תורת המספרים

14 בינואר 2016

1. **משפט חלוקה עם שארית *(Quotient Remainder Theorem)*:**
יהיו a,b שלמים, $a>0$. אזי קיימת הצגה יחידה $b=qa+r$, עם שלם q ושלם $0\leq r<a$.

2. **זהות בזו *(Bezout's Identity)*:**
יהיו a,b שלמים, לא שניהם 0, ונסמן $d=\gcd(a,b)$. אזי קיימים שלמים m,nשעבורם מתקיים $ma+nb=d$.

3. יהי a שלם. a ראשוני אם ורק אם a אי־פריק.

4. **המשפט היסודי של האריתמטיקה *(Fundamental Theorem of Arithmetics)*:**
יהי $a>1$ מספר שלם. אזי קיימת הצגה יחידה $a=p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$, כאשר k שלם, $r_1,r_2,\dots,r_k$ שלמים, וכן $p_1p_2\dots p_k$ אי־פריקים.

5. **אלגוריתם אוקלידס *(Euclid's Algorithm)*:**
דרך יעילה לחישוב $\gcd(a,b)$, וכן למציאת שלמים m,n כך שמתקיים $ma+nb=\gcd(a,b)$ על ידי סדרה של חלוקות עם שארית:

$$\begin{aligned}
a &= q_1b+r_1, 0\leq r_1<b\\
b &= q_2r_1+r_2, 0\leq r_2<r_1\\
r_1 &= q_3r_2+r_3, 0\leq r_3<r_1\\
&\vdots\\
r_{k-1} &= q_{k-1}r_k+r_{k+1}, 0\leq r_{k+1}<r_k\\
r_k &= q_kr_{k+1}+0
\end{aligned}$$

כעת מתקיים $\gcd(a,b)=r_{k+1}$.

6. יש אינסוף מספרים ראשוניים.

7. יש אינסוף ראשוניים מהצורה $4k+3$.

8. **משפט דיריכלה לסדרות חשבוניות *(Dirichlet's Theorem on Arithmetic Progressions)*:**
יהיו a,b שלמים זרים. יש אינסוף ראשוניים בסדרה החשבונית $(an+b)_{n\geq1}$.

9. **משפט המספרים הראשוניים *(Prime Number Theorem)*:**
תהי $\Pi(x)$ פונקציית ספירת הראשוניים - כמות הראשוניים עד המספר x. אזי מתקיים:

$$\lim_{x\to\infty}\frac{\Pi(x)}{\frac{x}{\log x}}=1$$

10. יהי $M_p=2^p-1$ ראשוני מרסן. אזי $n=\frac{1}{2}M_p(M_p+1)$ מספר מושלם.

11. יהי n מספר מושלם וזוגי. אזי קיים ראשוני מרסן $M_p=2^p-1$ כך שמתקיים $n=\frac{1}{2}M_p(M_p+1)$.

12. כל השלשות הפיתגוריות הן מהצורה $\left(u^2-v^2,2uv,u^2+v^2\right)$ עבור u,v טבעיים כלשהם.

13. היחס $a\equiv b\pmod n$ הוא יחס שקילות על השלמים.

14. החוג $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ (מסומן גם $\mathbb{Z}/n\mathbb{Z}$) הוא מחלקת נציגים ליחס השקילות מודולו n.

15. יהי a מספר שלם. המחלקה $a + n\mathbb{Z}$ הפיכה אם ורק אם $\gcd(a, n) = 1$.

16. ההופכי מודולו n הוא יחיד.

17. אוסף האיברים ההפיכים מודולו n (מסומן $\mathbb{Z}_n^*$) מהווה חבורה כפלית.

18. **פונקציית אוילר *(Euler's Totient Function)*:**
יהי n שלם. פונקציית אוילר של n, מסומנת $\phi(n)$, מוגדרת באופן הבא:

$$\phi(n) = |\mathbb{Z}_n^*| = |\{1 \leq a \leq n \mid \gcd(a, n) = 1\}|$$

19. יהיו k, n שלמים כאשר $k \in \mathbb{Z}_n^*$. אזי

$$x \equiv y \pmod{n} \iff kx \equiv ky \pmod{n}$$

20. יהיו k, n שלמים, ויהי r מחלק משותף שלהם. אזי

$$kx \equiv ky \pmod{n} \iff \frac{k}{r}x \equiv \frac{k}{r}y \pmod{\frac{n}{r}}$$

21. יהי $n = p = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, עבור $r_1, r_2, \ldots, r_k$ שלמים, $p_1 p_2 \ldots p_k$ ראשוניים. אזי

$$\phi(n) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

בפרט, ϕ כפלית, כלומר אם m, n זרים אז $\phi(mn) = \phi(m)\phi(n)$.

22. נגדיר

$$F(n) = \sum_{1 \leq d \mid n} \phi(d)$$

אזי מתקיים

$$F(n) = n$$

23. יהיו a, b, n שלמים. לקונגרואנציה $ax \equiv b \pmod{n}$ יש פתרון אם ורק אם $\gcd(a, n) \mid b$.

24. יהיו a, b, n שלמים. כל פתרון לקונגרואנציה $ax \equiv b \pmod{n}$ מקיים

$$\frac{a}{\gcd(a, n)}x \equiv \frac{b}{\gcd(a, n)} \pmod{\frac{n}{\gcd(a, n)}}$$

, ויש בדיוק $\gcd(a, n)$ פתרונות.

25. **משפט ווילסון *(Wilson's Theorem)*:**
יהי p שלם. p ראשוני אם ורק אם מתקיים:

$$(p-1)! \equiv -1 \pmod{p}$$

26. **משפט השאריות הסיני** ***(Chinese Remainder Theorem)***:
יהיו $n_1, n_2, \ldots, n_l$ שלמים זרים בזוגות, ויהיו $a_1, a_2, \ldots, a_l$ שלמים. אזי למערכת

$$\begin{aligned} x_1 &\equiv a_1 \pmod{n_1} \\ x_2 &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x_l &\equiv a_l \pmod{n_l} \end{aligned}$$

יש פתרון יחיד מודולו $n_1 n_2 \ldots n_l$.
ניסוח נוסף: יש איזומורפיזם בין חוג השאריות מודולו $n_1 n_2 \ldots n_l$ לבין המכפלה הישרה של חוגי השאריות מודולו n_i לכל $1 \leq i \leq l$, כלומר:

$$\mathbb{Z}_{n_1 n_2 \ldots n_l} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_l}$$

27. **המשפט הקטן של פרמה** ***(Fermat's Little Theorem)***:
יהי p ראשוני ויהי a שלם זר לו. אזי מתקיים

$$a^{p-1} \equiv 1 \pmod{p}$$

28. **משפט אויילר** ***(Euler's Theorem)***:
יהי n שלם ויהי a שלם זר לו. אזי מתקיים

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

29. יהי $n > 2$. $\phi(n)$ זוגי.

30. יהי $p(x) \in \mathbb{Z}[x]$ וכן n טבעי. אם $p(a) \equiv 0 \pmod{n}$ אז $x - a \mid p(x)$ מודולו n.

31. **משפט לגראנג'** ***(Lagrange's Theorem)***:
יהי p ראשוני, $0 \not\equiv p(x) \in \mathbb{Z}_p[x]$. לקונגרואנציה $p(x) \equiv 0 \pmod{p}$ יש לכל היותר $\deg(p(x))$ פתרונות שונים מודולו p.

32. יהי $p(x) \in \mathbb{Z}[x]$, ויהי $n = p_1^{r_1} p_2^{r_2} \ldots p_l^{r_l}$. יש פתרון לקונגרואנציה

$$p(x) \equiv 0 \pmod{n}$$

אם ורק אם יש פתרון לקונגרואנציות

$$p(x) \equiv 0 \pmod{p_i^{r_i}}$$

לכל $1 \leq i \leq l$. יתר על כן, אם לראשונה s פתרונות ולאחרות s_i פתרונות, לכל $1 \leq i \leq l$, אזי

$$s = \prod_{i=1}^{l} s_i$$

33. יהי n טבעי, ויהי a שלם זר לו. לכל מספר טבעי k, $a^k \equiv 1 \pmod{n}$ אם ורק אם $ord_n(a) \mid k$.

34. יהיו a, m, n שלמים כך שמתקיים $\gcd(a, n) = 1$. אזי מתקיים:

$$ord_n(a^m) = \frac{ord_n(a)}{\gcd(m, ord_n(a))}$$

35. אם a שורש פרימיטיבי מודולו n, אזי $\mathbb{Z}_n^* = \{a^m \mid 1 \leq m \leq \phi(n)\}$.

36. יהי a שורש פרימיטיבי מודולו n. a^m הוא שורש פרימיטיבי אם ורק אם $\gcd(m, \phi(n)) = 1$. לכן, אם קיים שורש פרימיטיבי אחד מודולו n, קיימים בדיוק $\phi(\phi(n))$ שורשים פרימיטיביים מודולו n.

37. קיים שורש פרימיטיבי מודולו n אם ורק אם $n = 2$ או $n = 4$ או $n = p^j$ או $n = 2p^j$, עבור ראשוני p ושלם j כלשהם.

38. יהיו a, n שלמים זרים. יש פתרון לקונגרואנציה $x^m \equiv a \pmod{n}$ אם ורק אם $a^{\frac{\phi(n)}{\gcd(m,\phi(n))}} \equiv 1 \pmod{n}$.

39. **מספר קרמייקל** ***(Carmichael Numbers)***:
n הוא מספר קרמייקל אם ורק אם הוא מהצורה $n = p_1 p_2 \dots p_k$ עבור $k \geq 3$ וראשוניים p_i כלשהם, ומתקיים $p_i - 1 \mid n - 1$ לכל $1 \leq i \leq k$.

40. **פונקציית קרמייקל** ***(Carmichael Function)***:
יהי n מספר שלם. פונקציית קרמייקל של n, מסומנת $\lambda(n)$, מוגדרת באופן הבא:

$$\lambda(n) = \max\{ord_n(a) \mid \gcd(a, n) = 1\}$$

41. אם $n = 2^{j_0} p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$ הפירוק של n לראשוניים, אזי מתקיים

$$\lambda(n) = lcm\left(\lambda\left(2^{j_0}\right), \phi\left(p_1^{j_1}\right), \dots, \phi\left(p_k^{r_k}\right)\right)$$

42. **סמל לז'נדר** ***(Legendre Symbol)***:
יהי p ראשוני ויהי a זר לו. סמל לז'נדר של a עם p, מסומן $\left(\frac{a}{p}\right)$, מוגדר באופן הבא:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{a is a quadratic residue modulu p} \\ -1 & \text{otherwise} \end{cases}$$

43. **קריטריון אוילר** ***(Euler's Criterion)***:
עבור $p \geq 3$ ראשוני ועבור a שזר לו, מתקיים

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

44. עבור $p \geq 3$ ראשוני יש בדיוק $\frac{p-1}{2}$ שאריות ריבועיות מודולו p.

45. יהי $p \geq 3$ ראשוני, ויהיו a, b שלמים זרים לו. אזי

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

46. יהי $p \geq 3$ ראשוני, ויהי a שלם זר לו. אזי

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

47. עבור $p \geq 3$ ראשוני, מתקיים

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

48. יהי $p \geq 3$ ראשוני ויהי j שלם. שלם a הוא שארית ריבועית מודולו p^j אם ורק אם

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

ובמקרה זה יש בדיוק שני פתרונות לקונגרואנציה

$$x^2 \equiv a \left(\mod p^j \right)$$

והם מהצורה $\{x_0, -x_0\}$.

49. יהי j שלם כלשהו, ויהי a שלם אי־זוגי כלשהו. אזי לקונגרואנציה $x^2 \equiv a \left(\mod 2^j \right)$:

(א) $j = 1$: תמיד יש פתרון יחיד - $\{1\}$.

(ב) $j = 2$: יש פתרון אם ורק אם $a \equiv 1 \left(\mod 4 \right)$, ואז יש שני פתרונות בדיוק - $\{x_0, -x_0\}$.

(ג) $j = 3$: יש פתרון אם ורק אם $a \equiv 1 \left(\mod 8 \right)$, ואז יש ארבעה פתרונות בדיוק - $\left\{x_0, -x_0, x_0 + 2^{j-1}, -x_0 + 2^{j-1}\right\}$.

50. יהי $n \geq 2$ טבעי כאשר $n = 2^{j_0} p_1^{j_1} p_2^{j_2} \dots p_r^{j_r}$ הוא הפירוק של n לראשוניים. לקונגרואנציה $x^2 \equiv a \left(\mod n \right)$ יש פתרון אם ורק אם מתקיים

$$\begin{aligned} a^{\frac{1}{2}\phi\left(p_i^{j_i}\right)} &\equiv 1 \left(\mod p_i^{j_i} \right) \\ a &\equiv 1 \left(\mod \gcd\left(8, 2^{j_0}\right) \right) \end{aligned}$$

ובמקרה זה, כמות הפתרונות היא בדיוק 2^{r+j}, כאשר r הוא כמות הראשוניים, וכאשר j מוגדר באופן הבא:

$$j = \begin{cases} 0 & j_0 = 0, 1 \\ 1 & j_0 = 2 \\ 2 & j_0 \geq 3 \end{cases}$$

51. **הלמה של גאוס *(Gauss's Lemma)*:**
יהי $p \geq 3$ ראשוני, ויהי a שלם זר לו. אזי מתקיים $\left(\frac{a}{p}\right) = (-1)^l$, כאשר

$$l = \left| \left\{ 1 \leq j \leq \frac{1}{2}(p-1) \mid \exists 0 \geq b \in \left[-\frac{1}{2}(p-1), \frac{1}{2}(p-1) \right]. b \equiv aj \left(\mod p \right) \right\} \right|$$

52. יהי $p \geq 3$ ראשוני. אזי

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

53. **חוק ההדדיות הריבועית של גאוס *(Gauss's Law of Quadratic Reciprocity)*:**
יהיו $p, q \geq 3$ ראשוניים. אזי מתקיים

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

54. **סמל יעקובי *(Jacobi Symbol)*:**
יהי n טבעי אי זוגי, ויהי a זר לו. אם $n = p_1 p_2 \dots p_l$ כאשר p_i ראשוניים לאו דווקא שונים, נגדיר את סמל יעקובי של a עם n, מסומן $\left(\frac{a}{n}\right)$, באופן הבא:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{l} \left(\frac{a}{p_i}\right)$$

55. תהי $F(x,y)=ax^2+bxy+cy^2$ תבנית ריבועית עם מקדמים שלמים. הטענות הבאות שקולות:

(א) קיים שלם k כך שמתקיים $\Delta=b^2-4ac=k^2$

(ב) קיימים $u,v,t,s\in\mathbb{Z}$ כך שמתקיים $F(x,y)=(ux+vy)(tx+sy)$

(ג) קיימים $u',v',t',s'\in\mathbb{Q}$ כך שמתקיים $F(x,y)=(u'x+v'y)(t'x+s'y)$

56. יהי Δ שלם ויהי $n\geq 1$ טבעי. קיימת תבנית ריבועית עם דיסקרימיננטה Δ שבה n מיוצג אם ורק אם קיים $x\in\mathbb{Z}$ כך שמתקיים

$$x^2\equiv\Delta\pmod{4n}$$

57. נאמר כי שתי תבניות ריבועיות $F(x,y),G(x,y)$ הן שקולות אם קיימת מטריצה $U\in SL_2(\mathbb{Z})$ כך שמתקיים $G(x,y)=F((x,y)U)$. יחס זה הוא יחס שקילות.

58. יהיו F,G תבניות ריבועיות שקולות. הדיסקרימיננטות שלהן שוות.

59. יהיו F,G תבניות ריבועיות שקולות. אזי הטווח שלהן זהה, ואוסף המספרים המיוצגים על ידי כל אחת מהן שווה.

60. תהי $U\in SL_2(\mathbb{Z})$ ויהיו u,v שלמים זרים. נסמן $(t,s)=(u,v)U$. אזי t,s זרים.

61. יהי $\Delta\equiv 0,1\pmod 4$ שאינו ריבוע שלם. בכל מחלקת שקילות עם דיסקרימיננטה Δ קיימת תבנית $F(x,y)=ax^2+bxy+cy^2$ שמקיימת $|b|\leq|a|\leq|c|$.

62. עבור דיסקרימיננטה Δשאינה ריבוע שלם, ישנן רק מספר סופי של מחלקות שקולות עם דיסקרימיננטה Δ.

63. יהי $0\geq\Delta\equiv 0,1\pmod 4$ שאינו ריבוע שלם. בכל מחלקת שקילות של תבניות ריבועיות לחלוטין עם דיסקרימיננטה Δ קיימת תבנית מצומצמת $F(x,y)=ax^2+bxy+cy^2$, כלומר מקיימת אחד משני התנאים הבאים:

(א) $-a<b\leq a<c$

(ב) $0\leq b\leq a=c$

64. שתי תבניות מצומצמות הן שקולות אם ורק אם הן שוות.

65. **משפט שני הריבועים של פרמה *(Fermat's Two Square Theorem)*:**
מספר טבעי n ניתן לרישום כסכום של שני ריבועים אם ורק אם כל ראשוני p המחלק את n ומקיים $p\equiv 3\pmod 4$ מחלק את n בחזקה זוגית.

66. **משפט שלושת הריבועים של לז'נדר *(Legendre's Three Square Theorem)*:**
מספר טבעי n ניתן לרישום כסכום של שלושה ריבועים אם ורק אם הוא לא מהצורה $4^a(8b-1)$ עבור שלמים $a\geq 0,b\geq 1$.

67. **משפט ארבעת הריבועים של לגרנז' *(Lagrange's Four Square Theorem)*:**
כל מספר טבעי ניתן לרישום כסכום של ארבעה ריבועים.

68. **משפט הקירוב של דיריכלה *(Dirichlet's Approximation Theorem)*:**
יהי θ ממשי ויהי N טבעי. קיימים שלמים $a,1\leq b\leq N$ כך שמתקיים

$$|b\theta-a|\leq\frac{1}{N}$$

69. יהי θ ממשי. השבר המשולב של θ סופי אם ורק אם θ רציונאלי.

70. יהיו $a_0,\ldots,a_n\neq 0$ שלמים. נגדיר שתי סדרות $\{p_n\},\{q_n\}$ של שלמים באופן הבא:

$$\begin{aligned}p_{k+1}&=a_{k+1}p_k+p_{k-1},\quad p_{-2}=0,\quad p_{-1}=1\\q_{k+1}&=a_{k+1}q_k+q_{k-1},\quad q_{-2}=1,\quad q_{-1}=0\end{aligned}$$

אזי מתקיים $[a_0,\ldots,a_n]=\frac{p_n}{q_n}$.

71. $\{q_n\}_{n\geq 1}$ היא סדרה עולה ממש של טבעיים.

72. לכל n טבעי

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

73. לכל $n \geq -2$ שלם, $\gcd(p_n, q_n) = 1$.

74. יהי $\theta \in \mathbb{R}\backslash\mathbb{Q}$, ויהיו $a_0, \dots a_n$ השלמים בפיתוח שלו לשבר משולב. עבור $[a_0, \dots, a_n] = \frac{p_n}{q_n}$ מתקיים

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \theta$$

וכן

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2} \to 0$$

75. יהי θ ממשי שהפיתוח שלו לשבר משולב מגיע לפחות עד a_{n+1}. אזי לכל שני שלמים $a, 1 \leq b \leq q_{n+1}$ מתקיים

$$|b\theta - a| \geq |q_n\theta - p_n|$$

אם מתקיים גם $b \leq q_n$ אזי מתקיים

$$\left|\theta - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n}|b\theta - a| = \frac{b}{q_n}\left|\theta - \frac{a}{b}\right| \leq \left|\theta - \frac{a}{b}\right|$$

76. עבור $p, q \geq 1$ שלמים ועבור x ממשי מתקיים

$$\left[\frac{p+x}{q}\right] = \left[\frac{p+[x]}{q}\right]$$

77. **משפט לגרנז'** ***(Lagrange's Theorem)***:
יהי θ ממשי. השבר המשולב של θ הוא מחזורי אם ורק אם θ הוא שורש של משוואה ריבועית במקדמים שלמים שאינו רציונאלי.
במילים אחרות: קיים מספר ממשי $\phi = [\overline{a_{n+1}, \dots, a_{n+m-1}}]$ כך שמתקיים $\theta = [a_0, \dots a_n, \phi]$ אם ורק אם קיימים $a, b, c \in \mathbb{Z}$ כך שמתקיים $b^2 - 4ac > 0$ ואינו ריבוע שלם, וכן מתקיים $a\theta^2 + b\theta + c = 0$.

78. יהי θ מספר אלגברי ממעלה שניה. הפיתוח של θ לשבר משולב הוא מחזורי טהור אם ורק אם $\theta > 1$ וגם $-1 < \theta' < 0$.

79. יהי $d > 0$ שלם שאינו ריבוע שלם. אז מתקיים

(א) המספרים $\frac{1}{\sqrt{d}-\left[\sqrt{d}\right]}$, $\sqrt{d} + \left[\sqrt{d}\right]$ הם בעלי פיתוח מחזורי טהור לשלב משולב.

(ב) המספר $\sqrt{d}$ הוא בעל פיתוח לשלב משולב מהצורה $[a_0, \overline{a_1, \dots a_n}]$.

80. יהי $d > 0$ שלם שאינו ריבוע שלם, ונסמן $\sqrt{d} = [a_0, \overline{a_1, \dots, a_m}]$, כאשר m הוא המחזור המינימלי. $(x, y) \in \mathbb{N}^2$ מהווה פתרון למשוואה $x^2 - dy^2 = 1$ אם ורק אם $(x, y) = (p_n, q_n)$ עבור n אי־זוגי המקיים $m \mid n+1$.

81. יהי $d > 0$ שלם שאינו ריבוע שלם. קיים פתרון יסודי $a + b\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$ כך שקבוצת הפתרונות למשוואה $x^2 - dy^2 = 1$ היא בדיוק

$$\left\{(x, y) \in \mathbb{Z}^2 \mid \exists n \in \mathbb{Z}. x + y\sqrt{d} = \pm\left(a + b\sqrt{d}\right)^n\right\}$$

82. יהי $d > 0$ שלם שאינו ריבוע שלם. אוסף הפתרונות למשוואה $x^2 - dy^2 = 1$, כאיברים בחוג $\mathbb{Z}\left[\sqrt{d}\right]$, מהווה תת־חבורה כפלית של $\mathbb{R}$, שנסמנה V_d.

83. יהי $d > 0$ שלם שאינו ריבוע שלם. הפתרון היסודי למשוואה $x^2 - dy^2 = 1$ הוא

$$z_0 = \min\left\{z \in V_d \mid z > 1\right\}$$

84. יהי $d > 0$ שלם שאינו ריבוע שלם, ויהי m אורך המחזור המינימלי בפיתוח של $\sqrt{d}$ לשבר משולב. אזי הפתרון היסודי למשוואה $x^2 - dy^2 = 1$ הוא

$$z_0 = \begin{cases} p_{m-1} + q_{m-1}\sqrt{d} & m \equiv 0 \pmod 2 \\ p_{2m-1} + q_{2m-1}\sqrt{d} & m \equiv 1 \pmod 2 \end{cases}$$

85. יהי $d > 0$ שלם שאינו ריבוע שלם, ויהי m אורך המחזור המינימלי בפיתוח של $\sqrt{d}$ לשבר משולב. אוסף כל האיברים ההפיכים בחוג $\mathbb{Z}\left[\sqrt{d}\right]$ הוא בדיוק

$$\left\{\pm\left(p_{m-1} + q_{m-1}\sqrt{d}\right)^n \mid n \in \mathbb{Z}\right\}$$

86. **משפט ליוביל** ***(Liouville's Theorem on Diophantine Approximation)*****:**
יהי θ מספר אלגברי ממעלה $n \geq 1$. קיים $c(\theta) > 0$ כך שלכל רציונאלי $\frac{a}{b} \neq \theta$, $b > 1$, מתקיים

$$\left|\theta - \frac{a}{b}\right| \geq \frac{c(\theta)}{b^n}$$

קשה יותר, אך עדיין נכון, שלא ניתן לקרב טוב יותר מאשר $\frac{1}{b^{2+\epsilon}}$.