תורת המספרים האלמנטרית | 80697

הרצאות | ד"ר אלכס גורביץ'

כתיבה | נמרוד רק

תשפ"א סמסטר ב'

תוכן העניינים

$\mathbb{I}$

הגדרה יהיו $a,b\in\mathbb{Z}$. נאמר כי a <u>מתחלק</u> ב-b (ונסמן $b\mid a$) אם קיים $c\in\mathbb{Z}$ שעבורו מתקיים $a=c\cdot b$.

הגדרה יהיו $a,b\in\mathbb{Z}$ כך ש-$a\neq 0$ או $b\neq 0$. $\gcd(a,b)=\max\{d\in\mathbb{Z}:d\mid a\ \vee\ d\mid b\}$ <u>המחלק המשותף המקסימלי</u> של a,b.

תכונות

יהיו $a,b\in\mathbb{Z}$.

1. $a\mid 1$.
2. $0\mid b$.
3. $a\mid a$.
4. אם $1\mid b$ אזי $|b|=1$.
5. אם $a_1\mid b$ וגם $a_2\mid b$ אזי $a_1+a_2\mid b$, $\forall a_1,a_2\in\mathbb{Z}$.
6. אם $a\mid b$ אזי $d\cdot a\mid b$, $\forall d\in\mathbb{Z}$.
7. אם $a\mid b$ וגם $a\neq 0$ אזי $b\leq |a|$.
8. $\gcd(a,b)\geq 1$.
9. $\gcd(a,b)=\gcd(b,a)$.
10. $\gcd(a,1)=1$.
11. $\gcd(a,0)=a$ עבור $a\neq 0$.

טענה יהיו $a,b,q\in\mathbb{Z}$ אזי $\gcd(a,b)=\gcd(a-qb,b)$.

הוכחה: נסמן $c=\gcd(a,b)$, $d=\gcd(a-qb,b)$. מהיות $c\mid b$ וגם $c\mid a$ אזי $c\mid a-qb$ ולכן c הוא מחלק משותף של $a-qb,b$ ומכאן גם ש- $c\leq d$. מהיות $d\mid a-qb$ וגם $d\mid b$ אזי $d\mid a=(a-qb)+qb$ ולכן d מחלק משותף של a,b ולכן $d\leq c$. ■

הגדרה יהיו $a\in\mathbb{Z}$, $b\in\mathbb{N}$. החלוקה של a ב-b עם שארית היא מציאת $q,r\in\mathbb{Z}$ כך ש- $a=qb+r$ וגם $0\leq r<b$.

משפט (אלגוריתם אוקלידס) יהיו $a,b\in\mathbb{N}$ כך ש- $a\geq b$. נגדיר את הסדרה c_n ע"י $c_1=a$, $c_2=a$ ו- c_{i+2} הוא שארית החלוקה של c_i ב-c_{i+1}, עבור $i\in\mathbb{N}$ המקיים $c_{i+1}\neq 0$ אזי c_n יורדת ממש.

מסקנה קיים $k\in\mathbb{N}$ שעבורו מתקיים $c_{k+1}=0$.

משפט $\gcd(a,b) = c_k$.

הוכחה: $\forall i \in [k-1]$ קיים $q_i \in \mathbb{Z}$ שעבורו $c_{i+2} = c_i - q_i c_{i+1}$, לכן

$$\gcd(a,b) = \gcd(c_1,c_2) = \gcd(c_2,c_3) = \cdots = \gcd(c_k,c_{k+1}) = \gcd(c_k,0) = c_k$$

■

משפט יהיו $a,b \in \mathbb{N}$. נגדיר $A = \{sa+tb : s,t \in \mathbb{Z}\}$. אזי $\min A \cap \mathbb{N} = \gcd(a,b)$.

הוכחה: $\forall s,t \in \mathbb{Z}$, $\gcd(a,b) \mid sa+tb$ ולכן $\gcd(a,b) \mid \min A \cap \mathbb{N}$ ולכן $\gcd(a,b) \leq \min A \cap \mathbb{N}$. נוכיח כי $\gcd(a,b) \in A \cap \mathbb{N}$ ונסיים. נביט בסדרה שהוגדרה באלגוריתם אוקלידס. נוכיח באינדוקציה כי $\forall i \in [k]$, $c_i \in A$ ונסיים.

בסיס: $c_1 = 1 \cdot a + 0 \cdot b$, $c_2 = 0 \cdot a + 1 \cdot b$.

צעד: נניח כי $c_1, \ldots, c_{i+1} \in A$ אזי קיימים $s_1,t_1,s_2,t_2 \in \mathbb{Z}$ שעבורם $c_i = s_1a+t_1b, c_{i+1} = s_2a+t_2b$, לכן

$$c_{i+2} = c_i - qc_{i+1} = (s_1 - qs_2)\,a + (t_1 - qt_2)\,b \in A$$

■

מסקנה $\{sa+tb : s,t \in \mathbb{Z}\} = \{k \cdot \gcd(a,b) : k \in \mathbb{Z}\}$.

דוגמה $a = 240, b = 46$.

$$\begin{aligned} 240 &= 5 \cdot 46 + 10 \\ 46 &= 4 \cdot 10 + 6 \\ 10 &= 1 \cdot 6 + 4 \\ 6 &= 1 \cdot 4 + 2 \end{aligned}$$

ולכן $c = (240,46,10,6,4,2)$, כלומר $\gcd(240,46) = 2$. נחפש s,t שעבורם $2 = s \cdot 240 + t \cdot 46$.

$$\begin{aligned} 2 &= 1 \cdot 6 + (-1) \cdot 4 \\ &= 1 \cdot 6 + (-1)(10-6) = -1 \cdot 10 + 2 \cdot 6 \\ &= (-1) \cdot 10 + 2 \cdot (46 - 4 \cdot 10) = 2 \cdot 46 + (-9) \cdot 10 \\ &= 2 \cdot 46 + (-9)(240 - 5 \cdot 46) = -9 \cdot 240 + 47 \cdot 46 \end{aligned}$$

III

דוגמה בהינתן $am \mid b$ וגם $a \nmid b$, האם בהכרח $m \mid b$? לא! $a=m=2,b=4$.

ואם $b<m,a$? גם לא! $a=m=6,b=4$.

טענה יהיו $a,b,m\in\mathbb{N}$ כך ש-$b\mid am$ וגם $\gcd(a,b)=1$ אזי $b\mid m$.

הוכחה: מהיות $b\mid am$, אזי קיים $k\in\mathbb{N}$ כך ש- $am=bk$. בגלל ש-$\gcd(a,b)=1$, קיימים $s,t\in\mathbb{Z}$ כך ש- $sa+tb=1$ ולכן $sam+tbm=m$ ולכן $sbk+tbm=m$, $b(sk+tm)=m$, כלומר $b\mid m$. ■

דוגמה אם $a\mid m$ וגם $b\mid m$, האם בהכרח $ab\mid m$? לא! כל בחירה $a=b=m\in\mathbb{N}$ לא תקיים זאת.

ואם $ab<m$? גם לא! $a=b=2,m=6$.

ואם $b\nmid a$ וגם $a\nmid b$? גם לא! $a=4,b=6,m=60$.

טענה יהיו $a,b,m\in\mathbb{N}$ כך ש-$a,b\mid m$ וגם $\gcd(a,b)=1$, אזי $a\cdot b\mid m$.

הוכחה: מהיות $a,b\mid m$, קיימים $k,l\in\mathbb{N}$ כך ש- $m=ka=lb$. מהיות $\gcd(a,b)=1$, קיימים $s,t\in\mathbb{Z}$ כך ש- $sa+tb=1$ ולכן $ab(sl+tk)=salb+tbka=sam+tbm=m$ ולכן $ab\mid m$. ■

טענה יהיו $a,b,p\in\mathbb{N}$ כך ש-p ראשוני, $p\mid ab$ וגם $p\nmid b$ אזי $p\mid a$.

הוכחה: מהיות p ראשוני ו-$p\nmid b$, מתקיים $\gcd(b,p)=1$ ולכן מטענה שהוכחנו לפניכן, $p\mid a$. ■

משפט (המשפט היסודי של האריתמטיקה) יהי $1<n\in\mathbb{N}$. אזי קיימים $p_1<\cdots<p_k$ מספרים ראשוניים ו-$s_1,\ldots,s_k\in\mathbb{N}$ יחידים כך ש- $n=p_1^{s_1}\cdot\cdots\cdot p_k^{s_k}$.

הוכחה: רשאית נוכיח קיום (באמצעות אינדוקציה שלמה).

בסיס ($n=2$): ברור

שלב ($2,\ldots,n-1\to n$): אם n ראשוני אז סיימנו. אחרת, n פריק ולכן קיימים $1\neq a,b\in\mathbb{N}$ כך ש- $ab=n$. נשים לב כי $b=\frac{n}{a},a=\frac{n}{b}<n$ ולכן מה"א קיימים ראשוניים ואינדקסים כרצוי עבור a,b ומכאן שקיימים כאלו גם עבור n.

עתה נוכיח יחידות. נניח בשלילה שקיים מספר טבעי שיש לו שני פירוקים שונים. נבחר n להיות המספר המינימלי שעבורו יש שני פירוקים שונים. נסמן $n=p_1^{s_1}\cdot\cdots\cdot p_k^{s_k}=q_1^{r_1}\cdot\cdots\cdot q_l^{r_l}$. נשים לב כי $\forall j\in[l]$ ו-$\forall i\in[k]$, $p_i\neq q_j$ כי אחרת ל- $\frac{n}{p_i}=\frac{n}{q_j}$ יהיו שני פירוקים שונים. מהיות $n=q_1^{r_1}\cdot\cdots\cdot q_l^{r_l}$ וגם $p_1\mid n$, מהטענה הקודמת קיים i כך ש- $p_1\mid q_i$ אבל q_i ראשוני ו-$p_1\neq 1$ ולכן $p_1=q_i$ סתירה. ■

נסמן ב-A את קבוצת כל המספרים הטבעיים ששארית הלחוקה שלהם ב-4 היא 1.

טענה אם $a,b\in A$ אזי $a\cdot b\in A$.

הוכחה: מהיות $a,b\in A$, קיימים $k,l\in\mathbb{N}_0$ כך ש- $a=4k+1,b=4l+1$ ולכן $ab=4\left(4kl+k+l\right)+1$ ולכן $ab\in A$. ■

הגדרה יהי $1\neq a\in A$. נאמר כי a "ראשוני" אם לא קיימים $1\neq b,c\in A$ כך ש- $a=bc$.

הערה ברור שכל מספר טבעי ראשוני ב-A הוא גם "ראשוני".

דוגמה $5,9,13,17,29,33$ הם "ראשוניים" אבל $25\in A$ לא ראשוני כי $5\cdot5=25$ ו- $5\in A$.

טענה כל מספר מ-A ניתן לפרק למכפלה של גורמים "ראשוניים".

הוכחה: כמו המשפט היסודי. ■

הערה הפירוק במקרה הזה לא בהכרח ראשוני, שכן $49^{1}\cdot9^{1}=21^{2}=441\in A$.

טענה קיימים אינסוף מספרים ראשוניים.

הוכחה: נניח בשלילה שיש מספר סופי של מספרים ראשוניים $p_{1},\dots,p_{k}$. נגדיר $a=p_{1}\cdot\dots\cdot p_{k}+1$. מהיות $p_i\mid a-1$, $\forall i\in[k]$, אזי a לא מתחלק באף אחד מהמספרים הראשוניים שלפניו בסתירה למשפט היסודי. ■

טענה קיימים אינסוף מספרים ראשוניים מהצורה $4n+3$, עבור $n\in\mathbb{N}$.

הוכחה: נניח בשלילה שקיים מספר סופי של מספרים כאלה $p_{1},\dots,p_{k}$. נגדיר $a=4\cdot p_{1}\cdot\dots\cdot p_{k}-1$. נשים לב כי כל מספר ראשוני גדול מ-2 נותן שארית 1 או 3 בחלוקה ב-4. מהיות $a+1$ מתחלק ב-2 ובכל מספר ראשוני עם שארית 3 בחלוקה ב-4, אזי a לא מתחלק באף אחד מהמספרים הראשוניים הנ"ל. לכן כל הגורמים הראשוניים של a מתחלקים בשארית 1 בחלוקה ב-4 (כלומר הם ב-A) ולכן מסגירות לכפל של A (שהוכחנו כבר), $a-1=4\cdot p_{1}\cdot\dots\cdot p_{k}-2$ מתחלק ב-4 סתירה! (כי $4\nmid4k-2$). ■

משפט (משפט דיריכלה) יהיו $d,r\in\mathbb{N}$ כך ש- $\gcd\left(d,r\right)=1$. אזי קיימים אינסוף מספרים ראשוניים מהצורה $dn+r$ עבור $n\in\mathbb{N}$.

הערה לא נוכיח את המשפט במסגרת הקורס אבל כן נוכיח כמה מקרים פרטיים שלו.

III

הגדרה יהיו $a,b,c\in\mathbb{N}$. נאמר כי $\left(a,b,c\right)$ היא <u>שלשה פיתגורית</u> אם $a^{2}+b^{2}=c^{2}$.

דוגמה $\left(3,4,5\right)$ היא שלשה פיתגורית כי $9+16=25$ וגם $\left(6,8,10\right)$ היא שלשה פיתגורית כי $36+64+100$.

טענה תהי (a,b,c) שלשה פיתגורית ו-$d\in\mathbb{N}$ אזי (da,db,dc) היא שלשה פיתגורית.

הגדרה תהי (a,b,c) שלשה פיתגורית. נאמר כי היא <u>שלשה פיתגורית פרימיטיבית</u> אם $\gcd(a,b)$.

טענה תהי (a,b,c) שלשה פיתגורית פרימיטיבית. אזי $\gcd(a,c)=\gcd(b,c)=1$.

הוכחה: נניח בשלילה כי $\gcd(a,c)=d>1$. לכן $d\mid c,a$ ולכן $d^2\mid a^2,c^2$ ולכן $d^2\mid c^2-a^2=b^2$ ולכן $d\mid b$ ומכאן ש-$\gcd(a,b)\geq d>1$ סתירה (ובאופן סימטרי עבור $\gcd(b,c)$). ■

טענה תהי (a,b,c) שלשה פיתגורית כך ש- $\gcd(a,c)=1$ או $\gcd(b,c)=1$ אזי (a,b,c) היא שלשה פיתגורית פרימיטיבית.

הוכחה: נניח בשלילה כי $\gcd(a,b)=d>1$. לכן $d\mid b,a$ ולכן $d^2\mid a^2,b^2$ ולכן $d^2\mid a^2+b^2=c^2$ ולכן $d\mid c$ ומכאן ש-$\gcd(a,c),\gcd(b,c)\geq d>1$ סתירה. ■

טענה תהי (a,b,c) שלשה פיתגורית. אזי קיימים $a',b',c',d\in\mathbb{N}$ כך ש- $a=a'd,b=b'd,c=c'd$ וגם (a',b',c') היא שלשה פיתגורית פרימיטיבית.

הוכחה: נסמן $d=\gcd(a,b)$. אזי $d\mid a,b,c$. נסמן $a'=\frac{a}{d},b'=\frac{b}{d},c'=\frac{c}{d}$. ברור כי (a',b',c') היא שלשה פיתגורית ומהיות $\gcd(a',b')=1$, נקבל כי (a',b',c') היא שלשה פיתגורית פרימיטיבית. ■

דוגמה $(5,12,13)$ וגם $(7,24,25)$ הן שלשות פיתגורית פרימיטיביות.

טענה $\forall l\in\mathbb{N}$, $\left(2l+1,2l^2+2l,2l^2+2l^2+2l+1\right)$ היא שלשה פיתגורית פרימיטיבית.

הוכחה: ניתן לחשב ולהגיע לכך שזו שלשה פיתגורית. בנוסף, $\gcd\left(2l^2+2l+1,2l^2+2l\right)=\gcd\left(2l^2+2l,1\right)=1$. ■

טענה יהיו $s,t\in\mathbb{N}$ כך ש- $s>t$, $\gcd(s,t)=1$ וגם $2\nmid s+t$, אזי $\left(2st,s^2-t^2,s^2+t^2\right)$ היא שלשה פיתגורית פרימיטיבית.

הוכחה: ניתן לחשב ולהגיע לכך שזו שלשה פיתגורית. נסמן $d=\gcd\left(s^2-t^2,s^2+t^2\right)$ אזי קיימים $k,l\in\mathbb{N}$ כך ש- $s^2+t^2=ld$ וגם $s^2-t^2=kd$ ולכן $(l+k)d=2s^2$ וכן $(l-k)d=2t^2$ ולכן $d\mid 2s^2,2t^2$. מהיות $2\nmid s^2+t^2$, אזי גם $2\nmid d$ ולכן $d\mid s^2,t^2$. נניח בשלילה כי $d>1$. לכן קיים p ראשוני כך ש- $p\mid d$ ולכן גם $p\mid s^2,t^2$. לכן $p\mid s,t$ (כי $\gcd(p,s)=1$) ולכן $1=\gcd(s,t)\geq p>1$ סתירה. ■

דוגמה עבור $s=5,t=2$ נקבל שהם עונים על התנאי הדרושים ולכן $\left(2st,s^2-t^2,s^2+t^2\right)=(20,21,29)$ היא שלשה פיתגורית.

טענה תהי (a,b,c) שלשה פיתגורית פרימיטיבית, אזי $2\nmid c$.

הוכחה: נניח בשלילה כי $2 \mid c$. נזכור כי $2 \nmid a,b$ (כי צריך שהסכום של הריבועים שלהם יהיה זוגי, ולכן או ששניהם זוגיים או ששניהם אי זוגיים, ואם הם היו זוגיים אז $\gcd(a,b) > 1$ וזה לא ייתכן). לכן קיימים $l,m \in \mathbb{N}$ כך ש- $a = 2l+1, b = 2m+1$ ולכן $c^2 = 4\left(l^2+l+m^2+m\right)+2 = a^2+b^2 \nmid 4$ אבל $4 \mid c^2$ סתירה. ∎

משפט יהיו $a,b,c,n \in \mathbb{N}$ כך ש- $ab = c^n$ וגם $\gcd(a,b) = 1$. אזי קיימים $a',b' \in \mathbb{N}$ כך ש- $a = (a')^n, b = (b')^n$.

הוכחה: נפרק את c לראשוניים, $c = p_1^{s_1} \cdot \dots \cdot p_k^{s_k}$, לכן $c^n = p_1^{ns_1} \cdot \dots \cdot p_k^{ns_k}$. $\forall i \in [k]$ מתקיים $p_i \mid c^n = ab$ ולכן $p_i \mid a$ או $p_i \mid b$. בה"כ $p_i \mid a$ אז $p_i \nmid b$ כי $\gcd(a,b) = 1$. לכן $\gcd\left(p_i^{ns_i}, b\right) = 1$ (לחזקה של ראשוני יש gcd גדול מ-1 עם מספר נוסף רק אם המספר האחר הוא גם חזקה של המספר הראשוני ההוא, כלומר ש-$p_i \mid b$ וזה לא המצב). מהיות $p_i^{ns_i} \mid c^n = ab$ אז מתקיים $p_i^{ns_i}$. מהיות $\gcd\left(p_i^{ns_i}, p_j^{ns_j}\right) = 1$ עבור $i \neq j$ (לא ברור למה זה עוזר) אזי קיימים $l,m \in \mathbb{N}$ כך ש-

$$a = l \prod_{p_i \in \mathbb{P}: p_i \mid a} p_i^{ns_i}, b = m \prod_{p_i \in \mathbb{P}: p_i \mid b} p_i^{ns_i}$$

(כי עבור כל ראשוני p_i שמחלק את a מתקיים גם $p_i^{ns_i} \mid a$ וכך באותו האופן עבור b). מהיות $ab = c^n = p_1^{ns_1} \cdot \dots \cdot p_k^{ns_k}$ אזי $lm = 1$ ולכן $l = m = 1$, ולכן

$$a = \prod_{p_i \in \mathbb{P}: p_i \mid a} p_i^{ns_i}, b = \prod_{p_i \in \mathbb{P}: p_i \mid b} p_i^{ns_i}$$

נגדיר

$$a' = \prod_{p_i \in \mathbb{P}: p_i \mid a} p_i^{s_i}, b' = \prod_{p_i \in \mathbb{P}: p_i \mid b} p_i^{s_i}$$

ונקבל כי $a = (a')^n, b = (b')^n$. ∎

משפט תהי (a,b,c) שלשה פיתגורית פרימיטיבית כך ש- $2 \mid a$. אזי קיימים $s,t \in \mathbb{N}$ כך ש- $s > t$, $\gcd(s,t) = 1$, $2 \nmid s+t$ וגם

$$a = 2st, b = s^2 - t^2, c = s^2 + t^2$$

הוכחה: מתקיים $a^2 = c^2 - b^2 = (c-b)(c+b)$. נסמן

$$u = \frac{c-b}{2}, v = \frac{b+c}{2}, w = \frac{a}{2}$$

ונשים לב כי מתקיים $2 \nmid b,c$ ולכן $u,v,w \in \mathbb{N}$. לכן מתקיים $(2w)^2 = (2u)(2v)$ ולכן $w^2 = uv$. בנוסף מתקיים $u-v = b, u+v = c$.
נסמן $\gcd(u,v) = d$. לכן $d \mid b,c$ ולכן $d = 1$. מהמשפט הקודם נקבל כי קיימים $s,t \in \mathbb{N}$ כך ש- $v = s^2, u = t^2$. לכן $w^2 = s^2t^2$ ולכן

$w = st$. מכאן נקבל כי

$$a = 2st, b = s^2 - t^2, c = s^2 + t^2$$

בנוסף $s > t$ כי $v > u$. $\gcd(s,t) = 1$ כי $\gcd(u,v)$. $2 \nmid s + t$ כי אחרת $2 \mid s^2 - t^2 = b$ וזה לא ייתכן. ■

$\mathbb{IV}$

משפט לא קיימים $a, b, c \in \mathbb{N}$ אזי $a^4 + b^4 = c^2$.

הוכחה: נניח בשלילה שקיימים a, b, c כאלה. נבחר a, b, c שמקיימים את המשוואה עם c מינימלי, לכן $\left(a^2, b^2, c\right)$ היא שלשה פיתגורית. נוכיח כי היא פרימיטיבית.

נניח בשלילה כי $\gcd\left(a^2, b^2\right) > 1$. נסמן $d = \gcd(a, b)$ ונשים לב כי $d > 1$ (כי אחרת נקבל כי $\gcd\left(a^2, b^2\right) = 1$). $d^4 \mid b^4, a^4$ ולכן $d^4 \mid a^4 + b^4 = c^2$ ולכן $d^2 \mid c$ ומתקיים $\left(\frac{a}{d}\right)^4 + \left(\frac{b}{d}\right)^4 = \left(\frac{c}{d^2}\right)^2$, כלומר ש-$\left(\frac{a}{b}, \frac{b}{d}, \frac{c}{d^2}\right)$ מקיים את המשוואה ומהיות $d > 1$ אזי $\frac{c}{d^2} < c$ וזו סתירה למינימליות של c. לכן $\gcd\left(a^2, b^2\right) = 1$ ולכן $\left(a^2, b^2, c\right)$ היא שלשה פיתגורית פרימיטיבית.

בה"כ a^2 זוגי b^2 אי זוגי. אזי קיימים $s, t \in \mathbb{N}$ כך ש- $s > t$, $\gcd(s,t) = 1$, $2 \nmid s + t$ וגם

$$a^2 = 2st, b^2 = s^2 - t^2, c = s^2 + t^2$$

מכאן ש-$t^2 + b^2 = s^2$ ולכן (t, b, s) היא שלשה פיתגורית פרימיטיבית. לכן $2 \nmid s$ ולכן $t \mid 2$, כלומר קיים $r \in \mathbb{N}$ כך ש- $t = 2r$. מכאן ש- $a^2 = 2s \cdot 2r$, ולכן $\left(\frac{a}{2}\right)^2 = sr$ וגם $\gcd(s,r) = 1$ כי $\gcd(s,t) = 1$. ממשפט שהוכחנו בהרצאה הקודמת, קיימים $k, l \in \mathbb{N}$ כך ש- $s = k^2, r = l^2$. מהיות (t, b, s) שלשה פיתגורית פרימיטיבית ו-$t \mid 2$ קיימים $g, h \in \mathbb{N}$ כך ש- $g > h$, $\gcd(g,h) = 1$, $2 \nmid g + h$ וגם

$$t = 2gh, b = g^2 - h^2, s = g^2 + h^2$$

לכן

$$2l^2 = 2r = t = 2gh$$

ולכן $gh = l^2$. מהמשפט המוזכר לעיל, קיימים $i, j \in \mathbb{N}$ כך ש- $g = i^2, h = j^2$ ולכן

$$k^2 = s = g^2 + h^2 = i^4 + j^4$$

כלומר (i,j,k) מקיים את המשוואה המקורית ובנוסף

$$k \leq k^2 = s \leq s^2 < s^2 + t^2 = c$$

ולכן $k < c$ בסתירה למינימליות של c. ■

$\mathbb{V}$

הגדרה תהי $f : \mathbb{N} \to \mathbb{Z}$. נאמר כי f היא <u>כפלית</u> אם $f \neq 0$ וגם $\forall a,b \in \mathbb{N}$ כך ש- $\gcd(a,b) = 1$ מתקיים $f(ab) = f(a) \cdot f(b)$.

טענה אם $f : \mathbb{N} \to \mathbb{Z}$ כפלית, אזי $f(1) = 1$.

הוכחה: מהיות $f \neq 0$, קיים $a \in \mathbb{N}$ כך ש- $f(a) \neq 0$. מהיות $\gcd(a,1) = 1$ מתקיים $f(a) = f(1 \cdot a) = f(1) \cdot f(a)$ ולכן $f(1) = 1$. ■

דוגמה $\delta(a) = \begin{cases} 1 & a = 1 \\ 0 & a \neq 1 \end{cases}$, $\forall n \in \mathbb{N}$.

דוגמה $1 : \mathbb{N} \to \mathbb{Z}$.

דוגמה $\mathrm{Im}(a) = a$, $\forall n \in \mathbb{N}$.

טענה יהיו $a,b \in \mathbb{N}$ כך ש- $\gcd(a,b) = 1$ ו-$d \in \mathbb{N}$ המקיים $d \mid ab$. אזי קיימים $d_1, d_2 \in \mathbb{N}$ כך ש- $\gcd(d_1,d_2) = 1$, $d_1 d_2 = d$, $d_1 \mid a$, $d_2 \mid b$.

הוכחה: אם $a = p_1^{s_1} \cdot \dots \cdot p_k^{s_k}, b = q_1^{t_1} \cdot \dots \cdot q_l^{t_l}$ הם הפירוקים של a,b לגורמים ראשוניים אזי $p_i \neq q_j$, $\forall i \in [k], j \in [l]$ וגם $ab = p_1^{s_1} \cdot \dots \cdot p_k^{s_k} \cdot q_1^{t_1} \cdot \dots \cdot q_l^{t_l}$ הוא פירוק של ab לגורמים ראשוניים. מהיות $d \mid ab$, אזי $d = ab = p_1^{u_1} \cdot \dots \cdot p_k^{u_k} \cdot q_1^{v_1} \cdot \dots \cdot q_l^{v_l}$ עבור $u_i, v_j \in \mathbb{N} \cup \{0\}$ ו- $u_i \leq s_i, \quad v_j \leq t_j$. נגדיר $d_1 = p_1^{u_1} \cdot \dots \cdot p_k^{u_k}$ ו- $d_2 = q_1^{v_1} \cdot \dots \cdot q_l^{v_l}$ ונקבל את הרצוי. ■

טענה אם $f : \mathbb{N} \to \mathbb{Z}$ כפלית אזי $F : \mathbb{N} \to \mathbb{Z}$ המוגדרת ע"י $F(a) = \sum_{d \in \mathbb{N} : d \mid a} f(d)$ גם כן כפלית.

הוכחה: יהיו $a,b \in \mathbb{N}$ כך ש- $\gcd(a,b) = 1$. לכן מהטענה נ"ל

$$F(ab) = \sum_{d \in \mathbb{N} : d \mid ab} f(d) = \sum_{d_1,d_2 \in \mathbb{N} : d_1 \mid a, d_2 \mid b} f(d_1 \cdot d_2) = \sum_{d_1,d_2 \in \mathbb{N} : d_1 \mid a, d_2 \mid b} f(d_1) \cdot f(d_2) = \left(\sum_{d_1 \in \mathbb{N} : d_1 \mid a} f(d_1) \right) \left(\sum_{d_2 \in \mathbb{N} : d_2 \mid b} f(d_2) \right) = F(a) \cdot$$

■

דוגמה אם $f=\delta$ אז $F=1$.

דוגמה אם $f=1$ אז $\forall a\in\mathbb{N}$, $F\left(a\right)$ היא מספר המחלקים של a. פ' זו מסומנת ב-d.
אם p ראשוני, $d\left(p\right)=2$. אם p ראשוני, $s\in\mathbb{N}$, אז המחלקים של p^{s} הם $1,\dots,p^{s}$ ולכן $d\left(p^{s}\right)=s+1$. אם $a=p_{1}^{s_{1}}\cdot\dots\cdot p_{k}^{s_{k}}$ אז $d\left(a\right)=d\left(p_{1}^{s_{1}}\right)\cdot\dots\cdot d\left(p_{k}^{s_{k}}\right)=\left(s_{1}+1\right)\cdot\dots\cdot\left(s_{k}+1\right)$.

דוגמה אם $f=\mathrm{Im}$ אז $\forall a\in\mathbb{N}$, $F\left(a\right)$ היא סכום המחלקים של a. פ' זו מסומנת ב-σ.
אם p ראשוני אז $\sigma\left(p\right)=p+1$. אם p ראשוני, $s\in\mathbb{N}$ אזי $\sigma\left(p^{s}\right)=1+\dots+p^{s}=\frac{p^{s+1}-1}{p-1}$. אם $a=p_{1}^{s_{1}}\cdot\dots\cdot p_{k}^{s_{k}}$ פירוק של a לראשוניים אזי $\sigma\left(a\right)=\frac{p_{1}^{s_{1}+1}}{p_{1}-1}\cdot\dots\cdot\frac{p_{k}^{s_{k}+1}}{p_{k}-1}$.

טענה יהי $a\in\mathbb{N}$. אזי $d\left(a\right)$ אי זוגי אם"ם קיים $b\in\mathbb{N}$ כך ש- $a=b^{2}$.

הוכחה: $d\left(a\right)$ אי זוגי אם"ם $s_{i}+1$ אי זוגי $\forall i$ שזה אם"ם s_{i} זוגי לכל i שזה אם"ם $\mathbb{N}\ni p_{1}^{\frac{s_{1}}{2}}\cdot\dots\cdot p_{k}^{\frac{s_{k}}{2}}=\sqrt{a}$.

לחלופין, נסמן $S=\left\{ x\in\mathbb{N}:x\mid a\right\}$. $\forall x\in S$ קיים $y\in S$ יחיד כך ש- $xy=a$. אם $\sqrt{a}\notin\mathbb{N}$ אזי $x\neq y$, $\forall x\in S$ ולכן $|S|=d\left(a\right)$ זוגי. אם $\sqrt{a}\in\mathbb{N}$ אזי אם $x=\sqrt{a}$, גם $y=\sqrt{a}$. $\forall x\neq\sqrt{a}$ מתקיים $x\neq y$ ולכן $|S|=d\left(a\right)$ אי זוגי. ■

$\mathbb{VI}$

הגדרה $\mu:\mathbb{N}\to\mathbb{Z}$ היא פ' מביאוס המוגדרת ע"י

$$\mu\left(a\right)=\begin{cases} 1 & a=1\\ 0 & \exists p\ s.t.\ p\ is\ prime\wedge p^{2}\mid a\\ \left(-1\right)^{k} & \exists p_{1}\neq\ldots\neq p_{k}\ primes\ s.t.\ a=p_{1}\cdot\dots\cdot p_{k} \end{cases}$$

טענה μ היא כפלית.

הוכחה: יהיו $1\neq a,b\in\mathbb{N}$ כך ש- $\gcd\left(a,b\right)=1$. אם קיים p ראשוני כך ש- $p^{2}\mid a$ או $p^{2}\mid b$ אז $p^{2}\mid ab$ ולכן $\mu\left(ab\right)=0=\mu\left(a\right)\cdot\mu\left(b\right)$.

אחרת, קיימים $p_{1},\dots,p_{k},q_{1},\dots,q_{l}$ ראשוניים שונים זה מזה כך ש- $a=p_{1}\cdot\dots\cdot p_{k}$ וגם $b=q_{1}\cdot\dots\cdot q_{l}$. בגלל ש- $\gcd\left(a,b\right)=1$, $p_{i}\neq q_{j}$, $\forall i,j$. לכן הפירוק של ab לגורמים ראשוניים הוא $ab=p_{1}\cdot\dots\cdot p_{k},q_{1}\cdot\dots\cdot q_{l}$. לכן

$$\mu\left(ab\right)=\left(-1\right)^{k+l}=\left(-1\right)^{k}\left(-1\right)^{l}\mu\left(a\right)\mu\left(b\right)$$

■

טענה $F\left(a\right)=\sum\limits_{d\in\mathbb{N}:d|a}\mu\left(d\right)=\delta\left(a\right)$.

הוכחה: שני האגפים הן פ' כפליות, ולכן מספיק להוכיח שהשוויון מתקיים עבור $a=p^{s}$ עבור p ראשוני ו-$s\in\mathbb{N}$ (משם אפשר לפצל את הגורמים ולאחד אותם מחדש בעזרת הפירוק היחיד לגורמים ראשוניים ולקבל את השוויון לכל מספר). מהיות המחלקים של p^{s} הם $1,\ldots,p^{s}$, מתקיים

$$F\left(a\right)=\mu\left(1\right)+\cdots+\mu\left(p^{s}\right)=1+\left(-1\right)+0+\cdots+0=\delta\left(p^{s}\right)$$

■

משפט (נוסחת ההיפוך של מביאוס) תהי $f:\mathbb{N}\to\mathbb{Z}$ כפלית ו-$F:\mathbb{N}\to\mathbb{Z}$ המוגדרת ע"י $F\left(a\right)=\sum\limits_{d\in\mathbb{N}:d|a}f\left(d\right)$ אז

$$f\left(a\right)=\sum_{d\in\mathbb{N}:d|a}F\left(d\right)\cdot\mu\left(\frac{a}{d}\right)=\sum_{c\in\mathbb{N}:c|a}F\left(\frac{a}{c}\right)\mu\left(c\right)$$

הוכחה:

$$\begin{aligned}\sum_{c\in\mathbb{N}:c|a}F\left(\frac{a}{c}\right)\mu\left(c\right) & =\sum_{c\in\mathbb{N}:c|a}\mu\left(c\right)\sum_{d\in\mathbb{N}:d|\frac{a}{c}}f\left(d\right)\\
 & =\sum_{c\in\mathbb{N}:c|a}\sum_{d\in\mathbb{N}:d|\frac{a}{c}}\mu\left(c\right)f\left(d\right)\\
 & =\sum_{c,d\in\mathbb{N}\times\mathbb{N}:cd|a}\mu\left(c\right)f\left(d\right)\\
 & =\sum_{d\in\mathbb{N}:d|a}\sum_{c\in\mathbb{N}:d|\frac{a}{c}}\mu\left(c\right)f\left(d\right)\\
 & =\sum_{d\in\mathbb{N}:d|a}f\left(d\right)\sum_{c\in\mathbb{N}:c|\frac{a}{d}}\mu\left(c\right)\\
 & =\sum_{d\in\mathbb{N}:d|a}f\left(d\right)\delta\left(\frac{a}{d}\right)\\
 & =f\left(a\right)\cdot1=f\left(a\right)\end{aligned}$$

■

הגדרה יהי $n\in\mathbb{N}$. נאמר כי n הוא <u>מושלם</u> אם $\sigma\left(n\right)=2n$, <u>מיותר</u> אם $\sigma\left(n\right)>2n$ ו<u>חסר</u> אם $\sigma\left(n\right)<2n$.

תכונות

1. אם p ראשוני אז הוא חסר, שכן $\sigma\left(p\right)=p+1$.

2. עבור $s\in\mathbb{N}$, $\sigma\left(2^{s}\right)=1+\cdots+2^{s}=2^{s+1}-1<2\cdot2^{s}$ כלומר 2^{s} חסר.

טענה יהי $s\in\mathbb{N}$ המקיים $2^{s}-1$ ראשוני אזי $n=2^{s-1}\left(2^{s}-1\right)$ מושלם.

הוכחה:

$$\sigma\left(2^{s-1}\left(2^{s}-1\right)\right)=\sigma\left(2^{s-1}\right)\sigma\left(2^{s}-1\right)=\left(2^{s}-1\right)\left(2^{s}-1+1\right)=2^{s}\left(2^{s}-1\right)=2\cdot\left(2^{s-1}\left(2^{s}-1\right)\right)$$

■

דוגמה

s	1	2	3	4	5	6	7	8
$2^{s}-1$	1	3	7	15	31	63	127	255
ראשוני	$\times$	$\checkmark$	$\checkmark$	$\times$	$\checkmark$	$\times$	$\checkmark$	$\times$
$2^{s-1}\left(2^{s-1}\right)$ (מושלמים)		6	28		496		8128	

טענה אם $s\in\mathbb{N}$ פריק אז $2^{s}-1$ פריק.

הוכחה: קיימים $1<t,u\in\mathbb{N}$ כך ש- $s=tu$ אז $2^{s}-1=2^{tu}-1=\left(2^{t}-1\right)\left(1+2^{t}+\cdots+2^{(u-1)t}\right)$ והגורמים הללו הם גדולים מ-1 ולכן המספר פריק. ■

דוגמה נסתכל רק על ראשוניים

s	11	13	17	...
$2^{s}-1$	2047			
ראשוני	$\times$ (מתחלק ב-23)	$\checkmark$	$\checkmark$	
$2^{s-1}\left(2^{s-1}\right)$ (מושלמים)				

הערה ידועים רק כ-50 מספרים $s\in\mathbb{N}$ כך ש- 2^{s-1} ראשוני.

הערה לא ידוע האם יש אינסוף מספרים כאלה.

משפט (אוילר) אם $n\in\mathbb{N}$ זוגי מושלם אזי קיים $s\in\mathbb{N}$ כך ש- $2^{s}-1$ ראשוני וגם $2^{s-1}\left(2^{s}-1\right)$ מושלם.

הוכחה: קיימים $m\in\mathbb{N}$ אי זוגי ו-$s\in\mathbb{N}$ כך ש- $n=2^{s}m$.

$$2^{s+1}m=2n=\sigma\left(n\right)=\sigma\left(2^{s}\right)\sigma\left(m\right)=\left(2^{s+1}-1\right)\sigma\left(m\right)$$

אבל $2^{s+1}-1,2^{s+1}$ הם מספרים עוקבים ולכן זרים ולכן $2^{s+1}\mid\sigma\left(m\right)$ כלומר קיים $t\in\mathbb{N}$ כך ש- $\sigma\left(m\right)=2^{s+1}t$. לכן

$$2^{s+1}m=\left(2^{s+1}-1\right)2^{s+1}t$$

כלומר $m=\left(2^{s+1}-1\right)t$.

נוכיח כי $t=1$ וכן ש- $2^{s+1}-1$ ראשוני. נניח בשלילה כי $t>1$ אזי $1,t,m$ הם שלושה גורמים שונים של m ולכן

$$\sigma\left(m\right)\geq 1+t+m=1+t+\left(2^{s+1}-1\right)t=1+2^{s+1}t=1+\sigma\left(m\right)$$

סתירה.

נוכיח כי $2^{s+1}-1$ ראשוני. נניח בשלילה כי קיים $u\in\mathbb{N}$ כך ש- $2^{s+1}-1\mid u$ וכן $1<u<2^{s+1}$.

$$\sigma\left(n\right)=\sigma\left(2^{s}\right)\sigma\left(2^{s+1}-1\right)\geq\left(2^{s+1}-1\right)\left(1+u+2^{s+1}-1\right)=\left(2^{s+1}-1\right)\left(2^{s+1}+u\right)>\left(2^{s+1}-1\right)2^{s+1}=2n$$

סתירה. ■

$\mathbb{VIII}$

הגדרה יהיו $a,b\in\mathbb{Z}$, $d\in\mathbb{N}$. נאמר כי a שקול ל-b מודולו d ונרשום $a\equiv b \mod d$ אם $d\mid a-b$.

תכונות

1. (רפלקסיביות) $a\equiv a \mod d$.
2. (סימטריה) אם $a\equiv \mod d$ אזי $b\equiv a \mod d$.
3. (טרנזיטיביות) אם $a\equiv b \mod d$ וגם $b\equiv c \mod d$ אזי $a\equiv c \mod d$.

הגדרה מחלקת השקילות של a מודולו d היא $[a]_d=\{x\in\mathbb{Z}:x\equiv a \mod d\}$.

דוגמה $d=3$. $[0]_3=\{\dots,-3,0,3,6,\dots\}$, $[1]_3=\{\dots,-2,1,4,7,\dots\}$.

טענה $a\equiv b \mod d$ אם"ם שארית החלוקה של a ב-d שווה לשארית החלוקה של b ב-d.

הוכחה: $\Rightarrow$: נסמן $a=q_1d+r, b=q_2d+r$ כאשר $q_1,q_2,r\in\mathbb{N}$, ולכן $a-b=(q_1-q_2)d$ ולכן $d\mid a-b$, כלומר $a\equiv b \mod d$.

$\Leftarrow$: $d\mid a-b$. קיימים $q_1,q_2,r_1,r_2\in\mathbb{N}$ וגם $0\leq r_1,r_2<d$ כך ש-

$$a=q_1d+r_1, b=q_2d+r_2$$

ולכן

$$d\mid(a-b)-(q_1-q_2)d=(a-q_1d)-(b-q_2d)=r_1-r_2$$

ובנוסף $0 \le -r_2 < -d$ ולכן $-d < r_1 - r_2 < d$ ולכן $r_1 - r_2 = 0$ (כי $d \mid r_1 - r_2$ והמספר היחיד בטווח הזה המתחלק ב-d הוא 0). ■

טענה אם $a \equiv b \mod d$ וגם $e \equiv f \mod d$ אזי $a + e \equiv b + f \mod d$ וגם $a \cdot e = b \cdot f \mod d$ (או בניסוח אחר, אם $b \in [a]_d$, $f \in [e]_d$, אזי $b + f \in [a + e]_d$ וכן $b \cdot f \in [a \cdot e]_d$).

הוכחה: $d \mid a - b, e - f$ ולכן קיימים $k, l \in \mathbb{Z}$ כך ש- $a - b = kd$, $e - f = ld$ ולכן $a = b + kd, e = f + ld$. לכן

$$a + e = b + f + (k + l) d$$

ולכן

$$d \mid (k + l) d = (a + e) - (b + f)$$

כלומר $a + e \equiv b + f \mod d$.

$$a \cdot e = (b + kd) (f + ld) = bf + bld + kdf + kld^2 = bf + (bl + kf + kld) d$$

ולכן $d \mid (bl + kf + kld) d = ae - bf$, כלומר $ae \equiv bf \mod d$. ■

מסקנה אם $a \equiv b \mod d$ אזי $a^n \equiv b^n \mod d$.

מסקנה על קבוצת המחלקות $\mathbb{Z}_d = \{[0]_d, \ldots, [d-1]_d\}$ מוגדרות פעולות חיבור וכפל שמקיימות את כל אקסיומות השדה פרט אולי לקיום הפכי.

דוגמאות

1. נחשב את שארית החלוקה של $179 \cdot 19$ ב-17. $179 \cdot 19 \equiv 9 \cdot 2 = 18 \equiv 1 \mod 17$.
2. נחשב את שארית החלוקה של $12^{21} + 14^{41}$ ב-13.

$$12^{21} + 14^{41} \equiv (-1)^{21} + 1^{41} = -1 + 1 = 0 \mod 13$$

3. נחשב את שארית החלקוה של 100^{100} ב-7.

$$100^{100} \equiv 2^{100} = 2^{3 \cdot 33 + 1} = \left(2^3\right)^{33} \cdot 2 = 8^{33} \cdot 2 \equiv 1^{33} \cdot 2 = 2 \mod 7$$

4. נחשב את שארית החלוקה של 5^{32} ב-19.

$$5^{32} = \left(5^2\right)^{16} \equiv 6^{16} = \left(6^2\right)^8 \equiv (-2)^8 = \left((-2)^2\right)^4 = 4^4 = 16^2 \equiv (-3)^2 = 8 \mod 19$$

טענה אם $a \in \mathbb{N}$ כך ש- $a \equiv 2 \mod 3$ אזי למשוואה $x^2 = a$ אין פתרון שלם.

הוכחה: נניח בשלילה כי $x \in \mathbb{Z}$ הוא פתרון למשוואה. שארית החלוקה של x ב-3 היא $0, 1, 2$.

אם $x \equiv 0 \mod 3$ אזי $a = x^2 = 0 (\mod 3)$ סתירה.

אם $x \equiv 1 \mod 3$ אזי $a = x^2 \equiv 1 (\mod 3)$ סתירה.

אם $x \equiv 2 \mod 3$ אזי $a = x^2 = 4 \equiv 1 (\mod 3)$ סתירה. ■

טענה אם (a, b, c) שלשה פיתגורית, אזי $3 \mid ab$.

הוכחה: נניח בשלילה כי $3 \nmid ab$. לכן a, b לא מתחלקים ב-3, ולכן a^2 ו-b^2 לא מתחלקים ב-3. לכן $a^2 \equiv b^2 \equiv 1 \mod 3$ ולכן $c^2 = a^2 + b^2 \equiv 2 \mod 3$ בסתירה לטענה הקודמת. ■

טענה אם $a \in \mathbb{N}$ מקיים $a \equiv 3 \mod 4$, אזי למשוואה $x^2 + y^2 = a$ אין פתרונות שלמים.

הוכחה: נניח בשלילה ש-$(x, y) \in \mathbb{Z} \times \mathbb{Z}$ הוא פתרון. שארית החלוקה של x ב-4 היא $0, \ldots, 3$. נבדוק מה שארית החלוקה של x^2 יכולה להיות ב-4.

$x \mod 4$	$x^2 \mod 4$
0	0
1	1
2	0
1	1

באותו האופן גם שארית החלוקה של y^2 ב-4 היא 0 או 1. לכן השארית של $x^2 + y^2$ היא $0, 1, 2$, כלומר היא לא 3, סתירה. ■

$\mathbb{VIII}$

טענה יהיו $a, b, c \in \mathbb{N}$ כך ש- $\gcd(a, b) = 1$. אזי קיים שלם $0 \le x \le b - 1$ יחיד המקיים $ax \equiv c \mod b$.

הוכחה: קיום:

קיימים $s,t\in\mathbb{Z}$ כך ש- $as+bt=1$ ולכן $asc=c-btc\equiv c \mod b$. נחלק את sc ב-b עם שארית ולכן קיימים $q,r\in\mathbb{N}$ כך ש- $0\leq r\leq b-1$ המקיימים $sc=qb+r$. לכן

$$ar=a\left(sc-qb\right)=asc-aqb\equiv c \mod b$$

כלומר $x=r$ מקיים את הנדרש.

יחידות: יהיו $x_1,x_2\in\mathbb{Z}$ המקיימים את הדרישות. לכן $ax_1\equiv ax_2 \mod b$, ולכן $b\mid a\left(x_1-x_2\right)$ ולכן $b\mid x_1-x_2$. בנוסף, $-\left(b-1\right)\leq x_1-x_2\leq b-1$ ולכן $x_1-x_2=0$ (אין עוד מספרים בטווח הזה המתחלקים ב-d), כלומר $x_1=x_2$. ■

מסקנה אם $a,b,c\in\mathbb{N}$ מקיימים $\gcd\left(a,b\right)=1$ אזי אוסף הפתרונות של הקונגרונאציה $ax\equiv c \mod b$ הוא $\left\{x_0+kb:k\in\mathbb{Z}\right\}$ כך ש- $ax_0=c \mod b$, $0\leq x_0\leq b-1$.

דוגמה נפתור את משוואות הקונגרואנציה $4x\equiv 3 \mod 19$. $\gcd\left(4,19\right)=1$. נמצא $s,t\in\mathbb{Z}$ כך ש- $4s+19t=1$, לדוגמה $s=5,t=-1$ ולכן $4\cdot 15=4\cdot 5\cdot 3=3+19\cdot 3\equiv 3 \mod 19$ ולכן אוסף הפתרונות הוא $\left\{15+19k:k\in\mathbb{Z}\right\}$.

טענה אם $a,b,c\in\mathbb{N}$ כך ש- $\gcd\left(a,b\right)\nmid c$, אזי למשוואה $ax\equiv c \mod b$ אין פתרונות שלמים.

הוכחה: נניח בשלילה שקיים x כזה, לכן קיים $k\in\mathbb{Z}$ כך ש- $ax-c=kb$ (כי $b\mid ax-c$) ולכן $\gcd\left(a,b\right)\mid ax-kb=c$ סתירה. ■

טענה אם $a,b\in\mathbb{N}$ ו-$d=\gcd\left(a,b\right)$, אזי $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$.

הוכחה: קיימים $s,t\in\mathbb{Z}$ כך ש- $as+bt=d$. לכן $\frac{a}{d}s+\frac{b}{d}t=1$. אם נסמן $d'=\gcd\left(\frac{a}{d},\frac{b}{d}\right)$, אזי $d'\mid\frac{a}{d}s+\frac{b}{d}t=1$ ולכן $d'=1$. ■

טענה אם $a,b,c\in\mathbb{N}$ ומתקיים $d=\gcd\left(a,b\right)\mid c$, אזי קיים $0\leq x\leq\frac{b}{d}-1$ יחיד כך ש- $ax\equiv c \mod b$.

הוכחה: נראה כי $x\in\mathbb{Z}$ מקיים $ax\equiv c \mod b$ אם"ם $\frac{a}{d}x\equiv\frac{c}{d} \mod \frac{b}{d}$.

$$ax\equiv c \mod d\iff ax-c=kb\iff\frac{a}{d}x-\frac{c}{d}=k\frac{b}{d}\iff\frac{a}{d}x\equiv\frac{c}{d} \mod \frac{b}{d}$$

ומטענה הנ"ל $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$, ולכן מהקיום והיחידות של פתרון משוואת הקונגרואציה עבור מספרים זרים, קיים x יחיד המקיים את הרצוי. ■

מסקנה אם $a,b,c\in\mathbb{N}$, $\gcd\left(a,b\right)=1$, אזי אוסף הפתרונות השלמים של הקונגרואנציה $ax\equiv c \mod b$ הוא $\left\{x_0+k\frac{b}{d\gcd(a,b)}:k\in\mathbb{Z}\right\}$ כך ש-$ax_0\equiv c\left(\mod b\right)$, $0\leq x_0\leq\frac{b}{\gcd(a,b)}-1$.

דוגמאות

נפתור את הקונגרואנציות הבאות.

1. $6x\equiv 13 \mod 21$. $\gcd(6,21)=3\nmid 13$ ולכן אין פתרונות שלמים.

2. $6x\equiv 15 \mod 21$. $\gcd(6,21)\mid 15$ ולכן המשוואה שקולה ל-$2x\equiv 5 \mod 7$. קיימים $s,t\in\mathbb{Z}$ כך ש- $2s+7t=1$. נבחר $s=-3, t=1$, לכן $asc=2\cdot(-3)\cdot 5=(1-7)\cdot 5\equiv 5 \mod 7$ ולכן אוסף הפתרונות הוא $\{6+7k : k\in\mathbb{Z}\}$.

טענה אם p ראשוני, $a\in\mathbb{N}$, $a\leq p-1$ אזי קיים $x\in\mathbb{N}$ יחיד כך ש- $x\leq p-1$ וגם $ax\equiv 1 \mod p$.

טענה אם p ראשוני, $a\in\mathbb{N}$, $a\leq p-1$, $a^2\equiv 1 \mod p$ אזי $a=1$ או $a=p-1$.

הוכחה: מהנתון $p\mid a^2-1=(a-1)(a+1)$, אזי $p\mid a+1$ או $p\mid a-1$. אם $p\mid a-1$, אז מהנתון $0\leq a-1\leq p-2$ ולכן $a-1=0$, ולכן $a=1$. אם $p\mid a+1$, אזי מהנתון $2\leq a+1\leq p$ ולכן $a+1=p$, כלומר $a=p-1$. ■

משפט (ווילסון) אם $p>2$ ראשוני אזי $(p-1)!\equiv -1 \mod p$.

הוכחה: $(p-1)!=1\cdot 2\cdot\cdots\cdot(p-1)$. משתי הטענות הקודמות, לכל $2\leq a\leq p-2$ קיים $2\leq x\leq p-2$ יחיד כך ש- $ax\equiv 1 \mod p$, $a\neq x$ (היחידות היא מהטענה ה-2 לפני אחרונה והשוני נובע מכך שאם זה היה שווה אז היינו מקבלים כי $a=1$ או $a=p-1$ בניגוד לטווח של a) כלומר כל המספרים מ-2 עד $p-2$ מתחלקים ל-$\frac{p-3}{2}$ זוגות שמכפלת המספרים בכל זוג שקולה ל-1 מודולו p. לכן $(p-2)!\equiv 1 \mod p$. לכן $(p-1)!=(p-2)!(p-1)\equiv -1 \mod p$. ■

$\mathbb{IX}$

משפט (השאריות הסיני) יהיו $a,b\in\mathbb{N}$ כך ש- $\gcd(a,b)=1$, ויהיו $c,d\in\mathbb{Z}$ כך ש- $0\leq c\leq a-1$, $0\leq d\leq b-1$, אזי קיים $x\in\mathbb{Z}$ יחיד כך ש- $0\leq x\leq ab-1$ וגם $\begin{cases} x & \equiv c \mod a \\ x & \equiv d \mod b \end{cases}$.

הוכחה: נגדיר $f:\{0,\dots,ab-1\}\to\{0,\dots,a-1\}\times\{0,\dots,b-1\}$ ע"י $f(x)=(r,s)$ כאשר r היא שארית החלקה של x ב-a ו-x היא שארית החלוקה של x ב-b. נוכיח כי f חח"ע. יהיו $0\leq x_1,x_2\leq ab-1$ כך ש- $f(x_1)=f(x_2)=(c,d)$. לכן

$$\begin{cases} x_1 & \equiv c \mod a \\ x_2 & \equiv c \mod a \end{cases}, \begin{cases} x_1 & \equiv d \mod b \\ x_2 & \equiv d \mod b \end{cases}$$

ולכן $\begin{cases} x_1 & \equiv x_2 \mod b \\ x_2 & \equiv x_2 \mod b \end{cases}$, ולכן $a,b \mid x_1 - x_2$ ומהיות $\gcd(a,b)=1$ אזי $ab \mid x_1 - x_2$ אבל $-(ab-1) \le x_1 - x_2 \le ab-1$ ולכן $x_1 - x_2 = 0$ ולכן $x_1 = x_2$. לכן בגלל שתחום ההגדרה והטווח של f באותו הגודל, אזי f על ולכן קיים x כך ש- $f(x) = (0,0)$. ■

הוכחה: (אלטרנטיבית) נגדיר את f כנ"ל. כדי להוכיח כי f על, ניקח $c,d \in \mathbb{Z}$ כך ש- $0 \le c \le a-1$, $0 \le d \le b-1$ ונבנה $0 \le x \le ab-1$, $x \in \mathbb{Z}$ כך ש- $f(x) = (c,d)$. מהיות $\gcd(a,b)=1$ אזי קיימים $s,t \in \mathbb{Z}$ כך ש- $as+bt=1$. נגדיר את x להיות שארית החלוקה של $asd+btc$ ב- ab. לכן $0 \le x \le ab-1$ וגם $x \equiv asd+btc \mod ab$. לכן

$$x \equiv asd + btc \equiv btc = (1-as)c = c - asc = c \mod a$$
$$x \equiv asd + btc \equiv asd = (1-bt)d = d - btd = d \mod b$$

ולכן $f(x) = (c,d)$. ■

מסקנה יהיו $a,b \in \mathbb{N}$ כך ש- $\gcd(a,b)=1$, ויהיו $c,d \in \mathbb{Z}$ כך ש- $0 \le c \le a-1$, $0 \le d \le b-1$, אזי אוסף הפתרונות של המשוואה $\begin{cases} x & \equiv c \mod a \\ x & \equiv d \mod b \end{cases}$ הוא $\{x_0 + kab : k \in \mathbb{Z}\}$ כאשר $0 \le x_0 \le ab-1$, $\begin{cases} x_0 & \equiv c \mod a \\ x_0 & \equiv d \mod b \end{cases}$.

דוגמאות

נפתור את מערכות משוואות הקונגורנציה הבאות

1. $\begin{cases} x & \equiv 4 \mod 7 \\ x & \equiv 3 \mod 19 \end{cases}$. $\gcd(7,19)=1$, לכן קיימים $s,t \in \mathbb{Z}$ כך ש- $19s + 7t = 1$. נבחר $s=3, t=-8$. לכן

$$x_0 = 4 \cdot 3 \cdot 19 + 3 \cdot (-8) \cdot 7 = 228 - 168 = 60$$

מקיים את מערכת המשוואות. לכן הפתרון הוא $\{60 + 133k : k \in \mathbb{Z}\}$.

2. $\begin{cases} x & \equiv 4 \mod 71 \\ x & \equiv 2 \mod 73 \end{cases}$. נשים לב כי $75 = 2 + 73 = 4 + 71$. לכן $x_0 = 75$ מקיים את המשוואות, לכן הפתרון הוא

$$\{75 + 5183k : k \in \mathbb{Z}\}$$

הגדרה יהי $n \in \mathbb{N}$. נסמן $A_n = \{n \ge x \in \mathbb{N} : \gcd(x,n) = 1\}$. נגדיר את <u>פונקציית אוילר</u> $\varphi : \mathbb{N} \to \mathbb{Z}$ ע"י $\varphi(n) = |A_n|$.

דוגמה

$$\varphi(1) = |\{1\}| = 1$$
$$\varphi(2) = |\{1\}| = 1$$
$$\varphi(3) = |\{1,2\}| = 2$$
$$\varphi(4) = |\{1,3\}| = 2$$
$$\varphi(5) = |\{1,2,3,4\}| = 4$$
$$\varphi(6) = |\{1,5\}| = 2$$

תכונות

1. אם p ראשוני אזי $\varphi(p) = |\{1,\dots,p-1\}| = p-1$.
2. $\varphi(2^n) = |\{1,3,\dots,2^n-1\}| = 2^{n-1}$.
3. אם p ראשוני אזי

$$\varphi(p^n) = |\{1,\dots,p^n\} \setminus \{p,2p,\dots,p^n\}| = p^n - \frac{p^n}{p} = (p-1)\,p^{n-1}$$

4. אם $\varphi(a) = 1$ אזי $a = 2$ או $a = 1$ (כי אחרת $a-1 \neq 1$ ולכן $\{1, a-1\} \subseteq A_n$ ואז $\varphi(a) \geq 2$).

משפט פ' אוילר היא פ' כפלית.

הוכחה: יהיו $a,b \in \mathbb{N}$ כך ש- $\gcd(a,b) = 1$. נוכיח כי $|A_{ab}| = |A_a \times A_b|$. נגדיר

$$f : \{0,\dots,ab-1\} \to \{0,\dots,a-1\} \times \{0,\dots,b-1\}$$

ע"י $f(x) = (r,s)$ כאשר r היא שארית החלקה של x ב-a ו-x היא שארית החלוקה של x ב-b. ראינו במשפט השאריות הסיני כי f חחע"ל. נותר להראות כי $f(A_{ab}) = A_a \times A_b$.

נוכיח כי $f(A_{ab}) \subseteq A_a \times A_b$. יהי $x \in A_{ab}$. לכן $\gcd(x,ab) = 1$. נסמן $f(x) = (r,s)$, לכן $x = qa + r$. קיימים $u,v \in \mathbb{Z}$ כך ש- $ux + vab = 1$. לכן

$$(uq + vb)\,a + ur = uqa + ur + vab = ux + vab = 1$$

ולכן $\gcd(a,r) = 1$ ובאותו האופן $\gcd(b,s) = 1$ ולכן $r \in A_a$ ו-$s \in A_b$ ולכן $f(x) \in A_a \times A_b$.

נוכיח כי $f(A_{ab}) \supseteq A_a \times A_b$. יהי $(r,s) \in A_a \times A_b$. מהיות f על, קיים $0 \le x \le ab-1$ כך ש- $f(x) = (r,s)$. נניח בשלילה כי $x \notin A_{ab}$. לכן $\gcd(x,ab) \neq 1$ ולכן קיים ראשוני כך ש- $p \mid \gcd(x,ab)$, כלומר $p \mid x, ab$. לכן $p \mid a$ או $p \mid b$. בה"כ $p \mid a$ ולכן $p \mid r = x - qa$ ולכן $p \mid \gcd(a,r)$, כלומר $r \notin A_a$ סתירה. ■

מסקנה אם $p_1, \ldots, p_k$ ראשוניים ומתקיים $n = p_1^{s_1} \cdot \ldots \cdot p_k^{s_k}$, אזי

$$\varphi(n) = (p_1 - 1) p_1^{s_i - 1} \cdot \ldots \cdot (p_k - 1) p_k^{s_k - 1} = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

מסקנה יהיו $n, p \in \mathbb{N}$ כך ש- p ראשוני ו-$p \mid n$. אזי $p - 1 \mid \varphi(n)$.

דוגמה נמצא את כל הטבעיים כך ש- $\varphi(n) = 14$. יהי p ראשוני כך ש- $p \mid n$. לכן $p - 1 \mid 14$. לכן $p - 1 = 1, 2, 7, 14$ לכן $p = 2, 3, 8, 15$ ולכן $n = 2^k \cdot 3^l$, $0 \le k, l \in \mathbb{Z}$.

אם $k, l \ge 1$ אזי $\varphi(n) = (2-1) 2^{k-1} \cdot (3-1) 3^{l-1}$

אם $k = 0, l \ge 1$ אזי $\varphi(n) = (3-1) 3^{l-1}$.

אם $k \ge 1, l = 0$ אזי $\varphi(n) = (2-1) 2^{k-1}$.

נשים לב כי אף אחד מהביטויים הללו אינו מתחלק ב-7 ולכן גם לא יכול להחלתק ב-14. לכן אין מספרים המקיימים את התנאי הרצוי.

דוגמה נמצא את כל הטבעיים כך ש- $\varphi(n) = 4$. יהי p ראשוני כך ש- $p \mid n$. לכן $p - 1 = 1, 2, 4$. לכן $p = 2, 3, 5$ ולכן $n = 2^k 3^l 5^m$.

אם $m \ge 1$ אזי $\varphi(n) = \varphi\left(2^k 3^l\right)(5-1) 5^{m-1} = 4$ ולכן $m = 1$ וגם $2^k \cdot 3^l = 2$ (כדי שפ' האוילר שלהם תהיה 1). לכן $n = 5, 10$.

אם $m = 0$ נחלק למקרים נוספים:

אם $k, l \ge 1$ אזי

$$\varphi(n) = (2-1) 2^{k-1} (3-1) 3^{l-1} = 2^k 3^{l-1} = 4$$

ולכן $k = 2, l = 1$ ולכן $n = 12$.

אם $l = 0, k \ge 1$ אזי $\varphi(n) = (2-1) 2^{k-1} = 4$ ולכן $k = 3$, כלומר $n = 8$.

אם $k = 0, l \ge 1$ אזי $\varphi(n) = 2 \cdot 3^{l-1} = 4$ ולזה אין פתרון.

לכן כל הערכים האפשריים הם $5, 8, 10, 12$.

$\mathbb{X}$

משפט (אוילר) יהיו $a, b \in \mathbb{N}$ כך ש- $\gcd(a,b) = 1$. אזי $a^{\varphi(b)} \equiv 1 \mod b$.

הוכחה: נתבונן ב-$A_b = \{b \geq x \in \mathbb{N} : \gcd(x,b) = 1\}$. אם $x \in A_b$ אזי $\gcd(ax,b) = 1$. נסמן ב-r את שארית החלוקה של ax ב-b.

לכן $r = ax - qb$ ולכן $\gcd(r,b)$ וגם $0 \leq r \leq b-1$, ולכן $r \in A_b$. נגדיר $f : A_b \to A_b$ ע"י $f(x)$ היא שארית החלוקה של ax ב-b.

נוכיח כי f היא חח"ע. יהיו $x_1, x_2 \in A_b$ כך ש- $r = f(x_1) = f(x_2)$. לכן $\begin{cases} ax_1 & = q_1 b + r \\ ax_2 & = q_2 b + r \end{cases}$. לכן $b \mid (q_1 - q_2) b = a(x_1 - x_2)$

ומהיות $\gcd(a,b) = 1$ אזי $b \mid x_1 - x_2$ אבל $-b < x_1 - x_2 < b$ ולכן $x_1 - x_2 = 0$ ולכן $x_1 = x_2$.

לכן f חח"ע וגם על, כלומר אם $A_b = \left\{s_1, \ldots, s_{\varphi(b)}\right\}$ אזי $A_b = \left\{f(s_1), \ldots, f\left(s_{\varphi(b)}\right)\right\}$. לכן

$$s_1 \cdot \ldots \cdot s_{\varphi(b)} = f(s_1) \cdot \ldots \cdot f\left(s_{\varphi(b)}\right) \equiv as_1 \cdot \ldots \cdot as_{\varphi(b)} = a^{\varphi(b)} \cdot s_1 \cdot \ldots \cdot s_{\varphi(b)} \mod b$$

ולכן $b \mid \left(a^{\varphi(b)} - 1\right) \cdot s_1 \cdot \ldots \cdot s_{\varphi(b)}$ אבל $\gcd(s_i, b) = 1$, $\forall i \in [\varphi(b)]$ ולכן $b \mid a^{\varphi(b)} - 1$ ולכן $a^{\varphi(b)} \equiv 1 \mod b$. ■

מסקנה (משפט פרמה הקטן) יהיו $a, p \in \mathbb{N}$ כך ש- p ראשוני ו-$a \nmid p$. אזי $a^{p-1} \equiv 1 \mod p$.

מסקנה יהיו $a, p \in \mathbb{N}$ כך ש- p ראשוני. אזי $a^p \equiv a \mod p$.

הוכחה: אם $p \nmid a$ זה נובע ישירות מהמסקנה הקודמת. אם $p \mid a$ אזי $a \equiv 0 \mod p$ ולכן $a^p \equiv 0 \mod p$. ■

דוגמאות

1. נחשב את שארית החלוקה של 10^{234} ב-47.

$$10^{234} = 10^{46 \cdot 5 + 4} = \left(10^{46}\right)^5 \cdot 10^4 \equiv 1^5 \cdot 10^4 = 100^2 \equiv 6^2 = 36 \mod 47$$

2. נוכיח כי $\forall k \in \mathbb{N}$ מתקיים $21 \mid 17^{12k} - 1$.

$\varphi(21) = (3-1)(7-1) = 12$ ומהיות $\gcd(17,21) = 1$ אזי ממשפט אוילר $17^{12} = 17^{\varphi(21)} \equiv 1 \mod 21$ ולכן $17^{12k} \equiv 1^k = 1 \mod 21$.

3. נוכיח כי $\forall k \in \mathbb{N}$ מתקיים $55 \mid 13^{20k} - 1$.

נוכיח כי $5 \mid 13^{20k} - 1$ וגם $11 \mid 13^{20k} - 1$. ממשפט פרמה הקטן מתקיים $13^4 = 13^{5-1} \equiv 1 \mod 5$ ולכן $13^{20k} = \left(13^4\right)^{5k} \equiv 1^{5k} = 1 \mod 5$. ממשפט פרמה הקטן מתקיים $13^{10} = 13^{11-1} \equiv 1 \mod 11$ ולכן $13^{20k} = \left(13^{10}\right)^{2k} \equiv 1^{2k} = 1 \mod 11$.

4. נוכיח כי $\forall k \in \mathbb{N}$ מתקיים $23 \mid 2^{11k} - 1$.

ממשפט פרמה הקטן מתקיים $5^{22} \equiv 1 \mod 23$ ולכן $2^{11} \equiv 25^{11} = \left(5^2\right)^{11} = 5^{22} \equiv 1 \mod 23$ ולכן $2^{11k} \equiv 1 \mod 23$.

5. נחשב את שארית החלוקה של 2^{50} ב-77.

נמצא את שארית החלוקה של 2^{50} ב-7 וב-11.

$$2^{50} = 2^{6\cdot 8+2} = \left(2^6\right)^8 \cdot 2^2 \equiv 1^8 \cdot 4 = 4 \mod 7$$

$$2^{50} = \left(2^{10}\right)^5 \equiv 1^5 = 1 \mod 11$$

נמצא $s,t\in\mathbb{Z}$ כך ש- $7s+11t=1$. נבחר $s=-3, t=2$. לכן

$$\begin{aligned}67 = 7\cdot(-3) + 11\cdot 2\cdot 4 &\equiv 7\cdot(-3) = 1 - 11\cdot 2 \equiv 1 \mod 11 \\ &\equiv 11\cdot 2\cdot 4 = (1-(-3)\,7)\,4 \equiv 4 \mod 7\end{aligned}$$

ולכן $2^{50}-67$ מתחלק ב-11 וב-77 ולכן גם ב-77. לכן התשובה היא 67.

$\mathbb{XI}$

ראינו בעבר כי אם p ראשוני אזי $2^p \equiv 2 \mod p$.

טענה עבור $n = 341 = 11\cdot 31$ מתקיים $2^n \equiv 2 \mod n$.

הוכחה: נוכיח כי $11, 31 \mid 2^{341}-2$. ממשפט פרמה הקטן מתקיים $2^{10} = 2^{11-1} \equiv 1 \mod 11$. לכן

$$2^{341} = \left(2^{10}\right)^{34} \cdot 2 \equiv 1^{34}\cdot 2 = 2 \mod 11$$

ממשפט פרמה הקטן $2^{30} = 2^{31-1} \equiv 1 \mod 31$ ולכן

$$2^{341} = \left(2^{30}\right)^{11} \cdot 2^{11} \equiv 1^{11}\cdot 2^{11} = 2^5\cdot 2^5\cdot 2 \equiv 2 \mod 31$$

■

הגדרה יהי $n\in\mathbb{N}$. נאמר כי n הוא פסואדו-ראשוני אם n פריק וגם $2^n \equiv 2 \mod n$.

טענה יהי $n\in\mathbb{N}$ כך ש- $2^n \equiv 2 \mod n$ ונגדיר $m = 2^n - 1$, אזי $2^m \equiv 2 \mod m$.

הוכחה: מהיות $n \mid 2^n - 2$, קיים $k \in \mathbb{N}$ כך ש- $kn = 2^n - 2$, לכן מתקיים

$$\begin{aligned}
2^m - 2 &= \left(2^{m-1} - 1\right) 2 \\
&= \left(2^{2^n - 2} - 1\right) \cdot 2 \\
&= \left(2^{kn} - 1\right) \cdot 2 \\
&= \left(\left(2^n\right)^k - 1\right) \cdot 2 \\
&= \left(2^n - 1\right)\left(1 + 2^n + \cdots + 2^{(k-1)n}\right) \cdot 2 \\
&= m\left(1 + \cdots + 2^{(k-1)n}\right) \cdot 2 \\
&\equiv 0 \mod m
\end{aligned}$$

■

מסקנה קיימים אינסוף מספרים פסאודו-ראשוניים אי זוגיים.

הוכחה: נבנה סדרה אינסופית באופן ריקורסיבי, $n_1 = 341$, $n_{i+1} = 2^{n_i} - 1$. נוכיח באינדוקציה כי n_i פסאודו ראשוני.

בסיס ($i = 1$): כבר הוכחנו.

צעד ($i \to i + 1$): מהטענה הקודמת מתקיים $2^{n_{i+1}} \equiv 2 \mod n_{i+1}$ ומהיות n_i פריק אזי n_{i+1} פריק ולכן n_{i+1} פסאודו-ראשוני. ■

משפט אם $p > 2$ ראשוני, אזי $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$.

הוכחה: ממשפט וילסון, $(p-1)! \equiv -1 \mod p$. אבל

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-2)(p-1) \\
&\equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot (-1)\frac{p-1}{2} \cdot \ldots \cdot (-2)(-1) \\
&= (-1)^{\frac{p-1}{2}} \cdot \left(\left(\frac{p-1}{2}\right)!\right)^2 \mod p
\end{aligned}$$

ולכן $(-1)^{\frac{p-1}{2}} \cdot \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \mod p$ ואם נכפול ב- $(-1)^{\frac{p-1}{2}}$, נקבל $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$. ■

טענה יהי $p > 2$ ראשוני. אזי למשוואת הקונגרואנציה $x^2 \equiv -1 \mod p$ קיים פתרון שלם אם"ם $p \equiv 1 \mod 4$.

הוכחה: $\Rightarrow$: קיים $k \in \mathbb{N}$ כך ש- $p = 4k + 1$. נבחר $x = \left(\frac{p-1}{2}\right)!$ ולכן

$$x^2 \equiv (-1)^{\frac{p+1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1 \mod p$$

$\Leftarrow$: נניח כי מתקיים $x^2 \equiv -1 \mod p$. נניח בשלילה כי $p \not\equiv 1 \mod 4$, כלומר $p \equiv 3 \mod 4$. לכן קיים $k \in \mathbb{N} \cup \{0\}$ כך ש-$p = 4k + 3$.

$$x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} = \left(x^2\right)^{\frac{4k+2}{2}} = \left(x^2\right)^{2k+1} \equiv (-1)^{2k+1} = -1 \mod p$$

אבל ברור כי $p \nmid x$ ולכן ממשפט פרמה הקטן $x^{p-1} \equiv 1 \mod p$ סתירה. ■

טענה קיימים אינסוף ראשוניים מהצורה $4n + 1$.

הוכחה: נניח בשלילה כי קיים מספר סופי של ראשוניים כאלה. נסמנם $p_1, \ldots, p_k$. נביט ב-$a = (2p_1 \cdot \ldots \cdot p_k)^2 + 1$. ברור כי $2, p_i \nmid a$, $\forall i \in [k]$. בנוסף לכל p ראשוני כך ש- $p \equiv 3 \mod 4$ מתקיים $p \nmid a$ כי אחרת $a \equiv 0 \mod p$ ולכן $x = 2p_1 \cdot \ldots \cdot p_k$ מהווה פתרון למשוואת הקונגרואנציה $x^2 + 1 \equiv 0 \mod p$ בסתירה לטענה הקודמת. לכן a לא מתחלק באף ראשוני סתירה. ■

טענה יהי $p > 3$ ראשוני. אם למשוואת הקונגרואנציה $x^2 + x + 1 \equiv 0 \mod p$ קיים פתרון שלם, אזי $p \equiv 1 \mod 6$.

הוכחה: נסמן את פתרון המשוואה ב-x. נניח בשלילה כי $p \not\equiv 1 \mod 6$, כלומר $p \equiv 5 \mod 6$, לכן קיים $k \in \mathbb{N} \cup \{0\}$ כך ש-$p = 6k + 5$.

$$x^3 - 1 = (x - 1)\left(x^2 + x + 1\right) \equiv 0 \mod p$$

מכאן $x^3 \equiv 1 \mod p$ ובפרט $p \nmid x$. לכן ממשפט פרמה הקטן

$$1 \equiv x^{p-1} = x^{6k+4} = \left(x^3\right)^{2k+1} \cdot x \equiv 1^{2k+1} \cdot x = x \mod p$$

ומכאן

$$3 = 1 + 1 + 1 \equiv x^2 + x + 1 \equiv 0 \mod p$$

סתירה. ■

XIII

הגדרה יהיו $a, n \in \mathbb{N}$. ה<u>מציין</u> של a מודולו n הוא $\min\{k \in \mathbb{N} : n \mid ka\}$.

דוגמה

a	1	2	3	4	5	6
המציין של a	6	3	2	3	6	1

טענה המציין של a מודולו n שווה ל-$\frac{n}{\gcd(a,n)}$.

הוכחה:

$$\frac{n}{\gcd\left(a,n\right)}\cdot a=ka=\frac{a}{\gcd\left(a,n\right)}n$$

נניח כי $k\in\mathbb{N}$ מקיים $n\mid ka$. לכן קיים $t\in\mathbb{N}$ כך ש- $nt=ka$ לכן

$$\frac{n}{\gcd\left(a,n\right)}\cdot t=k\cdot\frac{a}{\gcd\left(a,n\right)}$$

מהיות $\gcd\left(\frac{n}{\gcd(a,n)},\frac{a}{\gcd(a,n)}\right)=1$ אזי $k\mid\frac{n}{\gcd(a,n)}$ ולכן $k\leq\frac{n}{\gcd(a,n)}$. ■

מסקנה המציין של a מודולו n הוא תמיד מחלק של n.

מסקנה כמות המספרים בין $1,\ldots,n$ שהמציין שלהם מודולו n הוא n היא $\varphi\left(n\right)$.

טענה יהיו $n,m\in\mathbb{N}$ כך ש- $m\mid n$. אזי כמות המספרים בין 1 ל-n שהמציין שלהם מודולו n שווה ל-m היא $\varphi\left(m\right)$.

הוכחה: אם עבור $1\leq a\leq n$ המציין של a מודולו n שווה ל-m אזי $n\mid ma$, כלומר קיים $r\in\mathbb{N}$ כך ש- $nr=ma$ ולכן $a=r\frac{n}{m}$. ברור כי $1\leq r\leq m$. נסמן $d=\gcd\left(r,m\right)$ אזי $\frac{m}{d}a=\frac{r}{d}n$ מתחלק ב-n. בגלל שהמציין של a מודולו n שווה ל-m, מתקיים $\frac{m}{d}\leq m$ ולכן $d=1$.

נוכיח כי אם $1\leq r\leq m$ מקיים $\gcd\left(m,r\right)=1$ אזי המציין של $r\frac{n}{m}$ מודולו n הוא m. ברור כי $m\left(r\frac{n}{m}\right)$ מתחלק ב-n.

נניח כי עבור $k\in\mathbb{N}$ מתקיים $k\left(r\frac{n}{m}\right)$ מתחלק ב-n, אזי קיים $t\in\mathbb{N}$ כך ש- $nt=k\left(r\frac{n}{m}\right)$. לכן $tm=kr$ אבל מהיות $\gcd\left(m,r\right)=1$ אזי $k\mid m$ ולכן $m\leq k$ ולכן המציין של $r\cdot\frac{n}{m}$ מודולו n הוא m.

לכן $\forall r\in\left[m\right]$ כך ש-$\gcd\left(m,r\right)=1$ מתקיים שהמציין של $r\frac{n}{m}$ מודולו n הוא m וכל מספר שהמציין שלו מודולו n שווה ל-m הוא מהצורה $r\frac{n}{m}$ כאשר $\gcd\left(m,r\right)$, אזי מספר המספרים שהמציין שלהם מודולו n הוא m הוא מספר ה-r-ים כך ש-$\gcd\left(m,r\right)=1$, שזה בדיוק $\varphi\left(m\right)$.

■

טענה

$$n=\sum_{\mathbb{N}\ni m\mid n}\varphi\left(m\right)$$

הוכחה: $\forall m\in\mathbb{N}$ של n נסמן ב-S_m את קבוצת המספרים מ-1 עד n שהמציין שלהם מודולו n שווה ל-m.

ברור כי $S_{m_1} \cap S_{m_2} = \varnothing$ עבור $m_1 \neq m_2$. מהטענה הקודמת $|S_m| = \varphi(m)$ ומהיות המציין של כל מספר מודולו n מחלק את n אזי $\bigcup_{\mathbb{N} \ni m | n} S_m = \{1, \ldots, n\}$. לכן

$$\sum_{\mathbb{N} \ni m|n} \varphi(m) = \sum_{\mathbb{N} \ni m|n} |S_m| = \left| \bigcup_{\mathbb{N} \ni m|n} S_m \right| = |\{1, \ldots, n\}| = n$$

■

הגדרה יהיו $a, n \in \mathbb{N}$ כך ש-$\gcd(a, n) = 1$. <u>הסדר</u> של a מודולו n הוא $\min\left\{k \in \mathbb{N} : a^k \equiv 1 \mod n\right\}$.

הערה יהיו $a, n \in \mathbb{N}$ כך ש-$\gcd(a, n) = d > 1$, אז לא קיים $k \in \mathbb{N}$ כך ש- $a^k \equiv 1 \mod n$ כי אחרת $n \mid a^k - 1$ ולכן $d \mid a^k - 1$ בסתירה לכך ש-$d \mid a^k$.

טענה יהיו $a, n, k \in \mathbb{N}$ כך שהסדר של a מודולו n שווה ל-k, $l \in \mathbb{N}$. אזי $a^l \equiv 1 \mod n$ אם"ם $k \mid l$.

הוכחה: $\Leftarrow$: קיים $t \in \mathbb{N}$ כך ש-$l = tk$ ולכן $a^l = \left(a^k\right)^t \equiv 1^t = 1 \mod n$.

$\Rightarrow$: נחלק את l ב-k עם שארית ונקבל $l = tk + r$ כאשר $0 \leq r < k$, לכן $a^r = 1^t a^r \equiv \left(a^k\right)^t \cdot a^r = a^l \equiv 1 \mod n$ ולכן $r = 0$ (כי הוא קטן מהטבעי המינימלי שמקיים את הנוסחה הנ"ל) ולכן $l = tk$. ■

מסקנה יהיו $a, n, k \in \mathbb{N}$ כך שהסדר של a מודולו n שווה ל-k, אזי $k \mid \varphi(n)$ (ממשפט פרמה הקטן והטענה הקודמת).

טענה יהיו $a, n, k \in \mathbb{N}$ כך שהסדר של a מודולו n שווה ל-k ויהיו $i, j \in \mathbb{N}$. אזי $a^i \equiv a^j \mod n$ אם"ם $i \equiv j \mod k$.

הוכחה: $\Leftarrow$: קיים $t \in \mathbb{Z}$ כך ש-$j = i + tk$ ולכן

$$a^j = \left(a^k\right)^t \cdot a^i \equiv 1^t \cdot a^i = a^i \mod n$$

$\Rightarrow$: בה"כ $i < j$ ולכן

$$\left(a^{j-i} - 1\right) a^i = a^j - a^i \equiv 0 \mod n$$

ומהיות $\gcd\left(a^i, n\right) = 1$ מתקיים $n \mid a^{j-i} - 1$ ולכן $a^{j-i} \equiv 1 \mod n$. מהטענה הקודמת, $k = j - i$ ולכן $j \equiv i \mod k$. ■

טענה יהיו $a, n \in \mathbb{N}$ כך שהסדר של a מודולו n שווה ל-k ויהי $h \in \mathbb{N}$. אזי הסדר של a^h מודולו n שווה למציין של h מודולו k.

הוכחה: נסמן את המציין של h מודולו k ב-m, ולכן $k \mid mh$ ולכן מהטענה הקודמת

$$\left(a^h\right)^m = a^{mh} \equiv 1 \mod n$$

נניח כי $l \in \mathbb{N}$ מקיים $\left(a^h\right)^l \equiv 1 \mod n$ אזי מהטענה קודמת $k \mid lh$ ומהיות m המציין של h מודולו k, נסיק כי $m \leq l$. ■

XIII

הגדרה תהי R קבוצה. נאמר כי R היא חוג קומוטטיבי עם יחידה (או חוג) אם מתקיימות כל האקסיומות של שדה פרט (אולי) לאקסיומת ההופכי.

דוגמה $\mathbb{Z}$.

דוגמה $\mathbb{Z}_n = \left\{[0]_n, \ldots, [n-1]_n\right\}$ כאשר חיבור וכפל מוגדרים ע"י $[a]_n \cdot [b]_n = [a \cdot b]_n$, $[a]_n + [b]_n = [a+b]_n$.

הערה חוג לא בהכרח מקיים אין מחלקי אפס ($R = \mathbb{Z}_4$, $a = b = [2]_4$).

טענה $\mathbb{Z}_n$ שדה אם"ם n ראשוני.

הוכחה: אם n פריק אזי קיימים $a, b \in \mathbb{N}$, $a, b > 1$ כך ש- $ab = n$ ואז $a, b < n$ ולכן $[a]_n \neq [0]_n \neq [b]_n$ אבל $[a]_n \cdot [b]_n = [0]_n$ ולכן $\mathbb{Z}_n$ לא מקיים אין מחלקי אפס.

נניח כי n ראשוני. יהי $a \in \mathbb{Z}$ כך ש- $[a]_n \neq [0]_n$. אזי $\gcd(a, b) = 1$ ולכן ממשפט שהוכחנו קיים $n > x \in \mathbb{N}$ כך ש-n $ax \equiv 1 \mod n$ ולכן $[x]_n \in \mathbb{Z}_n$ וגם $[a]_n [x]_n = [1]_n$. ■

הגדרה יהי R חוג. קבוצת הפולינומים עם מקדמים ב-R מוגדרת ע"י

$$R[x] = \left\{\sum_{i=0}^{n} a_i x^i : a_I \in R, a_n \neq 0, n \in \mathbb{N}_0\right\} \cup \{0\}$$

נגדיר $\deg\left(a_n x^n + \cdots + a_0\right) = n$, המעלה של הפולינום. נגדיר בנוסף $\deg 0 = -\infty$.

הערה ניתן להגדיר פעולות חיבור וכפל כרגיל ובמקרה זה $R[x]$ הוא גם חוג.

הגדרה יהיו $f, g \in R[x]$, $g \neq 0$. לחלק את f ב-g עם שארית פירושו למצוא $q, r \in R[x]$ כך ש- $f = q \cdot g + r$ וגם $\deg r < \deg g$.

דוגמה $R = \mathbb{Z}$, $f = x, g = 2$. במקרה זה לא ניתן לחלק את g עם שארית (כי לכאורה $\frac{f}{g} = \frac{x}{2} \notin \mathbb{Z}[x]$).

טענה יהי F שדה, $f, g \in F[x]$, $g \neq 0$. אזי ניתן לחלק את f ב-g עם שארית.

הוכחה: נסמן $n = \deg f$, $m = \deg g$. אם $n < m$ נגדיר $r = f, q = 0$.

אחרת, נסמן את המקדם הראשי של g ב-b_m ונגדיר סדרת פולינומים f_i באופן ריקורסיבי:

$$f_1 = f,\ f_{i+1} = f_i - \frac{a_{n_i}}{b_m} x^{n_i - m} \cdot g : n_i = \deg f_i$$

לכן $\deg f_{i+1} < \deg f_i$. לכן קיים $k \in \mathbb{N}$ כך ש- $\deg f_k < \deg g$. נגדיר

$$r = f_k, q = \sum_{i=0}^{k} \frac{a_{n_i}}{b_m} x^{n_i - m}$$

ולכן $f - q \cdot g = r$. ■

טענה יהי F שדה, $f \in F[x]$, $a \in F$. נגדיר $g(x) = x - a \in F[x]$. אזי שארית החלוקה של f ב-g שווה ל-$f(a)$.

הוכחה: $f(x) = q(x)(x-a) + r(x)$. מהיות $\deg r < \deg g = 1$ מתקיים $r \in F$. נציב $x = a$ ונקבל $f(a) = q(a)(a-a) + r$. ■

הגדרה יהיו $f, g \in F[x]$. נאמר כי f <u>מתחלק</u> ב-g אם קיים $q \in F[x]$ כך ש-$f = q \cdot g$.

הגדרה יהי $f \in F[x]$, $a \in F$. נאמר כי a הוא <u>שורש</u> של f אם $f(a) = 0$.

מסקנה יהי F שדה, $f \in F[x]$, $a \in F$. אזי a שורש של f אם"ם f מתחלק ב-$(x-a)$.

טענה יהי F שדה, $f, g, h \in F[x]$ כך ש-$f = g \cdot h$, $a \in F$.

(i) אם a שורש של g, אזי a הוא שורש של f.

(ii) אם a שורש של f, אזי a הוא שורש של g או של h.

הוכחה: (i) $g(a) = 0$ ולכן $f(a) = 0 \cdot h(a) = 0$.

(ii) $f(a) = 0$ ולכן $g(a) h(a) = 0$ ולכן $g(a) = 0$ או $h(a) = 0$. ■

משפט יהי F שדה, $f \in F[x]$, $\deg f = n \geq 1$. אזי ל-f יש לכל היותר n שורשים ב-F.

הוכחה: באינדוקציה על n.

בסיס ($n = 1$): $f(x) = a_1 x + a_0$, $a_1 \neq 0$ ולכן $f(x) = a_1 \left(x + \frac{a_0}{a_1}\right)$ אזי $a = -\frac{a_0}{a_1}$ הוא שורש של f וברור שאין לו שורשים נוספים.

צעד ($n - 1 \to n$): אם ל-f אין שורשים סיימנו. אם $a \in F$ הוא שורש של f אזי קיימים $g \in F[x]$ כך ש- $f(x) = (x-a) g(x)$, $\deg g = n - 1$. מה"א, יש ל-g $n-1$ שורשים לכל היותר. מהטענה הקודמת כל שורש של f הוא שורש של g או שורש של $x - a$ ולכן ל-f יש לכל היותר n שורשים. ■

XIV

דוגמה עבור $n=7$, $\varphi(n)=6$ ולכן

a	1	2	3	4	5	6
הסדר של a	1	3	6	3	6	2

.

$n=8$, $\varphi(n)=4$ ולכן

a	1	3	5	7
הסדר של a	1	2	2	2

.

הגדרה נאמר כי a הוא שורש פרמיטיבי מודלו n אם הסדר של a מודולו n שווה ל-$\varphi(n)$.

טענה יהיו $a,n\in\mathbb{N}$, $\gcd(a,n)=1$, אזי a הוא שורש פרמיטיבי מודולו n אם"ם $\forall b\in\mathbb{N}$ כך ש-$\gcd(b,n)=1$ קיים $l\in\mathbb{N}$ כך ש-$b\equiv a^l \mod n$.

הוכחה: $\Leftarrow$: נסמן ב-r_i את שארית החלוקה של a^i ב-n, אזי $r_1,\dots,r_{\varphi(n)}$ שונים זה מזה (כי אחרת $a^i\equiv a^j \mod n$ ואז $i\equiv j \mod k$ עבור k המציין של a מודולו n ואז). מתקיים

$$\left\{r_1,\dots,r_{\varphi(n)}\right\}\subseteq\{x\in\mathbb{N}:\gcd(x,n)=1,x<n\}$$

ובגלל שמספר האיברים בשתי הקבוצות שוות, אזי הקבוצות שוות, ולכן לכל $n>x\in\mathbb{N}$, כך ש-$\gcd(x,n)=1$, קיים $1\le i\le\varphi(n)$ כך ש-$x=r_i$. $\forall b\in\mathbb{N}$ כך ש-$\gcd(b,n)=1$, נסמן ב-x את שארית החלוקה של b ב-n. לכן $x<n$ ו-$\gcd(x,n)=1$ ונקבל

$$b\equiv x=r_i\equiv a^i \mod n$$

$\Rightarrow$: נסמן ב-k את הסדר של a מודלו n ונסמן ב-r_i את שארית החלוקה של a^i ב-n. $\forall j\in\mathbb{N}$ קיים $1\le i\le k$ כך ש-$a^j\equiv a^i \mod n$ (כאשר i הוא שארית החלוקה של j ב-k). נניח בשלילה כי $k<\varphi(n)$, אזי קיים

$$r\in\{x\in\mathbb{N}:\gcd(x,n)=1,x<n\}$$

כך ש-$r\notin\{r_1,\dots,r_k\}$ סתירה. ■

הגדרה יהי p ראשוני, $a\in\mathbb{N}$, $p\nmid a$. לכן $\varphi(p)=p-1$ ולכן הסדר של a מודולו p מחלק את $p-1$. יהי $d\in\mathbb{N}$ כך ש-$d\mid p-1$. נגדיר $\psi(d)$ להיות כמות המספרים ב-$1,\dots,p-1$ כך שהסדר שלהם מודולו p שווה ל-d.

טענה

$$\sum_{\mathbb{N}\ni d\mid p-1}\psi(d)=p-1$$

הוכחה: $\forall d \in \mathbb{N}$ שמחלק את $p-1$ נסמן T_d את קבוצת המספרים מ-1 עד $p-1$ שהסדר שלהם מודולו p שווה ל-d. אזי מתקיים $|T_d| = \psi(d)$. ברור כי $d_1 \neq d_2 \Rightarrow T_{d_1} \cap T_{d_2} = \varnothing$. בגלל שהסדר של כל מספר מ-1 עד $p-1$ מודולו p מחלק את $p-1$ אזי $\bigcup_{\mathbb{N} \ni d|p-1} T_d = \{1,\ldots,p-1\}$. לכן

$$\sum_{\mathbb{N} \ni d|p-1} \psi(d) = \sum_{\mathbb{N} \ni d|p-1} |T_d| = \left| \bigcup_{\mathbb{N} \ni d|p-1} T_d \right| = |\{1,\ldots,p-1\}| = p-1$$

$\blacksquare$

טענה יהי p ראשוני, $\mathbb{N} \ni d \mid p-1$, אזי $\psi(d) \leq \varphi(d)$.

הוכחה: אם אין איברים מסדר d מודלו p, אזי $\psi(d) = 0$ ונקבל את הדרוש. אם הסדר של a מודולו p שווה ל-d, אזי $[1]_p, [a]_p, \ldots, \left[a^{d-1}\right]_p \in \mathbb{Z}_p$ הם שורשים של $x^d - [1]_p \in \mathbb{Z}_p[x]$ השונים זה מזה. לכן ל-$x^d - [1]_p$ אין שורשים נוספים ב-$\mathbb{Z}_p$. $\forall k \in [d-1]$, הסדר של a^k מודולו p שווה למציין של k מודולו d שהוא שווה ל-$\frac{d}{\gcd(d,k)}$. לכן הסדר של a^k מודולו p שווה ל-d אם"ם $\gcd(d,k) = 1$ ולכן $\psi(d) = \varphi(d)$. $\blacksquare$

משפט יהי p ראשוני, $\mathbb{N} \ni d \mid p-1$, אזי $\psi(d) = \varphi(d)$.

הוכחה:

$$p-1 = \sum_{\mathbb{N} \ni d|p-1} \psi(d) \leq \sum_{\mathbb{N} \ni d|p-1} \varphi(d) = p-1$$

נניח בשלילה שקיים $d \in \mathbb{N}$ כך ש-$d \mid p-1$ וגם $\psi(d) < \varphi(d)$. לכן $p-1 < p-1$ סתירה. $\blacksquare$

מסקנה בין המספרים $1,\ldots,p-1$ יש $\varphi(p-1)$ שורשים פרימיטיביים מודולו p.

$\mathbb{XV}$

טענה יהי $2 < s \in \mathbb{N}$. אזי אין שורש פרימיטיבי מודולו 2^n.

הוכחה: אם $s = 3$ כבר ראינו שאין שורש פרימיטיבי מודולו 8.

עבור $s > 3$ נניח בשלילה שקיים שורש פרימיטיבי מודולו 2^s ונסמנו ב-a. $\forall b \in \mathbb{N}$ כך ש-$\gcd(b,8) = 1$ מתקיים כי b אי זוגי ולכן $\gcd(b,2^s) = 1$. מהיות a שורש פרימיטיבי מודולו 2^s, קיים $l \in \mathbb{N}$ כך ש- $b \equiv a^l \mod 2^s$. מהיות $s > 3$ אזי $8 \mid 2^s$ ולכן $b \equiv a^l \mod 8$ ולכן a הוא שורש פרימטיבי מודולו 8 סתירה. $\blacksquare$

טענה יהי $2 < n \in \mathbb{N}$ אזי $2 \mid \varphi(n)$.

הוכחה: אם קיים $p > 2$ ראשוני כך ש-$n \mid p$ אזי $\varphi(n) \mid p - 1 = \varphi(p)$ ולכן $2 \mid \varphi(n)$. אחרת, קיים $s > 1$ כך ש-$n = 2^s$ ולכן $2 \mid 2^{s-1} = \varphi(n)$. ∎

טענה יהיו $2 < m, n \in \mathbb{N}$ כך ש-$\gcd(n, m) = 1$ אזי אין שורש פרימיטיבי מודולו mn.

הוכחה: יהי $a \in [nm - 1]$ כך ש-$\gcd(a, mn)$ ונוכיח כי $a^{\frac{\varphi(mn)}{2}} \equiv 1 \mod mn$. נראה שקילות מודולו m ו-n וממשפט השאריות הסיני נסיק כי ישנה שקילות מודולו mn.

$$a^{\frac{\varphi(mn)}{2}} = \left(a^{\varphi(m)}\right)^{\frac{\varphi(n)}{2}} \equiv 1^{\frac{\varphi(n)}{2}} = 1 \mod m$$

ובאותו האופן עבור n ולכן ממשפט השאריות הסיני קיבלנו את השקילות הרצוי. כלומר, מצאנו שהסדר של a קטן או שווה ל-$\frac{\varphi(mn)}{2}$ סתירה להגדרת ש"פ. ∎

מסקנה יהי $p > 2$ ראשוני, $4, p \mid l \in \mathbb{N}$ אזי אין ש"פ מודולו l.

הוכחה: יהי $s \in \mathbb{N}$ המקסימלי כך ש-$l \mid p^s$, נסמן $m = p^s$, $n = \frac{l}{m}$. נשים לב כי $4 \mid n$ וכן $m \mid p$. לכן $mn > 2$. בנוסף, $p \nmid n$ ולכן $\gcd(m, n) = 1$. לכן אין ש"פ מודולו $l = mn$. ∎

מסקנה יהיו $p, q > 2$ ראשוניים, $p, q \mid l \in \mathbb{N}$ אזי אין ש"פ מודולו l.

הוכחה: יהי $s \in \mathbb{N}$ מקסימלי כך ש-$l \mid p^s$ ונסמן $m = p^s$, $n = \frac{l}{m}$. נשים לב כי $q \mid n$ ובנוסף $m \mid p$ ולכן $m, n > 2$. מעבר לכך $p \nmid n$ ולכן $\gcd(m, n) = 1$ ולכן אין ש"פ מודולו $l = mn$. ∎

משפט (□) יהי $p > 2$ ראשוני, $n = p^s$ או $n = 2p^s$ אז קיים ש"פ מודולו n.

XVI

טענה יהי $p > 2$ ראשוני, $a \in \mathbb{N}$ ש"פ מודולו p, אזי $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

הוכחה: $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \mod p$ ולכן $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. a ש"פ מודולו p ולכן הסדר שלו מודולו p הוא $p - 1$ ולכן לא ייתכן כי $a^{\frac{p-1}{2}} \equiv 1 \mod p$ ולכן בהכרח ש-$a^{\frac{p-1}{2}} \equiv -1 \mod p$. ∎

משפט (ווילסון) יהי $p > 2$ ראשוני, אזי $(p-1)! \equiv -1 \mod p$.

הוכחה: יהי a ש"פ מודולו p. מהיות $p \nmid a$ אזי $p \nmid a^n$, $\forall n \in \mathbb{N}$. נסמן $A = [p-1]$ ונגדיר $f \in A^A$ ע"י $f(x)$ היא שארית החלוקה של a^x ב-p. הפ' מוגדרת היטב כי $\forall x$, $f(x) \neq 0$ כי $p \nmid a^x$. בגלל שהסדר של a מודולו p שווה ל-$p-1$, $\forall x \neq y \in A$ מתקיים $a^x \not\equiv a^y \mod p$ (כי $x \not\equiv y \mod p-1$ והוכחנו קשר בין סדר למציין). לכן f חח"ע ולכן היא גם על ולכן $A = \{f(1), \ldots, f(p-1)\}$ ולכן

$$(p-1)! = 1 \cdot \ldots \cdot (p-1) = f(1) \cdot \ldots \cdot f(p-1) \equiv a^1 \cdot \ldots \cdot a^{p-1}$$
$$= a^{1+\ldots+(p-1)} = a^{\frac{(p-1)p}{2}} = \left(a^{\frac{p-1}{2}}\right)^p \equiv (-1)^p = -1 \mod p$$

■

טענה (תנאי מספיק לקיום שורש מ--1) יהי p ראשוני. אם $p \equiv 1 \mod 4$ אזי למשוואה $x^2 \equiv -1 \mod p$ קיים פתרון שלם.

הוכחה: נסמן ב-a ש"פ מודולו p. נסמן $k = \frac{p-1}{4}$, $2k = \frac{p-1}{2}$. לכן $\left(a^k\right)^2 = a^{2k} = a^{\frac{p-1}{2}} \equiv -1 \mod p$ לכן $x = a^k$ הוא פתרון המשוואה. ■

טענה יהי p ראשוני. אם $p \equiv 1 \mod 6$ אז למשוואה הקונגרואציה $x^2 + x + 1 \equiv 0 \mod p$ קיים פתרון שלם (ראינו את הצד השני בעבר)

הוכחה: יהי a ש"פ מודולו p. נסמן $k = \frac{p-1}{6}$ אזי $2k = \frac{p-1}{3}$. לכן

$$\left(a^{2k} - 1\right)\left(a^{2k} + a^{2k} + 1\right) = \left(a^{2k}\right)^3 - 1 = a^{p-1} - 1 \equiv 0 \mod p$$

ולכן $p \mid a^{2k} - 1$ או $p \mid a^{4k+a2k+1}$. נשים לב כי $a^{2k} \not\equiv 1 \mod p$ כי אחרת יש סתירה למינימליות הסדרת של הש"פ. לכן $a^{4k} + a^{2k} + 1 \equiv 0 \mod p$ ולכן $x = a^{2k}$ הוא פתרון למשוואה. ■

II

תזכורת אם a הוא ש"פ מודולו n, אז $\forall b \in \mathbb{Z}$, $\gcd(b,n) = 1$ קיים $l \in \{0, \ldots, \varphi(n) - 1\}$ כך ש- $a^l \equiv b \mod n$.

תזכורת יהי p ראשוני, a ש"פ מודולו p. $\forall i \in \{0, \ldots, p-1\}$ נסמן ב-r_i את שארית החלוקה של a^i ב-p. אז $\{r_0, \ldots, r_{p-1}\} = \{1, \ldots, p-1\}$.

הגדרה יהי p ראשוני, a ש"פ מודולו p, $b \in \mathbb{Z}$, $p \nmid b$. <u>האינדקס</u> של b מודולו p ביחס ל-a הוא $i \in \mathbb{N} \cup \{0\}$ מינימלי כך ש-$a^i \equiv b \mod p$.

הערה נסמן את האינדקס ב-$\mathrm{ind}_a b$.

הערה מהטענה הנ"ל קיים תמיד $\mathrm{ind}_a b$.

תכונות של ind

1. $\text{ind}_a 1 = 0$.
2. $\text{ind}_a (b \cdot c) \equiv \text{ind}_a b + \text{ind}_a c \mod (p-1)$.
3. $\text{ind}_a b^s \equiv s \cdot \text{ind}_a b \mod (p-1)$.

דוגמה $p = 7$. $3, 5$ הם ש"פ מודולו 7.

b	1	2	3	4	5	6
$\text{ind}_3 b$	0	2	1	4	5	3
$\text{ind}_5 b$	0	4	5	2	1	3

טענה יהי p ראשוני, a שפ"מ p, $c, d \in \mathbb{N}$, $p \nmid c, d$, $s \in \mathbb{N}$. למשוואה $cx^s \equiv d \mod p$ קיים פתרון אם"ם למשוואה $\text{ind}_a c + s \cdot y \equiv \text{ind}_a d \mod (p-1)$ קיים פתרון ובמקרה זה $y = \text{ind}_a x$.

הוכחה: $\Rightarrow$: נניח כי $y = \text{ind}_a x$ (x כלשהו שמקיים את זה) הוא פתרון של המשוואה ולכן $a^y \equiv x \mod p$. לכן

$$c \cdot x^s \equiv a^{\text{ind}_a c} (a^y)^s = a^{\text{ind}_a c + sy} \equiv a^{\text{ind}_a d} \equiv d \mod p$$

$\Leftarrow$: נניח כי x הוא פתרון של המשוואה. נסמן $y = \text{ind}_a x$. לכן $a^y \equiv x \mod p$

$$a^{\text{ind}_a c + sy} = a^{\text{ind}_a c} (a^y)^s \equiv cx^s \equiv d \equiv a^{\text{ind}_a d} \mod p$$

ומהיות a ש"פ, $\text{ind}_a c + sy \equiv \text{ind}_a d \mod (p-1)$. ■

שאלה פתרו את המשוואה $2x^3 \equiv 5 \mod 7$.

פתרון נבחר $a = 5$. $\text{ind}_5 2 = 4, \text{ind}_5 5 = 1$ ולכן המשוואה שקולה ל-$3y + 4 \equiv 1 \mod 6$ ולכן $3y \equiv 3 \mod 6$ אם"ם $y \equiv 1 \mod 2$ (חלוקה ב-gcd) ולכן $y \equiv 1, 3, 5 \mod 6$ פותרים את המשוואה השקולה ולכן $x \equiv 5, 6, 3 \mod 7$ הם פתרונות המשוואה.

שאלה פתרו $3x^2 + x + 4 \equiv 0 \mod 7$.

פתרון המשוואה שקולה ל-$x^2 + 5x + 6 \equiv 0 \mod 7 \iff x^2 - 2x + 1 \equiv 2 \mod 7 \iff (x-1)^2 \equiv 2 \mod 7$ ועם $x' = x - 1$ נקבל $x'^2 \equiv 2 \mod 7$. נבחר $a = 5$. לכן המשוואה שקולה ל-$2y \equiv 4 \mod 6$ ובחלוקה ב-gcd נקבל שקילות ל-$y \equiv 2 \mod 3$ וזה מתקיים עבור $y \equiv 2, 5 \mod 6$ ולכן $x' \equiv 4, 3 \mod 7$ ולכן $x \equiv 4, 5 \mod 7$ הם פתרונות למשוואה המקורית.

III

הגדרה יהי $p > 2$ ראשוני ו-$k \in \mathbb{Z}$, $p \nmid k$. נאמר כי k הוא <u>שארית ריבועית</u> אם למשוואת הקונגרואנציה $x^2 \equiv k \mod p$ קיים פתרון ו<u>שארית אי ריבועית</u> אחרת.

דוגמה עבור $p=3$, 1 הוא שארית ריבועית ואילו 2 הוא שארית אי ריבועית.

טענה יהיו $p>2$ ראשוני, a ש"פ מודולו p, $k\in\mathbb{Z}$, $p\nmid k$. אזי k הוא שארית ריבועית מודולו p אם"ם $\mathrm{ind}_a k$ זוגי.

הוכחה: למשוואה $x^2 \mod p$ קיים פתרון אם"ם למשוואה $2y\equiv \mathrm{ind}_a k \mod p-1$ קיים פתרון. אם $\mathrm{ind}_a k$ זוגי, אזי $y=\frac{\mathrm{ind}_a k}{2}$ הוא פתרון למשוואה האחרונה. אחרת, נקבל $2\mid p-1\mid 2y-\mathrm{ind}_a k$ ולכן $\mathrm{ind}_a k$ זוגי סתירה. ■

מסקנה יהי $p>2$ ראשוני, a,b ש"פ מודולו p, $k\in\mathbb{Z}$, $p\nmid k$, אזי $\mathrm{ind}_a k\equiv \mathrm{ind}_b k \mod 2$.

מסקנה בין המספרים $1,\dots,p-1$ יש בדיוק $\frac{p-1}{2}$ שאריות ריבועיות.

הוכחה: נבחר a ש"פ מודולו p. אזי $k\mapsto \mathrm{ind}_a k$ מגדיר פ' חחע"ל מ-$\{1,\dots,p-1\}$ ל-$\{0,\dots,p-2\}$. בקבוצה $\{0,\dots,p-2\}$ יש $\frac{p-1}{2}$ מספרים זוגיים ולכן בקבוצה $\{1,\dots,p-1\}$ יש $\frac{p-1}{2}$ שאריות ריבועיות. ■

משפט (קריטריון אוילר) יהי $p>2$ ראשוני, $k\in\mathbb{Z}$, $p\nmid k$.

1. אם k ש"ר מודולו p אזי $k^{\frac{p-1}{2}}\equiv 1 \mod p$.
2. אם k ש"א מודולו p אזי $k^{\frac{p-1}{2}}\equiv -1 \mod p$.

הוכחה:

1. קיים $x\in\mathbb{Z}$ כך ש- $x^2\equiv k \mod p$. $p\nmid x$ כי $p\nmid k$ ולכן $k^{\frac{p-1}{2}}\equiv \left(x^2\right)^{\frac{p-1}{2}}=x^{p-1}\overset{\text{פרמה}}{\equiv} 1 \mod p$.
2. נבחר a ש"פ מודולו p. מהטענה הקודמת $\mathrm{ind}_a k$ אי זוגי ולכן $k^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}\cdot \mathrm{ind}_a k}=\left(a^{\frac{p-1}{2}}\right)^{\mathrm{ind}_a k}\overset{\text{מהטענה הבאה}}{\equiv}(-1)^{\mathrm{ind}_a k}=-1$ $\mod p$.

■

טענה יהי $p>2$ ראשוני, a ש"פ מודולו p, אזי $a^{\frac{p-1}{2}}\equiv -1 \mod p$.

הוכחה: $\left(a^{\frac{p-1}{2}}\right)^2=a^{p-1}\equiv 1 \mod p$ ולכן $a^{\frac{p-1}{2}}\equiv 1 \mod p$ או $a^{\frac{p-1}{2}}\equiv -1 \mod p$. מהיות a ש"פ, אזי הסדר של a מודולו p הוא $p-1$ ולכן $a^{\frac{p-1}{2}}\not\equiv 1 \mod p$ ולכן $a^{\frac{p-1}{2}}\equiv -1 \mod p$. ■

הגדרה יהי $p>2$ ראשוני ו-$k\in\mathbb{Z}$, $p\nmid k$. $\left(\frac{p}{k}\right)=\begin{cases}1 & \text{הוא ש"ר } k\\ -1 & \text{הוא ש"א } k\end{cases}$ הוא <u>סמל לז'נדר</u>.

הערה קריטריון אוילר קובע כי $\left(\frac{k}{p}\right)\equiv k^{\frac{p-1}{2}} \mod p$.

תכונות

1. יהיו $k,l \in \mathbb{Z}$ כך ש- $p \nmid k$ ו-$k \equiv l \mod p$, אזי $\left(\frac{k}{p}\right) = \left(\frac{l}{p}\right)$.
2. יהיו $k,l \in \mathbb{Z}$ כך ש- $p \nmid k$ ו-$k \equiv l^2 \mod p$, אזי $\left(\frac{k}{p}\right) = 1$.
3. יהיו $k,l \in \mathbb{Z}$ $p \nmid k,l$ אזי $\left(\frac{kl}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{l}{p}\right)$. **הוכחה:** מקריטריון אוילר $\left(\frac{kl}{p}\right) \equiv (kl)^{\frac{p-1}{2}} = k^{\frac{p-1}{2}} l^{\frac{p-1}{2}} \equiv \left(\frac{k}{p}\right)\left(\frac{l}{p}\right) \mod p$.
מאחר שהמספרים בשני האגפים הם או 1 או -1, אזי הם חייבים להיות שווים, כי אחרת נקבל $1 \equiv -1 \mod p$ סתירה. ∎
4. אם $p \equiv 1 \mod 4$ אזי $\left(\frac{-1}{p}\right) = 1$. אם $p \equiv 3 \mod 4$ אזי $\left(\frac{-1}{p}\right) = -1$.

דוגמאות לחישוב סמל לז'נדר

.1

$$\left(\frac{3}{23}\right) = \left(\frac{3+2\cdot 23}{23}\right) = \left(\frac{49}{23}\right) = \left(\frac{7^2}{23}\right) = 1$$

.2

$$\left(\frac{7}{23}\right) = \left(\frac{7-23}{23}\right) = \left(\frac{-16}{23}\right) = \left(\frac{-1\cdot 4^2}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{4^2}{23}\right) \overset{(4)}{=} 1\cdot(-1)$$

.3

$$\left(\frac{5}{17}\right) = \left(\frac{-12}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{3}{17}\right)\left(\frac{2^2}{17}\right) = 1\cdot 1\cdot\left(\frac{3}{17}\right) \equiv 3^8 = 81^2 \equiv (-4)^2 = 16 \equiv -1 \mod 17$$

טענה יהי $p > 2$ ראשוני כך ש-$q = 2p+1$ הוא גם ראשוני אזי -4 הוא ש"פ מודולו q.

הוכחה: הסדר של -4 מודולו q הוא מחלק של $q-1 = 2p$ (הסדר מחלק כל מספר שהעלה בחזקתו תניב 1 מודולו q) ולכן הוא אחד מהמספרים הבאים, $1, 2, p, 2p$.

אם הסדר של -4 מודולו q הוא 1 או 2 אזי $(-4)^2 \equiv 1 \mod q$ ולכן $15 \equiv 0 \mod q$ ולכן $q \mid 15$ ולכן $q = 3, 5$ וזה לא יתכן כי $p > 2$.

אם הסדר הוא p אזי $(-4)^p \equiv 1 \mod q$ $4^p = (-1)^p 4^p = -2^{2p} = -2^{q-1} \overset{\text{פרמה}}{\equiv} -1$ סתירה (q ראשוני אי זוגי). לכן בהכרח שהסדר של -4 מודולו q הוא $q-1 = 2p$ ולכן -4 הוא ש"פ מודולו q. ∎

III

משפט (הלמה של גאוס I) יהי $p>2$ ראשוני, $p\nmid a\in\mathbb{Z}$. $\forall i\in\left[\frac{p-1}{2}\right]$, נגדיר r_i להיות שארית החלוקה של ai ב-p. נסמן $R=\left\{r_i : i\in\left[\frac{p-1}{2}\right]\right\}$, $S=\left\{x\in R : x>\frac{p}{2}\right\}$, $n=|S|$. אזי $\left(\frac{a}{p}\right)=(-1)^n$.

הוכחה: נשים לב כי כל $r_i\in R$ שונים זה מזה כי אחרת היינו מקבלים ש-p מחלק מספר שקטן ממנו (וחיובי). נגדיר $T=R\backslash S\left\{x\in R : x\le\frac{p-1}{2}\right\}$, $U=\{p-x : x\in S\}\subseteq\left\{1,\dots,\frac{p-1}{2}\right\}$. $|T|=\frac{p-1}{2}-n, |U|=n$.

נוכיח כי $T\cap U=\varnothing$. נניח בשלילה כי קיים $x\in T\cap U$. מהיות $x\in T$ קיים $i\in\left[\frac{p-1}{2}\right]$ כך ש-$x\equiv ai \mod p$. מהיות $x\in U$ קיים $y\in S$ כך ש-$x=p-y$ ולכן קיים $j\in\left[\frac{p-1}{2}\right]$ כך ש-$y\equiv aj \mod p$. לכן $x+y=p$ ולכן $a(i+j)\equiv p\equiv 0 \mod p$ אבל $\gcd(a,p)=1$ ולכן $i+j\equiv 0 \mod p$ אבל $i,j\in\left[\frac{p-1}{2}\right]$ ולכן $i+j\le p-1$ סתירה.

לכן $|T\cup U|=|T|+|U|=\frac{p-1}{2}$ ובנוסף $T\cup U\subseteq\left\{1,\dots\frac{p-1}{2}\right\}$ ולכן $T\cup U=\left[\frac{p-1}{2}\right]$. נסמן $S=\{s_1,\dots,s_n\}$, $T=\left\{t_1,\dots,t_{\frac{p-1}{2}-n}\right\}$. לכן

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &= \prod_{x\in T\cup U} x \\
&= t_1\cdot\dots\cdot t_{\frac{p-1}{2}-n}\cdot(p-s_1)\cdot\dots\cdot(p-s_n) \\
&\equiv r_{i_1}\cdot\dots\cdot r_{i_{\frac{p-1}{2}-n}}\cdot\left(p-r_{i_{\frac{p-1}{2}-n+1}}\right)\cdot\dots\cdot\left(p-r_{i_{\frac{p-1}{2}}}\right) \\
&\equiv (-1)^n\cdot r_{i_1}\cdot\dots\cdot r_{i_{\frac{p-1}{2}}} \\
&\equiv (-1)^n\, ai_1\cdot\dots\cdot ai_{\frac{p-1}{2}} \\
&\equiv (-1)^n\, a^{\frac{p-1}{2}} i_1\cdot\dots\cdot i_{\frac{p-1}{2}} \\
&\equiv (-1)^n\, a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \mod p
\end{aligned}$$

כל המעבר לשאריות עובד כי השאריות שונות כולן (אחרת סתירה כי מספר שקטן מ-p מתחלק בו) ובנוסף $t_i\neq s_j$ כי הוכחנו ש-$T\cap U=\varnothing$.

אבל $\gcd\left(\left(\frac{p-1}{2}\right)!,p\right)=1$ ולכן $(-1)^n a^{\frac{p-1}{2}}\equiv 1 \mod p$ ולכן $a^{\frac{p-1}{2}}\equiv(-1)^n \mod p$ ומקריטריון אוילר $\left(\frac{a}{p}\right)\equiv(-1)^n \mod p$ ומהיות שני האגפים שווים ל-±1, אזי $\left(\frac{a}{p}\right)=(-1)^n$. ■

דוגמה $\left(\frac{5}{17}\right)$. $\left\{ai : i\in\left[\frac{p-1}{2}\right]\right\}=\{5,10,15,20,\dots,40\}$, $R=\{5,10,15,3,8,13,1,6\}$, $S=\{10,15,13\}$, $\left(\frac{5}{17}\right)=(-1)^3=-1$.

טענה יהי $p>2$ ראשוני.

$$\left(\frac{2}{p}\right)=\begin{cases}1 & p\equiv 1 \mod 8\\ -1 & p\equiv 3 \mod 8\\ -1 & p\equiv 5 \mod 8\\ 1 & p\equiv 7 \mod 8\end{cases}$$

הוכחה: נניח כי $p\equiv 1 \mod 8$. לכן קיים $k\in\mathbb{N}$ כך ש-$p=8k+1$. $R=\left\{r_1,\dots,r_{\frac{p-1}{2}}\right\}=\{2,4,\dots,2\cdot 4k\}$, $S=\{4k+2,4k+4,\dots,8k\}$ ולכן $n=|S|=2k$ ולכן $\left(\frac{2}{p}\right)=(-1)^{2k}=1$.

נניח כי $p\equiv 3 \mod 8$ ולכן קיים $k\in\mathbb{N}$ כך ש-$p=8k+3$. $R=\{2,\dots,2\cdot(4k+1)\}$, לכן $S=\{4k+2,\dots,8k+2\}$ ולכן $n=|S|=2k+1$ ולכן $\left(\frac{2}{p}\right)=(-1)^{2k+1}=-1$.

נניח כי $p\equiv 5 \mod 8$ ולכן $p=8k+5$, $R=\{2,\dots,2(4k+2)\}$, $S=\{4k+4,\dots 8k+4\}$ ולכן $n=|S|=2k+1$ ולכן $\left(\frac{2}{p}\right)=(-1)^{2k+1}=-1$.

נניח כי $p\equiv 7 \mod 8$ ולכן $p=7k+5$, $R=\{2,\dots,2(4k+3)\}$, $S=\{4k+4,\dots 8k+6\}$ ולכן $n=|S|=2k+2$ ולכן $\left(\frac{2}{p}\right)=(-1)^{2k+2}=1$. ■

מסקנה יהי $p>2$ ראשוני. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

הוכחה: נניח כי $p\equiv \pm1 \mod 8$, אז קיים $k\in\mathbb{N}$ כך ש-$p=8k\pm1$. $\frac{p^2-1}{8}=\frac{(8k\pm1)^2-1}{8}=\frac{64k^2\pm16k}{8}=2\left(4k^2+k\right)$ ולכן זוגי.

נניח כי $p\equiv \pm3 \mod 8$ אז קיים $k\in\mathbb{N}$ כך ש-$p=8k\pm3$. $\frac{p^2-1}{8}=\frac{(8k\pm3)^2-1}{8}=\frac{64k^2\pm48k+8}{8}=2\left(4k^2+3k\right)+1$ ולכן אי זוגי. ■

$\mathbb{IV}$

דוגמה $\left(\frac{50}{71}\right)=\left(\frac{2}{71}\right)\left(\frac{5^2}{71}\right)=1\cdot1=1$.

דוגמה $\left(\frac{53}{71}\right)=\left(\frac{-18}{71}\right)=\left(\frac{-1}{71}\right)\left(\frac{2}{71}\right)\left(\frac{3^2}{71}\right)=-1\cdot1\cdot1=1$.

טענה יש אינסוף מספרים ראשוניים מהצורה $8n+7$.

הוכחה: נניח בשלילה כי יש מספר סופי של מספרים ראשוניים מהצורה $8n+7$ ונסמנם $p_1,\dots,p_k$. נגדיר $a=8p_1^2\cdot\ldots\cdot p_k^2-1$. נשים לב כי למשוואה $x^2\equiv 2 \mod a$ יש פתרון. נגדיר $x=4p_1\cdot\dots\cdot p_k$ ולכן $x^2-2=16p_1^2\cdot\ldots\cdot p_k^2-2=2a\equiv 0 \mod a$ ולכן לכל ראשוני q כך ש-$q\mid a$ למשוואה $x^2\equiv 2 \mod q$ יש פתרון ($q\mid a\mid x^2-2$) ולכן $q\not\equiv 3 \mod 8$ וגם $q\not\equiv 5 \mod 8$ (אחרת $\left(\frac{2}{q}\right)=-1$ בסתירה לכך ש-a ש"ר מודולו 2). בנוסף, $q\not\equiv 7 \mod 8$ כי אחרת קיים i כך ש-$q=p_i$ (מהגדרת p_i) ולכן $a=8p_1^2\cdot\ldots\cdot p_k^2-1$ מתחלק ב-$p_i=q$ סתירה. בנוסף $2\nmid a$. לכן כל הגורמים הראשוניים של a נותנים שארית 1 בחלוקה ב-8. לכן נשאר רק $a\equiv 1 \mod 8$ ולכן $8p_1^2\cdot\ldots\cdot p_k^2\equiv 2 \mod 8$ סתירה. ■

משפט (הלמה של גאוס II) יהי $p>2$ ראשוני, $a\in\mathbb{N}$, $p\nmid a,2$ אזי $\left(\frac{a}{p}\right)=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{a\cdot i}{p}\right\rfloor}$.

הוכחה: $\forall i\in\left[\frac{p-1}{2}\right]$ נסמן את ב-r_i את שארית החלוקה של $a\cdot i$ ב-p. נסמן

$$R=\left\{r_1,\dots,r_{\frac{p-1}{2}}\right\},S=\left\{s\in R:x\geq\frac{p+1}{2}\right\},T=R\backslash S,U=\{p-x:x\in S\}$$

נסמן בנוסף $n=|S|$. מהלמה הקודמת מתקיים $T\uplus U=\left[\frac{p-1}{2}\right]$.

$$\begin{aligned}\sum_{i=1}^{\frac{p-1}{2}} a\cdot i &= \sum_{i=1}^{\frac{p-1}{2}}\left(\lfloor\frac{ai}{p}\rfloor p+r_i\right)\\ &= \sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor p+\sum_{i=1}^{\frac{p-1}{2}} r_i\\ &= \sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor p+\sum_{t\in T} t+\sum_{s\in S} s\\ &= \sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor p+\sum_{t\in T} t+\sum_{u\in U}(p-u)\\ &= \sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor p+\sum_{t\in T} t-\sum_{u\in U} u+pn\end{aligned}$$

ובנוסף $\sum_{i=1}^{\frac{p-1}{2}} i=\sum_{t\in T} t+\sum_{u\in U} u$ ולכן אם נחסיר את המשוואות נקבל

$$(a-1)\sum_{i=1}^{\frac{p-1}{2}} i=\sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor p-2\sum_{u\in U} u+pn$$

ובמודולו 2, משום ש-$a,p\equiv 1 \mod 2$, נקבל $0\equiv \sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor+n \mod 2$ ולכן $\sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor\equiv n \mod 2$ ולכן $\left(\frac{a}{p}\right)=(-1)^n=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{ai}{p}\rfloor}$ יחד עם הלמה של גאוס I. ■

דוגמה $a=5,p=17$.

$$\lfloor\frac{5}{17}\rfloor+\lfloor\frac{10}{17}\rfloor+\lfloor\frac{15}{17}\rfloor+\lfloor\frac{20}{17}\rfloor+\lfloor\frac{25}{17}\rfloor+\lfloor\frac{30}{17}\rfloor+\lfloor\frac{35}{17}\rfloor+\lfloor\frac{40}{17}\rfloor=0+0+0+1+1+1+2+2=7$$

ולכן $\left(\frac{5}{17}\right)=-1$.

משפט (חוק ההדדיות של גאוס) יהיו $p,q>2$ ראשוניים. אזי $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

הוכחה: נגדיר $A=\left[\frac{p-1}{2}\right]\times\left[\frac{q-1}{2}\right]$, $\ell=\left\{(x,y)\in\mathbb{R}^2:y=\frac{q}{p}x\right\}$ ונשים לב כי $A\cap\ell=\varnothing$ כי אם בשלילה קיים $(x,y)\in A$ כך ש-$y=\frac{q}{p}x$ אזי $yp=xq$ ולכן $p\mid xq$ ולכן $p\mid x$ ולכן $p\geq x$ בסתירה לכך ש-$x\leq\frac{p-1}{2}$.

נגדיר $B=\left\{(x,y)\in A: y<\frac{q}{p}x\right\},C=\left\{(x,y)\in A: y>\frac{q}{p}x\right\}$ ולכן $B\cap C=\varnothing$ וגם $B\cup C=A$ ולכן $|A|=|B|+|C|$.

$$|B|=\left|\underbrace{\left\{(1,y)\in A: y<\frac{q}{p}\right\}}_{\text{איברים } \lfloor\frac{q}{p}\rfloor}\cup\underbrace{\left\{(2,y)\in A: y<\frac{q}{p}\right\}}_{\text{איברים } \lfloor\frac{2q}{p}\rfloor}\cup\ldots\cup\underbrace{\left\{\left(\frac{p-1}{2},y\right)\in A: y<\frac{q}{p}\right\}}_{\text{איברים } \lfloor\frac{\left(\frac{p-1}{2}\right)q}{p}\rfloor}\right|=\sum_{i=1}^{\frac{p-1}{2}}\lfloor\frac{qi}{p}\rfloor$$

ובאותו האופן $|C|=\sum_{i=1}^{\frac{q-1}{2}}\lfloor\frac{pi}{q}\rfloor$ ולכן

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\overset{\text{הלמה השנייה}}{=}(-1)^{|C|}(-1)^{|B|}=(-1)^{|A|}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

■

מסקנה יהיו $q,p>2$ ראשוניים. אם $q\equiv 1 \mod 4$ או $p\equiv 3 \mod 4$ אזי $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$. אם $p\equiv 3 \mod 4$ וגם $p\equiv 3 \mod 4$ אז $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$.

דוגמה

$$\left(\frac{85}{97}\right)=\left(\frac{5}{97}\right)\left(\frac{17}{97}\right)\overset{97,5\equiv 1 \mod 4}{=}\left(\frac{97}{5}\right)\left(\frac{97}{17}\right)=\left(\frac{2}{5}\right)\left(\frac{12}{17}\right)$$
$$(-1)\left(\frac{2^2}{17}\right)\left(\frac{3}{17}\right)=(-1)\left(\frac{17}{3}\right)=(-1)\left(\frac{2}{3}\right)=(-1)(-1)=1$$

דוגמה

$$\left(\frac{79}{127}\right)=-\left(\frac{127}{79}\right)=-\left(\frac{48}{79}\right)=-\left(\frac{4^2}{79}\right)\left(\frac{3}{79}\right)=-\left(-\left(\frac{79}{3}\right)\right)=\left(\frac{1}{3}\right)=1$$

$\mathbb{V}$

טענה יהי $p>3$ ראשוני. $\left(\frac{3}{p}\right)=\begin{cases}1 & p\equiv 1 \mod 12\\ -1 & p\equiv 5 \mod 12\\ -1 & p\equiv 7 \mod 12\\ 1 & p\equiv 11 \mod 12\end{cases}$.

הוכחה: ■

1. $p \equiv 1 \mod 4$ וגם $p \equiv 1 \mod 3$ אז $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.
2. $p \equiv 1 \mod 4$ וגם $p \equiv 2 \mod 3$ אז $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.
3. $p \equiv 3 \mod 4$ וגם $p \equiv 1 \mod 3$ ולכן $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
4. $p \equiv 3 \mod 4$ וגם $p \equiv 2 \mod 3$ ולכן $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = 1$.

טענה יהי $2 < s \in \mathbb{N}$ כך ש-$p = 2^s - 1$ ראשוני. אזי $\left(\frac{3}{p}\right) = -1$.

הוכחה: מאחר ש-$4 \mid 2^s = p + 1$ מתקיים $p \equiv 3 \mod 4$. מאחר ש-p ראשוני גם s ראשוני ולכן $2 \nmid s$, כלומר $s = 2k + 1$ עבור $k \in \mathbb{N}$ ולכן

$$p = 2^s - 1 = 2^{2k+1} - 1 = 2 \cdot 4^k - 1 \equiv 2 \cdot 1^k - 1 = 1 \mod 3$$

ולכן $p \equiv 7 \mod 12$ ולכן $\left(\frac{3}{p}\right) = -1$. ■

משפט יהי $1 \neq s \in \mathbb{N}$ כך ש-$p = 2^s + 1$ ראשוני, אז s זוגי.

הוכחה: נניח בשלילה כי $2 \nmid s$ אזי כמו בטענה הקודמת $p \equiv 3 \mod 3$ ולכן $3 \mid p$ אבל $p > 3$ ולכן p לא ראשוני סתירה. ■

טענה יהי $1 \neq s \in \mathbb{N}$ כך ש-$p = 2^s + 1$ ראשוני אזי $3^{2^{s-1}} \equiv -1 \mod p$.

הוכחה: $2^s = p - 1 \mid 4$ מתקיים כי $p \equiv 1 \mod 4$. מהמשפט הנ"ל $2 \mid s$ ולכן $s = 2k$ עם $k \in \mathbb{N}$ ולכן

$$p = 2^s + 1 = 2^{2k} + 1 = 4^k + 1 \equiv 1^k + 1 = 2 \mod 3$$

ולכן $p \equiv 5 \mod 12$ ולכן $\left(\frac{3}{p}\right) = -1$. לפי קריטריון אוילר $3^{2^{s-1}} = 3^{\frac{p-1}{2}} \equiv -1 \mod p$. ■

טענה יהי $1 \neq s \in \mathbb{N}$ כך ש-$3^{2^{s-1}} \equiv -1 \mod 2^s + 1$ אזי $2^s + 1$ ראשוני.

הוכחה: יהי q גורם ראשוני של $2^s + 1$. אז $3^{2^{s-1}} \equiv -1 \mod q$. נסמן ב-$k$ את הסדר של 3 מודולו q. $3^{2^s} \equiv (-1)^2 = 1 \mod q$ ולכן $k \mid 2^s$ מתכונות הסדר. לכן $k = 2^l$ עבור $s \geq l \in \mathbb{N}$. אילו $l < s$ אז $l \leq s - 1$ ואז $3^{s^{s-1}} = 3^{2^l 2^{s-l-1}} = \left(3^k\right)^{2^{l-s-1}} \equiv 1 \mod q$ סתירה. לכן $l = s$ ולכן $k = 2^s$. מהיות $3^{q-1} \equiv 1 \mod q$ מתקיים כי $k \leq q - 1$ ולכן $q \geq 2^s + 1$. אבל $q \leq 2^s + 1$ ולכן $q = 2^s + 1$. ■

טענה יהי $s \in \mathbb{N}$ כך ש-2^s+1 ראשוני, אזי קיים $k \in \mathbb{N} \cup \{0\}$ כך ש-$s = 2^k$.

הוכחה: נניח בשלילה של-s יש גורם ראשוני אי זוגי q. אז $s = qm$, $m \in \mathbb{N}$.

$$2^s + 1 = (2^m)^q + 1 = (2^m+1)\left(1 - 2^m + (2^m)^2 - (2^m)^3 + \cdots + 2^{(q-1)m}\right)$$

■

הגדרה יהי p ראשוני. נגדיר $v_p : \mathbb{N} \to \mathbb{N} \cup \{0\}$ ע"י $v_p(n) = \max\left\{i \in \mathbb{Z} : p^i \mid n\right\}$, $\forall n$.

דוגמה $v_2(12) = 2$, $v_3(12) = 1$, $v_5(12) = 0$.

תכונות

1. יהי $n = p_1^{s_1} \cdot \ldots \cdot p_k^{s_k}$ פירוק של n גורמים ראשוניים. אז $v_{p_i}(n) = s_i$ ו-$v_p(n) = 0$ עבור $p \neq p_i$, $\forall i$.
2. $v_p(1) = 0$.
3. $v_p(a \cdot b) = v_p(a) + v_p(b)$.
4. $v_p\left(a^k\right) = k v_p(a)$.
5. אם $a \mid b$ אז $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.

$\mathbb{VI}$

כיצד נחשב את $v_p(n!)$, עבור p ראשוני, $n \in \mathbb{N}$? $v_p(n!) = \sum\limits_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$.

דוגמה $n = 10, p = 2$.

$$v_2(10!) = \lfloor \frac{10}{2} \rfloor + \lfloor \frac{10}{4} \rfloor + \lfloor \frac{10}{6} \rfloor + \lfloor \frac{10}{8} \rfloor = 5 + 2 + 1 + 0 = 8$$

טענה יהי p ראשוני, $n \in \mathbb{N}$ כך ש-$n < p \leq 2n$. אזי $v_p\left(\binom{2n}{n}\right) = 1$.

הוכחה: $v_2\left(\binom{2n}{n}\right) = v_p(2n!) - 2v_p(n!)$ ובמקרה זה $v_p(n!) = 0$ כי $\lfloor \frac{n}{p^i} \rfloor = 0$, $\forall i \in \mathbb{N}$. $v_p(2n!) = 1$ כי $1 \leq \frac{2n}{p} < 2$ ולכן $\lfloor \frac{2n}{p} \rfloor = 1$. בנוסף, $\frac{2n}{p^i} < 1$, $\forall i \geq 2$ ולכן $\lfloor \frac{2n}{p^i} \rfloor = 0$, $\forall i \geq 2$. ■

הגדרה נגדיר $\pi:[2,\infty)\to\mathbb{N}$ ע"י $\pi\left(x\right)=\left|\left\{ p\in\mathbb{N}:\text{ראשוני }p,p\leq x\right\} \right|$.

דוגמה $\pi\left(2\right)=1$, $\pi\left(\frac{5}{2}\right)=1$, $\pi\left(4\right)=2$.

תכונות של פונקצייה סופרת ראשוניים

1. π עולה (לא ממש).
2. $\pi\left(x\right)=\pi\left(\left\lfloor x\right\rfloor \right)$, $\forall x\geq2$.
3. $\pi\left(2n\right)\leq n$, $\forall n\in\mathbb{N}$.

משפט (צ'בישב) קיימים $0<c_{1},c_{2}\in\mathbb{R}$ כך ש-$c_{1}\frac{x}{\log_{2}x}\leq\pi\left(x\right)\leq c_{2}\frac{x}{\log_{2}x}$, $\forall x\geq2$, או במילים אחרות, $\pi\left(x\right)=\Theta\left(\frac{x}{\log_{2}x}\right)$.

טענה $\forall n\in\mathbb{N}$ מתקיים $\pi\left(2n\right)-\pi\left(n\right)\leq\frac{2n}{\log_{2}n}$.

הוכחה: הוכחנו כי $\forall p$ ראשוני כך ש-$n<p\leq2n$, מתקיים $p\mid\binom{2n}{n}$ ולכן $\left(\prod_{n<p\leq2n:\text{ראשוני }p}p\right)\mid\binom{2n}{n}$. $\pi\left(2n\right)-\pi\left(n\right)$ הוא מספר הראשוניים בין n (לא כולל) ל-$2n$ (כולל). לכן

$$n^{\pi\left(2n\right)-\pi\left(n\right)}<\left(\prod_{n<p\leq2n:\text{ראשוני }p}p\right)\leq\binom{2n}{n}=\frac{1\cdot2\cdot\ldots\cdot\left(2n-1\right)2n}{1\cdot1\cdot2\cdot2\cdot\ldots\cdot n\cdot n}<2^{2n}$$

כלומר $n^{\pi\left(2n\right)-\pi\left(n\right)}<2^{2n}$ וניקח $\log_{n}$ ונקבל $\pi\left(2n\right)-\pi\left(n\right)<2n\log_{n}2=\frac{2n}{\log_{2}n}$. ■

טענה יהי $r\in\mathbb{N}$, אזי מתקיים $\pi\left(2^{r}\right)\leq\frac{3}{r}2^{r}$.

הוכחה: נוכיח באינדוקציה על r.

בסיס ($r\leq5$): $\pi\left(2^{r}\right)\leq2^{r-1}=\frac{3}{r}2^{r}\frac{r}{6}<\frac{3}{r}2^{r}$.

צעד ($r\to r+1$):

$$\begin{aligned}\pi\left(2^{r+1}\right) & =\pi\left(2^{r+1}\right)-\pi\left(2^{r}\right)+\pi\left(2^{r}\right)\\
 & <\frac{2^{r+1}}{r}+\frac{3}{r}2^{r}\\
 & =\frac{5}{r}2^{r}\\
 & =\frac{5\left(r+1\right)2^{r+1}}{2r\left(r+1\right)}\\
 & <\frac{5}{2}\cdot\frac{6}{5}\cdot\frac{2^{r+1}}{r+1}\\
 & =\cdot\frac{32^{r+1}}{r+1}
\end{aligned}$$

■

טענה $\forall x\geq 2$,$\pi\left(x\right)\leq 6\frac{x}{\log_{2}x}$.

הוכחה: עבור $r=\lfloor\log_{2}x\rfloor$, $2^{r}\leq x<2^{r+1}$. בנוסף, $\frac{1}{r+1}<\frac{1}{\log_{2}x}\leq\frac{1}{r}$ ולכן

$$\pi\left(x\right)\leq\pi\left(2^{r+1}\right)\leq\frac{3}{r+1}2^{r+1}=\frac{6}{r+1}2^{r}<\frac{6}{\log_{2}x}x$$

■

טענה $\forall x\in\mathbb{R}$,$\lfloor 2x\rfloor-2\lfloor x\rfloor\in\{0,1\}$. נסמן $\{x\}=x-\lfloor x\rfloor$.

הוכחה:

$$\begin{aligned}\lfloor 2x\rfloor-2\lfloor x\rfloor&=\lfloor 2\left(\lfloor x+\{x\}\right)\rfloor-2\lfloor x\rfloor\\&=\lfloor 2\lfloor x\rfloor+2\left\{x\right\}\rfloor-2\lfloor x\rfloor\\&=2\lfloor x\rfloor+\lfloor 2\left\{x\right\}\rfloor-2\lfloor x\rfloor\\&=\lfloor 2\left\{x\right\}\rfloor\end{aligned}$$

■

טענה יהיו $r,n\in\mathbb{N}$ כך ש-$v_{p}\left(\binom{2n}{n}\right)\geq r$, אזי $p^{r}\leq 2n$.

הוכחה: נניח בשלילה כי $p^{r}>2n$.

$$\begin{aligned}v_{p}\left(\binom{2n}{n}\right)&=v_{p}\left((2n)!\right)-2v_{p}\left(n!\right)=\sum_{i=1}^{\infty}\left(\lfloor\frac{2n}{p^{i}}\rfloor-2\lfloor\frac{n}{p^{i}}\rfloor\right)=\sum_{i=1}^{r-1}\left(\lfloor\frac{2n}{p^{i}}\rfloor-2\lfloor\frac{n}{p^{i}}\rfloor\right)\\&\leq r-1\end{aligned}$$

סתירה. ■

טענה $\forall n\in\mathbb{N}$, מתקיים $\frac{n}{\log_{2}(2n)}\leq\pi\left(2n\right)$.

הוכחה: לפי הטענה הנ"ל, $\forall n,p\in\mathbb{N}$, p ראשוני, מתקיים $p^{v_{p}\left(\binom{2n}{n}\right)}\leq 2n$.

$$(2n)^{\pi(2n)}\geq\prod_{p|\binom{2n}{n}\text{ ראשוני}}p^{v_{p}\left(\binom{2n}{n}\right)}=\binom{2n}{n}=\frac{1\cdot 2\cdot\ldots\cdot(2n-1)\,2n}{1\cdot 1\cdot 2\cdot 2\cdot\ldots\cdot n\cdot n}\geq 2^{n}$$

ולכן $(2n)^{\pi(2n)} \ge 2^n$, ניקח $\log_{2n}$ ולכן $\pi(2n) \ge n\log_{2n} 2 = \frac{n}{\log_2(2n)}$. ■

טענה $\frac{1}{4} \cdot \frac{x}{\log_2 x} \le \pi(x)$, $\forall x \ge 2$.

הוכחה: נסמן $n = \lfloor \frac{x}{2} \rfloor$ ולכן $n \le \frac{x}{2} < n+1$ ולכן $2n \le x < 2n+2$. בנוסף, $n \le \frac{n+1}{2} < \frac{x}{4}$.

$$\pi(x) \ge \pi(2n) \ge \frac{n}{\log_2(2n)} \ge \frac{n}{\log_2 x} > \frac{1}{4} \cdot \frac{x}{\log_2 x}$$

■

מסקנה (משפט צ'בישב) עם $c_1 = \frac{1}{4}, c_2 = 6$.

הערה $\lim\limits_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log_2 x}} = \log_2 e$.

VIII

דוגמה נבדוק האם המספרים הראשונים הם סש"ר (סכום של ריבועיים (טבעיים)).

1	2	3	4	5	6	7	8	9	10
✓	✓	×	✓	✓	×	×	✓	✓	✓

טענה יהיו $m, n \in \mathbb{N}$ כך ש-n הוא סש"ר אזי ניתן להציג גם את $m^2 n$ כסש"ר.

הוכחה: ברור. ■

טענה (סגירות לסש"ר) יהיו $m, n \in \mathbb{N}$ סש"רים, אזי ניתן להציג גם את $m \cdot n$ כסש"ר.

הוכחה: קיימים $a, b, c, d \in \mathbb{Z}$ כך ש-$n = a^2 + b^2, m = c^2 + d^2$. לכן קיימים $e, f \in \mathbb{Z}$ כך ש-$(a+bi)(c+di) = e + fi$.

$$nm = |a+bi|^2 |c+di|^2 = |e+fi|^2 = e^2 + f^2$$

■

טענה יהי $p, n \in \mathbb{N}$ כך ש-p ראשוני, $p \equiv 3 \mod 4$ וגם $2 \nmid v_p(n)$. אז n לא סש"ר.

הוכחה: נניח בשלילה כי קיימים $a, b \in \mathbb{Z}$ כך ש-$n = a^2 + b^2$. נסמן $d = \gcd(a,b)$ ולכן $d^2 \mid a^2, b^2$ ולכן $d^2 \mid n$.

נסמן $n' = \frac{n}{d^2}$, לכן $n' = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2$. לכן מתקיים $2 \nmid v_p(n) - 2v_p(d) = v_p(n')$ ולכן $p \mid n'$. נסמן $u = \frac{a}{d}, v = \frac{b}{d}$. לכן $\gcd(u,v) = 1$ ולכן $p \nmid u$ או $p \nmid v$ (הם זרים).

בה"כ $u \nmid p$. אז קיים $w \in \mathbb{Z}$ כך ש-$uw \equiv 1 \mod p$, ולכן $w^2n' = w^2u^2 + w^2v^2$. לכן $0 \equiv w^2n' \equiv 1 + (wv)^2 \mod p$ ולכן wv הוא פתרון משוואת הקונגרואנציה $1 + x^2 \equiv 0 \mod p$ סתירה לכך שקיים פתרון כזה אם"ם $p \equiv 1 \mod 4$. ■

טענה יהיו $p \in \mathbb{N}$ ראשוני ו-$a, b, t \in \mathbb{Z}$ כך ש-$1 < t < p$ וגם $a^2 + b^2 = tp$. אז קיימים $c, d, u \in \mathbb{Z}$ כך ש-$c^2 + d^2 = up$ וגם $0 < u < t$.

הוכחה: קיימים $r, s \in \mathbb{Z}$ כך ש-$s \equiv b \mod t$ ו-$r \equiv a \mod t$ וגם $|r|, |s| < \frac{t}{2}$. לכן $r^2 + s^2 \equiv a^2 + b^2 \equiv 0 \mod t$. לכן קיים $u \in \mathbb{N} \cup \{0\}$ כך ש-$r^2 + s^2 = ut$. לכן

$$(ar + bs)^2 + (as - br)^2 = \left(a^2 + b^2\right)\left(r^2 + s^2\right) = ut^2p$$

אבל $ar + bs \equiv a^2 + b^2 \equiv 0 \mod t$ ובנוסף $as - br \equiv ab - ba = 0 \mod t$. נסמן $c = \frac{ar+bs}{t}, d = \frac{as-br}{t}$ ולכן נקבל $c^2 + d^2 = up$.

נוכיח כי $u < t$, נוכיח כי $ut < t^2$.

$$ut = r^2 + s^2 < \frac{t^2}{4} + \frac{t^2}{4} = \frac{t^2}{2} < t^2$$

בנוסף, $u \neq 0$ כי אחרת $r = s = 0$, כלומר $t \mid a, b$ ואז $t^2 \mid a^2 + b^2 = tp$ ולכן $t \mid p$ אבל $1 < t < p$ סתירה. ■

טענה יהי $p \in \mathbb{N}$ ראשוני כך ש-$p \equiv 1 \mod 4$, אז ניתן להציג את p כסש"ר.

הוכחה: קיים $x \in [p-1]$ כך ש-$p \mid x^2 + 1$. $t = \min\left\{z \in \mathbb{N} : \exists a, b \in \mathbb{Z}, a^2 + b^2 = zp\right\} = \min A$ הקבוצה הזו לא ריקה כי עבור $z = \frac{x^2+1}{p}$, מתקיים $x^2 + 1^2 = zp$. כמו כן,

$$t \leq \frac{x^2+1}{p} \leq \frac{(p-1)^2 + 1}{p} = \frac{p^2 - 2p + 2}{p} < \frac{p^2}{p} = p$$

נניח בשלילה כי $t > 1$. מהטענה הנ"ל, קיים $u < t$ שנמצא ב-A סתירה. ■

משפט יהי $n \in \mathbb{N}$. ניתן להציג את n כסש"ר אם"ם לכל $p \in \mathbb{N}$ ראשוני כך ש-$p \equiv 3 \mod 4$, מתקיים $2 \mid v_p(n)$.

הוכחה: $\Leftarrow$: כבר הוכחנו.

$\Rightarrow$: נפרק את n לגורמים ראשוניים, $n = 2^r p_1^{s_1} \cdot \ldots \cdot p_k^{s_k} \cdot q_1^{t_1} \cdot \ldots \cdot p_l^{t_l}$ כאשר p_i, q_j ראשוניים וכן $p_i \equiv 1 \mod 4, q_j \equiv 3 \mod 4$. לכן $2 \mid v_{q_j}(n)$ ולכן $2 \mid t_j$, $\forall j$. נסמן $m = q_1^{\frac{t_1}{2}} \cdot \ldots \cdot q_l^{\frac{t_l}{2}}$. לכן $n = 2^r p_1^{s_1} \cdot \ldots \cdot p_k^{s_k} m^2$. לכל i ניתן להציג את p_i כסש"ר. בנוסף ניתן להציג את 2 כסש"ר. משתי הטענות הראשונות נובע כי ניתן להציג את n כסש"ר. ■

$\mathbb{VIII}$

טענה יהיו $m, n \in \mathbb{N}$ כך שניתן להציג אותם כסכום של ארבעה ריבועים (סא"ר). אז ניתן להציג גם את mn כסא"ר.

הוכחה: קיימים $a, \ldots, h \in \mathbb{Z}$ כך ש-$m = a^2 + b^2 + c^2 + d^2, n = e^2 + f^2 + g^2 + h^2$. נגדיר

$$x_1 = a + bi, x_2 = c + di, y_1 = e + fi, y_2 = g + hi$$

לכן $m = |x_1|^2 + |x_2|^2 = \det \left(\begin{smallmatrix} x_1 & x_2 \\ -\overline{x_2} & \overline{x_1} \end{smallmatrix}\right)$ ובאותו האופן $n = |y_1|^2 + |y_2|^2 = \det \left(\begin{smallmatrix} y_1 & y_2 \\ -\overline{y_2} & \overline{y_1} \end{smallmatrix}\right)$.

$$\left(\begin{smallmatrix} x_1 & x_2 \\ -\overline{x_2} & \overline{x_1} \end{smallmatrix}\right) \left(\begin{smallmatrix} y_1 & y_2 \\ -\overline{y_2} & \overline{y_1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} x_1 y_1 - x_2 \overline{y_2} & x_1 y_2 + x_2 \overline{y_1} \\ -\overline{x_2} y_1 - \overline{x_1}\,\overline{y_2} & -\overline{x_2} y_2 + \overline{x_1}\,\overline{y_1} \end{smallmatrix}\right)$$

נגדיר $z_1 = x_1 y_1 - x_2 \overline{y_2}, z_2 = x_1 y_2 + x_2 \overline{y_1}$. לכן

$$\begin{aligned} mn &= \det \left(\begin{smallmatrix} x_1 & x_2 \\ -\overline{x_2} & \overline{x_1} \end{smallmatrix}\right) \det \left(\begin{smallmatrix} y_1 & y_2 \\ -\overline{y_2} & \overline{y_1} \end{smallmatrix}\right) \\ &= \det \left(\begin{smallmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{smallmatrix}\right) \end{aligned}$$

והמספרים z_1, z_2 הם שלמים.

$$\begin{aligned} z_1 &= (a + bi)(e + fi) - (c + di)(g - hi) \\ &= (ae - bf - cg - dh) + (af + be + ch - dg) \\ z_2 &= (a + bi)(g + hi) + (c + di)(e - fi) \\ &= (ag - bh + ce + df) + (ah + bg - cf + de) \end{aligned}$$

$\blacksquare$

טענה יהי $p \in \mathbb{N}$ ראשוני. אז למשוואת הקונגאונציה $x^2 + y^2 \equiv -1 \mod p$ קיים פתרון.

הוכחה: נסמן $S = \left\{\mathbb{N} \ni x \le p - 1 : \left(\frac{x}{p}\right) = 1\right\} \cup \{0\}$ כלומר כל המספרים שניתן לייצג כריבוע של מספר טבעי מודולו p. אז $|S| = \frac{p+1}{2}$. אם קיים $i \in \left\{0, \ldots, \frac{p-1}{2} - 1\right\}$ כך ש-$i \in S$ וגם $p - 1 - i \in S$ אז קיימים $x, y \in \mathbb{Z}$ כך ש-$x^2 \equiv i \mod p$ ו-$y^2 \equiv p - 1 - i \mod p$ וסיימנו. אחרת, $\left|S \setminus \left\{\frac{p-1}{2}\right\}\right| \le \frac{p-1}{2}$ (כי יש בדיוק $\frac{p-1}{2}$ זוגות של ש"ר או 0 וש"א, ואז חסר ש"ר אחד בזוגות, כי 0 לא ש"ר) ולכן $\frac{p-1}{2} \in S$. אז קיים $x \in \mathbb{Z}$ כך ש-$x^2 \equiv \frac{p-1}{2} \mod p$ וסיימנו. $\blacksquare$

מסקנה $\forall p \in \mathbb{N}$ ראשוני קיים $p > t \in \mathbb{N}$ כך שניתן להציג את tp כסא"ר.

הוכחה: לפי הטענה הנ"ל קיימים $x, y \in \mathbb{Z}$ כך ש- $p \mid x^2 + y^2 + 1$. קיימים $r, s \in \mathbb{Z}$ כך ש-$-\frac{p}{2} < r, s < \frac{p}{2}$ כך ש-$s \equiv y \mod p$ ו-$r \equiv x \mod p$. לכן $p \mid r^2 + s^2 + 1$. בנוסף, מתקיים $r^2 + s^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2$. נגדיר $t = \frac{r^2+s^2+1}{p}$ ונקבל $t < p$. ■

טענה יהי $p > 2$ ראשוני, $a, b, c, d, t \in \mathbb{Z}$ כך ש-$a^2 + b^2 + c^2 + d^2 = tp$, $1 < t < p$. אז קיימים $e, f, g, h, u \in \mathbb{Z}$ כך ש- $e^2 + f^2 + g^2 + h^2 = up$ וגם $0 < u < t$.

הוכחה: מקרה א': t אי זוגי. לכן קיימים $v, w, r, s \in \mathbb{Z}$ כך ש-$-\frac{t}{2} < r, s, v, w < \frac{t}{2}$ (קטן ממש כי t אי זוגי) כך ש-

$$r \equiv a \mod t$$

$$s \equiv b \mod t$$

$$v \equiv c \mod t$$

$$w \equiv d \mod t$$

ולכן $r^2 + s^2 + v^2 + w^2 \equiv 0 \mod t$. נגדיר $u = \frac{r^2+s^2+v^2+w^2}{t}$ ולכן $r^2 + s^2 + v^2 + w^2 = ut$ ולכן

$$\begin{aligned} ut^2p &= \left(a^2+b^2+c^2+d^2\right)\left(r^2+s^2+v^2+w^2\right) \\ &= (ar+bs+cv+dw)^2 + (as-br+cw-dv)^2 + (av-bw-cr+ds)^2 + (aw+bv-cr-ds)^2 \end{aligned}$$

ולכן

$$\alpha = ar + bs + cv + dw \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \mod t$$

$$\beta = as - br + cw - dv \equiv ab - ba + cd - dd = 0 \mod t$$

$$\gamma = av - bw - cr + ds \equiv ac - bd - ca + db \equiv 0 \mod t$$

$$\delta = aw + bv - cr - ds \equiv ab + bc - cb - ba = 0 \mod t$$

ולכן $up = \left(\frac{\alpha}{t}\right)^2 + \left(\frac{\beta}{t}\right)^2 + \left(\frac{\gamma}{t}\right)^2 + \left(\frac{\delta}{t}\right)^2$. $u > 0$ כי אחרת $r = s = v = w = 0$ ואז $t \mid a, b, c, d$ ולכן $t^2 \mid a^2 + b^2 + c^2 + d^2 = tp$ ולכן $t \mid p$ סתירה. בנוסף, $ut = r^2 + s^2 + v^2 + w^2 < \frac{t^2}{4} = t^2$ ולכן $u < t$.

מקרה ב': t זוגי: לכן בין המספרים a, b, c, d יש מספר זוגי של אי זוגיים. בה"כ $a \equiv b \mod 2$ ו-$c \equiv d \mod 2$. נגדיר

$$g = \frac{c+d}{2}, h = \frac{c-d}{2}, e = \frac{a+b}{2}, f = \frac{a-b}{2}, u = \frac{t}{2}$$

ונקבל את הרצוי. ■

טענה כל ראשוני ניתן להצגי כסא"ר.

הוכחה: נסמן $t=\min\left\{x<p:\exists a,b,c,d\in\mathbb{Z},a^2+b^2+c^2+d^2=xp\right\}=\min A$. מהמסקנה $A\neq\varnothing$ ולכן אכן קיים לה מינימום. אם $1<t$ אז מהטענה הנ"ל קיים $0<u<t$ כך ש- $u\in A$ בסתירה למינימליות. לכן קיימים $a,b,c,d\in\mathbb{Z}$ כך ש- $a^2+b^2+c^2+d^2=p$.

■

משפט (לגרנז') כל מספר טבעי ניתן להצגה כסא"ר.

הוכחה: כל מספר טבעי הוא מכפלה של ראשוניים ומסגירות לכפל של סא"ר ומהטענה נקבל את הרצוי. ■

IX

הגדרה $\mathbb{Z}[i]=\{a+bi\in\mathbb{C}:a,b\in\mathbb{Z}\}$.

הערה $\mathbb{Z}[i]$ סגורה לחיבור, כפל ונגדי, אך לא להופכי. לכן היא חוג.

הגדרה נגדיר $N:\mathbb{Z}[i]\to\mathbb{N}\cup\{0\}$, ע"י $N(a+bi)=|a+bi|^2=a^2+b^2$.

טענה $N(z_1z_2)=N(z_1)N(z_2)$.

הגדרה יהי R חוג ו-$a\in R$. נאמר כי a <u>הפיך</u> אם קיים $b\in R$ כך ש-$ab=1$. קבוצת האיברים ההפיכים ב-R מסומנת ב-R^*.

דוגמה $\mathbb{Z}^*=\{1,-1\}$, $\mathbb{F}[x]^*=\{c\in\mathbb{F}:c\neq 0\}$.

טענה $\mathbb{Z}[i]^*=\{z\in\mathbb{Z}[i]:N(z)=1\}$.

הוכחה: יהי $z\in\mathbb{Z}[i]$ כך ש-$N(z)=1$ אז $\overline{z}$ הוא הופכי של z כי $z\cdot\overline{z}=N(z)=1$. אם $z\in\mathbb{Z}[i]$ הפיך אזי קיים $z'\in\mathbb{Z}[i]$ כך ש-$z'z=1$. $N(z')N(z)=1$ אבל $N\in\mathbb{N}\cup\{0\}$ ולכן $N(z')=N(z)=1$. ■

מסקנה $\mathbb{Z}[i]^*=\{1,-1,i,-i\}$.

הוכחה: אם $a+bi\in\mathbb{Z}[i]^*$ אז $a^2+b^2=N(a+bi)=1$ ולכן או ש-$b=0$ ו-$a=\pm1$ או ש-$a=0$ ו-$b=\pm1$. ■

הגדרה נאמר כי $z_1\in\mathbb{Z}[i]$ מתחלק ב-$z_2\in\mathbb{Z}[i]$ אם קיים $q\in\mathbb{Z}[i]$ כך ש-$z_1=qz_2$.

טענה $\forall z_1\in\mathbb{Z}[i],z_2\in\mathbb{Z}[i]^*$ אזי $z_2\mid z_1$.

טענה אם $z_2\mid z_1\in\mathbb{Z}[i]$ אז $N(z_2)\mid N(z_1)$.

הוכחה: קיים $q\in\mathbb{Z}[i]$ כך ש-$z_1=qz_2$ ולכן $N(z_1)=N(q)N(z_2)$ ולכן $N(z_2)\mid Z(z_1)$. ■

מסקנה אם $N(z_1) \mid N(z_2)$ וגם $N(z_2) \mid N(z_1)$ אזי $N(z_1)=N(z_2)$.

מסקנה אם $z_1,z_2\in\mathbb{Z}[i]$ מקיימים $z_2 \mid z_1$ וגם $z_1 \mid z_2$ אזי קיים $q\in\mathbb{Z}[i]^*$ כך ש-$z_1=qz_2$ (פשוט להסתכל על המנה).

הגדרה יהיו $z_2,z_1\in\mathbb{Z}[i]$ כך ש-$z_1 \mid z_2$ וגם $z_2 \mid z_1$. במקרה כזה נאמר כי הם <u>חברים</u>.

הגדרה יהי $0\neq z\in\mathbb{Z}[i]$ נקרא פריק אם קיימים $z_1,z_2\in\mathbb{Z}[i]\setminus\mathbb{Z}[i]^*$ כך ש-$z=z_1z_2$.

הגדרה $0\neq z\in[i]$ נקרא ראשוני אם הוא לא פריק ולא הפיך.

טענה אם $z_1,z_2\in\mathbb{Z}[i]$ חברים אז z_1 ראשוני אם"ם z_2 ראשוני.

טענה אם $z_1,z_2\in\mathbb{Z}[i]$ ראשוניים כך ש-$z_1 \mid z_2$ אזי z_1,z_2 חברים.

טענה אם $z\in\mathbb{Z}[i]$ כך ש-$N(z)$ ראשוני ב-$\mathbb{N}$ אז z ראשוני ב-$\mathbb{Z}[i]$.

הוכחה: ברור כי $z\neq 0$ ו-$z\notin\mathbb{Z}[i]^*$. נניח כי $z_1,z_2\in\mathbb{Z}[i]$ כך ש-$z=z_1z_2$. מהיות $N(z)=N(z_1)N(z_2)$ אזי $N(z_1)=1$ או $N(z_2)$ ולכן $z_1\in\mathbb{Z}[i]^*$ או $z_2\in\mathbb{Z}[i]^*$ ולכן z ראשוני. ■

מסקנה יהי $a,b,p\in\mathbb{N}$ כך ש-p ראשוני וגם $p=a^2+b^2$ אז $a+bi$ ראשוני ב-$\mathbb{Z}[i]$.

מסקנה אם $p\in\mathbb{N}$ ראשוני כך ש-$p\equiv 1 \mod 4$ או $p=2$, אז p פריק ב-$\mathbb{Z}[i]$ וקיימים $z_1z_2\in\mathbb{Z}[i]$ ראשוניים ב-$\mathbb{Z}[i]$ כך ש-$p=z_1z_2$.

טענה אם p ראשוני כך ש-$p\equiv 3 \mod 4$ אז p ראשוני ב-$\mathbb{Z}[i]$.

הוכחה: נניח כי $z_1,z_2\in\mathbb{Z}[i]$ כך ש-$p=z_1z_2$. לכן $p^2=N(p)=N(z_1)N(z_2)$. אם $N(z_1)=1$ או $N(z_2)=1$ אז $z_1\in\mathbb{Z}[i]^*$ או $z_2\in\mathbb{Z}[i]^*$ וסיימנו. אחרת, $N(z_1)=N(z_2)=p$. נסמן $z_1=a+bi$. אז $a^2+b^2=p\equiv 3 \mod 4$ סתירה. ■

הערה יהיו $z_1,z_2\in\mathbb{Z}[i]$, $z_2\neq 0$. לחלק את z_1 ב-z_2 בשארית פירושו מציאת $q,r\in\mathbb{Z}[i]$ כך ש-$z_1=qz_2+r$ וגם $N(r)<N(z_2)$.

$\mathbb{X}$

טענה אם $z_1,z_2\in\mathbb{Z}[i]$, $z_2\neq 0$ אז ניתן לחלק את z_1 ב-z_2 עם שארית.

הוכחה: נסמן $\frac{z_1}{z_2}=z=a+bi\in\mathbb{C}$. נבחר $c,d\in\mathbb{Z}$ כך ש-$|a-c|\leq\frac{1}{2}$ וגם $|b-d|\leq\frac{1}{2}$. נגדיר $q=c+di$. נגדיר $r=z_1-qz_2$ ונוכיח כי $N(r)<N(z_2)$. נגדיר $N:C\to[0,\infty)$ ע"י $N(z)=|z|^2$ אזי $N(w_1,w_2)=N(w_1)N(w_2)$, $\forall w_1,w_2\in\mathbb{C}$.

$$\frac{N(r)}{N(z_2)}=N\left(\frac{r}{z_2}\right)=N\left(\frac{z_1-qz_2}{z_2}\right)=N(z-q)=(a-c)^2+(b-d)^2\leq\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2<1$$

לכן $N(r)<N(z_2)$. ■

טענה יהיו $z_1, z_2 \in \mathbb{Z}[i]$, $z_2 \neq 0$ אז קיים $w \in \mathbb{Z}[i]$ כך ש:

1. $z_1 \mid w$, $z_2 \mid w$.
2. אם $w' \in \mathbb{Z}[i]$ מקיים $z_1 \mid w'$ וגם $z_2 \mid w'$, אזי $w \mid w'$.

הוכחה:

1. בה"כ $|z_2| \leq |z_1|$. נבנה סדרה z באופן ריקורסיבי. z_{i+2} הוא שארית החלוקה של z_i ב-z_{i+1}, z_1, z_2 כבר מוגדרים. אז $N(z_{i+1}) < N(z_i)$ לכל $i \geq 2$ ולכן קיים $k \notin \mathbb{N}$ כך ש-$N(z_k) \neq 0$ אבל $N(z_{k+1}) = 0$. נגדיר $w = z_k$. לכן $z_{k-1} \mid w$ (הוא z_k הוא המחלק ב-z_{k-1} עם שארית שהיא $z_{k+1} = 0$) ולכן $z_{k-2} \mid w$ וכן הלאה עד z_1, z_2.
2. יהי $w' \in \mathbb{Z}[i]$ כך ש-$z_2 \mid w'$ וגם $z_1 \mid w'$. לכן $z_3 = z_1 - q_2 z_2 \mid w'$ וכן הלאה עד $z_k = w \mid w'$.

הגדרה $w \in \mathbb{Z}[i]$ המקיים את תנאי הטענה נקרא $\gcd(z_1, z_2)$.

הערה אם $w, \widetilde{w}$ הם $\gcd(z_1, z_2)$ אז ברור שהם חברים.

טענה אם $w \in \mathbb{Z}[i]$ הוא $\gcd(z_1, z_2)$ אז קיימים $s, t \in \mathbb{Z}[i]$ כך ש-$w = sz_1 + tz_2$.

הוכחה: כמו ב-$\mathbb{Z}$. ■

טענה אם $z_1, z_2 \in \mathbb{Z}[i]$, $p \in \mathbb{Z}[i]$ ראשוני גאוס כך ש-$p \mid z_1 z_2$ אז $p \mid z_1$ או $p \mid z_2$.

הוכחה: כמו ב-$\mathbb{Z}$. ■

משפט לכל $0 \neq z \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$ קיימים ראשוני גאוס $p_1, \ldots, p_k$ (לא בהכרח שונים) כך ש-$z = p_1 \cdot \ldots \cdot p_k$ ופירוק זה יחיד עד כדי סדר הגורמים וחברות. כלומר, אם $q_1, \ldots, q_l$ ראשוני גאוס כך ש-$z = q_1 \cdot \ldots \cdot q_l$ אז $l = k$ וקיימת $\sigma \in S_k$ כך ש-$p_i, q_{\sigma(i)}$ חברים, $\forall i \in [k]$.

הגדרה יהי $0 \neq a + bi \in \mathbb{Z}[i]$ נקרא <u>קנוני</u> אם $a > 0, b \geq 0$ (כלומר נמצא ברביע הראשון + ציר x במישור המרוכב).

טענה לכל $0 \neq z \in \mathbb{Z}[i]$ קיים חבר קנוני יחיד.

משפט לכל $0 \neq z \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$ קיימים $p_1, \ldots, p_k$ ראשוניי גאוס קנוניים ו-$s_1, \ldots, s_k \in \mathbb{N}$, ו-$e \in \mathbb{Z}[i]^*$ כך ש-$z = e p_1^{s_1} \cdot \ldots \cdot p_k^{s_k}$. פירוק זה יחיד עד כדי סדר.

דוגמה נמצא פירוק קנוני עבור $6 + 30i$. $6 + 30i = 2 \cdot 3(1 + 5i)$. $3 \equiv 3 \mod 4$ ולכן 3 ראשוני גאוס (כי ראשוני רגיל) אבל $2 = (1+i)(1-i)$ והנורמות של גורמים אלו הן ראשוניות ולכן הם ראשוניי גאוס. $N(1 + 5i) = 26$, $N(1 + i) = 2$ ונבדוק האם $1 + i$ מחלק את $1 + 5i$. הוא אכן כן ומקיים $1 + 5i = (1 + i)(3 + 2i)$ ולכן

$$
\begin{aligned}
6 + 30i &= (1 + i)(1 - i)\, 3\, (1 + i)(3 + 2i) \\
&= (-i) \cdot 3\, (1 + i)^3 (3 + 2i)
\end{aligned}
$$

וזה פירוק קנוני.

הגדרה יהי $0 \neq d \in \mathbb{Z}$. משוואה דיאפנטית $x^2 - dy^2 = 1$ נקראת <u>משוואת פל</u>.

הערה $\forall d$, $(1,0)$ ו-$(-1,0)$ הם פתרונות למשוואה. נקרא להם פתרונות טריוויאלים.

הערה אם $d < -1$ אז לא קיים פתרון לא טריוויאלי למשוואה. אם $d = -1$ אז הפתרונות הלא טריוויאליים היחידים הם $(0,1)$, $(0,-1)$.

הערה אם קיים $c \in \mathbb{N}$ כך ש-$d = c^2$ אז לא קיים פתרון לא טריוויאלי כי אם (x,y) הוא פתרון אז $(x-cy)(x+cy) = x^2 - (cy)^2 = x^2 - c^2y^2 = 1$ ולכן $x - cy = x + cy$ ולכן $y = 0$ כי $c \neq 0$ ולכן $x = \pm 1$ וזה פתרון טריוויאלי.

מעתה, $d \in \mathbb{N}$ ו-$d \neq c^2$, $\forall c \in \mathbb{N}$. ■

טענה אם $x, y, z, w \in \mathbb{Z}$ כך ש-$(z,w), (x,y)$ הם פתרונות למשוואה אז (u,v) הוא פתרון למשוואה כאשר $u = xz + dyw, v = xw + yz$.

הוכחה: מתקיים $x^2 - dy^2 = 1$ וגם $z^2 - dw^2 = 1$. לכן $\left(x - \sqrt{d}y\right)\left(x + \sqrt{d}y\right) = 1$ וגם $\left(z - \sqrt{d}w\right)\left(z + \sqrt{d}w\right) = 1$ ולכן

$$\left(x + \sqrt{d}y\right)\left(z + \sqrt{d}w\right) = xz + dyw + (xw + yz)\sqrt{d}$$

ולכן

$$u^2 - dv^2 = \left(u + \sqrt{d}v\right)\left(u - \sqrt{d}v\right) = \ldots = 1$$

■

דוגמה $d = 2$. $(3,2)$ הוא פתרון למשוואה. נציב בטענה את $(3,2)$ פעמיים. נקבל כי $(17,12) = (3 \cdot 3 + 2 \cdot 2 \cdot 2, 3 \cdot 2 + 2 \cdot 3)$ הוא גם פתרון למשוואה.

$\mathbb{XI}$

הערה אם בטענה $x, y, z, w > 0$ אז $u > x$ ו-$v > y$ ולכן אם למשוואה יש פתרון לא טריוויאלי אז יש לה אינסוף פתרונות.

הערה אם $(z,w), (x,y)$ פתרונות למשוואה ו-$x, y, z, w > 0$ אז התנאים הבאים שקולים:

1. $x < z$.
2. $y < w$.

3. $x+\sqrt{d}y<z+\sqrt{d}w$.

הגדרה יהי (x,y) פתרון למשוואה כך ש-$x,y>0$. (x,y) נקרא פתרון יסודי אם x מינימלי.

הערה אם (x,y) פתרון למשוואה אז $\left(x+\sqrt{d}y\right)=\frac{1}{x-\sqrt{d}y}$ ולכן (u,v) הוא פתרון למשוואה כאשר

$$u+\sqrt{d}v=\left(x-\sqrt{d}y\right)^{k}=\left(x+\sqrt{d}y\right)^{-1}$$

הערה יהי (x,y) פתרון למשוואה.

אם $x,y>0$ אם"ם $1<x+\sqrt{d}y$.

אם $x>0,y<0$ אם"ם $0<x+\sqrt{d}y<1$.

אם $x,y<0$ אם"ם $x+\sqrt{d}y<-1$.

אם $x<0,y>0$ אם"ם $-1<x+\sqrt{d}y<0$.

טענה יהי (x,y) פתרון יסודי, (u,v) פתרון כלשהו, אזי קיים $k\in\mathbb{N}$ כך ש-$u+\sqrt{d}v=\left(x+\sqrt{d}y\right)^{k}$.

הוכחה: נגדיר $k=\max\left\{l\in\mathbb{N}:u+\sqrt{d}v\geq\left(x+\sqrt{d}y\right)^{l}\right\}$. הקבוצה לא ריקה כי $x+\sqrt{d}y$ והמקסימום קיים כי $\lim\limits_{l\to\infty}\left(x+\sqrt{d}y\right)^{l}=\infty$. לכן מתקיים

$$\left(x+\sqrt{d}y\right)^{k}\leq u+\sqrt{d}v<\left(x+\sqrt{d}y\right)^{k+1}$$

ולכן

$$1\leq\left(u+\sqrt{d}v\right)\left(x-\sqrt{d}y\right)^{k}<x+\sqrt{d}y$$

נסמן $z+\sqrt{d}w=\left(u+\sqrt{d}v\right)\left(x-\sqrt{d}y\right)^{k}$. אם $1<z+\sqrt{d}w$ אז $z+\sqrt{d}w$ לא טריוויאלי אבל קטן מ-$x+\sqrt{d}y$ ולכן מהערה למעלה זה אומר ש-x לא מינימלי וזו סתירה לכך ש-$x+\sqrt{d}y$ יסודי. לכן $z+\sqrt{d}w=1$ ולכן $\left(x+\sqrt{d}y\right)^{k}=\left(\left(x-\sqrt{d}y\right)^{k}\right)^{-1}=\left(u+\sqrt{d}v\right)$.

■

טענה יהי $\alpha\in\mathbb{R}$, $m\in\mathbb{N}$ אזי קיים $0\neq h\in\mathbb{Z}$ כך ש-$\{h\alpha\}<\frac{1}{m}$ וגם $|h|\leq m$.

הוכחה: $[0,1)=[\frac{m-1}{m},1)\ldots\cup[\frac{1}{m},\frac{2}{m})\cup[0,\frac{1}{m})$. מתוך $0,\{\alpha\},\{2\alpha\},\ldots,\{m\alpha\}$ יהיו שניים ששייכים לאותו הקט, כלומר קיימים

$0 \le k \neq l \le m$ כך ש-$0 \le \{l\alpha\} - \{k\alpha\} < \frac{1}{m}$. נגדיר $h = l - k$ ולכן $|h| \le m$

$$\begin{aligned}\{h\alpha\} &= h\alpha - \lfloor h\alpha \rfloor = l\alpha - k\alpha - \lfloor h\alpha \rfloor \\ &= \lfloor l\alpha \rfloor + \{l\alpha\} - \lfloor k\alpha \rfloor - \{k\alpha\} - \lfloor h\alpha \rfloor \\ &\overset{z\in\mathbb{Z}}{=} (\{l\alpha\} - \{k\alpha\}) + z\end{aligned}$$

אם $z \ge 1$ אז $\{h\alpha\} \ge 1$ סתירה ואם $z \le -1$ אז $0 \le \{h\alpha\} < -1 + \frac{1}{m} \le 0$ סתירה ולכן $z = 0$ ולכן $\{h\alpha\} = \{l\alpha\} - \{k\alpha\} < \frac{1}{m}$. ■

הערה בניסוח הטענה יכולנו לרשום גם כי $\{h\alpha\} < \frac{1}{m} \le \frac{1}{|h|}$.

טענה יהי $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ אז קיימת סדרה $\{h_n\}_{n\in\mathbb{N}}$ של מספרים שלמים שונים זה מזה ומאפס כך ש-$\{h_n\alpha\} < \frac{1}{|h_n|}$ וגם $\{h_{n+1}\alpha\} < \{h_n\alpha\}$, $\forall n \in \mathbb{N}$.

הוכחה: נגדיר סדרה באופן ריקורסיבי: $h_1 = 1$.

נניח כי $h_n \in \mathbb{Z}\backslash\{0\}$ הוגדר. לכן $h_n\alpha \in \mathbb{R}\backslash\mathbb{Q}$ ולכן $\{h_n\alpha\} \neq 0$. נבחר $m > \frac{1}{\{h_n\alpha\}}$. מהטענה הנ"ל קיים $h_{n+1} \in \mathbb{Z}\backslash\{0\}$ כך ש-$\{h_{n+1}\alpha\} < \frac{1}{m} \le \frac{1}{|h_{n+1}|}$ ולכן גם $\{h_{n+1}\alpha\} < \{h_n\alpha\}$. ברור כי h_n שונים זה מזה כי אחרת $\{h_m\alpha\} = \{h_n\alpha\}$ סתירה. ■

XIII

טענה יהי $0 \neq y \in \mathbb{Z}$ כך ש-$\{yd\} < \frac{1}{|y|}$ אז עבור $x = \lfloor y\sqrt{d} \rfloor$ מתקיים כי $\left|x^2 - dy^2\right| < 1 + 2\sqrt{d}$.

הוכחה:

$$\begin{aligned}\left|x^2 - dy^2\right| &= \left|x - \sqrt{d}y\right| \left|x + \sqrt{d}y\right| \\ &= \left\{y\sqrt{d}\right\} \left|x - y\sqrt{d} + 2y\sqrt{d}\right| \\ &< \frac{1}{|y|} \left(\left|x - y\sqrt{d}\right| + 2\left|y\sqrt{d}\right|\right) \\ &< \frac{1}{|y|} \left(\frac{1}{|y|} + 2|y|\sqrt{d}\right) \\ &= \frac{1}{|y|^2} + 2\sqrt{d} \le 1 + 2\sqrt{d}\end{aligned}$$

■

מסקנה קיימת סדרה $((x_1, y_1), (x_2, y_2), \ldots)$ של זוגות של מספרים טבעיים שונים זה מזה כך ש-$\left|x^2 - dy^2\right| < 1 + 2\sqrt{d}$.

מסקנה קיים $0 \neq k \in \mathbb{Z}$ וסדרה $\left(\left(x_1, y_1\right), \left(x_2, y_2\right), \ldots\right)$ של מספרים טבעיים שונים זה מזה כך ש-$x^2 - dy^2 = k$.

משפט למשוואת פל קיים פתרון לא טריוויאלי.

הוכחה: יהי k כבמסקנה הקודמת. $\forall i \in \mathbb{N}$, נסמן r_i, s_i את שארית החלוקה של x_i, y_i ב-k. לכן קיימים $i \neq j \in \mathbb{N}$ כך ש-$x_i \equiv x_j \mod k$ וגם $y_i \equiv y_j \mod k$. אז קיימים $a, b \in \mathbb{Z}$ כך ש-$x_j = x_i + ak, y_j = y_i + bk$.

$$\begin{aligned}\left(x_i + \sqrt{d}y_i\right)\left(x_j - \sqrt{d}y_j\right) &= \left(x_i + \sqrt{d}y_i\right)\left(x_i + ak - \sqrt{d}\left(y_i + bk\right)\right) \\ &= \left(x_i + \sqrt{d}y_i\right)\left(\left(x_i - \sqrt{d}y_i\right) + k\left(a - \sqrt{d}b\right)\right) \\ &= k\left(1 + \left(x_i + \sqrt{d}y_i\right)\left(a - \sqrt{d}b\right)\right)\end{aligned}$$

לכן קיימים $u, v \in \mathbb{Z}$ כך ש-

$$\left(x_i + \sqrt{d}y_i\right)\left(x_j - \sqrt{d}y_j\right) = k\left(u + \sqrt{d}v\right)$$

ולכן מתקיים

$$\frac{x_i + \sqrt{d}y_i}{x_j + \sqrt{d}y_j} = \frac{\left(x_i + \sqrt{d}y_i\right)\left(x_j - \sqrt{d}y_j\right)}{\left(x_j + \sqrt{d}y_j\right)\left(x_j - \sqrt{d}y_j\right)} = \frac{k\left(u + \sqrt{d}v\right)}{k} = u + \sqrt{d}v$$

ולכן

$$\begin{aligned}x_i + \sqrt{d}y_i &= \left(x_j + \sqrt{d}y_j\right)\left(u + \sqrt{d}v\right) \\ x_i - \sqrt{d}y_i &= \left(x_j - \sqrt{d}y_j\right)\left(u - \sqrt{d}v\right)\end{aligned}$$

ולכן

$$\begin{aligned}k &= \left(x_I + \sqrt{d}y_i\right)\left(x_i - \sqrt{d}y_i\right) \\ &= \left(x_j + \sqrt{d}y_i\right)\left(x_j - \sqrt{d}y_j\right)\left(y + \sqrt{d}v\right)\left(u - \sqrt{d}v\right) \\ &= k\left(u^2 - dv^2\right) = k\end{aligned}$$

ולכן $u^2 - dv^2 = 1$. $(u, v) \neq (\pm 1, 0)$ כי אחרת $x_i + \sqrt{d}y_i = \pm\left(x_j + \sqrt{d}y_j\right)$ בסתירה לכך ש-$(x_i, y_i) \neq (x_j, y_j)$. ■

הגדרה <u>שבר משולב</u> הוא ביטוי מהצורה $a_0 + \frac{1}{a_1 + \frac{1}{\ddots a_{n-1} + \frac{1}{a_n}}}$ כאשר $a_0, \ldots, a_n \in \mathbb{R}$, $a_1, \ldots, a_n \geq 1$ ונסמן $[a_0; a_1, \ldots, a_n]$.

הערה $[a_0; a_1, \ldots, a_{n+1}] = \left[a_0; a_1, \ldots, a_n + \frac{1}{a_{n+1}}\right]$.

הגדרה שבר משולב $[a_0;a_1,\dots,a_n]$ נקרא <u>פשוט</u> אם $a_i\in\mathbb{Z}$, $\forall i$ וגם $a_n\neq 1$.

הערה אם $a_n>1$ אז $[a_0;a_1,\dots,a_n]=[a_0;a_1,\dots,a_n-1,1]$.

הערה הערך של שבר משולב פשוט הוא רציונאלי.

טענה $\forall q\in\mathbb{Q}$ קיים שבר משולב פשוט ששווה לו.

הוכחה: יהיו $m\in\mathbb{Z}$, $n\in\mathbb{N}$ כך ש-$q=\frac{m}{n}$ ו-$\gcd(m,n)=1$. נגדיר סדרה $\{q_n\}$ ע"י $q_0=q$, $q_{i+1}=\frac{1}{\{q_i\}}$. הסדרה מוגדרת כל עוד $q_i\notin\mathbb{Z}$. נבנה סדרת אוקלידס עבור m,n, $\{r_i\},\{a_i\}$ באופן הבא: $r_0=n$, $m=a_0r_0+r_1$, $r_0=a_0r_1+r_2$ וכו'. לכן $(m,r_0=n,r_1,\dots r_k=1)$ היא סדרת אוקלידס. כמו כן, $a_0=\lfloor q_0\rfloor$, $\{q_0\}=\frac{r_1}{r_0}$, וגם $a_1=\lfloor q_1\rfloor$, $\{q_1\}=\frac{r_0}{r_1}$ וכן הלאה. בסוף, $r_{k-1}=a_kr_k+0$. $q_k=\frac{r_{k-1}}{r_k}=r_{k-1}\in\mathbb{Z}$.

לכן

$$q=\lfloor q_0\rfloor+\cfrac{1}{\lfloor q_1\rfloor+\cfrac{1}{\ddots\frac{1}{\lfloor q_k\rfloor}}}=[\lfloor q_0\rfloor;\lfloor q\rfloor,\dots,\lfloor q_k\rfloor]=[a_0;a_1,\dots,a_k]$$

■

דוגמה $q=\frac{15}{11}$.

$$\frac{15}{11}=1+\frac{4}{11}=1+\frac{1}{\frac{11}{4}}=1+\frac{1}{2+\frac{3}{4}}=1+\frac{1}{2+\frac{1}{1+\frac{1}{3}}}=[1;2,1,3]$$

הגדרה <u>שבר משולב אינסופי</u> הוא ביטוי מהצורה $[a_0;a_1,\dots]$ כאשר $a_0,a_1,\dots\in\mathbb{R}$, $a_1,a_2,\dots\geq 1$ ונאמר כי הוא פשוט אם $a_i\in\mathbb{Z}$.

הגדרה יהי $z\in\mathbb{R}\backslash\mathbb{Q}$. נגדיר שבר משולב אינסופי פשוט המתאים ל-z באופן הבא. נגדיר סדרה $(z_0,z_1,\dots)$ באופן הבא: $z_0=z$, $z_{i+1}=\frac{1}{\{z_i\}}$ ונגדיר $a_i=\lfloor z_i\rfloor$. נגדיר $c_n=[a_0;a_1,\dots]$ המנה החלקית של n.

הערה $z_i\geq 1$, $\forall i\geq 1$ ולכן $a_i\geq 1$. בנוסף, $z_i\in\mathbb{R}\backslash\mathbb{Q}$ לכל i ולכן הסדרה $[a_0;a_1,a_2,\dots]$ היא אינסופית.

XIII

טענה עבור $[a_0;a_1,\dots]$ נגדיר סדרות $(p_n),(q_n)$ באופן הבא:

$$p_0=a_0,\ p_1=a_1a_0+1,\ a_np_{n-1}+p_{n-2}$$

$$q_0=1,\ q_1=a_1,\ q_n=a_nq_{n-1}+q_{n-2}$$

אזי $c_n = \frac{p_n}{q_n}$ (המנה החלקית).

הוכחה: באינדוקציה על n.

בסיס ($n = 0$): $c_0 = \frac{p_0}{q_0} = a_0$.

בסיס ($n = 1$): $c_a = a_0 + \frac{1}{a_1} = \frac{p_1}{q_1}$.

צעד ($k \to k+1$): נגדיר $c'_k = \left[a_0; a_1, \dots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right]$ ונסמן $(p'_n), (q'_n)$ סדרת המתאימות ל-c'_k. לכל $0 \le i \le k-1$, $p'_i = p_i, q'_i = q_i$. מה"א על c'_k מתקיים

$$\begin{aligned} c_{k+1} = c'_k = \frac{p'_k}{q'_k} &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} = \frac{a_k p_{k-1} + p_{k-2} + \frac{p_{k-1}}{a_{k+1}}}{a_k q_{k-1} + q_{k-2} + \frac{q_{k-1}}{a_{k+1}}} \\ &= \frac{p_k + \frac{p_{k-1}}{a_{k+1}}}{q_k + \frac{q_{k-1}}{a_{k+1}}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}} \end{aligned}$$

■

טענה $p_{n-1} q_n - p_n q_{n-1} = (-1)^n$.

הוכחה: באינדוקציה על n:

בסיס ($k = 1$): $a_0 a_1 - (a_1 a_0 + 1)\, 1 = (-1)^1$.

צעד ($k \to k+1$):

$$\begin{aligned} p_k q_{k+1} - p_{k+1} q_k &= p_k \left(a_{k+1} q_k + q_{k-1}\right) - \left(a_{k+1} p_k + p_{k-1}\right) q_k \\ &= p_k q_{k-1} - p_{k-1} q_k = (-1)\left(p_{k-1} q_k - p_k q_{k-1}\right) \\ &\overset{\text{ה"א}}{=} (-1)^{k+1} \end{aligned}$$

■

מסקנה $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1}}{q_{n-1} q_n}$.

מסקנה $\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_n}$.

הוכחה:

$$\begin{aligned}\frac{p_n}{q_n}-\frac{p_{n-2}}{q_{n-2}} &= \left(\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}\right)+\left(\frac{p_{n-1}}{q_{n-1}}-\frac{p_{n-2}}{q_{n-2}}\right)\\ &= \frac{(-1)^{n+1}}{q_{n-1}q_n}+\frac{(-1)^{n+2}}{q_nq_{n+1}}\\ &= \frac{(-1)^n(q_n-q_{n-2})}{q_{n-2}q_{n-1}q_n}\\ &= \frac{(-1)^n(a_nq_{n-1})}{q_{n-2}q_{n-1}q_n}\\ &= \frac{(-1)^n a_n}{q_{n-2}q_n}\end{aligned}$$

■

מסקנה הסדרה $c_0,c_2,c_4,\ldots$ עולה והסדרה $c_1,c_3,c_5,\ldots$ יורדת

מסקנה $c_{2l+1}>c_{2m}$, $\forall k,m\in\mathbb{N}\cup\{0\}$.

הוכחה: $c_{2l+1}>c_{2l+2m+1}>c_{2l+2m}\geq c_{2m}$. ■

מסקנה $(c_{2k+1}),(c_{2k})$ מתכנסות.

מסקנה $\lim\limits_{n\to\infty}c_{2n}=\lim\limits_{n\to\infty}c_{2n+1}$.

הוכחה: $\lim\limits_{n\to\infty}c_{2n}-c_{2n+1}=\lim\limits_{n\to\infty}\frac{(-1)^{2n+1}}{q_{2n-1}q_{2n}}=0$. ■

מסקנה c_n מתכנסת.

משפט יהי $z\in\mathbb{R}\backslash\mathbb{Q}$, $[a_0;a_1,a_2,\ldots]$ שבר משולב אינסופי פשוט מתאים ל-z אזי $\lim\limits_{n\to\infty}c_n=z$.

הוכחה: נסמן $c'_{n+1}=[a_0;a_1,\ldots,a_n,z_{n+1}]$ ולכן $z=c'_{n+1}$.

$$\begin{aligned}z-c_n=c'_{n+1}-c_n=\frac{p'_{n+1}}{q'_{n+1}}-\frac{p_n}{q_n} &= \frac{z_{n+1}p_n+p_{n-1}}{z_{n+1}q_n+q_{n-1}}-\frac{p_n}{q_n}\\ &= \frac{z_{n+1}p_nq_n+p_{n-1}q_n-z_{n+1}q_np_n-q_{n-1}p_n}{(z_{n+1}q_n+q_{n-1})q_n}\\ &= \frac{(-1)^n}{(z_{n+1}q_n+q_{n-1})q_n}\end{aligned}$$

ולכן $\lim\limits_{n\to\infty}z-c_n=0$. ■

דוגמה נפתח את $z=\sqrt{2}$ לשבר משולב אינסופי פשוט. $z_0=\sqrt{2}$ ולכן $a_0=\lfloor z_0\rfloor=1$.

$z_1=\frac{1}{z_0-\lfloor z_0\rfloor}=\frac{1}{\sqrt{2}-1}=\sqrt{2}+1$ ולכן $a_1=\lfloor z_1\rfloor=2$.

$z_2=\frac{1}{z_2-\lfloor z_1\rfloor}=\frac{1}{\sqrt{2}-1}=z_1$ ולכן $z_i=z_1$, $\forall i\geq 1$ ולכן $a_i=a_1$, $\forall i\geq 1$.

לכן $\sqrt{2}=[1;2,2,2,\dots]$.

דוגמה נפתח את $z=\sqrt{3}$. $z_0=\sqrt{3}$, $a_0=1$.

$z_1=\frac{1}{\sqrt{3}-1}=\frac{\sqrt{3}+1}{2}$ ולכן $a_1=1$.

$z_2=\frac{1}{\frac{\sqrt{3}-1}{2}}=\frac{2}{\sqrt{3}-1}=\sqrt{3}+1$ ולכן $a_2=2$.

$z_3=\frac{1}{\sqrt{3}-1}=\frac{\sqrt{3}+1}{2}$ ולכן $a_3=1$ ולכן $a_{2n}=a_2=2$ וגם $a_{2n+1}=a_1=1$, $\forall n\in\mathbb{N}$.

לכן $\sqrt{3}=[1;1,2,1,2,\dots]$.

דוגמה $z=[1;1,1\dots]$. מתקיים $z=[1;z]$ ולכן $z=1+\frac{1}{z}$ ולכן $z=\phi=\frac{1+\sqrt{5}}{2}$.

דוגמה $z=[3;5,1,4,1,4,\dots]$. נסמן $w=[1;4,1,4,\dots]$ ולכן מתקיים $w=[1;4,w]$ ולכן $w=1+\frac{1}{4+\frac{1}{w}}=1+\frac{w}{1+4w}$ ולכן $w=\frac{5w+1}{4w+1}$ ולכן $4w^2-4w-1=0$ ולכן $w=\frac{1+\sqrt{2}}{2}$ ולכן $z=3+\frac{1}{5+\frac{1}{w}}=\dots=6-2\sqrt{2}$.