משוואות פל – פתרונות לתרגיל

1. הוכיחו שאם $3n+1, 4n+1$ ריבועים אז $56|n$.

פתרון: $3n+1=a^2, 4n+1=b^2$, מוד 8 מראה $b^2\equiv 1(8)$ מכאן שn זוגי לכן $a^2\equiv 1(8)$ ואז $8|n$. מכיוון ש$(2a)^2-3b^2=1$ נקבל מפתרון $2+\sqrt{3}$ למשוואת פל $x^2-3y^2=1$. נשים לב ש$2a$ זוגי ולכן הפתרון שלנו באינקס איזוגי כי $u_{2r}=2u_r^2-1$. נשים לב ש$2+\sqrt{3}=7+4\sqrt{3}$ ולכן מקבלים $x_{k+4}=2\cdot 7x_{k+2}-x_k$. מכיוון ש $x_1, x_{-1}=2$ נותן ש$x_n\equiv \pm 2\ (7)$ לn איזוגי ולכן $7|a^2-1$ ולכן גם את n.■

2. אם $2+2\sqrt{28n^2+1}$ שלם אז הוא ריבוע.

פתרון: $m^2-7(2n)^2=1$ ורוצים ש$2+2m$ יהיה ריבוע. נשים לב שהפתרון המינימלי למשוואת פל $x^2-7y^2=1$ זה $8+3\sqrt{7}$ ולכן

$$m+2n\sqrt{7}=\left(8+3\sqrt{7}\right)^k\equiv\sqrt{7}^k(mod\ 2)\Longrightarrow 2|k$$

ולכן $m+2n\sqrt{7}=\left(a+b\sqrt{7}\right)^2$ ואז $m=2a^2-1$ ומכאן $2+2m=(2a)^2$. ■

3. מצאו את כל המספרים שהם גם משולשים וגם ריבועים.

פתרון: לפתור $n^2=\frac{m(m+1)}{2}$ זה כמו

$$(2m+1)^2-1=4m^2+4m=8n^2=2\cdot(2n)^2$$

שזה פשוט משוואת פל $x^2-2y^2=1$ כאשר x איזוגי וy זוגי. הפתרון היסודי $3+2\sqrt{3}$ וכל החזקות שלו יקיימו את תנאי הזוגיות. לכן זה פשוט מגיע מ$\left(3+2\sqrt{3}\right)^k$. ■

4. נסתכל על משוואת פל השלילית $x^2-dy^2=-1$.
   א. הראו אם $p|d$ הוא $3\ mod\ 4$ אז אין פתרון.
   ב. הראו שהכיוון ההפוך לא נכון.
   ג. הראו שאם $p=d$ ראשוני שהוא $1\ mod\ 4$ אז יש פתרון.
   ד. הראו שאם $d=pq$ ו$p,q\equiv 1(4)$ וגם $\left(\frac{p}{q}\right)=-1$ אז יש פתרון.

פתרון: א' ברור. ב' $d = 34 = 6^2 - 2$. הפתרון המינימלי לפל החיובי הוא $35 + 6\sqrt{34}$. משמע רוצים $35 + 6\sqrt{34} = \left(x + y\sqrt{34}\right)^2$ ואז $35 = x^2 + 34y^2$, $2xy = 6$ וזה לא קורה.

ג. ניקח פתרון יסודי למשוואת פל $x^2 - py^2 = \pm 1$. נטען שזה לא $+1$. אכן - $(x-1)(x+1) = (x^2 - 1) = py^2$ ומודולו 4 נסיק שy זוגי וx איזוגי. מכאן שאפשר לכתוב $\frac{x-1}{2} \cdot \frac{x+1}{2} = p\left(\frac{y}{2}\right)^2$ ואז מקבלים שאחד מהם ריבוע והשני הוא p ריבוע. בכל מקרה קיבלנו a^2, pb^2 במרחק 1, כלומר פתרון קטן יותר בסתירה.

ד. כמו קודם $(x-1)(x+1) = pqy^2$ והזוגיות עובד כמו קודם. צריך להסביר מדוע זה לא מתחלק p לאחד מהם וq לשני והסיבה היא שפתרון ל$pa^2 - qb^2 = \pm 1$ לא קיים מההנחה (מסתכלים מוד q). ■

5. (x_n, y_n) הפתרון הn למשוואת פל $x_n^2 - dy_n^2 = 1$ $((x_0, y_0) = (1,0))$. יהי p ראשוני אי זוגי.
   א. הוכיחו ש(x_n, y_n) מחזורי מודולו p ומצאו מחזור.
   ב. נניח ש$p | y_k$ הוכיחו ש$v_p(y_{k\ell}) = v_p(y_k) + v_p(\ell)$.

פתרון: א. $x_p + y_p\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^p \equiv x_1^p + y_1^p\sqrt{d}^p \equiv x_1 + y_1\left(\frac{d}{p}\right)\sqrt{d}$ ולכן רואים שיש מחזור שמחלק $p - \left(\frac{d}{p}\right)$. ■

ב. זה בעצם הרמת אקספוננט. ■

6. נניח ש$\frac{n^2+1}{m^2} + 4$ הוא ריבוע שלם, הראו שהוא שווה ל9.

פתרון: נכתוב $k^2 = \frac{n^2+1}{m^2} + 4$ אז נקבל

$$n^2 - (k^2 - 4) \cdot m^2 = -1$$

שזה משוואת פל שלילית. לk זוגי זה לא עובד מוד 4.

נשים לב ש$\mathbb{Z}\left[\frac{1+\sqrt{k^2-4}}{2}\right]$ גם הוא חוג כאשר k איזוגי ובאופן זהה לגמרי למשוואת פל נסיק שפתרונות ל$n^2 - (k^2 - 4)m^2 = -1$ כאשר n, m הם חצי שלמים מקיים את התכונה של משוואת פל שזה ציקלי.

אבל $\frac{1}{2}k + \frac{1}{2}\sqrt{k^2 - 4}$ בעל נורמה 1, ולכן נקבל שיש לנו $\left(a + b\sqrt{k^2 - 4}\right)^2 = \frac{k}{2} + \frac{1}{2}\sqrt{k^2 - 4}$ כאשר a, b הם חצי שלמים.

קל לראות מפה ש-$a = b = \pm\frac{1}{2}$ וזה נותן $k = 3$ (עם $3 + \sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^2$) כנדרש. ■

<u>הערה</u>: לפעמים מתייחסים גם ל-$x^2 - dy^2 = \pm 4$ כאשר $d \equiv 1(4)$ כמשוואת פל. כפי שנטען זה כמו למצוא יחידות בחוג $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

דוגמה למשל זה מספרי פיבונאצ'י ולוקס שמקיימים את $L_n^2 - 5F_n^2 = (-1)^n \cdot 4$.

7. פתרו $(2^n - 1)(3^m - 1) = x^2$.

פתרון: בהכ $n, m > 0$.
מודולו 3 נקבל ש$((-1)^n - 1) \equiv 1,0(3)-$ ולכן $n = 2n_0$ זוגי. מצד שני מודולו 4 נקבל $((-1)^m - 1) \equiv 0,1(4)-$ ולכן גם $m = 2m_0$ זוגי.

נשים לב שאם d הgcd בין הגורמים אז נקבל

$$(2^{n_0})^2 - 1 = dy^2, (3^{m_0})^2 - 1 = dz^2, x = dyz$$

ובעצם נקבל 2 פתרונות למשוואת הפל $u^2 - dv^2 = 1$ - ה $2^{n_0} + y\sqrt{d}, 3^{m_0} + z\sqrt{d}$.

אני טוען שאם הם $u_k + v_k\sqrt{d}, u_\ell + v_\ell\sqrt{d}$ אז k, ℓ שניהם איזוגיים. אכן אחרת נקבל $2^{n_0}\ or\ 3^{m_0} = 2u^2 - 1$ שהראשון לא מסתדר מוד 2 והשני לא מוד 3. מכאן k, ℓ איזוגיים. אבל אז $u_1 | u_k, u_\ell$ ולכן $u_1 = 1$ וזה סתירה. לכן אין פתרונות. ■

8. הוכיח שיש אינסוף רביעיות שלמים חיובים זרים (x, y, z, t) כך ש
$$x^3 + y^3 + z^2 = t^4$$

פתרון: נשים לב ש$1^3 + \cdots + n^3 = T_n^2$ ולכן $(n-1)^3 + n^3 + T_{n-1}^2 = T_{n+1}^2$. יש אינסוף מספרים משולשיים שהם ריבועים בעצמם ואז $T_{n+1} = t^2$ יפתור. ■

9. הוכיחו שלכל $n > 2$ יש שלמים חיוביים $a_1, \dots, a_n, b_1, \dots . b_n$ כך ש
$a_i a_{i+1} = b_i^2 + i$ (שעבורנו $a_{n+1} = a_1$).

פתרון: ניקח $a_i = i$ שעובד כמעט עד הסוף ונשנה אותו קצת.

נשנה רק בa_1 – אז אנחנו רוצים ש $2a_1 = b_1^2 + 1, na_1 = b_n^2 + n$. ניקח $b_n = n \cdot \widetilde{b_n}$ אז רוצים $a_1 = n \cdot \widetilde{b_n}^2 + 1$ וגם ש $2a_1 = b_1^2 + 1$. משמע ש

$2n\cdot\widetilde{b_n}^2+2=b_1^2+1$ כלומר לפתור $b_1^2-2n\cdot\widetilde{b_n}^2=1$ שזה משוואת פל.
אם $2n$ לא ריבוע אנחנו בטוב. אחרת ננסה לשנות רק את a_n . צריך

$$(n-1)a_n=b_{n-1}^2+n-1\ ,a_n=b_n^2+n$$

משמע רוצים לפתור $b_{n-1}^2+(n-1)=(n-1)(b_n^2+n)$ שזה המשוואה

$$x^2=(n-1)(y^2+n-1)$$

שזה $x^2-(n-1)y^2=(n-1)^2$. אם $n-1$ לא ריבוע אפשר עם פל. אחרת נכתוב $n-1=m^2$ ורוצים $(x-my)(x+my)=m^4$, לוקחים כל פירוק $m^2=AB$ ש$A>B$ ובאותה זוגיות ואז $x=\frac{mA+mB}{2},y=\frac{A-B}{2}$. אין פירוק כזה רק $m=2$ ואז $n=5$ ואנחנו במקרה הראשון. ■

10. נניח $x^2-dy^2=\pm1$ פתרון למשוואת פל עבורו y הוא d-חלק (כל גורם ראשוני שלו נמצא בd). אזי (x,y) הוא הפתרון היסודי.

פתרון: נרשום (x_n,y_n) הפתרונות למשוואת פל. נשים לב ש$m|n$ גורר $y_m|y_n$ ולכן צריך רק להוכיח שy_p הוא לא d-חלק עבור p ראשוני. נראה שאפילו $z_p=\frac{y_p}{y_1}$ הוא לא, נניח בשלילה. נשים לב ש

$$z_p=\binom{p}{1}x_1^{p-1}+\binom{p}{3}x_1^{p-3}\cdot y_1^2d+\cdots$$

ולכן אם ראשוני $q|z_p$, אז בגלל ש$q|d$ נסיק $q|p\cdot x_1^{p-1}$ ומכיוון שx_1,d זרים נקבל $q=p$. לכן z_p הוא חזקת p ו $p|d$. ל$p=2$ זה לא מסתדר כי $z_p=2x_1$.
ל$p=3$ אז במשוואת פל חיובית $z_p=4x_1^2-1=(2x_1-1)(2x_1+1)$ וזה לא חזקת 3 ובמשוואת פל שלילית $z_p=4x_1^2+1$ שלא חזקת 3 משיקולי מודולו ($3,x_1$ זרים מהנחה). ל$p>3$ אז בגלל ש$p|d$ מקבלים ש$z_p\nmid p^2$ ולכן $z_p=p$ אבל זה קטן מידי וסתירה. ■

11. א. פתרו $5^a-3^b=\pm2$.
ב. משפט Størmer – יהי $S=\{p_1,\dots,p_r\}$ קבוצת ראשוניים, אז יש לכל היותר 3^r-2^r זוגות מספרים S-חלקים שהפרשם 1 או 2 .

פתרון:

נוכיח את המשפט ונראה איך בונים את הפתרונות נשים לב שאם $x-1,x+1$ הם S-חלקים אז x^2-1 הוא S-חלק. אם $x,x+1$ הם S-חלקים אז $(2x+1)^2-1$ הוא S-חלק. לכן צריך לחסום את כמות המספרים מהצורה $s=n^2-1$ שהם S-חלקים.

נרשום $s = d \cdot m^2$ כאשר $v_p(d) = 1{,}2$ ואז נקבל $n^2 - dm^2 = 1$ ו m הוא d-חלק. לזה יש רק פתרון יחיד לפי התרגיל הקודם. יש $3^r - 2^r$ משוואות פל לפתור ובזאת ניצחנו.

בסעיף א' מקבלים את הפתרונות $5^0 - 3^1 = -2, 5^1 - 3^1 = 2, 5^2 - 3^3 = -2$. ■

12. הראו כי למשוואה $y^2 + 1 = x^n$ אין פתרונות שלמים מלבד $(x, y) = (1,0)$.

פתרון: ל n זוגי זה קל. ל n איזוגי אז $y^2 - x \cdot \left(x^{\frac{n-1}{2}}\right)^2 = -1$. מתרגיל 13 זה הפתרון הקטן ביותר ל $n^2 - x \cdot m^2 = -1$.
מודולו 4 רואים ש y זוגי. נפרק ב $\mathbb{Z}[i]$ ונקבל $(y+i)(y-i) = x^n$ ולכן בגלל שהם זרים ו n איזוגי $y + i = (a+bi)^n = \alpha^n$. מפה רואים $2bi = \alpha - \bar{\alpha} \mid \alpha^n - \bar{\alpha}^n = 2i$ שגורר $b = \pm 1$. זה אומר ש $x = a^2 + 1$. אבל הפתרון הבסיסי למשוואת הפל $n^2 - (a^2+1) \cdot m^2 = -1$ הוא $(n, m) = (a, 1)$ ולכן $x = 1$ כנדרש. ■

13. אם m, n, p שלמים חיוביים כך ש $m + n + p - 2\sqrt{mnp} = 1$ אז לפחות אחד מהם הוא ריבוע.

פתרון: $(m+n+p-1)^2 = 4mnp$, נגדיר $a = 2m - 1$ ו b, c דומים אז

$$(a+b+c+1)^2 = 4(n+m+p-1)^2 = 16mnp = 2(a+1)(b+1)(c+1)$$

שפותחים סוגריים זה $a^2 + b^2 + c^2 - 2abc = 1$ ואפשר לרשום זאת כ $(a^2-1)(b^2-1) = (ab-c)^2$ ובאופן דומה ל $bc - a$. נסיק שיש d שאינו ריבוע ו u, v שלמים שאפשר לכתוב

$$a^2 - 1 = du^2, b^2 - 1 = dv^2, c^2 - 1 = dw^2$$
$$|ab - c| = duv, |bc - a| = dvw$$

משמע ש a, b, c הם קורדינטות ראשונות לפתרון משוואת פל $x^2 - dy^2 = 1$. נאמר $a = x_{k_1}, b = x_{k_2}, c = x_{k_3}$. אם k_1 הוא זוגי אז עבור $\ell_1 = \frac{k_1}{2}$ מתקבל $m = \frac{x_{2\ell_1}+1}{2} = x_{\ell_1}^2$ כנדרש. לכן צריך להראות שאחד מבין ה k_i הוא זוגי. אבל אם נסדר אותם $a \geq b \geq c$ אז $c = ab - duv$ אז נקבל $k_1 - k_2 = k_3$ ולכן אחד מהם הוא זוגי.■

<u>הערה</u>: למשוואה $a^2 + b^2 + c^2 - 2abc = 1$ - בממשיים יש משמעות גיאומטרית של $a = \cos\alpha$ שזו זהות של משולש.

קיבלנו שבכללי הפתרונות למשוואה ב16 זה $\frac{x_{k_1}+1}{2},\frac{x_{k_2}+1}{2},\frac{x_{k_3}+1}{2}$ שלוקחים איזשהו פתרון למשוואת פל והסכום של זוג מבין k_1,k_2,k_3 שווה לשלישי.

14. נניח שa,b מספרים טבעיים גדולים מ1 וחסרי ריבועים. אז אחד מהמשוואות $ax^2-by^2=-1$, $ax^2-by^2=1$ היא חסרת פתרון.

פתרון: נניח אחרת $ax^2-by^2=-1$ ו $au^2-bv^2=1$. נגדיר $T=uy-vx$ אז פתיחת סוגרים מראה

$$au^2+by^2+abT^2-2abuyT=1$$

אכן –

$$au^2+by^2+ab(u^2y^2-2uyvx+v^2x^2)-2abuy(uy-vx)=$$

$$=au^2+by^2+abu^2y^2-2abuyvx+abv^2x^2-2abu^2y^2+2abuyvx=$$

$$=au^2+by^2-abu^2y^2+(by^2+1)(au^2+1)=1$$

לכן יש פה את המשוואה $m+n+p-1=2\sqrt{nmp}$ ל
$$m=au^2,n=by^2,p=abT^2$$

וזה סתירה לתרגיל הקודם (שים לב שa,b זרים ומניחים שחסרי ריבועים). ■

15. נניח כי x,y מספרים שלמים עבורם $x(y+1),y(x+1)$ שניהם ריבועים. הראו כי אחד מבין x,y הוא ריבוע.

פתרון:

נכתוב $x=an^2,y=bm^2$ כאשר a,b חסרי ריבועים. אז $an^2(bm^2+1)$ הוא ריבוע וגם $bm^2(an^2+1)$. מכאן ש $(bm^2+1)=a\cdot s^2$ וכן $an^2+1=b\cdot t^2$ אבל זה בדיוק פתרונות לשתי המשוואות "פל" $an^2-bt^2=-1,as^2-bm^2=1$ - בסתירה לתרגיל הקודם. ■

16. נסמן (x_n,y_n) הפתרונות למשוואת פל. הראו ש x_{4n} איננו ריבוע.

פתרון: נשים לב ש$x_{4n}=T_4(x_n)=8x_n^4-8x_n^2+1$. משמע נפתור את המשוואה

$$y^2=8x^4-8x^2+1$$

שזה כמו $y^2 - 2\cdot(2x^2-1)^2 = -1$. זה משוואת פל שהפתרונות שלה הם $1+\sqrt{2}$ בחזקה איזוגית. בפרט $y + (2x^2-1)\sqrt{2} = \left(1+\sqrt{2}\right)\cdot\left(a+b\sqrt{2}\right)^2$ כאשר $a^2 - 2b^2 = \pm 1$. נקבל

$$y + (2x^2-1)\sqrt{2} = a^2 + 2b^2 + 4ab + (a^2 + 2b^2 + 2ab)$$

מכאן ש$2x^2 - 1 = a^2 + 2b^2 + 2ab$. נשים לב ש a, b זרים.

נשים לב שלמשוואה $m^4 - 2n^2 = 1$ אין פתרונות מלבד $(1,0)$.

אכן - $\frac{m-1}{2}\cdot\frac{m+1}{2}\cdot\frac{m^2+1}{2} = \left(\frac{n}{2}\right)^2$ ומספרים זרים ולכן יש ריבועים עוקבים ונקבל רק את הפתרון $(1,0)$.

נניח ש$a^2 - 2b^2 = 1$: אז נקבל $2x^2 = 2a^2 + 2ab = 2a(a+b)$ ולכן גם a הוא ריבוע, וקיבלנו את המשוואה $m^4 - 2n^2 = 1$ שיש פתרון טריוויאלי.

אם $a^2 - 2b^2 = -1$ אז נקבל $2x^2 = 4b^2 + 2ab = 2b(a+2b)$ ולכן $b, a+2b$ ריבועים. אבל $a+2b$ הוא קורדינטת x ב$(a+b\sqrt{2})(\sqrt{2}+1)$ ולכן שוב מהמשוואה $m^4 - 2n^2 = 1$ אין פה פתרונות. ■

17. הראו כי הפתרונות היחידים למשוואה $y^2 = x^3 + 1$ הם $(0,1), (3,2)$.

פתרון: [שבו המלך] נשים לב $y^2 = (x+1)(x^2 - x + 1)$. נשים לב ש

$m = \gcd(x+1, x^2 - x + 1) = \gcd(x+1, 3) \in \{1,3\}$.

אם $m = 1$ אז $x^2 - x + 1$ ריבוע וזה סתירה כי הוא ממש בין $(x-1)^2, x^2$.

לכן $m = 3$. נקבל $x + 1 = 3k^2, x^2 - x + 1 = 3\ell^2$.

$$x = 3k^2 - 1 \quad , \quad (2x-1)^2 + 3 = 3(2\ell)^2$$

משמע נקבל

$$(2\ell)^2 - 3\cdot(2k^2-1)^2 = 1$$

ואנחנו עכשיו הולכים לפתור את המשוואה הזו. משוואת הפל $x^2 - 3y^2 = 1$ בעלת הפתרון היסודי $2+\sqrt{3}$ ומהסתכלות מודולו 2 נסיק

$$2\ell + (2k^2-1)\sqrt{3} = \left(2+\sqrt{3}\right)^{2n+1} = \left(2+\sqrt{3}\right)\cdot\left(a+b\sqrt{3}\right)^2$$

כאשר $a^2 - 3b^2 = 1$. מכאן נקבל

$$2k^2 - 1 = a^2 + 3b^2 + 4ab$$

שזה נותן

$$2k^2 = 2a(a+2b) \to k^2 = a(a+2b)$$

אם a איזוגי אז a ריבוע ומקבלים שיש פתרון למשוואה $u^4 - 3b^2 = 1$.

אם a זוגי אז $a, a+2b$ שניהם פעמיים ריבוע. אבל $a+2b$ הוא קורדינטת y של

ה $(2+\sqrt{3})(a+b\sqrt{3})$ ולכן נקבל פתרון למשוואה $z^2 - 3(2t^2)^2 = 1$. לזה אפשר שוב להשתמש בPell והפעם להסיק שהחזקה של $z + 2t^2\sqrt{3}$ היא זוגית ולכן

$$z + 2t^2\sqrt{3} = \left(c + d\sqrt{3}\right)^2 = c^2 + 3d^2 + 2cd\sqrt{3}$$

לכן $z = c^2 + 3d^2,\ t^2 = cd$ ולכן c, d ריבועים ונקבל שוב פתרון למשוואה $u^4 - 3v^2 = 1$ (שעבורה גם v ריבוע).

מכאן שאנו רוצים לפתור את המשוואה הזו. כלומר למצוא $x_n + y_n\sqrt{3} = \left(2+\sqrt{3}\right)^n$ עבורו x_n ריבוע. כיוון ש$x_n^2 - 3y_n^2 = 1$, מודולו 8 נסיק שx_n איזוגי. נשים לב שזה אומר שn מתחלק ב4 – בבירור זה גורר שהוא זוגי ואם $n = 4r + 2$

$$\left(2+\sqrt{3}\right)^{4r+2} = \left(7+4\sqrt{3}\right)^{2r+1} \equiv (-1)^{2r+1}\ (mod\ 4) \equiv -1\ (mod\ 4)$$

מהתרגיל הקודם אם n מתחלק ב4 מקבלים את הפתרון הטריוויאלי.

שמגלגלים אותו אחורה לתרגיל שלנו זה $3^2 = 2^3 + 1$. ■

18. נסמן (x_n, y_n) הפתרונות למשוואת פל $x^2 - dy^2 = 1$.

א. הראו שאם x_n ריבוע וn איזוגי אז x_1 ריבוע.

ב. *** הראו שאם x_n ריבוע אז $n = 1,2$.

פתרון: א. נסמן $\alpha = x_1 + y_1\sqrt{d}$ הפתרון היסודי. אז $x_n = \frac{1}{2}(\alpha^n + \bar{\alpha}^{-n})$ כאשר

$$\alpha + \bar{\alpha} = 2x_1\ , \alpha \cdot \bar{\alpha} = 1$$

הסדרה x_n מקיימת את הרקורסיה $(x_0 = 1, x_1 = x_1)$

$$x_{n+2} = 2x_1 \cdot x_{n+1} - x_n$$

לn איזוגי נגדיר $z_n = \frac{x_n}{x_1}$ שהוא שלם. נשים לב ש $z_{n+2} + z_n = 2x_{n+1}$. לכן אם ניקח 2 משוואות כאלה אז

$$z_{n+4} + 2z_{n+2} + z_n = 2(x_{n+3} + x_{n+1}) = 4x_1 \cdot x_{n+2} \equiv 0\ (mod\ 4x_1)$$

מכיוון ש$z_1 \equiv 1, z_3 = 4x_1^2 - 3 \equiv\ -3\ (mod\ 4x_1)$ נסיק מהרקורסיה כי

$z_n \equiv (-1)^{\frac{n-1}{2}} n \ (mod\ 4x_1)$. בפרט $z_n \equiv 1 (mod\ 4)$.

כמו כן, x_n הוא איזוגי ל n זוגי (מהרקורסיה). אם x_1 זוגי אז $v_2(x_1) = v_2(x_n)$ לכל n איזוגי באינדוקציה (שוב מהרקורסיה).

נטען שלכל n,m איזוגיים וזרים מתקיים $\left(\frac{z_n}{z_m}\right)_L = 1$. אכן, נסביר זו באינדוקציה על $|nm|$.

נשים לב ש$x_{n+2m} \equiv -x_n \ (mod\ x_m)$ כי אם $\alpha^m + \alpha^{-m} \equiv 0$ אז $\alpha^{2m} \equiv -1$. מכאן נובע ש $z_{n-2m} \equiv -z_n \ (mod\ z_m)$ [כאשר $z_{-t} = z_t$] . מהדדיות ריבועית $\left(\frac{z_n}{z_m}\right)_L = \left(\frac{z_n}{z_m}\right)_L$ ומהאינפורמציה מודולו 4 וממה שראינו הרגע אפשר לבצע ירידה (להוריד (n,m) ל $(m,|n-2m|)$).

נניח כעת שx_{n_0} הוא ריבוע. אז מהדיון על זוגיות x_1 נסיק ש$v_2(x_1)$ זוגי (כי הוא או 0 או $v_2(x_{n_0})$) ולכן נתעלם מסוגיות ב2. ניקח לm שהוא $1\ mod\ 4$ וזר לx_1, n_0 נקבל

$$1 = \left(\frac{z_m}{x_{n_0}/z_{n_0}}\right)_L = \left(\frac{z_m}{x_1}\right)_L = \left(\frac{(-1)^{\frac{m-1}{2}} m}{x_1}\right)_L = \left(\frac{m}{x_1}\right)_L$$

מהטענה וההנחה שזהו ריבוע. מכאן $\left(\frac{m}{x_1}\right)_L = 1$ כמעט לכל m (שמקיים תכונה מוד 4 וזר לn_0) – מפה ברור שx_1 חייב להיות ריבוע. כנדרש עבור סעיף א. ■

אני לא יודע לפתור את ב' באופן פשוט – תוצאה של Ljunggren [אחרי סעיף א']. אמור להיות הוכחה שמשתמשת ברעיונות הp-אדים של Skolem שחוסמת את כמות הפתרונות ואז משתמשים בא' ■

19. פתרו את המשוואה $x^2 - 48 \cdot y^4 = 1$ בשלמים.

פתרון: נכתוב את זה בתור $x^2 - 3 \cdot (4y^2)^2 = 1$. הפתרון היסודי לפל זה $2 + \sqrt{3}$ ובגלל ש$2y$ זוגי נסיק ש$x + 4y^2\sqrt{3}$ ריבוע. משמע $\left(a + b\sqrt{3}\right)^2$. לכן $4y^2 = 2ab$ שזה אומר $ab = 2y^2$. נזכור $a^2 - 3b^2 = 1$.
נשים לב שאם a ריבוע אז יש לנו x_n שהוא ריבוע אבל $x_1 = 2, x_2 = 7$ לא ריבועים משמע ש $a = 1$ ו$b = 0$.

לכן $a = 2t^2$ פעמיים ריבוע ו$b = s^2$ ריבוע – אבל אז מקבלים $4t^4 - 3s^4 = 1$ שזה $(2t^2 - 1)(2t^2 + 1) = 3s^4$ ובפרט (מסתכלים מוד 3) $2t^2 - 1$ חזקת 4 שזה

$$u^4 - 2t^2 = -1$$

המשוואה הזו קלה לפתרון - $\frac{u^4+1}{2} = t^2$ ואז $t^4 = \left(\frac{u^2-1}{2}\right)^2 + u^4$ וזה שלשה פיתגורית עם 2 ריבועים. מקבלים שהפתרון היחיד הוא $u = 1, t = 1$.

זה נותן את הפתרון $y = 1, x = 7$ לבעיה המקורית. ■

20. ** מצאו את כל המספרים שהם משולשים, ריבועים ומחומשים.

פתרון:

אנחנו רוצים

$$\frac{n(n+1)}{2} = m^2 = \frac{k(3k-1)}{2} = A$$

משמע

$$(2n+1)^2 - 2(2m)^2 = 1$$

$$(6k-1)^2 - 6(2m)^2 = 1$$

נשים לב ש

$$(2n+1)^2 + (4m)^2 = (6k-1)^2$$

ולכן מפיתגורס יש שלמים p, q כך ש:

$$2n+1 = p^2 - q^2\ , 2m = pq, 6k-1 = p^2 + q^2$$

ועכשיו המשוואה הפכה ל:

$$(p^2 - q^2)^2 - 2(pq)^2 = 1$$

כלומר

$$p^4 - 4p^2q^2 + q^4 = 1$$

ונהפוך את זה ל

$$(p^2 - 2q^2)^2 - 3(q^2)^2 = 1$$

או באופן סמטרי. מכיוון שאחד מבין p, q זוגי אז קיבלנו משוואה $x^2 - 3y^4 = 1$ שy זוגי שזה בדיוק התרגיל הקודם – יש את $(1,0), (7,2)$. אם אחד מבין p, q הוא 0 אז מקבלים את $A = 1$. אם $q = 2$ אז $p^2 - 2q^2 = \pm 7$ וזה $p^2 = 15,1$ אז $p = 1$ ולא מקבלים פתרון. באופן סמטרי יש את $q = 1, p = 2$ ששוב נותן את $A = 1$.

לכן 1 הוא המספר המשולשי-ריבועי-מחומשי היחיד. ■

21. מצאו את כל הטבעיים $k < 100$ כך שיש $n \neq 0$ שלם עבורו המספרים $2n^2+1, kn^2+1, 2kn^2+1$ כולם ריבועים.

פתרון: נניח כי $a^2 = 2n^2+1,\ \ b^2 = kn^2+1,\ \ c^2 = 2kn^2+1$

אז נסיק ש $a^2 - 2n^2 = 1, c^2 - 2b^2 = -1$. מכיוון ש$b > n$ יש ℓ כך ש

$$c + b\sqrt{2} = \left(1+\sqrt{2}\right)^{2\ell+1}\left(a + n\sqrt{2}\right)$$

אם $\ell \geq 1$ אז

$$c + b\sqrt{2} \geq \left(7+5\sqrt{2}\right)\left(a+n\sqrt{2}\right) = (7a+10n) + (7n+5a)\sqrt{2}$$

מכאן נקבל $b \geq 7n + 5a$ שזה אומר

$$\sqrt{kn^2+1} \geq 7n + 5\sqrt{2n^2+1}$$

ומפה $kn^2 + 1 \geq 49n^2 + 70n\sqrt{2n^2+1} + 50n^2 + 25 > 100n^2 + 1$ בסתירה להנחת הגודל על k. לכן $\ell = 0$ ו$c + b\sqrt{2} = \left(1+\sqrt{2}\right)\left(a+n\sqrt{2}\right)$. מפה

$$\sqrt{kn^2+1} = b = a + n = n + \sqrt{2n^2+1}$$

שמפה

$$(k-3)n^2 = 2n\sqrt{2n^2+1}$$

ולכן $(k-3)^2n^2 = 4(2n^2+1)$ משמע $[(k-3)^2 - 8]\cdot n^2 = 4$ אז $n = 2, k = 6$ וזה אכן פתרון. ■