28/11

בס"ד

קונגרואנציות - שקילויות

א) הגדרה

יהיו a,b שני מספרים שלמים $a,b\in Z$ ומספר m טבעי $m\in Z^+$, אזי אם מתקיים: $m|a-b$, נאמר כי a שקול ל-b מודולו m ונרשום: $a\equiv b(\mathrm{mod}\ m)$ או בקיצור $a\equiv b(m)$.

ב) משפטים

(1) **משפט:** יהיו $a,b\in Z$ ו-$m\in Z^+$, אזי מתקיים $a\equiv b(m)$ אם ורק אם קיים $k\in Z$ כך שמתקיים לגם $a=b+k\cdot m$, $a\equiv b(m)\Longleftrightarrow a=b+k\cdot m$.

הוכחה: כיוון ראשון - נניח $a\equiv b(m)$ אזי מתקיים מההגדרה של יחס זה $m|a-b$. לפי משפט החלוקה קיים $k\in Z$ כך ש-$m\cdot k=a-b$, כלומר $a=b+m\cdot k$. מ.ש.ל.

כיוון שני - נניח כי $a=b+m\cdot k$, ולכן $mk=a-b$. מכאן ש-$m|a-b$, ולכן $a\equiv b(m)$ לפי הגדרת יחס זה. מ.ש.ל.

(2) **משפט:** יהיו $a,b\in Z$ ו-$m\in Z^+$, אזי מתקיים $a\equiv b(m)$ אם ורק אם ל-a ול-b יש את אותה השארית לאחר חלוקה ב-m. כלומר קיימים $k,j\in Z$ כך שמתקיים: $a=k\cdot m+\underline{r}$, $b=j\cdot m+\underline{r}$. במילים אחרות יחס זה הוא להיות עם אותה שארית אחר חלוקה ב-m.

הגדרה זו נכונה לשני מספרים חיוביים או שני מספרים שליליים, אם קיים מספר אחד שלילי ואחד חיובי, לדוגמא $3\equiv-2(5)$, נשים לב כי אכן $5|3-(-2)$ אולם לחלוקה של שניהם ב-5 יש שארית שונה. ובכל זאת משפט זה מתקיים כי $-2=-1\cdot5+3$ ו-$3=0\cdot5+3$.

הוכחה: כיוון ראשון - נניח $a\equiv b(m)$, לפי משפט קודם קיים $K\in Z$ כך ש-$a=b+k\cdot m$, ולפי משפט החלוקה עבור b ו-m קיימים $j,r\in Z$ כך ש-$b=jm+r$. אם נציב את המשוואה השנייה בראשונה נקבל $a=m(k+j)+r$. נשים לב כי השארית של a,b שווה. מ.ש.ל.

כיוון שני - נניח $a=km+r$ ו-$b=jm+r$. צ"ל $m|a-b$. נשים לב שאם נחסר את a מ-b נקבל $a-b=(km+r)-(jm+r)=m(k-j)$, מכאן שאכן $m|a-b$, ולכן $a\equiv b(m)$. מ.ש.ל.

5/12

בס"ד

ג) יחס שקילות

יהי $m\in Z^+$ נגדיר את היחס הבא: $R_{\equiv m}=\{(a,b)\in Z^2 : a\equiv b(m)\}$, זהו בעצם היחס שאנו עוסקים בו בפרק זה.

<u>משפט:</u> יחס $R_{\equiv m}$ הוא יחס שקילות. המשמעות היא שהוא מחלק את כל המספרים השלמים (z) ל-m מחלקות זרות, כלומר שכל איבר נמצא בדיוק במחלקה אחת, אין איבר שנמצא ביותר ממחלקה אחת או ללא מחלקה. כל שני איברים מאותה מחלקה מקיימים את היחס $R_{\equiv m}$ וכל שני איברים שאינם באותה קבוצה אינם מקיימים את היחס.

מספר המחלקות הוא m. נשים לב כי עבור $m=1$ יש מחלקת שקילות אחת כי כל מספר מתחלק באחת, עבור $m=2$ יש שתי מחלקות זוגיים ואי-זוגיים, ועבור $n=m$ יש n מחלקות.

<u>הוכחה:</u> יש להוכיח שלוש תכונות:

(1) רפלקסיביות- לכל $a\in Z$ מתקיים: $a\equiv a(m)$. נובע מכך ש- $m|a-a=0$ לכל $a\in Z$.

(2) סימטריות- יהי $a,b\in Z$ אזי $a\equiv b(m)$ אם ורק אם $b\equiv a(m)$. נובע מכך ש- $m|a-b$ אם ורק אם $m|b-a$.

(3) טרנזיטיביות- יהי $a,b,c\in Z$ כך ש- $a\equiv b(m)$ וגם $b\equiv c(m)$ אזי $a\equiv c(m)$. נשים לב כי $m|a-b$ וכן $m|b-c$. מכאן שקיימים $k,n\in Z$ כך ש- $km=a-b$ ו- $nm=b-c$. אם נחבר בין המשוואות נקבל: $km+nm=a-b+b-c$ מכאן $a-c=m(k+n)$, כלומר אכן $m|a-c$.

<u>הגדרה:</u> יהי $x\in Z$ ויהי $m\in Z^+$ נסמן $[x]_m$ את מחלקת השקילות של $R_{\equiv m}$ שמכילה את x. כלומר היחס $R_{\equiv m}$ מחלק את המספרים השלמים למחלקות שקילות, באחת מהם מופיע x, אזי $[x]_m$ מייצג את כל האיברים במחלקת שקילות זו.

דוגמא: $[25]_5$ מייצגת את מחלקת השקילות שבה כל האיברים עם שארית 0 לאחר חלוקה ב-

$[25]_5=0,5,10,15,20,25,30,\dots$

ד) מערכת שאריות שלמה

קבוצת מספרים שלמים $S\subseteq Z$ תיקרא "מערכת שאריות שלמה" עבור m אם לכל $y\in Z$ קיים איבר <u>יחיד</u> ב-S שקונגרואנטי ל-y. כלומר, שבקבוצה S יש בדיוק m איברים שלכל איבר יש שארית שונה לאחר חלוקה ב-m, כך שלכל $y\in Z$ קונגרואנטי לאיבר יחיד ב-S.

דוגמא: עבור $m=5$ $S=\{25,6,17,38,4\}$ מערכת שאריות שלמה.

$25 \bmod 5=\underline{0}$, $6 \bmod 5=\underline{1}$, $17 \bmod 5=\underline{2}$, $38 \bmod 5=\underline{3}$, $4 \bmod 5=\underline{4}$

משפט: יהי $m\in\mathbb{Z}^+$. כל קבוצה שלם m איברים שונים שלוקים מודולו m מהווה מערכת שאריות שלמה שלם m.

הוכחה: תהי קבוצה S של m איברים שונים שלוקים מודולו m. לפי משפט החלוקה לכל איבר a ב-S אחד"ים $r_a\in\{0,1,\dots,m-1\}$. נגדיר קבוצה R המכילה את כל השאריות השונות. נניח בשלילה כי S אינה מערכת שאריות שלמה, כלומר שמספר האיברים ב-R קטן מ-m כך שלכל היותר יש $m-1$ איברים ב-R. אזי מ"ש שני איברים כלשהם $a_i,a_j\in S$ כך ש-$r_{a_i}=r_{a_j}$. ומכאן $a_i\equiv a_j(m)$ שזו סתירה להגדרת S.

ה) **מערכת שאריות מודולרית: חיבור וכפל**

בסעיף זה נלמד כיצד אפשר פעולות מערכת שאריות כאן חיבור, חיסור, כפל ומעלה על שלמים. אלא שמעלה הפעולה יותר מורכבת, לכן נדון בה בנפרד בסעיף הבא.

יהי $a,b,c,d,p,q\in\mathbb{Z}$ ויהי $m\in\mathbb{Z}^+$ כך שמתק"ק $a\equiv b(m)$ וגם $p\equiv q(m)$.

1) **חיבור:** $a+p\equiv b+q(m)$.

הוכחה: לפי משפט החלוקה ק"מ k,j כך ש-$a-b=km$ ו-$p-q=jm$. נ"ש שגם $(a+p)-(b+q)$ מתחלק ב-m. אכן $(a+p)-(b+q)=(a-b)+(p-q)=km+jm=(k+j)m$. מ.ש.ג.

2) **חיסור:** $a-p\equiv b-q(m)$.

הוכחה: לפי משפט החלוקה ק"מ k,j כך ש-$a-b=km$ ו-$p-q=jm$. נ"ש שגם $(a-p)-(b-q)$ מתחלק ב-m. אכן $(a-p)-(b-q)=(a-b)-(p-q)=km-jm=(k-j)m$. מ.ש.ג.

3) **כפל:** $ap\equiv bq(m)$.

הוכחה: לפי משפט החלוקה ק"מ k,j כך ש-$a-b=km$ ו-$p-q=jm$. נ"ש שגם $ap-bq$ מתחלק ב-m. אכן $ap-bq=ap-aq+aq-bq=a(p-q)+(a-b)q=ajm+kmq=(aj+kq)m$. כלומר $ap-bq\mid m$. ולכן $ap\equiv bq(m)$. מ.ש.ג.

Scanned with CamScanner

1) אריתמטיקה מודולרית: חלוקה

יהי $a,b,c\in\mathbb{Z}$ ויהי $m\in\mathbb{Z}^+$ כך שמתקיים: $ac\equiv bc(m)$. לא ניתן לחלק את השקילות ב-c מבלי שנשנה את m, כלומר מבלי שנשנה את עולם החלוקה. כדי שנוכל לחלק נלמד את המשפט הבא.

<u>משפט:</u> $ac\equiv bc(m)$ אם ורק אם $a\equiv b\left(\frac{m}{(m,c)}\right)$. כלומר ניתן לחלק את השקילות ב-c אבל צריך לחלק גם את m ב-gcd של (m,c).

<u>הוכחה:</u> כיוון ראשון - נניח כי $ac\equiv bc(m)$, כלומר $m|ac-bc=c(a-b)$. לכן לפי משפט החלוקה קיים $k\in\mathbb{Z}$ כך ש-$m\cdot k=c(a-b)$. נגדיר שני מספרים r,s כך: $r=\frac{c}{(m,c)}$, $s=\frac{m}{(m,c)}$. לפי משפט ( ) ב-gcd $(r,s)=1$. נשים לב כי $c=r\cdot\overset{gcd}{(m,c)}$ ו- $m=s\cdot(m,c)$. אם נציב ערכים אלו במשוואה נקבל כי $s\cdot\cancel{(m,c)}\cdot k=r\cdot\cancel{(m,c)}\cdot(a-b)$, מכאן $s\cdot k=r(a-b)$. לכן $s|r(a-b)$. מכיוון ש-$(s,r)=1$ אזי בהכרח $s|a-b$. לפי הגדרת s מתקיים: $\frac{m}{(m,c)}\Big|a-b$, כלומר $a\equiv b\left(\frac{m}{(m,c)}\right)$. מ.ש.ל.

כיוון שני - נניח $a\equiv b\left(\frac{m}{(m,c)}\right)$, צ"ל $ac\equiv bc(m)$. דרך ההוכחה זהה בדיוק להוכחה בכיוון ראשון אלא שנעבוד מלמטה למעלה.

<u>דוגמא:</u> $14\equiv 8(6)\Rightarrow 7\cdot2\equiv 4\cdot2(6)\Rightarrow 7\equiv 4\left(\frac{6}{(6,2)}\right)\Rightarrow 7\equiv 4\left(\frac{6}{2}\right)\Rightarrow 7\equiv 4(3)$ ✓

מסקנות: (1) אם $(c,m)=1$ אזי $a\equiv b(c)$ אם ורק אם $ac\equiv bc(m)$

(2) אם P ראשוני כך ש-$P\nmid c$, כלומר $(c,P)=1$, אזי שים $a\equiv b(P)$ אם ורק אם $ac\equiv bc(P)$

2) שקילות לינארית

<u>הגדרה:</u> משוואה מודולרית מהצורה $a\cdot x\equiv b(m)$ נקראת "שקילות לינארית". נשים לב כי אם $x_0\in\mathbb{Z}$ הינו פתרון למשוואה, אזי כל איבר מהמחלקת שקילות $[x_0]_m$ הינו פתרון למשוואה.

<u>משפט:</u> יהיו $x_1=x_0+\left(\frac{m}{(a,m)}\right)\cdot t_1$, $x_2=x_0+\left(\frac{m}{(a,m)}\right)\cdot t_2$ שני פתרונות למשוואה $ax\equiv b(m)$. אזי מתקיים: $x_1\equiv x_2(m)$ אם ורק אם $t_1\equiv t_2((a,m))$. נסמן $d=(a,m)$.

משפט זה יעזור לנו להוכיח משפט חשוב בהמשך.

הוכחה: כיוון ראשון - נניח כי $x_1\equiv x_2(m)$, כלומר $x_0+\left(\frac{m}{d}\right)t_1\equiv x_0+\left(\frac{m}{d}\right)t_2(m)$. אזי לפי אריתמטיקה מודולרית ניתן לחסר x_0 ולחלק ב-$\left(\frac{m}{d}\right)$, ואז נקבל $t_1\equiv t_2\left(\frac{m}{\left(\frac{m}{d}\right)}\right)\Rightarrow t_1\equiv t_2(d)$. מ.ש.ל.

כיוון שני - נניח $t_1\equiv t_2(d)$ צ"ל $x_1\equiv x_2(m)$. דרך ההוכחה זהה לחלוטין לכיוון ראשון, רק שנוכיח מלמטה למעלה.

5/12

בס״ד

משפט: משוואת שקילות לינארית $ax\equiv b(m)$ פתירה אם ורק אם $(a,m)|b$, אחרת למשוואה אין פתרון.

הוכחה: לפי משפט (1) בסע׳ ג׳ מתקיים: $ax=b+k\cdot m$, ומכאן $ax-km=b$. נשים לב כי זוהי משוואה דיאופנטית שלפי סע׳ ה׳ באלגו׳ אוקלידס למשוואה כזו יש פתרון אם ורק אם $(a,m)|b$. מ.ש.ל.

משפט: אם המשוואה $ax\equiv b(m)$ פתירה אזי יש לה (a,m) פתרונות שאינם שקולים. כלומר [illegible] מחלקות שקילות (a,m) מהוות פתרון למשוואה. נסמן $d=(a,m)$.

הוכחה: כמו שראינו בהוכחת משפט קודם משוואת שקילות לינארית היא משוואה דיאופנטית. אזי לפי סע׳ ה׳ באלג׳ אוקלידס, מכיוון שהנחנו שלמשוואה כי יש פתרון, אזי יש אינסוף פתרונות מהצורה $x=x_0+\left(\frac{m}{d}\right)\cdot t$, $k=k_0-\left(\frac{a}{d}\right)\cdot t$. מכאן שכל פתרונות המשוואה שנציב במקום x מהצורה $x=x_0+\left(\frac{m}{d}\right)\cdot t$, כאשר ההבדל בין כל פתרון הוא בערך t. נותר להראות כי קבוצת כל פתרונות אלו מתחלקת ל-d מחלקות שקילות מודולו m. לפי המשפט הראשון בסע׳ זה, שני פתרונות x_1,x_2 אינם שקולים אם t_1,t_2 אינם שקולים. לכן כדי לקבל את כל הפתרונות הלא שקולים נציב את כל קבוצת השאריות של d. ומכאן שיש לנו d פתרונות לא שקולים. מ״ש

ח) הופכי מודולארי

באריתמטיקה רגילה ראינו תכונה שלכל מספר x יש מספר הופכי x^{-1} כך שאם נכפיל אותם זה בזה נקבל: $x\cdot x^{-1}=1$, $y\cdot y^{-1}=1$. גם באריתמטיקה מודולארית קיימת תכונה כזו. נתבונן על השקילות הלינארית $a\cdot x\equiv 1(m)$. ההופכי המודולארי של a מודולו m, אותו נסמן $\tilde{a}$, הוא מספר שמקיים $a\cdot\tilde{a}\equiv 1(m)$ או באופן כללי יותר $[a]_m\cdot[\tilde{a}]_m=[1]_m$. מכיוון שיש רק מספר אחד כזה אנו דורשים שלשקילות הלינארית $ax\equiv 1(m)$ יהיה פתרון יחיד, וכמו שלמדנו בסע׳ קודם מתקיים רק אם $(a,m)=1$. מכאן נלמד שבניגוד לאריתמטיקה רגילה שם תמיד יש מספר הופכי, באריתמטיקה מודולארית יכול להיות שאין מספר הופכי מודולארי וזה כאשר $(a,m)\neq 1$.

* נהוג לסמן מספר הופכי מודולרי a^{-1} בדומה לסימון באריתמטיקה רגילה, אולם כדי למנוע בלבולים נסמן $\tilde{a}$.

הגדרה: יהי $m\in\mathbb{Z}^+$ ו-$a\in\mathbb{Z}$ כך ש-$(a,m)=1$. אזי $\tilde{a}$ הינו הופכי מודולארי של $a(m)$ אם מתקיים $a\cdot\tilde{a}\equiv 1(m)$.

דוגמאות: (1) מהו ההופכי מודולארי של $7(31)$? התשובה היא 9. $7\cdot 9=63 \Rightarrow 63\equiv 1(31)$ ✓.

(2) " " " $5(10)$? אין. מפני ש-$(5,10)=5\neq 1$.

" " " $0(m)$? אין. מפני ש-$0\not\equiv 1(m)$ לכל m.

12/12 בס"ד

שימוש: אם ידוע לנו היפכי מודולארי $\tilde{a}$ של $a(m)$, נוכל לפתור כל שקילות לינארית מהצורה $a\cdot x\equiv b(m)$ בשיטה הבאה: $a\cdot x\equiv b(m) /\cdot\tilde{a} \Rightarrow \tilde{a}\cdot a\cdot x\equiv \tilde{a}\cdot b(m) \Rightarrow \boxed{x\equiv \tilde{a}\cdot b(m)}$

משפט: יהי p ראשוני. לכל $a\in[1,p-1]$ יש היפכי מודולו p. כלומר יש $\tilde{a}$ כך ש- $a\cdot\tilde{a}\equiv 1(p)$.

הוכחה: בגלל ש-p ראשוני אזי לכל מספר הנמוך מ-p מתקיים $(a,p)=1$.

משפט: יהי $m\in\mathbb{Z}^+$ ו-$a\in\mathbb{Z}$ כך ש-$(a,m)=1$. נאמר ש-a היפכי לעצמו מודולו m אם $a^2\equiv 1(m)$

הוכחה: נשים לב שמתקיים $a\cdot a\equiv 1(m)$ לכן a עצמו עונה על דרישת מספר היפכי מודולרי.

משפט: יהי p ראשוני ו-$a\in\mathbb{Z}$ כך ש-$(a,p)=1$, אזי a היפכי לעצמו מודולו m אם ורק אם $a\equiv 1(p)$ או $a\equiv -1(p)$. המשמעות היא ש-1 ו-$p-1$ הם ההפכיים לעצמם מפני שיוצא מהמשפט ש-$p|a+1$ או $p|a-1$, ומכיוון ש-p מחלק רק את עצמו ו-0, אזי a יכול להיות או $a=p-1$ או $a=1$.

הוכחה: כיוון ראשון - נניח a היפכי לעצמו, צ"ל $a\equiv 1(p)$ או $a\equiv -1(p)$. אם a היפכי לעצמו אזי $a^2\equiv 1(p)$, אזי לפי הגדרת השקילות מתקיים $p|a^2-1 \Rightarrow p|(a+1)(a-1)$. היות ו-$p$ ראשוני $p|a-1$ או $p|a+1$, לכן $a\equiv 1(p)$ או $a\equiv -1(p)$. מ.ש.ל.

כיוון שני - נניח $a\equiv \pm 1(p)$, צ"ל a היפכי לעצמו מודולו m. נעלה בריבוע את ההנחה (מותר לפי אריתמטיקה מודולרית) ונקבל $a^2\equiv (\pm 1)^2(p) \Rightarrow a^2\equiv 1(p) \Rightarrow a\cdot a\equiv 1(p)$, ומכאן ש-$a$ היפכי לעצמו.

דוגמא: אם $p=7$ אזי למספרים 6-0 יש מספר היפכי מודולו p והם:

קנוני	0	1	2	3	4	5	6
היפכי	אין	1	4	5	2	3	6

6) משפט השאריות הסיני

משפט השאריות הסיני עוזר לנו לפתור מערכת שקילויות לינאריות ללא מקדם מהצורה:

$$\begin{aligned} x_1&\equiv a_1(n_1)\\ x_2&\equiv a_2(n_2)\\ &\vdots\\ x_r&\equiv a_r(n_k)\end{aligned}$$

כאשר לכל $i\in[k]$ $(a_i,n_i)=1$, וגם $n_1,n_2,\dots,n_k$ זרים בזוגות.

לפני שנוכיח משפט זה נצטרך ונוכיח שני משפטי עזר.

משפט עזר 1: יהיו $a,b\in\mathbb{Z}$ ויהיו $m_1,m_2,\dots,m_k\in\mathbb{Z}^+$ כך שלכל $i\in[k]$ מתקיים $a\equiv b(m_i)$, אזי גם מתקיים $a\equiv b(m_1\cdot m_2\cdot\ldots\cdot m_k)$, וגם $a\equiv b(\mathrm{Lcm}(m_1,m_2,\dots,m_k))$.

הוכחה: לפי ההנחה $m_i|a-b$ לכל $i\in[k]$. לכן $m_1\cdot m_2\cdot\ldots\cdot m_k|a-b$, ואזי גם $\mathrm{lcm}(m_1,m_2,\dots,m_k)|a-b$.

משפט עזר 2: יהיו $a,b\in\mathbb{Z}$ ויהיו $m_1,m_2\in\mathbb{Z}^+$ כך שמתקיים $a\equiv b(\mathrm{lcm}(m_1,m_2))$, אזי $a\equiv b(m_1)$ וגם $a\equiv b(m_2)$

הוכחה: לפי ההנחה $\mathrm{Lcm}(m_1,m_2)|a-b$. כלומר קיים $j\in\mathbb{Z}$ כך ש- $j\cdot\mathrm{Lcm}(m_1,m_2)=a-b$ ואז $a=j\cdot\mathrm{Lcm}(m_1,m_2)+b$. ובנוסף ישנם $k_1,k_2\in\mathbb{Z}$ כך ש- $\mathrm{Lcm}(m_1,m_2)=k_1m_1=k_2m_2$. לכן $a=jk_1m_1+b=jk_2m_2+b$. נפרק את b לפי משפט החלוקה $b=m_1\cdot\lambda+(b \bmod m_1)$ ואז $a=m_1(j\cdot k_1+\lambda)+(b \bmod m_1)$, כלומר $a\equiv b(m_1)$ בנפרד.

*מפני שהמשוואה יוצא של-a ו-b אותה שארית אחרי חלוקה ב-m_1.

12/12

בס"ד

<u>משפט השאריות הסיני</u> - תהי מערכת שקילויות לינארית כמו שתיארנו בתחילת הסעיף אזי למערכת זאת קיים פתרון <u>"יחודי"</u> מודולו $\prod_{i=1}^{r} n_i$, כלומר פתרון "יחודי" X זה מקיים: $X \equiv a_i(n_1\cdot n_2\cdot\ldots\cdot n_r)$ לכל $i\in[r]$. פתרון זה גם מקיים את כל מערכת המשוואות משום שלפי משפט עזר 2 שלמדנו יוצא ש-$X\equiv a_i(n_i)$ לכל $i\in[r]$ כנדרש.

הפתרון של המערכת הוא: $X=\sum_{i=1}^{r} a_i\cdot m_i\cdot y_i$.

a_i - הוא המספר השקול ל-x לפי האינדקס של השקילות הלינארית.

m_i - נגדיר $k\in[r]$ נחשב את m_i כך: $m_i = \frac{\prod_{k=1}^{r} n_k}{n_i} = \frac{n_1\cdot n_2\cdot\ldots\cdot n_i\cdot\ldots\cdot n_r}{n_i}$.

y_i - הוא המספר ההופכי המודולארי של m_i מודולו n_i כך שמתקיים: $m_i\cdot y_i\equiv 1(n_i)$. $y_i=\tilde{m}_i$

<u>הוכחה:</u> נחלק לשני הוכחות: קיום ויחידות.

<u>קיום</u> - נשים לב כי m_i מכיל את כל האיברים $n_1\cdot n_2\cdot\ldots\cdot n_r$ מלבד n_i, ומכיוון שכל איברים אלו זרים בזוגות לפי ההגדרה אזי נוכל להסיק כי $(m_i,n_i)=1$ לכל $i\in[r]$. עוד נשים לב כי לכל $k\in[r]\setminus i$ n_i מופיע בכל m_k, לכן $n_i|m_k$.

נחזור להוכחה. צריך להוכיח כי לכל $i\in[r]$ מתקיים $X\equiv a_i(n_i)$. ולפי איך שהגדרנו את X צריך להתקיים: $a_1m_1y_1+a_2m_2y_2+\ldots+a_im_iy_i+\ldots+a_rm_ry_r\equiv a_i(n_i)$. מכיוון ש-$n_i|m_k$ לכל $k\in[r]\setminus i$ כמו שהסברנו מתקיים $a_km_ky_k\equiv 0(n_i)$ לכל $k\in[r]\setminus i$. לכן נוכל להחליף את כל הביטויים במשוואה מלבד $a_im_iy_i$ ב-0, ולקבל $a_im_iy_i\equiv a_i(n_i)$. לפי הגדרת m_i ו-y_i אמרנו שמתקיים $m_i\cdot y_i\equiv 1(n_i)$, לכן נחליף אותם ב-1 ונקבל $a_i\equiv a_i(n_i)$ כנדרש. מ.ש.ל.

<u>יחידות</u> - בנ"ח בשלילה כי ישנם שני פתרונות X_1,X_2 למערכת השקילות הלינארית. כך ש-$X_1\not\equiv X_2(\prod_{i=1}^{r} n_i)$ כלומר שמתקיים $X_1\equiv a_i(n_i)$ וגם $X_2\equiv a_i(n_i)$ לכל $i\in[r]$. מכאן שגם מתקיים $X_1\equiv X_2(n_i)$ לכל $i\in[r]$. ולפי משפט עזר 1 שלמדנו מתקיים: $X_1\equiv X_2(\prod_{i=1}^{r} n_i) \Rightarrow X_1\equiv X_2(n_1\cdot n_2\cdot\ldots\cdot n_r)$, סתירה להנחה! לכן לא יכולים להיות שני פתרונות לא שקולים למערכת זו.

<u>דוגמא:</u> מצא X המקיים את מערכת השקילויות הלינאריות הבאה

$$\begin{cases} x\equiv 1\ (5) \\ x\equiv 2\ (6) \\ x\equiv 3\ (7) \end{cases}$$

פתרון:

$m_1=\frac{5\cdot6\cdot7}{5}=6\cdot7=42$. $\quad 42\cdot y_1\equiv 1(5)\Rightarrow 42\cdot3\equiv126\equiv1(5)\Rightarrow y_1=3$

$m_2=\frac{5\cdot6\cdot7}{6}=5\cdot7=35$. $\quad 35\cdot y_2\equiv 1(6)\Rightarrow 35\cdot5\equiv175\equiv1(6)\Rightarrow y_2=5$

$m_3=\frac{5\cdot6\cdot7}{7}=5\cdot6=30$. $\quad 30\cdot y_3\equiv 1(7)\Rightarrow 30\cdot4\equiv120\equiv1(7)\Rightarrow y_3=7$

$X=\sum_{i=1}^{3} a_i\cdot m_i\cdot y_i = 1\cdot42\cdot3+2\cdot35\cdot5+3\cdot30\cdot4=\boxed{836}$

$836\equiv1(5)\Rightarrow 5|835\Rightarrow 5\cdot167=835$ ✓. $836\equiv2(6)\Rightarrow 6|834\Rightarrow 6\cdot139=83$ ✓

$836\equiv3(7)\Rightarrow 7|833\Rightarrow 7\cdot119=833$ ✓

12/12

בס"ד

משפטי וילסון, פרמה ואוילר

א) משפט וילסון

משפט וילסון: יהי p ראשוני, אזי מתקיים: $(p-1)!\equiv -1\ (p)$.

הוכחה: בפרק הקודם בסעיף ח' הוכחנו כי אם p ראשוני אזי לכל $1\le a\le p-1$ יש מספר הופכי מודולו p, כלומר קיים $\tilde{a}$ כך ש-$a\cdot\tilde{a}\equiv 1(p)$. עוד הוכחנו שם כי $p-1$ ו-1 הופכיים לעצמם, ואילו כל שאר המספרים $2,3,\dots,p-2$ מתחלקים לזוגות של a,b כך ש-$a\cdot b\equiv 1(p)$. כתוצאה מכך מתקיים: $2\cdot 3\cdot\ldots\cdot(p-2)\equiv 1(p)$, כי ניתן לפרק את המכפלה $2\cdot 3\cdot\ldots\cdot(p-2)$ לזוגות של מספרים השקולים ל-1. אם נכפיל את השקילות בשני הצדדים ב-$p-1$ נקבל: $2\cdot 3\cdot\ldots\cdot(p-2)\cdot(p-1)\equiv(p-1)!\equiv p-1\equiv -1(p)$. זאת מכיוון ש-$p\equiv 0\ (p)$. מ.ש.ל.

משפט וילסון הפוך: יהי $2\le n\in\mathbb{Z}$, אם מתקיים: $(n-1)!\equiv -1\ (n)$ אזי n מספר ראשוני.

הוכחה: יהי $2\le n\in\mathbb{Z}$ כך שמתקיים: $(n-1)!\equiv -1(n)$. צ"ל n ראשוני. נניח בשלילה כי n אינו ראשוני אלא פריק, כך שישנם a,b ראשוניים כך שמתקיים $n=a\cdot b$. מכיוון ש-$a<n$ אזי בהכרח $a|(n-1)!$. לפי ההנחה והגדרת קונגרואנציות $n|(n-1)!+1$, ומכיוון ש-$a|n$ אזי $a|(n-1)!+1$. לפי משפט (2) במשפט החלוקה ח"ב להתקיים: $a|(n-1)!+1-(n-1)!=1$, כלומר $a|1$, אך הגדרנו a ראשוני כך ש-$a\ge 2$. סתירה! לכן לא ניתן להניח n פריק אלא n ראשוני. המסקנה משני המשפטים: n ראשוני אם ורק אם $(n-1)!\equiv -1(n)$.

מסקנה: יהי $2\le n\in\mathbb{Z}$ n ראשוני אם ורק אם $(n-2)!\equiv 1(n)$

הוכחה: לפי משפט וילסון n ראשוני אם ורק אם $(n-1)!\equiv -1(n)$. נשים לב כי $n-1)!\equiv -1\equiv n-1\ (n)$ היות ו-$n,n-1$ מספרים עוקבים אזי $(n,n-1)=1$. נחלק את השקילות ב-$n-1$. $\frac{n-1)!}{n-1}\equiv\frac{n-1}{n-1}\left(\frac{n}{1}\right)$

לכן $(n-2)!\equiv 1(n)$. מ.ש.ל.

ב) משפט פרמה הקטן

לפני שנציג את משפט פרמה הקטן נוכיח משפט עזר שיעזור לנו להוכיח את משפט פרמה הק

משפט עזר: יהי p ראשוני ויהי $a\in\mathbb{Z}^{+}$ כך ש-$(a,p)=1$. ידוע כי סדרת המספרים $1,2,\dots,p-1$ מהווה מערכת שאריות שלמה חוץ משארית 0, וכל שני איברים אינם שקולים מודולו p, כלומר לכל מספר יש שארית שונה. אם נכפיל סדרה זו ב-a, נגלה כי גם $a,2a,\dots,a\cdot(p-1)$ מהווה מערכת שאריות שלמה עבור p חוץ מ-0, וכל שני איברים אינם שקולים מודולו p.

19/12 בס"ד

2) הוכחת אי-ראשוניות באמצעות פרמה הקטן

באמצעות משפט פרמה הקטן נוכל להוכיח כי מספר אינו ראשוני. אולם לא נוכל להוכיח בוודאות באמצעות משפט זה כי n ראשוני. אם נתון לנו מספר n ונרצה להבדיק ראשוניות שלו, אזי אם נצליח למצוא a כך ש-$a^n \not\equiv a(n)$ אז הוכחנו n אינו ראשוני, מפני שלפי משפט פרמה הקטן (ניסוח שני) אם n ראשוני חייב להתקיים: $a^n \equiv a(n)$.

אולם אם אכן נמצא מספר a המקיים $a^n \equiv a(n)$ אזי לא הוכחנו ש-n ראשוני.

דוגמא: האם 63 ראשוני? נחפש מספר a כך ש-$a^{63} \equiv a(63)$. לשם כך נחפש מספר b כך כך ש-$b \equiv 1(63)$. נבחר $b=64$, אזי מתקיים: $64 \equiv 2^6 \equiv 1(63)$

כעת נעשה את התהליך הבא: $2^{63} \equiv 2^3 \cdot 2^{60} \equiv 2^3 \cdot (2^6)^{10} \equiv 2^3 \cdot 1^{10} \equiv 2^3(63)$

נשים לב כי $2^3 \not\equiv 2(63)$, לכן $2^{63} \not\equiv 2(63)$. מכאן ש-63 אינו ראשוני, ואכן $63=9\cdot 7$.

3) מספר פסודו-ראשוני

הגדרה: מספר פריק n "יקרא "פסודו-ראשוני" (מתחזה לראשוני) מבסיס b אם מתקיים $b^n \equiv b(n)$. במילים אחרות, מספר שאינו ראשוני אך לא ניתן להוכיח שאינו ראשוני באמצעות משפט פרמה הקטן (כמו שלמדנו בסעיף קודם) כאשר בחרנו לנסות להוכיח עם המספר b, ייקרא "פסודו-ראשוני מבסיס b". אמנם ישנו בסיס מסוים c שעבורו נצליח להוכיח באמצעות משפט פרמה הקטן, כי n אכן אינו ראשוני, כלומר שמתקיים $c^n \not\equiv c(n)$.

דוגמא: המספר 341 הינו פסודו-ראשוני מבסיס 2. נשים לב כי 341 אכן פריק $341=11\cdot 31$. נוכיח $2^{341} \equiv 2(341)$. בפרק קודם (סעיף ג') למדנו כי אם מתקיים $a \equiv b(m_1)$ וגם $a \equiv b(m_2)$ כאשר $(m_1,m_2)=1$, אזי גם מתקיים $a \equiv b(m_1 \cdot m_2)$. לכן אם נוכיח כי מתקיים $2^{341} \equiv 2(11)$ וגם $2^{341} \equiv 2(31)$ הוכחנו $2^{341} \equiv 2(341)$.

מכיוון ש-11 ראשוני ו-$(2,11)=1$ אז לפי משפט פרמה הקטן מתקיים: $2^{10} \equiv 1(11)$

נבצע את התהליך הבא: $2^{341} \equiv 2 \cdot (2^{10})^{34} \equiv 2 \cdot 1^{34} \equiv 2(11) \Rightarrow$ מ.ש.ל

נחפש b כך ש-$b \equiv 1(31)$. נבחר $b=32$, אזי מתקיים: $32 \equiv 2^5 \equiv 1(31)$

נבצע את התהליך הבא: $2^{341} \equiv 2 \cdot (2^5)^{68} \equiv 2 \cdot 1^{68} \equiv 2(31) \Rightarrow$ מ.ש.ל

הוכחנו 341 פסודו ראשוני מבסיס 2. אמנם 341 אינו פסודו-ראשוני עבור בסיס 7. נראה כי $7^{341} \not\equiv 7(341)$. נשתמש בכך ש-$7^3 \equiv 343 \equiv 2(341)$ וגם ב-$2^{10} \equiv 1024 \equiv 1(341)$. נבצע את התהליך

$7^{341} \equiv (7^3)^{113} \cdot 7^2 \equiv 2^{113} \cdot 7^2 \equiv (2^{10})^{11} \cdot 2^3 \cdot 7^2 \equiv 1^{11} \cdot 2^3 \cdot 7^2 = 392 = 51 \not\equiv 7(341) \Rightarrow$ מ.ש.ל

19/12 בס"ד

הוכחה: נחלק את ההוכחה לשני חלקים: (1) שארית 0 לא נוצר, (2) שלא נוצר שום נציג למחלקת שקילות.

(1) נניח בשלילה כי קיים $k\in[1,p-1]$ כך ש-$a\cdot k\equiv 0(p)$, אזי $p|a\cdot k$. ה"ת ו-$p\nmid a$ מכיוון שהנחנו $(a,p)=1$, וכן $p\nmid k$ מכיוון שהוא ראשוני אזי $p\nmid a\cdot k$. סתירה! לכן לא קיים k כזה.

(2) נניח בשלילה כי קיימים $k_1,k_2\in[p-1]$ כך ש-$k_1\not\equiv k_2(p)$ וגם $a\cdot k_1\equiv a\cdot k_2(p)$. אזי אם נחלק שקילות זו ב-a נקבל $k_1\equiv k_2(p)$ מכיוון ש-$(a,p)=1$, שזו סתירה להנחה.
לכן לא קיימים k_1,k_2 כאלו.

<u>משפט פרמה הקטן:</u> יהי p ראשוני ויהי $a\in\mathbb{Z}$ כך ש-$(a,p)=1$, אזי $a^{p-1}\equiv 1(p)$.

הוכחה: לפי המשפט עבר לכל מספר בסדרה $1,2,\ldots,p-1$ ניתן להתאים מספר שקול מודולו p בסדרה $a,2a,\ldots,a(p-1)$. לכן בהכרח מתקיים: $a\cdot 2a\cdot\ldots\cdot a(p-1)\equiv 1\cdot 2\cdot\ldots\cdot(p-1)(p)$, כלומר $a^{p-1}\cdot(p-1)!\equiv(p-1)!(p)$. נחלק את השקילות ב-$(p-1)!$. מכיוון של-p ול-$(p-1)!$ אין פקטורים ראשוניים משותפים, אזי $((p-1)!,p)=1$. לכן נקבל $a^{p-1}\equiv 1(p)$. מ.ש.ל.

<u>משפט פרמה הקטן (ניסוח שני):</u> יהי p ראשוני ויהי $a\in\mathbb{Z}$ אזי $a^p\equiv a(p)$.

הוכחה: בניסוח השני לא ידוע אם $p|a$ או לא כמו שידוע בניסוח ראשון, לכן יש שני מקרים:
(1) $p\nmid a$ - אז ניתן להשתמש בניסוח ראשון $a^{p-1}\equiv 1(p)$. נכפול ב-a את השקילות ונקבל $a^p\equiv a(p)$.
(2) $p|a$ - אז בוודאי שגם $p|a^p$. בנוסף מתקיים $a\equiv 0(p)$ וגם $a^p\equiv 0(p)$, כלומר הם באותה מחלקת שקילות. לכן $a^p\equiv a(p)$. מ.ש.ל.

הערה - נשים לב כי לפי משפט זה, a^{p-2} הינו ההופכי של a מודולו p. זאת כי מתקיים: $a^{p-1}\equiv a\cdot a^{p-2}\equiv 1(p)$.

<u>שימוש במשפט פרמה הקטן:</u> אם נרצה לחשב את השארית החיובית מינימלית (במילים אחרות הקנונית) של מספר בחזקה גבוהה כגון a^n מודולו p, כך ש-p ראשוני, ו-$p\nmid a$ כלומר $(a,p)=1$, אזי נוכל לעשות זאת בקלות באמצעות משפט פרמה הקטן במקום להסתבך בחישובים של מספרים גדולים מאוד.

דוגמא: מהי השארית הקנונית של 3^{201} מודולו 11? מכיוון ש-11 ראשוני ו-$(3,11)=1$ לפי משפט פרמה הקטן מתקיים: $3^{10}\equiv 1(11)\Rightarrow(3^{10})^{20}\equiv 1^{20}(11)\Rightarrow 3\cdot 3^{200}\equiv 3\cdot 1(11)\Rightarrow 3^{201}\equiv 3(11)$

$[3^{201}] = 3$

19/12

בס"ד

ה) מספרי קרמייקל (Car-michael)

הגדרה: מספר פריק n ייקרא "מספר קרמייקל" אם לכל $b\in\mathbb{Z}^+$ כך ש-$(b,n)=1$ מתקיים: $b^{n-1}\equiv 1(n)$ או $b^n\equiv b(n)$. מספרי קרמייקל דומים למספרים פסודו ראשוניים בכך שהם מקיימים את משפט פרמה הקטן אך אינם ראשוניים. אלא שאם מספר הינו פסודו-ראשוני רק עבור בסיס מסוים אז עבור בסיסים אחרים ניתן להוכיח כי אינו ראשוני באמצעות משפט פרמה הקטן, אך במספרי קרמייקל עבור כל בסיס זר ל-n לא ניתן להשתמש במשפט פרמה הקטן להוכיח ש-n אינו ראשוני.

במילים אחרות, אם מספרים פסודו-ראשוניים מקשים על השימוש במשפט פרמה הקטן לבדיקת ראשוניות, מספרי קרמייקל הופכים את זה לבלתי אפשרי.

דוגמא: 561 הינו מספר קרמייקל. נשים לב כי אכן 561 פריק $561=3\cdot 11\cdot 17$. נראה כי לכל $b\in\mathbb{Z}^+$ כך ש-$(b,561)=1$ מתקיים: $b^{560}\equiv 1(561)$. לפי משפט בפרק שקילויות (סעיף ג') אם נוכיח $b^{560}\equiv 1(3)$ וגם $b^{560}\equiv 1(11)$ וגם $b^{560}\equiv 1(17)$, אז מתקיים $b^{560}\equiv 1(3\cdot 11\cdot 17)\Rightarrow b^{560}\equiv 1(561)$ וס"מ.נ. לכן נוכיח שלושה שקילויות אלו. מכיוון ש-$(b,561)=1$ כלומר b זר ל-561, אז הוא גם זר לכל הפקטורים שלו, לכן מתקיים $(b,3)=(b,11)=(b,17)=1$. ומכיוון ש-$3,11,17$ ראשוניים ניתן להשתמש במשפט פרמה הקטן ולקבל $b^2\equiv 1(3),\ b^{10}\equiv 1(11),\ b^{16}\equiv 1(17)$.

נבצע את התהליך הבא על כל השקילויות ונקבל.

$$\left.\begin{array}{l} b^{560}\equiv (b^2)^{280}\equiv 1^{280}\equiv 1\ (3)\\ b^{560}\equiv (b^{10})^{56}\equiv 1^{56}\equiv 1\ (11)\\ b^{560}\equiv (b^{16})^{35}\equiv 1^{35}\equiv 1\ (17)\end{array}\right\} b^{560}\equiv 1(3\cdot 11\cdot 17)\Rightarrow b^{560}\equiv 1(561)$$

מ.ש.ל.

משפט: יהי $n=q_1\cdot q_2\cdot\ldots\cdot q_k$ כאשר $q_1,q_2,\ldots,q_k$ ראשוניים שונים, כלומר אין ראשוני בחזקה גבוהה מ-1 בפקטוריזציה של n, או במילים אחרות n "חופשי מריבועים". אם לכל $i\in[k]$ מתקיים: $q_i-1\mid n-1$, אז n הינו מספר קרמייקל.

הוכחה: יהי n כמו במשפט חופשי מריבועים, כך שלכל $i\in[k]$ מתקיים $q_i-1\mid n-1$. צ"ל ש-n הינו מספר קרמייקל, כלומר לכל $b\in\mathbb{Z}^+$ כך ש-$(b,n)=1$ מתקיים: $b^{n-1}\equiv 1(n)$. היות ו-b זר ל-n אז הוא גם זר לכל הפקטורים שלו, לכן לכל $i\in[k]$ מתקיים $(b,q_i)=1$. מכיוון שכל q_i ראשוני אז לפי משפט פרמה הקטן $b^{q_i-1}\equiv 1(q_i)$, לכל $i\in[k]$. היות ו-$q_i-1\mid n-1$ לפי משפט החלוקה קיים $m\in\mathbb{Z}$ כך ש-$m\cdot(q_i-1)=n-1$. לכן לכל $i\in[k]$ מתקיים: $b^{n-1}\equiv b^{m(q_i-1)}\equiv b^{(q_i-1)^m}\equiv 1^m\equiv 1(q_i)$ ולפי המשפט שהזכרנו לעיל, נוכיח כי: $b^{n-1}\equiv 1(q_1\cdot q_2\cdot\ldots\cdot q_k)\equiv 1(n)$ מ.ש.ל.

m זו החזקה המשלימה. בדוגמא לעיל $m=280,56,35$.

26/12 בס״ד

סעיף זה והבא הם הקדמה למשפט אוילר.

1) כמות המספרים הזרים ל-n – $\varphi(n)$

הגדרה: יהי $n\in\mathbb{Z}^+$. נסמן ב-$\varphi(n)$ את כמות המספרים הטבעיים הקטנים מ-n שזרים אליו.

כלומר $\varphi(n)=|\{x\in[n]:(x,n)=1\}|$.

דוגמאות: $\varphi(30)=|\{1,7,11,13,17,19,23,29\}|=8$. $\varphi(7)=|\{1,2,3,4,5,6\}|=6$. $\varphi(4)=|\{1,3\}|=2$.

משפט: לכל $n\in\mathbb{Z}^+\setminus\{1\}$ מתקיים:

(1) אם n פריק מתקיים: $\varphi(n)\le n-2$. מפני ש-n אינו זר לעצמו ויש לפחות גורם ראשוני אחד שהוא אינו זר לו.

(2) n ראשוני אם ורק אם $\varphi(n)=n-1$. מפני שכל המספרים חוץ מ-n זרים למספר ראשוני.

הגדרה: פונקציה f תיקרא "פונקציה כפלית" אם מתקיים: $f(m\cdot n)=f(m)\cdot f(n)$ לכל $(m,n)=1$.

נקראת "פונקציית אוילר"

משפט: הפונקציה $\varphi(n)^*$ היא פונקציה כפלית. כלומר, אם $(m,n)=1$ אזי $\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)$.

הוכחה: לפי הגדרת $\varphi(m\cdot n)$ מתקיים $\varphi(m\cdot n)=|\{x\in[m\cdot n]:(x,mn)=1\}|$. לפי משפט ? מ-gcd, האומר $(a,b)=1$ וגם $(a,c)=1$ אם ורק אם $(a,bc)=1$, אזי מתקיים גם: $\varphi(m\cdot n)=|\{x\in[m\cdot n]:(x,b)=1\wedge(x,c)=1\}|$.
מכאן נלמד שכדי לספור את כל המספרים שזרים ל-$m\cdot n$ מספיק לספור את כל המספרים ב-$[mn]$ שזרים ל-m ומתוכם לקחת את אלו שזרים גם ל-n. נבנה את הטבלה הבאה שמכילה את כל המספרים ב-$[mn]$.

$$\begin{array}{cccccc}
1 & 2 & 3 & \cdots & r & \cdots\ m \\
m+1 & m+2 & m+3 & \cdots & m+r & \cdots\ 2m \\
2m+1 & 2m+2 & 2m+3 & \cdots & 2m+r & \cdots\ 3m \\
3m+1 & 3m+2 & 3m+3 & \cdots & 3m+r & \cdots\ 4m \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
(n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & (n-1)m+r & \cdots\ nm
\end{array}$$

כל עמודה היא מהצורה $qm+r$ כאשר $r\in[m]$ קבוע לכל עמודה, ו-$q\in[0,n-1]$ משתנה ערך בכל עמודה. לפי משפט עזר באלגוריתם אוקלידס מתקיים: $(qm+r,m)=(r,m)$.

מכיוון ש-r קבוע בכל עמודה אזי יוצא ממשפט זה שבכל עמודה כל האיברים שייכים לאותה מחלקת שקילות. אנו מחפשים עמודות כך ש-$(r,m)=1$. מכיוון ש-$r\in[m]$ וב-$[m]$ יש $\varphi(m)$ איברים הזרים ל-m, יוצא שיש $\varphi(m)$ עמודות שלמות הזרות ל-m. נוכיח כי בכל עמודה כזו יש $\varphi(n)$ איברים הזרים ל-n. אם נוכיח כי בכל עמודה כזו אין שני איברים שקולים מודולו n, כלומר שכל עמודה הזרה ל-m היא מערכת שאריות קנונית שלמה עבור n, אז סיימנו, כי כל מערכת כזאת מכילה בדיוק $\varphi(n)$ איברים שזרים ל-n. יהי עמודה $qm+r$, ונניח בשלילה שקיימים $q_1,q_2\in[0,n-1]$ כך ש-$q_1\not\equiv q_2$, אך $q_1m+r\equiv q_2m+r\ (n)$. מכיוון ש-$q_1,q_2<n$ והם שונים אזי $q_1\not\equiv q_2\ (n)$. היות ולפי ההנחה במשפט מתקיים $(m,n)=1$ נחסיר את r ונחלק ב-m את המשוואה $q_1m+r\equiv q_2m+r\ (n)$, ונקבל $q_1\equiv q_2\ (n)$, וזו סתירה ולכן אין שני איברים בעמודה השקולים ל-n, וכל עמודה היא מערכת שאריות קנונית שלמה ל-

שאלה: בתחילת סעיף זה ראינו שלכל מספר ראשוני p מתקיים: $\varphi(p)=p-1$. כיצד נחשב את $\varphi(p^k)$ כאשר $k>0$?

תשובה: לפי ההגדרה $\varphi(p^k)=|\{x\in[p^k]:(x,p^k)=1\}|$. נשים לב כי בפקטוריזציה של p^k יש רק ראשוני אחד p, ולכן כל המספרים $y\in[p^k]$ המקיימים $(y,p^k)\neq 1$ הם בהכרח כפולה של p. לכן ניתן להגדיר מחדש $\varphi(p^k)=|[p^k]\setminus\{y\in[p^k]:p|y\}|$. כלומר נוריד מ-$[p^k]$ את כל הכפולות של p עד p^k, שהם: $1\cdot p, 2\cdot p,\ldots,p^{k-1}\cdot p$. ניתן לראות בבירור שיש p^{k-1} מספרים כאלו, לכן: $\boxed{\varphi(p^k)=p^k-p^{k-1}=p^k(1-\frac{1}{p})}$

שאלה: בתחילת סעיף זה ראינו שלכל מספר פריק n מתקיים: $\varphi(n)\le n-2$. כיצד נחשב את $\varphi(n)$?

תשובה: יהי $1<n\in\mathbb{Z}^+$ כך שהפקטוריזציה שלו היא $n=p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_k^{a_k}$. לכן $\varphi(n)=\varphi(p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_k^{a_k})$
מכיוון שהוכחנו ש-$\varphi(n)$ היא פונקציה כפלית מתקיים: $\varphi(n)=\varphi(p_1^{a_1})\cdot\varphi(p_2^{a_2})\cdot\ldots\cdot\varphi(p_k^{a_k})$.
נשתמש בתשובה לשאלה לעיל לחישוב $\varphi(p)$ כש-p ראשוני, נקבל: $\varphi(n)=p_1^{a_1}(1-\frac{1}{p_1})\cdot p_2^{a_2}(1-\frac{1}{p_2})\cdot\ldots\cdot p_k^{a_k}(1-\frac{1}{p_k})$
נמצא כי: $\boxed{\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdot\ldots\cdot(1-\frac{1}{p_k})}$

ט) קבוצת שאריות מצומצמת

הגדרה: יהי $n\in\mathbb{Z}^+$ ויהי קבוצה $A\subseteq\mathbb{Z}$ כך ש-$|A|=\varphi(n)$. אזי A תיקרא "מערכת שאריות מצומצמת מודולו n" אם מתקיימים שני תנאים:

(1) לכל $a\in A$ מתקיים $(a,n)=1$.

(2) כל שני איברים ב-A אינם קונגרואנטים אחד לשני מודולו n.

דוגמא: $A=\{1,3,5,7\}$ הינה מערכת שאריות מצומצמת *קנונית* מודולו 8.

משפט: יהי $n\in\mathbb{Z}^+$, ותהא $\{r_1,r_2,\ldots,r_{\varphi(n)}\}$ מערכת שאריות מצומצמת מודולו n, ויהי $a\in\mathbb{Z}$ כך ש-$(a,n)=1$, אזי $\{a\cdot r_1,a\cdot r_2,\ldots,a\cdot r_{\varphi(n)}\}$ גם היא מערכת שאריות מצומצמת מודולו n.
משפט זה דומה למשפט עבר בסעיף ב', אלא ששם n היה ראשוני וקבוצת השאריות הייתה כל השאריות מלבד 0. נוכיח שאכן הקבוצה החדשה מקיימת את (1) ו-(2) בהגדרה.

הוכחה: (1) יהי $a\cdot r_j$ איבר כלשהו בקבוצה החדשה, יש להוכיח $(a\cdot r_j,n)=1$. מכיוון שלפי ההנחה $j,n)=1$ וגם $(a,n)=1$, נמצא שגם ל-r_j וגם ל-a אין פקטורים משותפים עם n. לכן אכן מתקיים $(a\cdot r_j,n)=1$

(2) יהיו r_i,r_j איברים שונים בקבוצה המקורית כך שמתקיים $r_i\not\equiv r_j\,(n)$. נניח בשלילה כי $r_i\equiv a\cdot r_j\,(n)$
נחלק את השקילות ב-a. מכיוון ש-$(a,n)=1$ נקבל $r_i\equiv r_j\,(n)$ בסתירה להנחה! לכן אין שני איברים בקבוצה החדשה שהם קונגרואנטים מודולו n.

26/12 בס"ד

משפט: יהי $n\in\mathbb{Z}^+$, ותהי $\{r_1,r_2,\dots,r_{\varphi(n)}\}$ מערכת שאריות מצומצמת מודולו n ויהי $a\in\mathbb{Z}$ כך ש-$(a,n)=1$. אזי מתקיים: $ar_1\cdot ar_2\cdot\ldots\cdot ar_{\varphi(n)}\equiv r_1\cdot r_2\cdot\ldots\cdot r_{\varphi(n)}\ (n)$

הוכחה: לפי הגדרת מערכת שאריות מצומצמת ולפי משפט קודם נסיק כי לכל איבר בצד שמאל יש איבר יחיד שקול בצד ימין וכולם זרים ל-n. בנוסף יש אותה כמות איברים השני הצדדים $\varphi(n)$. לכן השקילות מתקיימת.

ח) משפט אוילר

משפט אוילר: יהי $n\in\mathbb{Z}^+$ ויהי $a\in\mathbb{Z}$ כך ש-$(a,n)=1$. אזי מתקיים: $a^{\varphi(n)}\equiv 1\ (n)$.

הוכחה: תהי $\{r_1,r_2,\dots,r_{\varphi(n)}\}$ מערכת שאריות מצומצמת מודולו n. לפי משפט אחרון בסעיף קודם מתקיים $ar_1\cdot ar_2\cdot\ldots\cdot ar_{\varphi(n)}\equiv r_1\cdot r_2\cdot\ldots\cdot r_{\varphi(n)}\ (n)$. נוכל לכתוב זאת גם כך $a^{\varphi(n)}(r_1\cdot r_2\cdot\ldots\cdot r_{\varphi(n)})\equiv r_1\cdot r_2\cdot\ldots\cdot r_{\varphi(n)}\ (n)$. נצמצם איברים שקולים, היות ולכל $i\in[\varphi(n)]$ ל-r_i ול-n אין פקטורים משותפים מפני שהם זרים, מתקיים $((r_1\cdot r_2\cdot\ldots\cdot r_{\varphi(n)}),n)=1$. לכן נקבל $a^{\varphi(n)}\equiv 1\ (n)$. מ.ש.ל.

מסקנה: $a^{\varphi(n)-1}$ הינו ההופכי של a מודולו n. היות ולפי משפט אוילר מתקיים $a\cdot a^{\varphi(n)-1}\equiv 1\ (n)$