הדדיות ריבועית

הגדרה: סימן לז'אנגד:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \exists x \neq 0, x^2 \equiv a \ mod \ p \\ 0, & if \ a = 0 \\ -1, & else \end{cases}$$

תזכורת, קריטריון אוילר:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod \ p$$

<u>משפט ההדדיות הריבועית:</u> יהיו p, q ראשוניים אי-זוגיים אזי מתקיים:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

נספח למשפט, לכל ראשוני אי-זוגי p מתקיים ש-

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

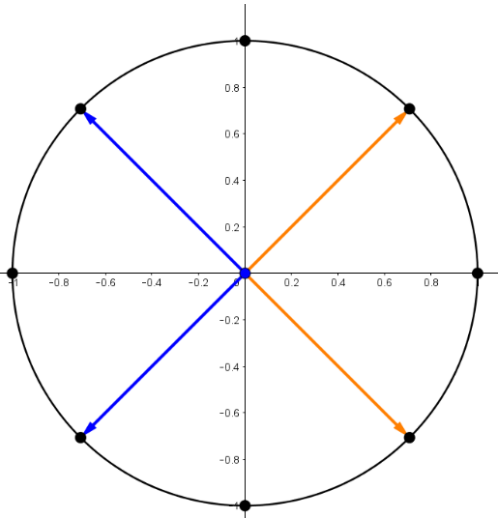
הוכחה ראשונה:

אנחנו הולכים להסתכל על הרחבה של השדה $\mathbb{Z}/p\mathbb{Z}$. נסמן שורש יחידה פרימיטיבי מסדר n ב-ζ_n, כלומר $\zeta_n = e^{\frac{2\pi i}{n}}$. אנחנו הולכים לעבוד עם $\mathbb{Z}/p[\zeta_n]$, אלו מספרים מהצורה

$$\sum_i a_i \zeta_n^i$$

כאשר $a_i \in \mathbb{Z}/p$.

נתחיל מהוכחת ההנספח. נעבוד ב-$\mathbb{Z}/p[\zeta_8]$. נסמן $\tau = \zeta_8 + \zeta_8^{-1}$ (באיור τ הוא סכום הווקטורים הכתומים). נחשב את $\tau^p \ mod \ p$ בשתי דרכים. ראשית, קל לראות ש-



$$\tau^p \equiv \zeta_8^p + \zeta_8^{-p} \ mod \ p$$

כמובן ש-ζ_8^p תלוי ב-p מוד 8, אם $p \equiv 1 \ mod \ 8$ אז $\zeta_8^p \equiv \zeta_p$ ולכן $\tau^p \equiv \tau$. אם $p \equiv -1 \ mod \ 8$ אז $\zeta_8^p \equiv \zeta_8^{-1}$ ושוב $\tau^p \equiv \tau$. אם p הוא 3 או 5 מוד 8 אז $\zeta_8^p \equiv -\zeta_8^{-1}$ או $\zeta_8^p = -\zeta_8^p$, בהתאמה, ובשני המקרים מקביל ש-$\tau \equiv -\tau$.
יש דרך קצרה לרשום את כל המקרים בנוסחה אחת, מתקיים ש-

$$\tau^p \equiv (-1)^{\frac{p^2-1}{8}} \cdot \tau \ mod \ p .$$

עכשיו נחשב את τ^p בדרך אחרת. נשים לב ש- $\zeta_8 = \frac{\sqrt{2}+\sqrt{2}i}{2}$ ולכן $\tau = \sqrt{2}$. נובע ש -

$$\tau^p = \tau \cdot (\tau^2)^{\frac{p-1}{2}} = \tau \cdot (2)^{\frac{p-1}{2}} \equiv \tau \left(\frac{2}{p}\right) mod \ p$$

נשווה בין שתי הזהויות שהוכחנו ונקבל:

$$\blacksquare \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}$$

ננסה להכיל את הרעיון של ההוכחה לנספח להוכחה של המשפט הכללי. ההכלה של τ היא הסכום הבא, שנקרא סכום גאוס:

$$G = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta_p^i$$

שוב נחשב את $G^q \ mod \ q$ בשתי דרכים שונות. כמו מקודם בפעם הראשונה נפתח מבינום:

$$G^q \equiv \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^q \zeta_p^{qi} \ mod \ q \equiv \sum_{i=1}^{p-1} \left(\frac{q^2 i}{p}\right)^q \zeta_p^{qi} \ mod \ q$$
$$\equiv \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \cdot \left(\frac{q}{p}\right) \zeta_p^t \equiv \left(\frac{q}{p}\right) G \ mod \ q$$

עכשיו נחשב בדרך האחרת. כמו בהוכחה של הנספח, כל פעם נוציא G^2 מחוץ לסוגריים. ראשית נחשב את G^2:

$$G^2 = \sum_{i,j=1}^{p-1} \left(\frac{ij}{p}\right) \zeta_p^{i+j}$$

נסמן $j = ic$ ונקבל ש-

$$G^2 = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \sum_{i=1}^{p-1} \zeta_p^{i(1+c)} = (p-1)\left(\frac{p-1}{p}\right) + \sum_{c=1}^{p-2} \left(\frac{c}{p}\right) \cdot (-1)$$
$$= (p-1)\left(\frac{p-1}{p}\right) + \left(\frac{-1}{p}\right) + \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \cdot (-1)$$
$$= p \cdot \left(\frac{-1}{p}\right)$$

ועכשיו ל-G^q.

$$G^q = G \cdot (G^2)^{\frac{q-1}{2}} = G \cdot \left(p \cdot \left(\frac{-1}{p}\right)\right)^{\frac{q-1}{2}}$$
$$\equiv G \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \; mod\; q$$

נשווה בין שתי הנוסחאות ונקבל ש-

$$G\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv G\left(\frac{q}{p}\right) \; mod\; q$$

על פי מה שהוכחנו $G^2 = p \cdot \left(\frac{-1}{p}\right)$ ולכן אפשר לחלק ב-G מוד q ונקבל ש-

$$\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv \left(\frac{q}{p}\right) \; mod\; q$$

המספרים בשני האגפים הם ± 1 ולכן השוויון נכון גם בלי $mod\; q$ וניצחנו!!

<u>הערה מגניבה שלא קשורה להוכחה:</u>

בהוכחה הסתכלנו על הרחבה של $\mathbb{Z}/p\mathbb{Z}$ עם שורש יחידה מסדר n.
במקום זה היה אפשר להסתכל על $\mathbb{Z}[\zeta_n]$ ולהסתכל מוד p על השדה הזה, מתברר ששני הדברים שקולים.

במילים פורמליות: $\mathbb{Z}[\zeta_n]$ אלו מספרים מהצורה

$$\sum_i a_i \, \zeta_n^i$$

כאשר a_i שלמים. להסתכל מוד p אומר להגדיר יחס שקילות: נגיד ש-$m, k \in \mathbb{Z}[\zeta_n]$ שקולים מוד p אם קיים $z \in \mathbb{Z}[\zeta_n]$ כך ש-$m - k = p \cdot z$.
כיוון אחד ברור: אם m, k שקולים בתור מספרים ב-$\mathbb{Z}/p[\zeta_n]$ זה אומר שלכל חזקה של ζ_n המקדם ב-a שקול למקדם ב-b, כלומר אם $m = \sum m_i \zeta_n^i$ ו-$k = \sum_i k_i \, \zeta_n^i$ אז $m_i - k_i = pz_i$ עבור z_i שלם ולכן ניתן לבחור $z = \sum_i z_i \, \zeta_n^i$ ונקבל ש-m, k שקולים גם בתור מספרים ב-$\mathbb{Z}[\zeta_n]/p$.

הכיוון השני יותר מעניין. מספיק להראות שאם $m,k\in\mathbb{Z}$ שקולים בתור מספרים ב-$\mathbb{Z}[\zeta_n]/p$ אז הם שקולים בתור מספרים ב-$\mathbb{Z}/p$.
בשביל זה אנחנו צריכים להוכיח מספר תכונות של $\mathbb{Z}[\zeta_n]$.

<u>למה:</u> כל המספרים ב-$\mathbb{Z}[\zeta_n]$ הם שלמים אלגבריים, כלומר כל מספר ב-$\mathbb{Z}[\zeta_n]$ הוא שורש של פולינום מתוקן עם מקדמים שלמים.

<u>הוכחה:</u> נזהיר שההוכחה לטענה זו אינה לגמרי אלמנטרית ומשתמשת באלגברה לינארית, אבל ממש קצת אז בתקווה תצליחו להבין.

נתון לנו $z=\sum a_i\zeta_n^i$, נתבונן ב-p זהויות המתקבלות מכפל של הזהות שלנו ב-ζ_n^j כאשר $0\le j\le n-1$. כלומר

$$z\zeta_n^j=\sum_i a_{i,j}\zeta_n^i$$

נגדיר ווקטור $v=(1,\zeta_n,\zeta_n^2,\dots,\zeta_n^{n-1})$ ונקבל שמתקיים ש-

$$Av=zv$$

כאשר A זו המטריצה של ה-$a_{i,j}$ים, כלומר המקדמים בזהויות שלנו.
לפיכך z הוא ערך עצמי של A ולכן הוא שורש של הפולינום האופייני של A, אבל A זו מטריצה עם ערכים שלמים ולכן לפולינום האופייני שלה יש מקדמים שלמים, וזה בדיוק מה שרצינו ■

עכשיו נוכיח את הכיוון ההפוך: נניח ש-a,b שלמים וקיים $z=\frac{a}{b}\in\mathbb{Z}[\zeta_n]$ כך ש-$m-k=pz$, במילים אחרות $z=\frac{m-k}{p}$ אבל m,k שלמים ולכן z רציונלי, אבל הוא גם שלם אלגברי. טענה מוכרת היא שכל רציונלי שהוא שלם אלגברי חייב להיות שלם. מהטענה נובע ש-z שלם ולכן m,k שקולים מוד p מעל השלמים וזה מה שרצינו.

<u>הוכחת הטענה המוכרת:</u> אם $\frac{m}{n}$ רציונלי (ברישום מצומצם) ושורש של פולינום מתוקן עם מקדמים שלמים אז

$$c_0+\frac{c_1m}{n}+c_2\cdot\frac{m^2}{n^2}+\cdots+c_k\cdot\frac{m^k}{n^k}+\frac{m^{k+1}}{n^{k+1}}=0$$

ולכן

$$m^{k+1}=n(-c_0\cdot n^k-c_1\cdot m\cdot n^{k-1}+\cdots.)$$

אנחנו מניחים ש-m,n זרים ולכן חייב להתקיים ש-$n=1$.

הוכחה שנייה:

שוב נתחיל מהוכחת הנספח. נתבונן בכל השאריות הזוגיות מודולו p: $2,4,6,\dots,p-1$. נחלק את כל השאריות שלנו ב-2, נקבל את השאריות $1,2,\dots,\frac{p-1}{2}$ ועכשיו נחליף סימן לכל השאריות האי-זוגיות. כלומר 1 יהפוך ל-$p-1$, 3 ל-$p-3$ וכך הלאה. חזרנו לרשימה של השאריות הזוגיות ולכן המכפלה של כל השאריות נשמרה.

נרשום את כל זה בנוסחאות:

$$\prod_{i=1}^{\frac{p-1}{2}} 2i = 2^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} i = \left(\frac{2}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} i \cdot (-1)^i \cdot (-1)^i =$$

$$= \left(\frac{2}{p}\right) (-1)^{\sum_{i=1}^{\frac{p-1}{2}} i} \prod_{i=1}^{\frac{p-1}{2}} i \cdot (-1)^i = \left(\frac{2}{p}\right) (-1)^{\frac{p^2-1}{8}} \prod_{i=1}^{\frac{p-1}{2}} 2i$$

ולכן

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

וזה מה שרצינו.

ההוכחה למשפט הכללי תהיה דומה, שוב נתבונן בכל השאריות הזוגיות (הסיבה שזה טוב היא שיש $\frac{p-1}{2}$ מהן, זה לא היה קשור לזה שרצינו את סימן לז'נדר ספציפית של 2). כמו מקודם נרצה להוציא מכל אחת מהשאריות גורם של q, להחליף סימנים ולחזור למכפלה המקורית. הפעם יהיה לנו יותר קל דווקא להכפיל ב-q ולא לחלק (זה כמובן לא משנה, פשוט יותר נוח).

עבור a-שארית חלוקה ב-p, נסמן ב-r_a את שארית החלוקה של qa ב-p. כלומר

$$qa = p\left\lfloor\frac{qa}{p}\right\rfloor + r_a$$

נטען שהקבוצות $\{2,4,\dots,p-1\}$ ו-$\{2q\cdot(-1)^{r_2}, 4q\cdot(-1)^{r_4}, \dots, (p-1)q\cdot(-1)^{r_{p-1}}\}$ זהות.
נשים לב שכל האיברים בקבוצה השנייה מתאימים לשאריות זוגיות

מודולו p, אכן אם qa זוגי אז מכפילים אותו ב-(-1) בחזקה זוגית ואם qa אי-זוגי אז מכפילים אותו ב-(-1) בחזקה אי-זוגית ובכך מחליפים את הזוגיות מודולו p.

כעט צריך להסביר שבקבוצה השנייה כל השאריות שונות מזו וזה יסביר ששתי הקבוצות זהות.
נניח בשלילה שקיימים a, a' שונים כך ש-

$$qa \cdot (-1)^{r_a} \equiv qa' \cdot (-1)^{r_{a'}} \; mod \; p$$

נצמצם את q ונקבל ש-$a \equiv \pm a'$ אבל a ו-a' זוגיים ולכן לא יכולים להיות מינוס זה של זה, לפיכך $a = a'$ בסתירה.

מצאנו שתי קבוצות זהות, נכפיל את האיברים של כל אחת מהקבוצות ונשווה בין המכפלות:

$$\prod_{2|a} a \equiv \prod_{2|a} aq(-1)^{r_a} \; mod \; p$$

מכפלת ה-aים מתקזזת ואנו נשארים עם:

$$1 \equiv q^{\frac{p-1}{2}}(-1)^{\sum r_a} \; mod \; p$$

במילים אחרות קיבלנו:

$$\left(\frac{q}{p}\right) \equiv (-1)^{\sum r_a} \; mod \; p$$

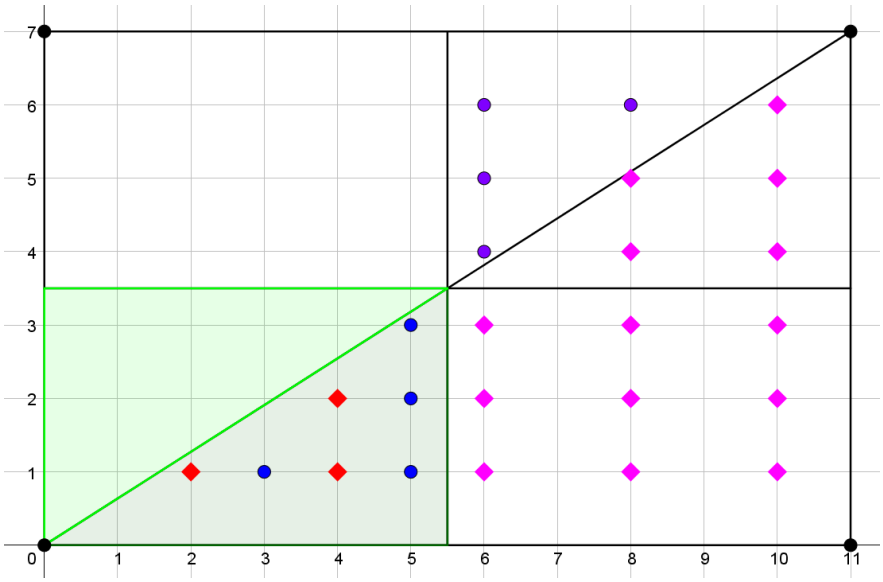
שני הגפים שווים ל-1 בערכם המוחלט ולכן השוויון האחרון כמובן נכון גם ללא מודולו. נשאר להבין את הזוגיות של $\sum r_a$. נבין את r_a בצורה "גיאומטרית": נצייר מלבן $[0,p] \times [0,q]$ ונטען ש-$\sum r_a$ סופר את כמות הנקודות עם קואורדינטה x זוגית, שנמצאות בתוך המלבן אבל מתחת לאלכסון. אכן משוואת האלכסון היא $y = \frac{qx}{p}$ כאשר נציב $x = a$ נקבל ש-$y = \frac{qa}{p}$ וכמות הנקודות השלמות מתחת לנקודה הזו שווה בדיוק ל-r_a.
נחלק את הנקודות שלנו לשתי קבוצות, נקודות אדומות שנמצאות בחצי הראשון (כלומר כאשר $a < \frac{p}{2}$) ונקודות וורודות שנמצאות בחצי השני (כלומר $a > \frac{p}{2}$), ראו איור להמחשה עבור $p = 11, q = 7$. נחליף את הנקודות הוורודות בנקודות שנמצאות בחצי השני אבל מעל לאלכסון,

נקרא לנקודות אלו סגולות. בכל עמודה החלפנו r_a נקודות וורודות ב-$q-1-r_a$ נקודות סגולות ולכן לא שינינו את זוגיות של כמות הנקודות. נשקף את הנקודות הסגולות ביחס למרכז המלבן, את הנקודות המשוקפות נצבע בכחול. נשים לב שהנקודות הכחולות נמצאות מתחת לאלכסון ויש להן קואורדינטה x אי-זוגית. הנקודות האדומות והכחולות ביחד נותנות את כל הנקודות בחצי הראשון שנמצאות מתחת לאלכסון (השטח שצבוע בירוק קהה בציור), נסמן את הכמות הזו ב-n.

נסכם, קיבלנו ש-

$$\sum r_a \equiv n \ mod \ 2$$

או במילים אחרות ש-$\left(\frac{q}{p}\right) = (-1)^n$.



באופן דומה נקבל ש-$\left(\frac{p}{q}\right) = (-1)^m$ כאשר m מסמן את כמות הנקודות השלמות שנמצאות במלבן, שקואורדינטת ה-y שלהן קטנה מ-$\frac{q}{2}$ ונמצאות בין האלכסון לציר ה-y (השטח שצבוע בירוק בהיר בציור). נשים לב ש-$m+n$ שווה לכמות הנקודות השלמות שנמצאות ברבע הראשון של המלבן (השטח הירוק), כלומר הנקודות שנמצאות בתוך המלבן $\left[0,\frac{p}{2}\right] \times [0,\frac{q}{2}]$, לפיכך $m+n = \frac{p-1}{2} \cdot \frac{q-1}{2}$ ולפיכך נובע:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

<u>הוכחה שלישית, גרסה ראשונה.</u>

נסמן ב-K_p את כמות הפתרונות שיש למשוואה

$$x_1^2 - x_2^2 + x_3^2 - \ldots + x_p^2 = 1$$

מעל ל-$\mathbb{Z}_{/q}$. נחשב את K_p בשתי דרכים.

<u>דרך ראשונה:</u> נספור את כמות הדרכים לכתוב את 1 כסכום של p שאריות, לכל דרך נחשב את כמות האפשרויות לקבל אותה בתור פתרון למשוואה. כלומר אנחנו מסתכלים על כל השאריות $a_1, \ldots, a_p$ שסכומן הוא 1 מוד q וכך שכל $a_i \equiv (-1)^{i+1} x_i^2$. לשקילות האחרונה יש בדיוק

$$1 + \left(\frac{(-1)^{i+1} a_i}{q}\right)$$

פתרונות ולכן כמות הפעמים שאפשר לקבל את $a_1, \ldots, a_p$ בתור פתרון למשוואה היא

$$\prod_{i=1}^{p} \left(1 + \left(\frac{(-1)^{i+1} a_i}{q}\right)\right)$$

ולפיכך הנוסחה ל-K_P היא:

$$K_p = \sum_{a_1 + a_2 + \ldots a_p = 1} \prod_{i=1}^{p} \left(1 + \left(\frac{(-1)^{i+1} a_i}{q}\right)\right)$$

נפתח סוגרים במכפלה, יש שלושה סוגים של ביטויים שיתקלו בפתיחת סוגריים: מכפלה של 1ים, מכפלה שבה כל ה-a_i מופיעים ושאר המכפלות בהן לפחות אחד מה-a_i מופיע ולפחות אחד לא מופיע. נטען שלכל מחובר מהסוג השלישי הסכום הכולל על כל ההצבות האפשריות ל-a_iים, מתאפס. נניח ללא הגבלת הכלליות ש-a_2 מופיע במכפלה ו-a_1 לא מופיע בה. נשים לב שהתנאי $a_1 + \ldots + a_p \equiv 1$ לא רלוונטי יותר כיוון ש-a_1 ידאג להביא את המכפלה ל-1. כלומר אנחנו רוצי להוכיח ש-

$$\sum_{a_2, \ldots, a_p} \left(\frac{a_2 \cdot \ldots \cdot a_p}{q}\right) \stackrel{?}{=} 0$$

כאשר מבין $a_3, \ldots, a_p$ חלק מהגורמים עלולים לא להופיע במכפלה.

ראשית נתעלם מהמחוברים בהם אחד מבין $a_2,..,a_p$ שווה ל-0. נשים לב שלכל $1 \le t \le q-1$ ולכל בחירה של הערכים של $a_3,\dots,a_p$ קיים ערך יחיד של a_2 עבורו $\left(\frac{a_2\cdot\dots\cdot a_p}{q}\right)=t$ ולפיכך מתקיים ש-

$$\sum_{a_2,\dots,a_p}\left(\frac{a_2\cdot\dots\cdot a_p}{q}\right)=\sum_{t=1}^{p-1}\sum_{1\le a_3,\dots,a_p\le q-1}\left(\frac{t}{q}\right)$$
$$=(q-1)^{p-2}\sum_{t=1}^{p-1}\left(\frac{t}{q}\right)=0$$

כאשר השוויון האחרון נובע מכך שבדיוק מחצית מהשאריות הן שאריות ריבועיות.

סך הכל נקבל ש-

$$K_p=\sum_{a_1+a_2+\cdots a=1}1+\left(\frac{(-1)^{\frac{p-1}{2}}a_1\dots a_p}{q}\right)\equiv$$

$$\equiv q^{p-1}+\left(\frac{(-1)^{\frac{p-1}{2}}p^{-p}}{q}\right)\ mod\ p\equiv 1+(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{p}{q}\right)$$

<u>דרך שנייה:</u> נחליף משתנים, x_1 יוחלף ב-x_2+x_1 ונקבל:

$$x_1^2+x_3^2-\dots+x_p^2-1=-2x_1x_2$$

נחלק את קבוצת הפתרונות לשתיים: מתי ש-$x_1=0$ ומתי ש-$x_1\neq 0$. אם $x_1=0$ אז יש qK_{p-2} פתרונות כי x_2 יכול להיות כל דבר ואחרי זה נשאר עם אותה המשוואה אבל x_1,x_2 נמחקו. במקרה השני, לכל בחירה של $x_3,x_4,\dots,x_p$ ו-$x_1\neq 0$ קיים x_2 יחיד, כלומר יש $q^{p-2}(q-1)$ פתרונות כאלו. קיבלנו את הנוסחה:

$$K_p=q^{p-1}-q^{p-2}+qK_{p-2}=q^{p-1}-q^{p-3}+q^2K_{p-4}=\dots$$
$$=q^{p-1}-q^{\frac{p-1}{2}}+q^{\frac{p-1}{2}}K_1$$

ברור ש-$K_1=2$ ולכן $K_p=q^{p-1}+q^{\frac{p-1}{2}}$.

נשווה בין שני הביטויים ונקבל ש-

$$1 + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) \equiv 1 + \left(\frac{q}{p}\right) \ mod\ p$$

וזה מה שרצינו.

<u>הוכחה שלישית, גרסה שנייה.</u>

הפעם נספור את כמות הנקודות על ספירה q ממדית מעל $\mathbb{Z}/p$. כלומר נספור את כמות הפתרונות למשוואה:

$$x_1^2 + x_2^2 + \ldots x_{q-1}^2 + x_q^2 = 1$$

כאשר $x_i \in \mathbb{Z}_{/p}$. נסמן ב-K_q את כמות הפתרונות.

ראשית נחשב את $K_q \ mod\ q$. נשים לב שלכל פתרון $(x_1, x_2, \ldots, x_q)$ ולכל $a \in \mathbb{Z}_{/q}$ גם $(x_{a+1}, x_{a+2}, \ldots, x_{a+q})$ הוא פתרון. יתר על כן, לכל a מתקבל פתרון שונה, אלה אם $x_1 \equiv \cdots \equiv x_q \ mod\ p$. קיבלנו שקבוצת הפתרונות מתחלקת ל-qיות של פתרונות ועוד קצת פתרונות ש-"נשארים בצד" ולא נכנסים ל-qיות שלנו. הפתרונות שנשארים בצד מתאימים לפתרונות של המשוואה

$$qx^2 = 1\ mod\ p$$

ויש בדיוק $1 + \left(\frac{q}{p}\right)$ פתרונות למשוואה הזו. סך הכל קיבלנו ש-

$$K_q = 1 + \left(\frac{q}{p}\right)\ \ mod\ q$$

כעט נחשב את K_q במדויק. נעשה זאת באופן אינדוקטיבי. נעביר אגפים במשוואה:

$$x_1^2 + x_2^2 + \ldots + x_{q-2}^2 = 1 - x_{q-1}^2 - x_q^2$$

אם $x_{q-1}^2 + x_q^2 = r$ אז אנחנו רוצים סופרים נקודות על ספרה $q-2$ ממדית שהרדיוס בריבוע שלה הוא $r-1$. לכל r נחשב את כמות הדרכים להציג אותו בתור $x_{q-1}^2 + x_q^2$, נסכום על כל ה-rים ונקבל נוסחה רקורסיבית לכמות הנקודות על ספירה q ממדית כתלות בספרות $q-2$ ממדיות.

נסמן ב-$K_{n,r}$ את כמות הנקודות על ספירה n ממדית שהרדיוס בריבוע שלה הוא r. נתחיל מהמקרה הדו ממדי, כלומר נחשב את כמות הפתרונות ל-$x_{q-1}^2 + x_q^2 = r$. נספור את כמות הדרכים לכתוב את r

כסכום של שתי שאריות: $r = a + b$, כל אופציה אמורה להיספר $\left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right)$ פעמים, הרי יש $1 + \left(\frac{a}{p}\right)$ פתרונות ל-$x_q^2 = a$ וכנ"ל עבור b. לפיכך נקבל ש-

$$K_{2,r} = \sum_{a+b=r} \left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right)$$
$$= \sum_{a+b=r} \left(1 + \left(\frac{a}{p}\right) + \left(\frac{b}{p}\right) + \left(\frac{ab}{p}\right)\right)$$

המחוברים $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right)$ נסכמים ל-0 הרי a עובר על כל שארית פעם אחת בדיוק ויש כמות זהה של שאריות ריבועיות ולא ריבועיות. בשביל לחשב את הסכום על המחובר האחרון, נציב $b = r - a$ ונקבל שצריך לחשב את הסכום: $\sum \left(\frac{a(r-a)}{p}\right)$. נתעלם מהמחובר שמתאים ל-$a = 0$, הוא בכל מקרה מתאפס. בכל מחובר אחר, נחלק ב-a^2 את הביטוי בתוך הסוגריים ונקבל:

$$\sum_a \left(\frac{a(r-a)}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{\frac{r}{a} - 1}{p}\right) = -\left(\frac{-1}{p}\right)$$

אם $r \neq 0$ אז $\frac{r}{a} - 1$ עובר על כל השאריות למעט השארית -1 ולכן הסכום שווה ל-$-\left(\frac{-1}{p}\right)$. אם $r = 0$ אז כל המחוברים בסכום שווים ל-$\left(\frac{-1}{p}\right)$. סך הכל נקבל ש-

$$K_{2,r\neq 0} = p - \left(\frac{-1}{p}\right), \qquad K_{2,0} = p + (p-1) \cdot \left(\frac{-1}{p}\right)$$

נציב את הביטויים שקיבלנו בנוסחה עבור $K_{n,r}$:

$$K_{n,r} = \sum_{0 \leq x_{n-1}, x_n \leq p} K_{n-2, a - x_{n-1}^2 - x_n^2} =$$

$$= \left(p - \left(\frac{-1}{p}\right)\right) \sum_{0 \le a \le p-1, a \ne r} K_{n-2,a} + K_{n-2,r}\left(p + \left(\frac{-1}{p}\right)(p-1)\right) =$$

$$= \left(p - \left(\frac{-1}{p}\right)\right) \sum_{a=0}^{p-1} K_{n-2,a} + K_{n-2,r}\left(p\left(\frac{-1}{p}\right)\right)$$

נשים לב שהסכום במחובר הראשון שווה ל-p^{n-2}, הרי כל נקודה במרחב ה-$n-2$ ממדי נמצאת על ספירה מרדיוס כלשהו ולפיכך נקבל ש-

$$K_{n,r} = p^{n-1} - \left(\frac{-1}{p}\right)p^{n-2} + K_{n-2,r}\left(p\left(\frac{-1}{p}\right)\right)$$

זו נוסחה רקורסיבית שנוכל להמשיך לפתוח. נציב ב-$K_{n-2,r}$ ביטוי דומה שתלוי ב-$K_{n-4,r}$ נקבל ש-

$$K_{n,r} = p^{n-1} - \left(\frac{-1}{p}\right)p^{n-2} + \left(\frac{-1}{p}\right)p^{n-2} - p^{n-3}\left(\frac{-1}{p}\right)^2 +$$

$$+p^2\left(\frac{-1}{p}\right)^2 K_{n-4,r} = p^{n-1} - p^{n-3}\left(\frac{-1}{p}\right)^2 + p^2\left(\frac{-1}{p}\right)^2 K_{n-4,r}$$

נבחר $n = q, r = 1$ ונמשיך באופן דומה עד שנגיע ל-$K_{1,1}$ שכמובן שווה ל-2. סך הכל נקבל את הנוסחה הבאה:

$$K_{q,1} = p^{q-1} - p^{\frac{q-1}{2}}\left(\frac{-1}{p}\right)^{\frac{q-1}{2}} + p^{\frac{q-1}{2}}\left(\frac{-1}{p}\right)^{\frac{q-1}{2}} K_{1,1} =$$

$$= p^{q-1} + p^{\frac{q-1}{2}}\left(\frac{-1}{p}\right)^{\frac{q-1}{2}}$$

נעשה מודולו q ונשווה עם הביטוי האחר שקיבלנו. מהנוסחה שפיתחנו כרגע נובע ש-

$$K_q \equiv 1 + \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \; mod\; q$$

ולפני כן הוכחנו ש-

$$K_q = 1 + \left(\frac{q}{p}\right) \; mod\; q$$

נשווה בין הביטויים ונצחנ!

הוכחה רביעית

נתבונן ב-$Z^*_{/pq}$, כלומר כל השאריות מודולו pq שזרות ל-pq. יש $(p-1)(q-1)$ שאריות כאלו, נחלק אותן לשתי קבוצות כך שמבין כל זוג שאריות $(x,-x)$ תבחר בדיוק שארית אחת. יש מספר דרכים לעשות זאת. ראשית ניתן לבחור את השאריות שקטנות מ-$\frac{pq}{2}$, זה כמובן מקיים את התנאים.
דרך נוספת לעשות את החלוקה משתמשת במשפט השאריות הסיני שאומר שקיימת התאמה חח"ע ועל בין השאריות ב-$Z^*_{/pq}$ לבין זוגות של שאריות ב-$Z^*_{/p} \times Z^*_{/q}$. בשביל החלוקה שלנו נבחר את כל השאריות ב-$Z^*_{/pq}$ שמתאימות לזוגות $(a,b) \in Z^*_{/p} \times Z^*_{/q}$ כאשר $1 \le a \le \frac{p-1}{2}$. קל לראות שהחלוקה הזו מקיימת את התנאי שרצינו, בחרנו בדיוק חצי משאריות מודולו pq וקל לראות שלא בחרנו שתי שאריות x,y כך ש-$x \equiv -y \ mod \ pq$, אכן אם זה היה המצב אז $x \equiv -y \ mod \ p$ בסתירה לכך ש-$1 \le a \le \frac{p-1}{2}$.

מכל זוג $(x,-x)$ נבחרה בדיוק שארית אחת ולכן מכפלת כל האיברים בקבוצה הראשונה שווה עד כדי סימן למכפלת האיברים בקבוצה השנייה.

נחשב את המכפלה בכל קבוצה במודולו p ומודולו q, ונשווה בין שתי המכפלות.

נתחיל מהקבוצה השנייה שבנינו, נסמן את מכפלת האיברים שלה ב-Π_2. מתקיימת השקילות הבאה:

$$\Pi_2 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^{q-1} \ mod \ p$$

נשים לב ש-$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (p-1)! \cdot (-1)^{\frac{p-1}{2}} \ mod \ p$ ולכן

$$\Pi_2 \equiv \left((p-1)! \cdot (-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}+\frac{q-1}{2}} mod \ p .$$

עכשיו נחשב את המכפלה מודולו q:

$$\Pi_2 \equiv \left((q-1)!\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} mod \ q .$$

נעבור לקבוצה הראשונה: נחלק את אברי הקבוצה ל-$\frac{q-1}{2}-1$ בלוקים מהצורה $p\cdot k+1,\dots,p(k+1)-1$, כאשר $0\le k\le \frac{q-1}{2}-2$ ועוד "חצי בלוק" נוסף $\left(\frac{q-1}{2}-1\right)\cdot p+1,\dots,\left(\frac{q-1}{2}-1\right)\cdot p+\frac{p-1}{2}$.

נשים לב שלא כל המספרים בבלוקים האלו נמצאים בקבוצה, הרי עלינו להוריד את המספרים שמתחלקים ב-q. כלומר עלינו להוריד את המספרים $q, 2q, \dots, \frac{p-1}{2}\cdot q$.

מודולו p, מכפלת האיברים בכל בלוק היא $(p-1)!$ והמכפלה של החצי בלוק האחרון היא $\left(\frac{p-1}{2}\right)!$. סך הכל נקבל:

$$\Pi_1 \equiv \frac{\left((p-1)!\right)^{\frac{q-1}{2}}\cdot\left(\frac{p-1}{2}\right)!}{q\cdot 2q\cdot\ldots\cdot\left(\frac{p-1}{2}\cdot q\right)} \equiv \frac{\left((p-1)!\right)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}}$$
$$\equiv \frac{\left((p-1)!\right)^{\frac{q-1}{2}}}{\left(\frac{q}{p}\right)} \equiv (-1)^{\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right)\ mod\ p$$

באופן דומה נקבל ש-

$$\Pi_1 \equiv (-1)^{\frac{p-1}{2}}\cdot\left(\frac{p}{q}\right)\ mod\ q$$

נזכור ש-$\Pi_1 \equiv \pm 1\cdot\Pi_2\ mod\ pq$ ולכן יש שתי אפשרויות, או ש-$\Pi_1 \equiv \Pi_2\ mod\ p$ ו-$\Pi_1 \equiv \Pi_2\ mod\ q$ או ש-$\Pi_1 \equiv -\Pi_2\ mod\ p$ ו-$\Pi_1 \equiv -\Pi_2\ mod\ q$, לא יתכן ש-$\Pi_1 \equiv \Pi_2\ mod\ p$ אבל $\Pi_1 \equiv -\Pi_2\ mod\ q$.

מודולו q ההבדל בסימן בין Π_1 ל-Π_2 הוא $\left(\frac{p}{q}\right)$ ואילו מודולו p ההבדל בסימנים הוא $\left(\frac{q}{p}\right)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. כפי שאמרנו, ההבדלים בסימנים צריכים להיות שווית ולכן

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$