# טענות בתורת המספרים

***<u>הגדרות:</u>***

- מספר a יקרא הפיך אם קיים b כך ab=1 . (1 = איבר היחידה בחבורה)
- מספר a יקרא אי פריק אם a לא הפיך ולכל פירוק a=bc או b או c הפיכים.
- מספר טבעי a יקרא מורכב אם a=bc ו $b > 1, c > 1$
- מספר טבעי יקרא ראשוני אם הוא שונה מ1 ואינו מורכב, כלומר יש לו רק שני מחלקים שונים טבעיים.
- $\gcd(a,b) = d \leftrightarrow d|a, d|b \; and \; \forall c: c|a \; c|b \rightarrow c|d$. יחיד עד כדי כפל בהפיך.
- נאמר a,b זרים אם $\gcd(a,b) = 1$
- פולינום יקרא מתוקן אם המקדם של החזקה הגבוה ביותר שלו הוא אחד.

***<u>חלוקה:</u>***

- $a|b \; \wedge \; b|a \; \rightarrow a = \pm b$
- $a|b \; \wedge \; b|c \; \rightarrow a|c$
- <u>חלוקה בשארית:</u> עבור a,b מספרים שלמים קיימם q,r כך ש $a = qb + r$ ו $r < b$. הוכחה מהסתכלות על הקבוצה $a - xb$ לכול x שלם ולקיחת האיבר האי שלילי הקטן ביותר.
- $a|bc \; and \; \gcd(a,b) = 1 \rightarrow a|c$ נובע מכך שלשני איברים יש צ"ל שהוא ה gcd, ואז הכפלה בc.
- אם $a_i$ זר ל m לכול i אז המכפלה שלהם גם זרה ל m.
- אם $\gcd(a_i, a_j) = 1$ לכול i,j שונים ו $a_i|n$ לכול i אז המכפלה שלהם גם מחלקת את N. נובע מאינדוקציה והעובדה שכול איבר זר למכפלת כול השאר ולכן ניתן לכתוב צ"ל שלהם שייתן אחד ואז נכפיל באן את שני האגפים.
- $p|\binom{p}{k}$ לכול $1 \leq k < p$ כי $p! = \binom{p}{k} k! \, (p-k)!$ ומתקיים $p|p!$ וכמו כן $p \nmid k! \, (p-k)!$ כי p ראשוני וk קטן מ p ושונה מאפס. לכן $p|\binom{p}{k}$

***<u>ראשוניים:</u>***

- כול מספר שלם שונה מאפס הוא מכפלה של ראשוניים ו -1. הוכחה באינדוקציה מפגרת. ולכן לכול מספר שלם a ומספר ראשוני p נסמן $ord_p(a)$ להיות החזקה הגבוה ביותר של p שמחלקת את a.
- בתחום אוקלידי לכול p ראשוני מתקיים $p|bc \rightarrow p|b \; or \; p|c$
- הפירוק לראשוניים בZ הוא יחיד והחזקה של כול ראשוני בפירוק היא בדיוק הסדר שלו במספר.
- יש אינסוף ראשוניים. מניחים בשלילה שיש כמות סופית ומייצרים אחד חדש.
- יש אינסוף ראשוניים $p \equiv 3(4)$ כי מספר שהוא 3 מוד 4 לפחות אחד מהגורמים הראשונים שלו הוא שלוש מוד 4 (כי כולם אי זוגיים אז הם או 1 או 3, ואם כולם אחד גם הכפל אחד) לכן נניח שיש כמות סופית, נכפיל את כולם ואז בארבע ונחסיר אחד. זה 3 מוד 4, ולכן יש ראשוני 3 מוד 4 שמחלק אותו, ולכן יצרנו ראשוני חדש.
- יש אינסוף ראשוניים $p \equiv 1(4)$. נניח בשלילה שיש רשימה סופית ונסתכל על $(2p_1 \dots p_n)^2 + 1$ אזי קיים גורם ראשוני p שמחלק אותו. $p \neq p_i$ וכמו כן מתקיים שהמספר לעיל הינו פתרון למשוואה $x^2 \equiv -1 \; (p)$ ולכן 1- הוא שארית ריבועית ולכן $p \equiv 1(4)$ ולכן הרשימה לא סופית.
- <u>משפט דירכלה:</u> עבור סדרה חשבונית $a + nd$ אם $\gcd(a,d) = 1$ אז יש אינסוף ראשוניים בה.
- <u>משפט המספרים הראשוניים:</u> $\lim_{x \to \infty} \frac{\pi(x)}{x/logx} = 1$ כאשר $\pi(x) = |\{p: p \leq x\}|$

- קיים מקום שהחל ממנו בין כול מספר טבעי להוא כפול שתיים יש ראשוני. נובע מחישוב גבולות ומשפט המספרים הראשוניים.
- השארת רימאן: $|\pi(x) - \int_0^x \frac{1}{\log t} dt| < \frac{1}{8\pi}\sqrt{x}logx$
- עבור מספר גדול מספיק יש ראשוני בינו לבין איקס ופעמים הוא והמספר הזה הוא 2567. נובע ממשחקי חדווא עם הטענה לעיל.
- השערת גולדבאך: כול מספר זוגי גדול מארבע הוא סכום של שני ראשוניים(לא בהכרח שונים)
- השערת טרנארי: כול מספר אי זוגי הוא גדול מחמש סכום של שלושה ראשוניים (מוכח!)
- השערת התאומים: יש אינסוף ראשוניים שההפרש בינהם הוא 2. (הוכח השנה שיש אינסוף ראשנויים שההפרש בינהם קטן מ70 מיליון)
- מספרי מרסן: $2^p - 1$ אם נרצה שזה יהיה ראשוני אז $a = 2$ ו $n\ prime$ כי $a - 1|a^n - 1$ (נוסחא פשוטה) וכנ"ל אם n מורכב. לכן נרצה $2^p - 1$
- המשפט האחרון של פרמה: $x^n + y^n = z^n$ לא קיימים פתרונות שלמים עבור $n > 2$

***משוואות לינאריות:***

- הגדרה: משווה דויפאנטית לינארית $ax + by = c$ כאשר פותרים עבור x,y שלמים. תנאי הכרחי לקיום פתרון $\gcd(a,b)|c$. ואם זה מתקיים אז יש אינסוף, כך שאם $x_0, y_0$ פתרון אז כול פתרון אחר $x = x_0 + \frac{b}{d}n; y = y_0 - \frac{a}{d}n$ כאשר $d = \gcd(a,b)$. והפתרון $x_0, y_0$ נובע מכתיבת a,b כסכום שמניב את המ.מ.מ ואז הכפלה במה שצריך כדי לקבל את c. העובדה שכול פתרון אחר הוא מהצורה הנ"ל נובעת מחיסור המשוואת, חלוקה ב d והעובדה שלאחר החלוקה הם זרים.
- הגדרה: קונגרואנציה לינארית $ax \equiv b(m)$ כאשר פותרים עבור x וכול השאר שלמים. יש פתרון אמ"מ $\gcd(a,m)|b$ מאותה הסיבה כמו לעיל. ואם יש פתרון אז יש בדיוק $\gcd(a,m)$ פתרונות שונים מודולו m בדיוק כמו לעיל.

***חוגים:***

- קבוצה עם שתי פעולות, אסוציאטיביות, קומוטטיביות לחיבור, איבר אפס, איבר יחידה! ופילוג וקיום איבר נגדי לחיבור.
- אידאל: תת קבוצה של חוג אם היא סגורה לחיבור בתוך עצמה, ולכפל בכול איבר בחוג. אידאל ראשי הוא אידאל שמוגדר ככול האברים שהם כפל באיבר כלשהו בחוג.
- כול אידאל ב Z הוא אידאל ראשי, למעשה כול אידאל בתחום אוקלידי הוא אידאל ראשי, נובע מקיום חלוקה בשארית ולקיחת איבר חיובי מינמלי, שהוא למעשה ה gcd.
- מחלק אפס x הינו איבר בחוג שונה מאפס כך שקיים y שונה מאפס כך ש $xy = 0$
- תחום שלמות הוא חוג ללא מחלקי אפס. למשל חוג השלמים.
- תחום אוקלידי הוא תחום שלמות עם העתקת נורמה וחלוקה בשארית. בתחום שלמות כול אידאל הוא ראשי, יש מ.מ.מ, כול איבר לא הפיך הוא מכפלה של אי פריקים, כול איבר אי פריק הוא ראשוני כלומר $\pi|ab$ ו $\pi$ אי פריק אז הוא מחלק לפחות אחד מהם ויש פירוק יחיד לראשוניים.
- הפיכים: עבור חוג A נגדיר $A^x = \{a \in A : a|1\}$. זו חבורה.

***קונגרואנציה:***

- הגדרה: $a \equiv b\ mod(m) \leftrightarrow m|(a-b)$ , זה יחס שקילות.
- מחלקות קונגרואציה: קבוצת כול האיברים שקונגרואנטים מודלו m. יש בדיוק m כאלה, לא יכול להיות יותר מחלוקה בשארית, ולא פחות כי ההפרש בין שניים קטן מ m.
- השאריות מתנהגות יפה בחיבור ובכפל, הן למעשה חוג ונסמן $Z/_{nZ}$. עבור n ראשוני זה למעשה שדה כי למשוואה $ax \equiv 1(n)$ יש בדיוק פתרון אחד לכול a זר ל n ואם n ראשוני זה כולם, ולכן כולם הפיכים ולכן שדה.

- <u>משפט השאריות הסיני:</u> עבור מערכת המשוואות $x \equiv b_i \ mod(m_i)$ אם $m_i$ זרים אז יש פתרון, וכול שני פתרונות נבדלים בm כאשר $m = \Pi m_i$. לכול גורם $m_i$ נסתכל על מכפלת כול השאר מלבד הוא, היא זרה לו ולכן יש צירוף שלהם שנותן 1. $r_i m_i + s_i n_i = 1$ כאשר $n_i$ זה מכפלת כול השאר. נסתכל רק על $s_i n_i$ ברור כי הוא מקיים $s_i n_i \equiv 0(m_j)$ לכול $j \neq i$ ו $s_i n_i \equiv 1(m_i)$ ולכן נכפיל ב $b_i$ ונקבל כי $x_0 = \sum b_i s_i n_i$ הוא פתרון למערכת. כול שני פתרונות נבדלים ב$m_i$ בכול רכיב בנפרד ולכן ב m סה"כ.
- $a \equiv b(p^l)$ אז מתקיים $a^p \equiv b^p(p^{l+1})$ כי $a = b + c * p^l$ לכן $a^p = b^p + b^{p-1}cp^{l+1} + A$ מנוסחאת הבינום כאשר כול האיברים ב A מכילים חזקה של p שגדולה מ l+1 ולכן $a^p \equiv b^p\left(p^{l+1}\right)$
- עבור ראשוני שונה משתיים $(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1}\ \left(p^l\right)$ לכול a שלם. מוכיחים באינדוקציה ושמים לב כי $\left((1 + ap)^{p^{l-2}}\right)^p \equiv \left(1 + ap^{l-1}\right)^p\ (p^{l+1})$ מהנחת האינדוקציה פלוס הטענה שלעיל ולכן מחוקי חזקות $(1 + ap)^{p^{l-1}} \equiv 1 + ap^l + B\ \left(p^{l+1}\right)$ כאשר B נוצר מנוסחאת הבינום ולכן $B \equiv 0\left(p^{l+1}\right)$

***<u>פונקציית אוילר:</u>***

- <u>הגדרה:</u> $\phi(m) = |\{1 \leq x \leq m: \gcd(x, m) = 1\}|$ או במילים אחרות כמה איברים הפיכים יש בחוג $Z/_{mZ}$
- <u>משפט אוילר:</u> $a^{\phi(m)} \equiv 1(m)$ לכול a,m כך ש $m > 2\ ; \gcd(a, m) = 1$. נובע מהעובדה שההפיכים מודולו m זה חבורה אבלית מגודל $\phi(m)$
- <u>משפט פרמה:</u> (מקרה פרטי של אוילר) $a^{p-1} \equiv 1(p)$ לכול p ראשוני.
- $\phi\left(p^l\right) = p^l - p^{l-1} = (p-1)p^{l-1}$ (ברור, כי רק החזקות של p לא זרות לו)
- פונקציית אוילר כפלית עבור מספרים זרים. נובע מהסתכלות על חבורת ההפיכים מודולו המכפלה שלהם ולעשות ממנה איזומורפיזם של חבורות לחבורה שהיא המכפלה הקרטזית של ההפיכים מודלו אחד כפול ההפיכים מודולו השני. זה איזומורפיזים כי הם זרים ולכן יש פתרון יחיד ממשפט השאריות. ולכן יש שוויון עוצמות.
- $m = \Pi p_i^{q_i}$ אז $\phi(m) = \mathrm{m}\Pi(1 - \frac{1}{\mathrm{p_i}})$
- <u>משפט גאוס:</u> $n = \sum_{(d|n)} \phi(d)$. נחלק את כול המספרים $\{1,2, \dots, n\}$ לקבוצות זרות לפי ה gcd שלהם עם n ונסמן $S_d$ קבוצת כול האיברים שהgcd שלהם עם n הוא d. ברור שיהיו לנו קבוצות כאלה כמספר המחלקים של n. נשים לב $|S_d| = \left|\left\{S: \gcd\left(S, \frac{n}{d}\right) = 1\right\}\right| = \phi(\frac{n}{d})$ ולכן משום שאיחוד כול הקובצות הללו זה כול n נקבל $n = \sum_{(d|n)} \phi(\frac{n}{d}) = \sum_{(d|n)} \phi(d)$
- יש בדיוק $\phi(d)$ איברים מסדר d עבור $d|(p-1)$ ו p ראשוני. ממשפט גאוס $p - 1 = \sum_{(d|p-1)} \phi(d)$ וכמו כן p-1 זה מספר האיברים ההפיכים מודולו p ולכן מתקיים כי $p - 1 = \sum_{(d|p-1)} \psi(d)$ כאשר $\psi(d)$ זה מספר האיברים שהם מסדר d וזה נובע מכך שכול סדר מחלק את גודל החבורה, ושלכול איבר יש סדר אחד בדיוק ולכן איחודם זה כול החבורה. לכן $\sum \phi(d) = \sum \psi(d)$ וכעת נוכיח כי $\psi(d) \leq \phi(d)$ ולכן יש שוויון. עבור הפולינום $x^d - 1 = 0$ יש בדיוק d פתרונות והם $\{1, x, x^2, \dots, x^{d-1}\}$ כאשר x איבר מסדר d (נניח $\psi(d) \neq 0$) לכן כול פתרון הוא מהצורה הזו. יהי $y = x^a$ פתרון לפולינום, כלומר איבר מסדר d. אם a לא זר לd נקבל שיש חזקה יותר קטנה של y שתהפוך אותו לאחד ולכן הוא לא באמת מסדר d ולכן a זר ל d. ויש לכול היותר $\phi(d)$ איברים שזרים ל d וקטנים לו ולכן $\psi(d) = \phi(d)$ כנדרש.
- עבור p ראשוני יש בדיוק $\phi(p-1)$ איברים מסדר p-1 כמו שהוכח לעיל, ולכן זו כמות הש"פ, ולכן לכול p ראשוני קיים שורש פרמיטיבי!

***<u>חבורות:</u>***

- <u>הגדרה:</u> קבוצה סגורה של איברים עם פעולה אחת, אסוציאטיבית, קיים איבר יחידה, והופכי לכול איבר. אם היא גם קומוטטיבית לפעולה אז היא אבלית.
- <u>חבורה ציקלית:</u> חבורה שקיים איבר a כך שלכול $x \in G$ קיים n כך ש $a^n = x$ (כלומר יוצר)
- ההפיכים בחוג הם חבורה לכפל.
- בחבורה אבלית סופית כול איבר בחזקת גודל החבורה הוא שווה לאיבר היחידה וזה נובע מהעובדה שיש חוק צמצום ולכן אם ניקח את כול האיברים בחבורה ונכפיל בa נקבל n איברים שונים חדשים, אבל יש רק אן איברים ולכן המכפלה שלהם שווה למכפלת האיברים המקורים, היא אבלית ולכן אפשר לשחק עם הכפל ולקבל שa בחזקת גודל החבורה זה ההפיך. לכן נסמן $ord(a)$ להיות החזקה הקטנה ביותר שהופכת את a לאיבר היחידה.

***<u>שורשים פרימיטיבים:</u>***

- אם n זה הסדר של איבר בחבורה אז $\{a, a^1, \dots, a^{n-1}\}$ קבוצה של איברים שונים! כי אחרת אם שניים שווים, נחלק ונקבל סתירה למינמליות של הסדר. כמו כן אלא כול התוצאות שיכולות להתקבל מחזקה של a, מחילוק בשארית בסדר.
- אם $a^m = 1$ אז m הוא כפול של הסדר של a. נובע מחלוקה בשארית ומינמליות הסדר. ולכן הסדר של כול איבר בחבורה מחלק את גודלה (כי הוכחנו שכול איבר בחזקת הגודל זה אחד)
- <u>טענה:</u> איבר הוא יוצר של חבורה אמ"מ הסדר שלה הוא גודלה. נובע מכך שמספר האיברים השונים שיכולים לצאת מהעלאת מספר בחזקה זה הסדר שלו, ולכן כדי שהוא יצור את כולם הסדר שלו צריך להיות כמספר האיברים בחבורה. ולכן חבורה סופית היא ציקלית אמ"מ יש איבר שהסדר שלו הוא גודלה.
- <u>שורש פרימיטיבי:</u> מספר הוא שורש פרימיטיבי מודלו m אם הוא יוצר את חבורות ההפיכים ב $(Z/_{mZ})$, בפרט הוא עצמו הפיך מודלו m (ולכן זר לו)
- אם איבר אינו יוצר בחבורה אז קיים ראשוני בפירוק לראשונים של הסדר כך שהאיבר בחזקת גודל החבורה חלקי הראשוני הזה יוצא אחד.
- לכול ראשוני קיים ש"פ. נובע מכך שמספר האיברים מסדר p-1 הוא $\phi(p-1) \neq 0$
- $ord_{p^l}(1+ap) = p^{l-1}$ לכול a שזר לp. כי $(1+ap)^{p^{l-1}} \equiv \left(1+ap^l\right)\left(p^{l+1}\right)$ לכן $(1+ap)^{p^{l-1}} \equiv 1(p^l)$ ולכן הסדר מחלק את $p^{l-1}$, אבל לכול חזקה קטנה יותר של פי נפעיל שוב את הטענה אבל הפעם עליה ונקבל שזה לא קונג לאחד, ולכן זה בדיוק הסדר.
- לכול $p^l$ קיים ש"פ לכול $l$ ו $p\ prime$. תחילה נקח שורש פרמיטיבי מודולו p, קיים אחד כזה. ניתן להניח כי $g^{p-1} \neq 1(p^2)$ כי אחרת נקח את $g+p$ שגם הוא שורש פרמיטיבי, ולפחות אחד מהם לא 1 מודולו הריבוע (נובע מלפתוח בינום והעובדה ששורש פרמיטיבי זר לראשוני). נראה כי $\phi(p^l)|n$ לכול n שמקיים $g^n \equiv 1(p^l)$ וזה יוכיח שהסדר של g הוא גודל החבורה ולכן ש"פ. נשים לב $\phi(p^l) = (p-1)p^{l-1}$ ומההנחה $g^{p-1} = 1+ap$ כאשר a לא מחלק את P. ולכן מהטענה על הסדר של $1+ap$ נקבל ש $p^{l-1}|n$ לכן $n = p^{l-1}n'$ . ממשפט פרמה מתקיים $g^p \equiv g(p)$ ולכן $1 \equiv g^n(p^l) \to 1 \equiv g^n(p) \to 1 \equiv \left(g^{n'}\right)^{p^{l-1}} \equiv g^{n'}$ ולכן הסדר של g בחבורת ההפיכים מודולו p מחלק את 'n כלומר $(p-1)|n'$ כי g ש"פ ולכן $\phi(p^l)|n$ ולכן זה הסדר, כי הוא בפרט מחלק את הסדר והסדר מחלק אותו ממשפט אוילר.
- לכול $p^l * 2$ גם יש שורש פרמיטיבי. זה נובע מכפליות פונקציות אוליר והעובדה ש $\phi(2) = 1$ ושל$p^l$ יש ש"פ ולכן הוא גם ש"פ מודולו $p^l * 2$ כי שום חזקה שקטנה מהסדר של החבורה הזו לא תהפוך אותו לאחד.
- לשום מספר אחר מלבד $2,4,p,p^l$ אין שורש פרמיטיבי (p לא 2). כי עבור כול $m = m_1 m_2$ מתקיים $\phi(m) = \phi(m_1)\phi(m_2)$ כי הם זרים ושניהם שונים משתיים ולכן הפי שלהם זוגי לכן

נשים לב כי ממשפט אוילר $x^{\frac{\phi(m)}{2}} = \left(x^{\phi(m_1)}\right)^{\frac{\phi(m_2)}{2}} \equiv 1(m_1)$ וכנל עבור $m_2$ ולכן משום שהם זרים יש גם פתרון מודולו המכפלה ממשפט השאריות הסיני, ולכן שום x אינו ש"פ.

- נשים לב שלשמונה אין שורש פרמיטיבי (מבדיקה) ולכן נובע שלכול חזקה של שתיים שגדולה משמונה אין ש"פ כי אם היה הוא היה גם עבור שמונה.
- נשים לב שאם g ש"פ מודולו m אז $g^k$ ש"פ מודולו m אמ"מ $\gcd(k, \phi(m)) = 1$ נובע ממשחקים עם מינמליות הסדר. ולכן בהנתן שקיים ש"פ כלשהו אז יש בדיוק $\phi(\phi(m))$ שורשים פרימיטיבים מודולו m, כי הש"פ הראשון פורש את כול החבורה, ולכן רק החזקות שלו שזרות לפי של אם יהיו גם ש"פ.

***<u>שאריות מסדר n:</u>***

- a זר ל m יקרא שארית מסדר n מודולו m אם קיים איקס כך ש $x^n \equiv a(m)$
- <u>קרטריון אוילר:</u> עבור m שקיים לו ש"פ אז a זר ל m שארית ריבועית מסדר n אמ"מ מתקיים $a^{\frac{\phi(m)}{d}} \equiv 1(m)$ כאשר $d = \gcd(n, \phi(m))$. נשים לב כי קיים ש"פ נסמן g. לכן $a \equiv g^b$ ו $x \equiv g^y$ ולכן $a \equiv x^n$ אמ"מ $g^b \equiv g^{ny}$ אמ"מ $g^{ny-b} \equiv 1$ אמ"מ $ord(g)|(ny - b)$ אמ"מ $ny \equiv b(\phi(m))$ (כי g ש"פ ולכן זה הסדר שלו) ולמשוואה הזו יש פתרון עבור y אמ"מ $\gcd(n, \phi(m)) \mid b$. לכן אם a היא שארית מסדר n אז $\gcd(n, \phi(m)) | b$ ולכן $a^{\frac{\phi(m)}{d}} = g^{b\frac{\phi(m)}{d}}$ ולכן $1 = g^{\phi(m)\frac{b}{d}} = a^{\frac{\phi(m)}{d}}$. מצד שני אם $a^{\frac{\phi(m)}{d}} \equiv 1(m)$ אז $a^{\frac{\phi(m)b}{d}} = 1$ לכן $\phi(m)|\frac{\phi(m)b}{d}$ ולכן $k\phi(m) = \frac{b}{d}\phi(m)$ ולכן $\frac{b}{d} = k$ כאשר k שלם ולכן $b|d$ ולכן יש שארית מסדר n.
- <u>קריטריון אוילר ריבועי:</u> $x^2 \equiv a(p)$ ניתנת לפתרון אמ"מ $a^{\frac{p-1}{2}} \equiv 1(p)$. נובע מהקריטריון הכללי או ניתן להוכיח המקרה הפרטי בעזרת ש"פ.

***<u>שאריות ריבועיות:</u>***

- $a$ שארית ריבועית מודלו $p^l$ אמ"מ הוא שארית ריבועית מודולו $p$. אם יש פתרון מודולו $p^l$ ברור כי אותו הפתרון הוא פתרון גם מודולו p. בהנתן פתרון $b^2 \equiv a(p)$ נבחר g ש"פ מודולו p ומודולו $p^l$ (קיים כזה) אז $a \equiv g^m(p^l)$ ולכן גם $a \equiv g^m(p)$ כמו כן $b \equiv g^n(p)$ לכן $b^2 \equiv g^{2n}(p)$ לכן $g^{2n-m} \equiv 1(p)$ לכן $p - 1|2n - m$ ולכן m זוגי ולכן $m = 2k$ אז $a = g^{2k}(p^l)$ לכן $a = \left(g^k\right)^2(p^l)$ ולכן שארית ריבועית. דרך נוספת להוכיח את זה זה בעזרת למת הנזל, אם יש פתרון מודולו p ניתן להעלות אותו לפתרון מודולו p^k כי הנגזרת לא מתאפסת.
- $a$ שארית ריבועית מודולו חזקה של שתיים רק אם הוא שארית ריבועית מודולו 8. נובע מהעובדה שלחבורת ההפיכים מודולו כול חזקה של שתיים יש שני יוצרים, חמש ומינוס אחד.
- $a$ שארית ריבועית מודלו $m = 2^e p_1^{e_1} \dots p_n^{e_n}$ אמ"מ הוא שארית ריבועית מודולו כול אחד בנפרד. כלומר מתקיים $a^{\frac{p_i-1}{2}} \equiv 1(p_i)$ (נשים לב שהחלקי שתיים נובע מקריטריון אוילר עבור חזקה שתיים והעובדה ש $\phi(p)$ תמיד זוגי לכול ראשוני מלבד 2) ובנוסף a שארית ריבועית מודולו $2^e$ כלומר אם e גדול משלוש אז התנאי שרשום לעיל, אחרת אם e הוא שתיים צריך שa שארית ריבועית מודולו 4. נובע ממשפט השאריות הסיני.
- <u>סימון לג'נדרה:</u> עבור p ראשוני אי זוגי ai שלם נסמן $\left(\frac{a}{p}\right)$ המוגדר להיות 1 אם a שארית ריבועית מודלו p, -1 אם הוא אי שארית, ולא מוגדר אם a לא הפיך מודלו p.
  - $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(p)$ נובע משילוב של קריטריון אוילר ומשפט פרמה.
  - $a \equiv b(p) \rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

- $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. נובע ישירות מסעיף א (אינטואיציה: אם שניהם שארית ריבועית ברור שהכפל גם שארית ריבועית. אם שניהם לא שארית ריבועית אז שניהם נוצרים מחזקה אי זוגית של הש"פ ולכן המכפלה היא חזקה זוגית של הש"פ ולכן שארית ריבועית)

- יש אותה כמות של שאריות ריבועיות כמו של אי שאריות. נובע מהעובדה ש $a^{\frac{p-1}{2}}\equiv\pm1$ יש $\frac{p-1}{2}$ שורשים לכול היותר הן עבור מינוס והן עבור פלוס. אבל לכול איבר בחבורה, אם נעלה אותו בחזקה זו נקבל או אחד או מינוס אחד, ולכן איחוד השורשים שלהם זה כול החבורה ולכן יש p-1 שורשים ביחד, ולכן חצי חצי.
- $-1$ שארית ריבועית מודולו p ראשוני אמ"מ $p\equiv1(4)$ נובע ישירות מנוסחת אוילר.
- 2 שארית ריבועית מודולו p אמ"מ $p\equiv\pm1(8)$ וזה נובע מכך ש $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ וזה נובע שנסתכל על המספרים האי זוגיים כמינוס הנגדי שלהם שהוא זוגי מודולו p אי זוגי. ונקבל שכול מספר קונגרואנטי למינוס אחד אחד בחזקה הנכונה כפול שתיים כפול משהו שקטן ממחצית של p-1. נכפיל את כול המשוואות האלה, נקבל עצרת בשני האגפים, נצמצם ונקבל סכום של סדרה חשבונית ובנוסף נשתמש בקריטריון אוילר.
- ***<u>חוק ההדדיות הריבועית:</u>*** עבור שני ראשוניים $p,q$ אי זוגיים מתקיים כי אם אחד לפחות הוא 1 מוד 4 אז $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$ ואם שניהם 3 מוד 4 אז $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$ (ללא הוכחה!!!) עדיין דורש להיות מסוגלים לפרק לראשוניים כדי לגלות האם שארית ריבועית או לא.
- ***<u>סימן יעקובי:</u>*** עבור b אי זוגי $\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_n}\right)$ כאשר $b=p_1\dots p_n$. נשים לב שהוא מקיים את אותן התכונות שמקיים סימן לגנדרה. נשים לב כי אם סימן יעקובי שווה אחד זה לא אומר שa שארית ריבועית, אבל אם הוא כן שארית אז מובטח שסימן יעקובי הוא אחד.

***<u>הצפנה במפתח פומבי: RSA!!</u>***

- בהנתן מספר כך ש $n=pq$ ו pq ראשוניים אז לדעת את pq זה כמו לדעת את $\phi(n)$ ולא ידוע כיום אלגוריתם פולינמיאלי בלוג המספר.
- צד אחד בוחר שני מספרים ראשוניים גדולים p,q ומכפיל אותם כדי לקבל n. הוא מסוגל לחשב את $\phi(n)$ כי הוא יודע הפירוק לראשונים. לאחר מכן הוא בוחר מפתח e שזה מספר זר ל $\phi(n)$ ומחשב לו הופכי,d, מודולו $\phi(n)$ במהירות(אלגוריתם אוקלידס). לאחר מכן הוא מפרסם את n ואת e שזה המפתח הפומבי. כדי לשלוח הודעה מוצפנת אליו כול בנאדם בעולם צריך לקחת את P הטקסט שלו ולבצע $p^e\ mod(n)$, כדי לפענח כול מה שצריך לעשות זה לקחת את c הטקסט המוצפן ולבצע $c^d mod\ (n)$ ולכן בסופו של דבר נקבל $p^{ed}mod(m)$ אבל $ed\equiv1(\phi(n))$ ולכן ממשפט פרמה נקבל פשוט את p. נשים לב כי בהנתן n קשה מאוד לחשב את $\phi(n)$ כי זה שקול לפירוק לראשונים, ולא ניתן למצוא את ההופכי מבלי לדעת את $\phi(n)$

***<u>בדיקת ראשוניות:</u>***

- <u>עדי פרמה:</u> בהנתן מספר n, מספר b שקטן ממנו יקרא עד פרמה אם $b^{n-1}\neq1(n)$ משום שאם n היא ראשוני אז לא יכול להתקיים b כזה ממשפט פרמה, ולכן b הוא עד שn מורכב.
- <u>מספר קרמייקל:</u> הוא מספר מורכב שאין לו עדי פרמה. כלומר לכול b מתקיים $b^{n-1}\equiv1(n)$ למרות שהוא לא ראשוני.
  - ברור כי מספר קרמייקל לא יכול להיות זוגי כי אז $n-1$ יהיה אי זוגי ואז $-1$ יהיה עד.
  - למספר קרמייקל אין גורם ראשוני שמחלק אותו פעמיים או יותר. נניח בשלילה כי $p^l$ מחלק את n(וL הסדר שלו ב n) אז נסתכל על ש"פ g מודולו $p^l$ מההנחה מתקיים $g^{n-1}\equiv1(n)$ ולכן $g^{n-1}\equiv1(p^l)$ ולכן $n-1|ord_g(p^l)$ ולכן $(p-1)p^{l-1}|n-1$ אבל $l\geq2$ ולכן $p|n-1$ אבל $p|n$ סתירה.

- אם n מספר קרמייקל אז לכול ראשוני $p|n$ מתקיים $p-1|n-1$ וזאת משום שלכול ראשוני קיים ש"פ בחבורת ההפיכים שלו, שהש"פ בחזקת n-1 יתן 1, ולכן הסדר של החבורה מחלק את n-1, וסדר החבורה זה בדיוק p-1 כנדרש.
- אם $n=p_1 \dots p_r$ כך ש $p_i$ ראשוניים אי זוגיים שונים, ומתקיים $p_i-1|n-1$ אז n מספר קרמייקל משום שלכול b קטן מn וזר לו מתקיים $b^{n-1} \equiv 1(p_i)$ לכול p כי הסדר מחלק אותו. ולכן המכפלה שלהם מחלקת את $b^{n-1}-1$ ולכן $b^{n-1} \equiv 1(n)$

- <u>סולובי שטראסה:</u> נשים לב כי אם n ראשוני אי זוגי ו b זר לו אז $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right)(n)$ ולכן בהנתן מספר n אם נמצא עד b כך ש $b^{\frac{n-1}{2}} \neq \left(\frac{b}{n}\right)(n)$ אז n אינו ראשוני. אזי בהנתן מספר אן חשוד נגריל כמות של מספרים שקטנים ממנו ונבדוק שהם זרים לו, אם אחד מהם לו אז הוא מורכב. אם כולם זרים עבור כולם נעלה בחזקה ונשווה לסימן יעקובי שלהם, אם איפשהו אין שוויון אז אן מורכב, אחרת אן עבר את המבחן ובסיכוי חצי במספר האיברים שהגרלנו טעינו והוא למעשה מורכב.
- עבור n מורכב אי זוגי קיים לפחות עד אחד. אם n אינו קרמייקל אז קיים עד פרמה, ואותו העד יהיה גם עד סולובי שטראסה. נניח והוא כן קרמייקל אז אין ראשוני שמחלק אותו פעמיים, ולכן לכול p גורם ראשוני שלו מתקיים $\gcd\left(p,\frac{n}{p}\right)=1$, נבחר b כלשהו אי שארית מודולו p(בהכרח יש כזה) וממשפט השאריות הסיני נמצא $x \equiv b(p)$ ; $x \equiv 1\left(\frac{n}{p}\right)$ לכן x הוא אי שארית מודולו p וכן שארית מודולו $\frac{n}{p}$ ולכן סימן יעקובי $\left(\frac{b}{n}\right)=\left(\frac{b}{p}\right)\left(\frac{b}{n/p}\right)=-1$ אבל בבירור $b^{\frac{n-1}{2}} \equiv 1(\frac{n}{p})$ כי ככה בחרנו אותו ולכן $b^{\frac{n-1}{2}} \neq \left(\frac{b}{n}\right)\left(mod\ \frac{n}{p}\right)$ ולכן גם מודולו n אין שוויון ולכן הוא עד.
- עבור n מורכב ואי זוגי לפחות חצי מהמספרים שקטנים ממנו וזרים לו הם עדי סולובי שטראסה עבורו. תהי $\{a_1, \dots a_k\}$ קבוצה של איברים שונים זרים לn וקטנים ממנו כך שהם לא עדים כלומר $a_i^{\frac{n-1}{2}} \equiv \left(\frac{a_i}{n}\right)(n)$. הוכחנו שקיים לפחות עד b זר לאן אחד לכך שאן מרוכב, כלומר $b^{\frac{n-1}{2}} \neq \left(\frac{b}{n}\right)(n)$. נסתכל על הקבוצה $\{r_1, \dots, r_k\}$ שהיא השאריות של חילוק $a_i b$ ב n. מובטח כי השאריות שונות משום ש $a_i$ שונים וכולם קטנים מאן. כעת נראה כי $r_i \neq a_j$ ולכן קיבלנו 2k איברים שונים זרים לn ולכן $2k \leq \phi(n)$ כנדרש. ברור כי השאריות שונות מ $a_i$ משום שהשאריות הן למעשה עדים כי $r_i^{\frac{n-1}{2}} \neq \left(\frac{a_i}{n}\right)\left(\frac{b}{n}\right) \equiv \left(\frac{r_i}{n}\right)$.
- <u>רבין מילר:</u> בהנתן מספר n חשוד מתקיים $n-1=2^S t$ כך ש t אי זוגי. נגריל בסיס b כלשהו זר ל n וקטן ממנו, נחשב את הסדרה הבאה $a_0 = b^t(n)\ a_1 = a_0^2(n) \dots a_s = b^{2^s t}(n)$. אם האיבר הראשון בסדרה הוא פלוס מינוס אחד נאמר כי אן עובר את המבחן ונגריל בסיס אחר. אם האיבר הראשון אינו פלוס מינוס אחת אבל איפשהו לאורך הסדרה מופיע $-1$ גם כן נאמר שאן עבר ונגריל אחד אחר. אולם אם האיבר הראשון אינו פלוס מינוס אחת ולאורך כול הסדרה מלבד האיבר האחרון ממש, כולם שונים ממינוס אחד אז אן אינו ראשוני, כי אם הוא היה ראשוני אז מפרמה האיבר הממש אחרון היה 1 ולכן אם מדובר בשדה ראשוני, ולא התחלנו מאחד בתחילת השרשרת אז איפשהו בדרך היינו חייבים לעבור במינוס אחד, כי יש רק שני מספרים שהם בריבוע נותנים אחד(במידה והוא אכן ראשוני וזה שדה).
  - <u>עדים:</u> נשים לב כי עדי פרמה הם גם עדי רבין מילר, משום שעבור עד פרמה $a_s \neq 1(n)$ ולכן מובטח שבשום מקום לאורך השרשרת לא היה אחד או מינוס אחד ולכן זה גם עד רבין מילר.
  - לכול מספר קיים עד רבין מילר. אם הוא מהצורה $p^l$ הוא אינו קרמייקל ולכן יש עד פרמה ולכן גם עד רבין מילר. אם הוא לא מהצורה הזו אז ניקח $p^l|n$ כך ש $l$ זה הסדר שלו לכן ממשפט השאריות הסיני אפשר למצוא b כך ש $b \equiv 1(n/p^l)$ ו $b \equiv -1(p^l)$ ולכן עבור האיבר הראשון בסדרה $a_0 \equiv b^t(n)$ משום שt אי זוגי מובטח $a_0 \equiv -1\ (p^l)$ וכמו כן

$(n/p^l)$ $a_0 \equiv 1$ ולכן $a_0 \neq \pm 1(n)$ אבל $a_1 \equiv a_0^2 \equiv 1(n)$ ולכן לא יהיה $-1$ לאורך כול הסדרה והאיבר הראשון אינו 1- ולכן זהו עד לכך שאן מורכב.

- אם אן מורכב לפחות שלושת רבעי מהזרים לו הם עדי רבין מילר (ללא הוכחה)

***<u>פולינומים:</u>*** הפולינומים זה חוג עם חיבור וכפל, זה למעשה תחום שלמות.

- פולינום זה לא הפונקציה שהוא מגדיר אלא ביטוי המקדמים. מעל כול שדה סופי(כלומר מודולו מספר ראשוני p) מתקיים $x^p - x \equiv 0$ אבל זה לא פולינום האפס.
- ההפיכים בחוג הפולינומים הם רק ההפיכים בשדה, כי פולינום ממעלה אחד או יותר כפול שום פולינום שאינו האפס לא יקטין מעלתו ולכן לא יהיה שווה אחד.
- יש חלוקה בשארית בחוג הפולינומים. מוכיחים באינדוקציה על המעלה וטיפול במקדם הגדול ביותר.
- כול פולינום שאינו קבוע הוא מכפלה של אי פריקים, באינדוקציה ממש כמו בשלמים, ולכן משום קיום אלגוריתם אוקלידס אז הפירוק הוא יחיד כי $ord_q(fg) = ord_q(f) + ord_q(g)$ כי אם ראשוני מחלק מכפלה של שניים אז הוא מחלק לפחות אחד.
- לפולינום ממעלה n יש לכול היותר n שורשים. באינדוקציה, והעובדה שאם מספר הוא שורש של פולינום אז המשוואה הלינארית שהוא שורש שלה מחלקת את הפולינום (מחלוקה בשארית) ולכן באופן טריוויאלי אם שני פולינום ממעלה n מזדהים על n+1 נקודות אז הם זהים (כי לפולינום ההפרש יש יותר מדי שורשים)
- $(p)$ $(p-1)! \equiv -1$ נובע מכך שהפולינום $x^{p-1} - 1 - (x-1)(x-2)\dots(x-(p-1))$ מתאפס על p-1 נקודות שונות ממשפט פרמה, אבל הוא ממעלה קטנה מ-p1 ולכן הוא פולינום האפס ולכן עבור הצבה של אפס נקבל $(p-1)! \equiv (-1)^{p-1} \equiv -1$ אבל p אי זוגי. (עבור 2 זה קל)
- למשוואה $x^d = 1$ כאשר $d|(p-1)$ יש בדיוק d פתרונות. יש לכול היותר d כי זה פולינום. יש בדיוק מחלוקה בשארית עם $x^{p-1} - 1$ שלו יש בדיוק p-1 מפרמה. והעובדה שאנחנו יודעים איך נראית החלוקה של שני הפולינומים האלה.

***<u>דברים אקראים ויפים:</u>***

- <u>רציונלי על המעגל:</u> לפתור את המשוואה $x^2 + y^2 = z^2$ בשלמים שקול ללמצוא נקודות רציונליות על מעגל היחידה. כדי לעשות זאת נעביר ישר מנקודה רציונלית על המעגל שתחתוך את המעגל ותגיע לציר האיקס. ברור שאם נקודת החיתוך עם המעגל רציונלית אז גם נקודת החיתוך עם ציר איקס רציונלית ולכן זה תנאי הכרחי (מדמיון משולשים). הטענה היא שזה גם תנאי מספיק. זה נובע מהצבה בנוסחא של המעגל את הקשר שקיבלנו מהדמיון, ושימוש בנוסחאת וייטה למשוואה ריבועית. כך ניתן למיין את כול הנקודות הרציונליות על המעגל.
- <u>למת הנזל:</u> נרצה למצוא שורשים שלמים של פולינום עם מקדמים שלמים מודולו m. יהיה $f(x) \in F[x]$ כך ש $f(r) \equiv 0(p^{k-1})$ נרצה למצוא שורש ל $p^k$ שהוא גם שקול ל r מודולו $p^{k-1}$
  - $f'(r) \neq 0(p)$ אז קיים ויחיד t כך ש $f\left(r + tp^{k-1}\right) \equiv 0\left(p^k\right)$ וt נתון על ידי הנוסחא הבאה $t = -\left(f'(r)\right)^{-1} f(r)/p^{k-1}$. זה מוגדר היטיב כי $f'(r) \neq 0$ ולכן הפיך מודולו p כמו כן $f(r) \equiv 0\left(p^{k-1}\right)$ ולכן $p^{k-1}|f(r)$
  - $f'(r) \equiv 0(p)$ אז
    - $f(r) \equiv 0\left(p^k\right)$ אז לכול t שלם $f\left(r + tp^{k-1}\right) \equiv 0(p^k)$
    - $f(r) \neq 0(p^k)$ אין פתרון מודולו $p^k$ כך שהוא שקול ל r מודולו $p^{k-1}$
  - <u>הוכחה של למת הנזל:</u> נובע מפיתוח טיילור של הפולינום וההבחנה שכול המקדמים בו הם שלמים ולכן אם נפתח סביב r ונציב $f\left(r + tp^{k-1}\right)$ נקבל שכמעט הכול מצמצם

מהמודולו $p^k$ ולכן $f'(r)tp^{k-1} \equiv -f(r)(p^k)$ ולכן ניתן לצמצם $f'(r)t \equiv \frac{f(r)}{p^{k-1}}(p)$ ולכן כול המקרים מתקיימים כנדרש.

- <u>מסקנה:</u> אם יש פתרון לפולינום מודולו p והנגזרת לא מתאפסת מודולו p אז יש פתרון לכול חזקה של p והוא מקיים $r_k = r_{k-1} - f(r_{k-1})(f'(r_1))^{-1}$ משום שכול הפתרונות שקולים מודולו p אז גם הנגזרות שקולות ולכן גם ההופכי ולכן ניתן להשתמש בהופכי של הראשון.
- ***<u>חוג השלמים של גאוס:</u>*** $Z[i] = \{a + bi | a, b \in Z\}$. נגדיר נורמה למספר כנ"ל $N(\alpha) = \alpha\bar{\alpha}$. מתקיים שנורמה תמיד מספר שלם ואי שלילי, ואפס אמ"מ $\alpha = 0$. כמו כן נורמה היא כפלית. איבר הפיך בחבורה הזו אמ"מ הנורמה שלו 1.
  - <u>חלוקה בשארית:</u> ניתן לחלק בשארית בחוג הנ"ל. כלומר לכול $\alpha, \beta$ קיימים $q, r$ כך ש $\alpha = q\beta + r$ ו $N(r) < N(\beta)$. נסתכל על $\frac{\alpha}{\beta} \in Q[i] = x + iy$ ולכן ניתן לקחת את השלמים הקרובים ביותר ל $x, y$ נסמן אז $m, n$ ו $q = n + mi$. ברור כי $r = \alpha - q\beta$. מתקיים $\frac{N(r)}{N(\beta)} = N\left(\frac{r}{\beta}\right) = N\left(\frac{\alpha - q\beta}{\beta}\right) = (x - m)^2 + (y - n)^2 < \frac{1}{2}$; $\alpha = q\beta + r$
  - <u>סכומי ריבועים:</u> נשים לב כי כול שלם שמקיים $n = x^2 + y^2$ הוא בהכרח נורמה של איזשהו שלם גאוסיני. כמו כן נשים לב כי מכפלה של שני סכומי ריבועים היא גם סכום ריבועים כי נורמה היא כפלית כלומר $n = N(\alpha)$ ו $q = N(\beta)$ אז $nq = N(\alpha\beta)$ ולכן גם סכום ריבועים, לכן נתעניין מתי ראשוני הוא סכום ריבועים. נשים לב שראשוני שהוא שלוש מוד ארבע אינו סכום ריבועים משיקולי שארית חלוקה בארבע. נשים לב שכול ראשוני שהוא אחד מוד 4 הוא סכום ריבועים וזה משום ש1- הוא שארית ריבועית עבורו ולכן $p | m^2 + 1$ עבור m כלשהו ולכן $p | (m + i)(m - i)$ אבל בברור הוא לא מחלק אף אחד מהם ולכן לא יתכן שהוא ראשוני, אבל נשים לב שהנורמה שלו היא הוא בריבוע ולכן הפירוק שלו לגורמים צריך להיות לשני מספרים שהנורמה שלהם היא p כי הוא כן ראשוני מעל השלמים. ולכן הפירוק חייב להיות $p = (x + yi)(x - yi)$ משום שהחלק המדומה חייב להעלם, ולכן נקבל שפי הוא סכום ריבועים.
  - <u>פריקים:</u> נשים לב שעבור $p \in Z$ ראשוני הוא פריק ב $Z[i]$ אמ"מ הוא נורמה (ובפרט אם הוא 3 מוד 4 הוא נשאר אי פריק). אם הוא נורמה ברור שהוא פריק כי הוא מכפלה שלא מספר והצמוד שלו. אם הוא פריק אז הנורמה שלו זה הוא בריבוע וזה שווה למכפלת הנורמות, אבל p ראשוני בשלמים ולכן נורמת כול אחד מהגורמים שלו שווה לp ולכן הוא נורמה.
- ***<u>משוואת פל:</u>*** $x^2 - dy^2 = 1$ כאשר d אינו ריבוע (כי אחרת היה רק פתרון אחד כי ריבוע ועוד אחד הוא לעולם לא ריבוע פרט לאחד) וכמו כן d חיובי כי אחרת היה רק הפתרון הטריוויאלי. אז הפתרונות של משוואת פל הם $x \in Z[\sqrt{d}]$ כך שהנורמה שלהם אחד, כי הנורמה שלהם היא בדיוק משוואת פל, ולכן מכפליות הנורמה כול חזקה של הפתרון היא גם פתרון כי הנורמה תשאר אחד, וכמו כן גם ההופכי של הפתרון יהיה פתרון (ברור שאם x פתרון למשוואת פל אז הוא הפיך בחוג $Z[\sqrt{d}]$ כי הנורמה שלו אחד). כמו כן חלוקה של שני פתרונות גם תניב פתרון כי נורמה כפלית והנורמה של שניהם אחד ולכן גם של החלוקה.
  - ***<u>משוואת פל שלילית:</u>*** $x^2 - dy^2 = -1$ כלומר איברים שהנורמה שלהם מינוס אחד. לכן ברור שפתרון של פל שלילית בריבוע יהיה פתרון של פל. יתר כל כן כול פתרון של פל חיובית הוא מכפלת פתרונות של פל שלילית (דורש הוכחה).
  - ***<u>משפט דירכלה:</u>*** לכול $\xi$ אי רציונלי יש אינסוף רציונלים מצומצמים $\frac{p}{q} \in Q$ כך ש $\left|\frac{p}{q} - \xi\right| < \frac{1}{q^2}$. לכול n טבעי ניתן לחלק את הקטע $[0,1)$ לn קטנים חצי פתוחים בגודל 1/n. כעת נסתכל על $0, \xi, 2\xi, \dots, n\xi$ ולכולם נתבונן בחלק השברי. משובך היונים יש שניים שהם באותו תת קטע של הקטע $[0,1)$ ולכן המרחק ביניהם קטן מ 1/n אזי $|(k\xi - [k\xi]) - (j\xi - [j\xi])| < \frac{1}{n}$ כאשר K ו j שונים. לכן $[j\xi] - [k\xi] = x \in Z$ ולכן

מתקיים $|x-(j-k)\xi|<\frac{1}{n}$ וכמו כן $y=j-k\neq 0$ ולכן $|x-y\xi|<\frac{1}{n}$ לכן מתקיים $\left|\frac{x}{y}-\xi\right|<\frac{1}{ny}$ אבל $y\leq n$ ולכן $\left|\frac{x}{y}-\xi\right|<\frac{1}{y^2}$ אזי מצאנו אחד. כדי למצוא את הבא נבצע אותו התהליך עבור n טבעי חדש המקיים $n>\frac{1}{\left|\frac{x}{y}-\xi\right|}$ משום שקסי אי רציונלי המכנה לעולם לא יתאפס ולכן זה מוגדר וקיים טבעי כזה. אז נמצא קירוב חדש ומובטח שהוא שונה מהקירוב הישן, משוב שהקרוב הישן קרוב עד כדי 1/m מהאופן שבו בחרנו את m והקירוב החדש קרוב יותר מ 1/m

- קיים M כך ש $|x^2-dy^2|<M$ עבור אינסוף זוגות $(x,y)$. ממשפט דירכלה יש אינסוף זוגות $(x,y)$ כך ש $\left|x-y\sqrt{d}\right|<\frac{1}{y}$ כי $\sqrt{d}$ אי רציונלי. ולכן מאש משולש נקבל $|x^2-dy^2|=\left|x+y\sqrt{d}\right|\left|x-y\sqrt{d}\right|\leq\frac{1}{y}\left|x-y\sqrt{d}+2y\sqrt{d}\right|\leq\frac{1}{y^2}+2\sqrt{d}$ ולכן אם נבחר $M=2\sqrt{d}+1$ נצחנו. לכן יש ערך שמתקבל אינסוף פעמים משובך היונים.
- ***<u>למשוואת פל יש פתרון לא טריוויאלי:</u>*** ממה שראינו לעיל יש אינסוף זוגות שונים כך ש $x^2-dy^2=m$ עבור m כלשהו ולכן בהרכח קיימים שני זוגות של פתרונות ששני הרכיבים שלהם קונגרואנטים מודולו m משובך היונים. אזי $a,b$ שני פתרונות כנל ולכן מחישוב ישיר נקבל $m|a\bar{b}$ ולכן $a\bar{b}=m(u+vd)$ ולכן יש שוויון גם בנורמות והנרומה של a,b היא m ולכן נקבל $N(u+vd)=1$ ומובטח לנו שזה לא הפתרון הטריוויאלי כי אז היינו מקבלים ששני הפתרונות שהתחלנו איתם היו זהים.
- ***<u>למשוואת פל יש אינסוף פתרונות:</u>*** ידוע כי קיים לפחות פתרון אחד ולכן ניתן להסתכל על הפתרון ששני רכיביו חיוביים המינמלי נסמנו $\alpha$ ברור גם כי $\pm\alpha^n$ הינו גם פתרון. נראה שאלו כול הפתרונות. נניח יש פתרון אחר $\beta$ חיובי כך ש $\beta\neq\alpha^n$ ולכן מתקיים $\alpha^n<\beta<\alpha^{n+1}$ ולכן $1<\bar{\alpha}^n\beta<\alpha$ ולכן אם נוכיח ש $\bar{\alpha}^n\beta$ חיובי זו סתירה למינמליות של $\alpha$ כי ברור שהוא פתרון כי הנורמה שלו 1. מוכיחים שהפתרון אכן חיובי ממשחקי אלגברה והופכיות והעובדה שהופכי של מספר חיובי הוא גם חיובי, וההופכי של גדול מאחד הוא קטן מאחד. עבור פתרון שהרכיב השני שלו שלילי אז ההופכי שלו יהיה חזקה של הפתרון המינמלי ולכן הוא חזקה שלילית שלו. עבור פתרון שהרכיב הראשון שלילי, נסתכל על הנגדי שלו וזה פתרון שהרכיב שלו חיובי ולכן הוא חזקה מתאימה.

- ***<u>שברים משולבים:</u>*** שבר משולב סופי הינו $a_0+\frac{1}{a_1+\frac{1}{\ddots a_{n-1}+\frac{1}{a_n}}}$ כך שכולם מלבד $a_0$ חיוביים. אם כולם שלמים זה יקרא שבר משולב סופי פשוט.
  - כול מספר רציונלי ניתן לכתוב כשבר משולב סופי פשוט. זה נובע מסופיות אלגוריתם אוקלידס. נשים לב אבל שהכתיבה לא יחידה.
  - נגדיר $p_k=a_kp_{k-1}+p_{k-2}$ ו $q_k=a_kq_{k-1}+q_{k-2}$ כאשר $a_k$ זה האיברים בשבר המשולב, ו $p_0=a_0$ $q_0=1$ $p_1=a_0a_1+1$ ו $q_1=a_1$ אז $c_j=[a_0,\dots a_j]$ כלומר הפיתוח עד השלב ה j מקיים $c_j=\frac{p_j}{q_j}$ ונקרא הקונברגנט מוכיחים באינדוקציה ולפי ההגדרה של הסדרות.
  - $p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}$ כנ"ל באינדוקציה ולפי הגדרה. ולכן $\gcd(p_k,q_k)=1$
  - עוד כול מיני טענות באינדוקציה שגוררות שהקומברגנטים הזוגיים זו סדרה עולה והאי זוגיים סדרה יורדת.
  - נגדיר שבר משולב אינסופי להיות סדרה אינסופית כמו לעיל אזי קיים לה גבול כי היא בנויה משני תתי סדרות מתכנסות כי הן מונוטוניות חסומות וההפרש בינהן שואף לאפס. בדרך כלל סדרה כזאת תתכנס למספר אי רציונלי.
  - בהנתן מספר אי רציונלי ניתן לייצר שבר משולב ששואף אליו על ידי לקיחת כול פעם הערך השלם, ולקיחת ההופכי של החלק השברי ואז שוב החלק השלם וחוזר חלילה.

- <u>שבר משולב מחזור:</u> קיים מחזור החל ממקום מסוים, וזה מתכנס למספר אי רציונלי מסדר ריבועי שזה רציונלי ועוד שורש של רציונלי.
- עבור משוואת פל ניתן לפתח את $\sqrt{d}$ לשבר משולב ולפי אורך המחזור והסדרה שהתקבלה במהלך הפיתוח ניתן לדעת הפתרונות למשוואה החיובית והשלילית והאם קיים בכלל פתרונות לשלילית.