

$$x_1=a-d, x_2=a+d, x_3=b-c, x_4=b+c, y_1=c-d, y_2=c+d. \tag{4}$$

Hence, the equation (2) boils down to

$$2a^3+6ad^2+2b^3+6bc^2-4c^3-12cd^2=0, \tag{5}$$

when substitution is made of (4) in (2). Arranging the equation (5) in terms of b, and letting

$$b=\frac{x}{3(2c-a)}, \quad d=\frac{y}{9(2c-a)^2}, \tag{6}$$

we see that (5) is transformed to the elliptic curve

$$y^2 = x^3 + 27c^2(2c-a)^2x + 27(2c-a)^3(a^3 - 2c^3).$$

Therefore, by substituting (6) in (4), and $x = A/B^2$, $y = C/B^3$ we get

$$\begin{aligned}
x_1 &= \frac{36aB^3c^2 - 36a^2B^3c + 9a^3B^3 - C}{9B^3(-2c+a)^2},\\
x_2 &= \frac{36aB^3c^2 - 36a^2B^3c + 9a^3B^3 + C}{9B^3(-2c+a)^2},\\
x_3 &= -\frac{A - 6c^2B^2 + 3cB^2a}{3B^2(-2c+a)},\\
x_4 &= -\frac{A + 6c^2B^2 - 3cB^2a}{3B^2(-2c+a)},\\
y_1 &= \frac{36c^3B^3 - 36aB^3c^2 + 9a^2B^3c - C}{9B^3(-2c+a)^2},\\
y_2 &= \frac{36c^3B^3 - 36aB^3c^2 + 9a^2B^3c + C}{9B^3(-2c+a)^2}.
\end{aligned}$$

Hence, choosing appropriate a's, c's, and using the fact that $(\kappa x_1, \ldots, \kappa y_2)$ is a solution to (2) if $(x_1, \ldots, y_2)$ is, we can eliminate the denominators. The result now follows immediately. □

Computations show that Theorem 2.1 yields primitive solutions for suitable choices of a's and c's. Specifically, for $a = 1$ and $c = 5$, the resulting curve $\mathcal{C}$ is of rank 1 with generator $G = (81, 243)$. In Table **??**, for this value of a and c, it is given the first 10 primitive solutions, i.e., integral solutions with

$$\gcd(x_1, x_2, x_3, x_4, y_1, y_2) = 1$$

satisfying (2), corresponding to the points ρG, $\rho = 1, \ldots, 10$, on $\mathcal{C}$.

In the following, we show an infinitude of primitive solutions to (3) with two different methods.

Proposition 2.2. *Suppose $G = (A/B^2, C/B^3)$ is a rational point on the elliptic curve*

$$\mathcal{E} : y^2 - 8xy - 560y = x^3 + 10x^2 - 4900x - 49000,$$

with $A, B, C \in \mathbb{Z}$. Let

$$\begin{aligned}
x_1 &= 7000B^6 + 1300AB^4 - 180CB^3 + 50A^2B^2 - 18CAB + C^2 - A^3,\\
x_2 &= (10B^2 + A)(700B^4 + 80AB^2 - 10CB + A^2),\\
x_3 &= 10B(10B^2 + A)(140B^3 + 14AB - C),\\
x_4 &= C(100B^3 + 10BA - C),\\
y_1 &= (10B^2 + A)(700B^4 + 80AB^2 - 6CB + A^2),\\
y_2 &= -7000B^6 - 1300AB^4 + 140CB^3 - 50A^2B^2 + 14CAB - C^2 + A^3.
\end{aligned}$$

Then $(x_1, x_2, x_3, x_4, y_1, y_2)$ is an integral solution to (3).

ρG	$x_1, x_2, x_3, x_4, y_1, y_2$
G	1, 2, −3, 12, 7, 8
$2G$	7295, −7292, 1284, 1299, 7301, −7286
$3G$	−1126126, 159033304, −139133709, 650402181, 314688230, 474847660
$4G$	2835217547309434, −2825906056829425, 978569831281182, 1025127283681227, 2853840528269452, −2807283075869407
$5G$	−162175506348931352367092, 599296824776285464492949, −278902809026435165444727, 1906703783110335395184558, 712067130505776871884622, 1473539461630993688744663
$6G$	58827136365626461611567859922793083, −5817841318647698193043961248214708 3, 29359841049443864300569207555465890, 326034569451912627062104447586958 90, 60124582723925420973824354804085083, −5688096682817802256818311760085 5083
$7G$	−49624850150894076309289205332613500326236700739, 11315545475870635029 8664379430113187674973613832, −164379043868396976681678915495928965572 16577263, 301215118652221672278707978937905540186467988202, 77436359064 730471669461142862385874371237125447, 24021666397433089827741472762511 2562372447440018
$8G$	65319272235063642923030738432883802794799620913226183763841705, −63629893141020164899119107696983792336151041821937880750757694, 41007644285639457434072383276718254050563755608154218187499238, 49454539755856847553630536956218306343806651064595733252919293, 68698030423150598970853999904683823712096779095802789790009727, −60251134952933208851295846225183771418853883639361274724589672
$9G$	−61553783807026097550674360015370879122224543446631497847911018643654 8318797684, 1099032223027316613817283911991397086567890194614919728737 709563507356212150126, 13488935243043501425119169270734725357268709343 0874185167614473045400451977299, 2552361277215713205803893251895788730 300910894173897936460611358399439918739509, 35145093184385030111433702 3521667799469044085830894522038088567705067467907200, 2066020992941427 890438364535666773677259179714912129229254908317648971998855010
$10G$	389058566163314129483766682685243013033797674642369251539796001902657 0534892838907963031333021952, −36975825237794883227202885196790539085 86230161267251563086547028075759838453979876932528198971655, 280210481 627420453328041793530249355951449887529751427704277776007880031933207 4207326719003787096, 3767120505542469393867309471169374668273231801079 719038599842714832853801526369362479234674038581, 42765919373404472390 724234411991825738414699167365744200207860009281919277705569700240376 01122546, −3311576248072182378485531905332301465082736990954369658463 721046174138445576261814871521930871061

Table 1: Some primitive solutions of (2)

Proof. By Section 6.2 of [13], the equation (3) with the variables defined as in (4), i.e.,

$$(a-d)^6 + (a+d)^6 + (b-c)^6 + (b+c)^6 = 2(c-d)^6 + 2(c-d)^6,$$

holds if

$$\begin{cases} 5a^2 + 2b^2 = 7c^2, \\ 2a^2 + 5b^2 = 7d^2. \end{cases} \tag{7}$$

Dividing both sides (7) by b^2 and letting $u = a/b$, $v = c/b$, and $w = d/b$, we get

$$\begin{cases} 7v^2 - 5u^2 = 2, \\ 7w^2 - 2u^2 = 5. \end{cases} \tag{8}$$

We see that this system has the rational point $(u, v, w) = (1, 1, 1)$ easily, hence it is an elliptic curve (see [14, Section 2.5.4]). We parameterize the solutions of the intersection. We let $u = 1+t$, and $v = 1 + mt$. We easily find $t = -2(7m-5)/(7m^2-5)$ which gives rise to

$$\begin{aligned} u &= \frac{7m^2 - 14m + 5}{7m^2 - 5}, \\ v &= -\frac{7m^2 - 10m + 5}{7m^2 - 5}. \end{aligned} \tag{9}$$

Substituting the first solution in (9) into the second equation in (8), we find

$$W^2 = 49m^4 - 56m^3 + 26m^2 - 40m + 25, \tag{10}$$

where $W = (7m^2 - 5)w$. The quartic (10) is thus transformed to the Weierstrass curve (7) via

$$\begin{aligned} m &= \frac{10(x+10)}{y}, \\ W &= \frac{5(-y^2 + 2x^3 + 40x^2 + 8xy + 200x + 80y)}{y^2}. \end{aligned} \tag{11}$$

Now in view of substitution (11) in (9), we have

$$\begin{aligned} u &= \frac{14000B^6 + 2800AB^4 - 280CB^3 + 140A^2B^2 - 28ACB + C^2}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2}, \\ v &= -\frac{14000B^6 + 2800AB^4 - 200CB^3 + 140A^2B^2 - 20ACB + C^2}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2}, \\ w &= \frac{200AB^4 + 80CB^3 + 40A^2B^2 + 8ACB + 2A^3 - C^2}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2}, \end{aligned}$$

which gives rise to

$$x_1 = -\frac{2b(-7000B^6 - 1300AB^4 + 180CB^3 - 50A^2B^2 + 18ACB + A^3 - C^2)}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2},$$

$$x_2 = \frac{2b(10B^2 + A)(700B^4 + 80AB^2 - 10CB + A^2)}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2},$$

$$x_3 = \frac{20bB(10B^2 + A)(140B^3 + 14AB - C)}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^22},$$

$$x_4 = \frac{2bC(100B^3 + 10AB - C)}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2},$$

$$y_1 = -\frac{2b(10B^2 + A)(700B^4 + 80AB^2 - 6CB + A^2)}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2},$$

$$y_2 = \frac{2b(-7000B^6 - 1300AB^4 + 140CB^3 - 50A^2B^2 + 14ACB + A^3 - C^2)}{14000B^6 + 2800AB^4 + 140A^2B^2 - C^2}.$$

The result now follows immediately by disregarding the signs and eliminating the denominators. □

The elliptic curve $\mathcal{E}$ is of rank 1 with generator $G = (-50, 400)$ as proved with Sage software ([12]). There exist thus an infinite number of rational points on $\mathcal{E}$. Hence, we see there will be infinitely many integral (and hence primitive) solutions to (3). By suitably swapping x_i's or y_j's, we can make each solution primitive.

In Table 2 it is given the first 10 primitive solutions for (3) corresponding to the points ρG, $\rho = 1, \ldots, 10$, on $\mathcal{E}$.

Theorem 2.3. *Suppose $G = (A/B^2, C/B^3)$ is a rational point on the elliptic curve*

$$\mathcal{F} : y^2 - 28xy - 560y = x^3 - 20x^2 - 400x + 8000,$$

with $A, B, C \in \mathbb{Z}$. Let

$$\begin{aligned}
x_1 &= 10B(A - 20B^2)(-C + 4BA - 80B^3)\\
&\quad \times(8000B^6 - 400AB^4 - 160CB^3 - 20A^2B^2 + 8ACB + A^3 - C^2),\\
x_2 &= C(10BA - 200B^3 - C)\\
&\quad \times(8000B^6 - 400AB^4 - 160CB^3 - 20A^2B^2 + 8ACB + A^3 - C^2),\\
x_3 &= C(-2880000B^9 + 416000AB^7 - 49600CB^6 - 19200A^2B^5 + 5360CAB^4 - 520C^2B^3\\
&\qquad +240A^3B^3 - 164CA^2B^2 + 26AC^2B + 2BA^4 - C^3 + CA^3),\\
x_4 &= 10B(A - 20B^2)(-C + 4BA - 80B^3)(8000B^6 - 400AB^4 - 20A^2B^2 + C^2 + A^3),\\
y_1 &= (10BA - 200B^3 - C)(-C + 4BA - 80B^3)\\
&\quad \times(8000B^6 - 400AB^4 - 160CB^3 - 20A^2B^2 + 8ACB + A^3 - C^2),\\
y_2 &= 6BC(A - 20B^2)(8000B^6 - 400AB^4 - 160CB^3 - 20A^2B^2 + 8ACB + A^3 - C^2).
\end{aligned}$$

Then $(x_1, x_2, x_3, x_4, y_1, y_2)$ is an integral solution to (3).

ρG	$x_1, x_2, x_3, x_4, y_1, y_2$
G	10, 3, 6, 5, 2, 9
$2G$	748, 6825, 6188, 825, 6545, 468
$3G$	294980814, 167258645, 116149310, 424781613, 76803578, 385435881
$4G$	1611626831293800, 472142139598129, 1972014239074200, 385857731290031, 1834962739338049, 248806231553880
$5G$	169280045930984897985710, 766162774482929349174093, 215671440212152020147774, 601359500949692140233845, 110074106304949854596618, 706956834856894305785001
$6G$	24162393727739161761330318090016508, 62173283061810327660763122221135975, 85445671984843141634653596093911 72, 17581409447538972607172016581918025, 22035521033790707882945691030094865, 40904556122325788876916851612143 32
$7G$	963369115267589138599991716498009622317963 1766, 512380228858579637637 1165 5583389686893536535205, 58626195221526976890951988715452314794316543610, 8 41963709039820780776541251348805660079923 7923, 5332577953702543033262 4982 73202762461599430642, 55539136084831312116449074475167020655116736329
$8G$	5807885578299478374803464068559171363422949355299453843304400, 7978846104064400728877402716521229276381057199714658394268641, 3687311741856522778834532228253029346662652841754786220776400, 12567482345806431542162320959505013373438711424746784414908961, 11333451143156893933504327758166192333290032569003055215852801, 2453280539206985170176539026914208306513973986011057021720240
$9G$	1900474957883880169894162278688246486271578381611419711192069436171932 3 6096410, 807847117338301169357829000924121711348167848181075467786303986 4344711814883, 1834579218194279478400247626031684144201580932791206188 68 19201605699779831 3846, 836863952820344454792548901682445695862708334698 8 5630962540017173739415448 05, 492876836631319354605615688020471993255450 8 4733889827615510570107616077885 62, 186897792981318198841894094739788151 4 4623066815272019920289496076361013207 0089
$10G$	841486404184812262835945787414190146173842091960231337336346958858756 34 930540346244398956157468, 277638328639015162224542178509475514630542290 9 327720731575471580190954278519192689711019588 31625, 149100350046932894 13 946608347118859209593736548431786617178680754014145787447958060862152 14 64668, 15669237446913155099458835063420571679331127219830221304248899079 176459488601604439130083368 1625, 249641206368299190537501016936725404451 203359709684509319094130232562922840937273863312678910225, 5615151814776 52545965534171686689044380452779729355698951816680993431299195583511366 09676236068

Table 2: Some primitive solutions of (3)

Proof. We let $(x_1, \ldots, y_2)$ satisfy

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2y_1^2 + 2y_2^2, \tag{12}$$

where $x_1, \ldots, y_2$ are defined as in (4). It is readily to check that (12) holds if and only if $a^2 + b^2 = c^2 + d^2$. Making a substitution $(a, b, c, d) = (a, a+r, a+s, a+t)$ we get a parameterized solution

$$\begin{cases} a = -r^2 + s^2 + t^2, \\ b = r^2 - 2rs - 2rt + s^2 + t^2, \\ c = -r^2 + 2rs - s^2 - 2st + t^2, \\ d = -r^2 + 2rt - 2st - t^2 + s^2. \end{cases} \tag{13}$$

Substituting (13) in (3) and brushing aside the uninteresting possibilities from the resulting equation, we get

$$-5rs^2 + 7ts^2 + 5r^2s - 2r^2t + 2rt^2 - 7st^2 = 0,$$

which gives rise to the following solution

$$r = \frac{5s^2 - 2t^2 \pm \sqrt{25s^4 + 176s^2t^2 + 4t^4 - 140s^3t - 56st^3}}{2(5s - 2t)}. \tag{14}$$

Hence, the quartic on the right hand side of (14) must be a square, say u^2,

$$u^2 = 25s^4 + 176s^2t^2 + 4t^4 - 140s^3t - 56st^3. \tag{15}$$

But (15) is birationally equivalent to the elliptic curve

$$y^2 - 28xy - 560y = x^3 - 20x^2 - 400x + 8000$$

via the standard transforms

$$\begin{aligned} t &= \frac{10(x-20)s}{y}, \\ u &= \frac{5(-y^2 + 2x^3 - 80x^2 + 28xy + 800x - 560y)s^2}{y^2}, \end{aligned} \tag{16}$$

Substituting r, s, t arising from (14)–(16) into (13), we get

$$x_1 = \frac{20B(A - 20B^2)(8000B^6 - 400AB^4 - 160CB^3 - 20A^2B^2 + 8ACB + A^3 - C^2)s^2}{C^2(-C + 4AB - 80B^3)},$$

$$\begin{aligned} x_2 = &-\frac{2(-8000B^6 + 1200AB^4 - 360CB^3 - 60A^2B^2 + 18ACB + A^3 - C^2)s^2}{C^2(-C + 4AB - 80B^3)^2}, \\ &\times (8000B^6 - 400AB^4 - 20A^2B^2 + A^3 + C^2), \end{aligned}$$

$$\begin{aligned} x_3 = &\frac{2(8000B^6 - 400AB^4 - 160CB^3 - 20A^2B^2 + 8ACB + A^3 - C^2)s^2}{C^2(-C + 4AB - 80B^3)^2}, \\ &\times (-8000B^6 + 1200AB^4 - 360CB^3 - 60A^2B^2 + 18ACB + A^3 - C^2), \end{aligned}$$

$$x_4 = \frac{20(A-20B^2)(8000B^6-400AB^4-20A^2B^2+A^3+C^2)Bs^2}{C^2(-C+4AB-80B^3)},$$

$$y_1 = \frac{2(8000B^6-400AB^4-160CB^3-20A^2B^2+8ACB+A^3-C^2)s^2}{C^2(-C+4AB-80B^3)} \times (-C+10AB-200B^3),$$

$$\begin{aligned} y_2 = -\frac{2(A-20B^2)s^2}{C^2(-C+4AB-80B^3)^2} &\times (3200000B^{10}-480000AB^8+176000CB^7 \\ &+16000A^2B^6-8800ACB^5+800A^3B^4+560C^2B^4-440A^2CB^3-8AC^2B^2 \\ &-60A^4B^2+6C^3B+22A^3CB+A^5-C^2A^2). \end{aligned}$$

The result now follows immediately by disregarding the signs and eliminating the denominators. □

The elliptic curve $\mathcal{F}$ is a rank 1 curve with generator $G = (-100, -800)$. There exist thus an infinite number of rational points on $\mathcal{F}$. Hence, there are infinitely many integer (and hence primitive) solutions to (3). Using Sage, one can easily observe that minimal model of both $\mathcal{E}$ and $\mathcal{F}$ is

$$y^2 = x^3 - x^2 - 180x + 900,$$

which is a cyclic infinite group isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. This shows that the solutions given in Proposition 2.2 and Theorem 2.3 are typically the same. We note that applying the well known identity

$$(rp-sq)^2 + (sp+rq)^2 = (rp+sq)^2 + (sp-rq)^2,$$

due to P. Pasternak [8, p. 252] instead of (13) in the proof of the above theorem, also gives rise to the same result, and that our methods do not make (3) reduce to one with lower m or n.

References

[1] Bremner, A., A geometric approach to equal sums of sixth powers, *Proc. London Math. Soc.*, Vol. 43, 1981, 544–581.

[2] Brudno, S., On generating infinitely many solutions of the Diophantine equation $A^6 + B^6 + C^6 = D^6 + E^6 + F^6$, *Math. Comp.*, Vol. 24, 1970, 453–454.

[3] Brudno, S., I. Kaplansky, Equal sums of sixth powers, *J. Number Theory*, Vol. 6, 1974, 401–403.

[4] Brudno, S., Triples of sixth powers with equal sums, *Math. Comp.*, Vol. 30, 1976, 646–648.

[5] Choudhry, A., On equal sums of sixth powers, *Indian J. pure appl. Math.*, Vol. 25, 1994, 837–841.

[6] Choudhry, A., On equal sums of sixth powers, *Rocky Mountain. J. Math.*, Vol. 30, 2000, 843–848.

[7] Delorme, J.-J., On the Diophantine equation $x_1^6 + x_2^6 + x_3^6 = y_1^6 + y_2^6 + y_3^6$, *Math. Comp.*, Vol. 59, 1992, 703–715.

[8] Dickson, L. E., *History of the Theory of Numbers II*, Chelsea Publishing Company, New York, 1920.

[9] Lander, L. J., T. R. Parkin, J. L. Selfridge, A survey of equal sums of like powers, *Math. Comp.*, Vol. 21, 1967, 446–459.

[10] Subba-Rao, K., On sums of sixth powers, *J. London Math. Soc.*, Vol. 9, 1934, 172–173.

[11] Resta, G., J.-C. Meyrignac, The smallest solutions to the Diophantine equation $x^6 + y^6 = a^6 + b^6 + c^6 + d^6 + e^6$, *Math. Comp.*, Vol. 72, 2003, 1051–1054.

[12] Sage software, Version 4.5.3, `http://www.sagemath.org`

[13] T. Piezas's website, avaible from `http://sites.google.com/site/tpiezas/023`

[14] Washington, L. C., *Elliptic Curves: Number Theory and Cryptography*, 2nd ed., CRC Press, Taylor & Francis Group, Boca Raton, FL, 2008.