1 חשבון שאריות

שאלה 1: מה הספרה האחרונה של המספר $2011^{17} + 17^{2011}$?
פתרון שאלה 1: ספרה אחרונה של מספר זו גם שארית החלוקה שלו ב־10. אם שני מספרים מסתיימים ב־1, גם המכפלה שלהם מסתיימת ב־1. בפרט, 2011^{17} מסתיים ב־1. זה מקרה פרטי של עובדה כללית: שארית חלוקה של מכפלה תלויה רק בשארית החלוקה של הגורמים.

אנו נשתמש בהמשך בסימון הבא: $x \equiv y \mod n$ אם ל־x, y אותה שארית חלוקה ב־n.

טענה: אם $x \equiv a \mod n$, $y \equiv b \mod n$ אז $xy \equiv ab \mod n$.
הוכחה: $x \equiv a \mod n$ כאשר $x = a + nk$. באותו אופן $y = b + nl$. לכן $xy = (a+nk)(b+nl) = ab + n(al + bk + nkl)$, לכן $xy \equiv ab \mod n$.

תרגיל: להוכיח שגם שארית חלוקה של סכום והפרש תלויה רק בשארית החלוקה של המחוברים.

המשך פתרון שאלה 1: $17^{2011} = 17^{2010} \cdot 17 \equiv 49^{1005} \cdot 17 \equiv (-1)^{1005} \cdot 7 = -7 \equiv 3 \mod 10$. לכן בסה"כ $2011^{17} + 17^{2011} \equiv 1 + 3 = 4 \mod 10$, כלומר המספר נגמר ב־4.

שאלה 2: להוכיח שלמשוואה $x^2 - 3y^2 = 2011$ אין פתרונות.
הוכחה: נבדוק שאריות מודולו 4: $x^2 + y^2 \equiv 3 \mod 4$. אילו שאריות יכולות להיות מודולו 4 לריבוע של מספר? השארית של הריבוע תלויה רק בשארית של המספר שמעלים בריבוע. לכן מספיק לבדוק 4 נציגים: $0^2 \equiv 0 \mod 4$, $1^2 \equiv 1 \mod 4$, $2^2 \equiv 0 \mod 4$, $3^2 \equiv 1 \mod 4$. השארית יכולה להיות רק 0 או 1. הסכום $x^2 + y^2$ יכול לתת שארית של 0, 1 או 2 מודולו 4, אבל אף פעם לא 3. לכן אין פתרונות למשוואה.

מוסר השכל מהשאלה הוא, שצריך להסתכל על ריבועים מודולו 4.ולפעמים מודולו 8.

תרגיל: מה השאריות האפשריות של ריבוע מודולו 8?

ראינו שאפשר לחבר, לחסר ולהכפיל שאריות מודולו n. אם בנוסף $n = p$ ראשוני, אפשר גם לחלק שאריות. קודם נדבר על מספרים ראשוניים:

1.1 מספרים ראשוניים

הגדרה: מספר $p > 1$ נקרא ראשוני אם לא ניתן להציג אותו כמכפלה של שני מספרים שלמים, שאינם ± 1.
דוגמאות: $2, 3, 5$ ראשוניים. $4 = 2 \cdot 2$, $6 = 2 \cdot 3$ אינם ראשוניים.
הערה: לפעמים אנחנו נעבוד עם מספרים שלמים, לא רק חיוביים, ונתעלם מהסימן. במקרה זה, השוואה בין שני מספרים נעשית על ידי השוואת הגודל של הערכים המוחלטים.
משפט אוקלידס: יש אינסוף מספרים ראשוניים.
הוכחה: נניח בשלילה שכל הראשוניים הם $p_1, ..., p_n$. נתבונן במספר $Q = p_1 ... p_n + 1$. לכל מספר טבעי ישנו ראשוני שמחלק אותו (למה?). נבחר ראשוני q שמחלק את Q. היות ו־ q מחלק גם את $p_1 ... p_n$, הוא מחלק גם את 1. סתירה.
תרגיל: להוכיח שיש אינסוף ראשונים מהצורה $4k + 3$.

המשפט היסודי של האריתמטיקה: לכל מספר שלם ישנו פירוק למכפלת ראשוניים חיוביים וסימן (כלומר ± 1). הפירוק יחיד (עד כדי שינוי סדר הגורמים).
הוכחה: קיום הפירוק מיידי מהגדרה: נתחיל ממספר שלם כלשהו. אם הוא ראשוני, סיימנו. אחרת, נציג אותו כמכפלה של שני שלמים ששונים מ־± 1, ולכן גם קטנים ממנו ממש בערך מוחלט. ממשיכים באינדוקציה על הערך המוחלט של המספר. נשאר להראות את יחידות הפירוק: נניח $p_1 ... p_k = q_1 ... q_l$ (כולם ראשוניים חיוביים) ונראה $k = l$, ושהגורמים אותם גורמים עד כדי תמורה. p_1 מחלק את המספר שמימין. היינו רוצים לומר שהיות והוא ראשוני, הוא חייב לחלק את אחד המספרים מימין. בשביל ההוכחה, נזדקק למושג המחלק המשותף הגדול ביותר

:GCD -

הגדרה: $gcd(a,b)$ הוא המספר הגדול ביותר שמחלק את a,b.

כיצד מוצאים GCD? למשל ע"י פירוק לגורמים ראשוניים. אבל כרגע עדיין אסור לנו, כי לא הוכחנו יחידות. נניח $a>b>0$, נתבונן בזוג $a-b,b$. קל לראות (תרגיל) שכל מחלק של שני המספרים האלה, מחלק גם את הזוג (a,b)ת ולהפך. לכן גם ה־GCD מתלכד. הרעיון הוא לחזור על הפעולה הזו הרבה פעמים.
דוגמא: $(8,3)\to(5,3)\to(3,2)\to(2,1)\to(1,1)\to(0,1)\to(0,1)$.
התהליך התייצב, ואנו רואים שהמחלק המשותף הגדול ביותר הוא 1. אנו גם רואים שניתן להגיע לסוף יותר מהר על ידי חלוקה עם שארית.

אלגוריתם אוקלידס: בהינתן $(a_0>a_1)$, עושים סדרת חלוקות עם שארית:

$$a_0=k_0a_1+a_2\to a_1=k_1a_2+a_3\to a_2=k_2a_3+a_4\to,...$$

ובכל פעם $0\le a_j<a_{j-1}$/ התהליך עוצר כאשר אי אפשר לחלק יותר, כלומר קיבלנו שארית $a_{n+1}=0$. ואז $a_n=gcd(a_0,a_1)$.
ע"י העברות אגף קל לראות:
מסקנה 1 מאלגוריתם אוקלידס: קיימים u,v שלמים כך ש־ $gcd(a_0,a_1)=a_0u+a_1v$. סיבה:

$$a_2=a_0-k_0a_1\Rightarrow a_3=a_1-k_1a_2=A_3a_0+B_3a_1\Rightarrow ...\Rightarrow a_n=A_na_0+B_na_1$$

.

שני מספרים a,b נקראים זרים אם $gcd(a,b)=1$. נראה שבמקרה הזה מתקיימת גם טענה הפוכה:
טענה: אם קיימים u,v כך ש־$au+bv=1$ אז a,b זרים.
הוכחה: תרגיל.
תרגיל: $gcd(a,b)$ הוא המספר הקטן ביותר כך שלכל u,v שלמים, $ua+vb$ הוא כפולה שלמה שלו.

1.2 המשפט היסודי - המשך

ועכשיו, בחזרה להוכחת המשפט היסודי.

טענה עיקרית: אם c זר ל־ a,b, אז c זר למכפלה ab.
הוכחה: אם $uc+va=1$, $sc+tb=1$ אז גם $(uc+va)(sc+tb)=usc^2+utcb+vsca+vtab=cX+abY=1$ ולכן c זר ל־ab.
מסקנה: אם p מחלק את ab, אז p מחלק את a או את b.
סיבה: p ראשוני, ולכן לכל מספר x יש שתי אפשרויות: p מחלק את x או ש־p זר ל־x.

ולכן ניתן להסיק מהשוויון $p_1...p_k=q_1...q_l$ שכל p_i מחלק איזשהו q_j, ומראשוניות־שווה לו. מצמצמים וממשיכים. זה מסיים את הוכחת המשפט היסודי.

ראשוניות חשובה בשביל שנוכל לחלק שאריות. בתור דוגמא שבה אי אפשר לחלק, נסתכל על שאריות מודולו 6. $3x\equiv 2 \mod 6$ היא משוואה לא פתירה, ואילו ל־$4x\equiv 2 \mod 6$ מספר פתרונות שונים.

מסקנה 2 מאלגוריתם אוקלידס: לשארית לא אפסית מודולו מספר ראשוני p יש שארית הפכית יחידה. כלומר, למשוואה $ax\equiv 1 \mod p$ עבור a זר ל־p יש פתרון יחיד מודולו p. x קיים כי קיימים x,y כך ש־ $ax+py=1$.
את יחידות הקיום של x אפשר לראות בשתי דרכים:
דרך 1: $ax\equiv ay\equiv 1$ גורר $x\equiv x\cdot 1\equiv x(ay)\equiv(xa)y\equiv y$.
דרך 2: $ax\equiv ay\equiv 1$ גורר $a(x-y)\equiv 0$, לכן $p|a(x-y)$. a זר ל־p, לכן $p|(x-y)$ כלומר $x\equiv y \mod p$.

שאלה 3 (משפט וילסון) חשבו את $(p-1)! \mod p$.
פתרון: לכל שארית יש שארית הפכית. לכן התשובה אמורה להיות 1. נבדוק : $p=3$ ונקבל... $2\equiv -1$. והסיבה - שיש שאריות שהפוכות לעצמן. נראה שיש בדיוק שתי שאריות הפוכות לעצמן בדיוק שהפוכות לעצמן:
$1/x\equiv x\Leftrightarrow x^2\equiv 1\equiv p|(x-1)(x+1)$. לכן התשובה היא : -1. פרט למקרה $p=2$, שבו $1\equiv -1 \mod 2$, ואז $(2-1)!\equiv 1$.

לפני השאלה הבאה, נדגיש שכעת אנו יכולים לייצג מספרים רציונלים מודולו p ע"י שאריות, כך שסכום מתאים לסכום וכפל מתאים לכפל וחילוק מתאים לחילוק: ההסתייגות היחידה היא, שהמכנה לא צריך להתחלק ב־p.

ניסוח מדוייק: לכל $q = \frac{m}{n}$ כך ש־ $n \neq 0 \mod p$ נתאים את השארית $q \mod p = mn^{-1} \mod p$. לא קשה לראות שחיבור, כפל וחילוק של שברים עם מכנה זר ל־p שומרים על התכונה הזו של המכנה (תחת ההסתייגות שאסור לחלק באפס מודולו p, כלומר שבר שהמונה שלו מתחלק ב־p). פעולות החשבון נשמרות, כלומר:

$(q+r) \mod p = q \mod p + r \mod p$

$(q \cdot r) \mod p = (q \mod p) \cdot (r \mod p)$

$(q/r) \mod p = (q \mod p)(r \mod p)^{-1}$ כאשר $r \mod p \neq 0$.

שאלה 4: להוכיח שאם $1 + 1/2 + 1/3 + .. + 1/(p-1) = m/n$, $p \neq 2$, אז $p|m$.
הוכחה: כאשר מחברים את כל השאריות הלא־אפסיות מודולו p, $1 + ... + (p-1) \equiv 0 \mod p$ (עבור כל שארית מופיעה שארית נגדית). מכאן שגם $1/1 + ... + 1/(p-1) \equiv 0 \mod p$. ואז $m/n \equiv 0$, לכן $m \equiv 0 \mod p$ וסיימנו.

שאלה 5 (מגיליס): למצוא k מינימלי כך ש־ $\frac{3^{44}-1}{80} = a_1^4 + ... + a_k^4$.
פתרון. קודם כל, $3^4 - 1 = 80$, ולכן $\frac{3^{44}-1}{80} = (3^4)^{10} + ... + 3^4 + 1$ הפעם נבדוק מודולו 16: חזקה רביעית של מספר היא תמיד 0 או 1. מספר זוגי בבירור נותן 0, ובכל מקרה

$$(x+2)^4 = (x^2+4x+4)^2 \equiv x^4 + 2x^2(4x+4) = x^4 + 8x^2(x+1) \equiv x^4 \mod 16$$

לכן מודולו 16 המספר בשאלה הוא 11, וברור שאי אפשר לעשות פחות מחוברים כי צריך לצבור לפחות 11 שאריות 1. לכן $k = 11$ מינימלי.

2 משפט פרמה הקטן

המשפט נוסח ע"י פרמה והוכח ע"י אוילר.
משפט: עבור p ראשוני, מתקיים לכל שלם a כי $a^p \equiv a \mod p$. בפרט לכל a זר ל־p מתקיים ש־ $a^{p-1} \equiv 1 \mod p$.
זה משפט חשוב, ולכן נראה 3 הוכחות שונות.
הוכחה 1: $(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}$. המקדמים $\binom{p}{k}$ כולם מתחלקים ב־p (למה?) ולכן $(x+y)^p \equiv x^p + y^p \mod p$. מכאן $a^p = (1 + ... + 1)^p \equiv 1 + ... + 1 = a \mod p$.

הוכחה 2: נתבונן בכל השאריות הלא אפסיות מודולו p: $1, ..., p-1$. היות והכפלה בשארית לא טריויאלית היא פעולה הפיכה, ברשימה $a, 2a, ..., (p-1)a$ מופיעות שוב כל השאריות הלא טריוילאיות, כל אחת פעם אחת בדיוק. לכן מכפלת כל האיברים שווה: $(p-1)! \equiv a^{p-1}(p-1)!$. $(p-1)!$ הפיך, לכן נחלק בו ונקבל $a^{p-1} \equiv 1$. את המקרה $p|a$ בודקים בנפרד.

הוכחה 3: פיצה! נתבונן בפיצה עם p משולשים, יש a תוספות שונות, ובכל משולש יש תוספת אחת בדיוק. ואנחנו רוצים לספור כמה פיצות שונות אפשר להרכיב ככה, כאשר שתי פיצות הן שונות אם אחת לא מתקבלת מהשנייה ע"י סיבוב. חישוב גס : a^p חלוקות של תוספות, p סיבובים. סה"כ: a^p/p. לא מדוייק, כי לפעמים הסיבוב מעביר את הפיצה בדיוק לעצמה. מתי זה קורה? אם נניח שסיבוב לא־טריויאלי כלשהו העביר פיצה לעצמה, אפשר לחזור על הסיבוב שוב ושוב. אם נעקוב אחרי משולש ספציפי, היות ו־p ראשוני המשולש יעבור במיקומי כל שאר המשלושים, ויחזור לעצמו רק אחרי p סיבובים. לכן יש רק תוספת אחת בפיצה, יש a פיצות כאלה, וברור שכל פיצה כזאת באמת עוברת רק לעצמה תחת כל סיבוב. לכן, חישוב מדוייק: $N = a + (a^p - a)/p$. בפרט $(a^p - 1)$ מתחלק ב־ p, כנדרש.
עכשיו נוכל להגדיר סדר של שארית מודולו p:
הגדרה: $ord_p(a) = \min\{k : a^k \equiv 1\}$.
הוכחנו ש־ $ord(a) \leq p-1$, ולמעשה הוכחנו יותר:
טענה: $ord_p(a)|(p-1)$.
רעיון הוכחה החזקות k שעבורן $a^k \equiv 1 \mod p$ מהוות סדרה חשבונית (הוכיחו זאת!).

שאלה 6 (IMO 2005) למצוא כל המספרים הטבעיים שזרים לאיברי הסדרה $2^n + 3^n + 6^n - 1$, $n \geq 1$

פתרון: היינו רוצים להציב $n=1$ ולקבל 0, שלא זר לכלום. זה אפשרי בעזרת משפט פרמה הקטן: עבור ראשוני p ניקח $n \equiv -1 \mod (p-1)$. אז $2^n+3^n+6^n-1 \equiv 1/2+1/3+1/6-1 \equiv 0 \mod p$. הטריק הזה לא עובד כאשר $p=2$ או $p=3$, אבל לא קשה להציב ערכי n קטנים שנותנים מספרים שמתחלקים ב־2 או 3. לכן רק 1 זר לכל איברי הסדרה.

2.1 שאריות ריבועיות

מתי מספר מסויים הוא ריבוע מודולו p? נתבונן בשארית $a \neq 0$ מודולו p. המספר $b=a^{(p-1)/2}$ מקיים $b^2 \equiv 1$, ולכן $b \equiv \pm 1 \mod p$. אם $b=a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \mod p \Leftarrow a \equiv x^2$. לכן $ord_p(a)$ מחלק את $(p-1)/2$ הוא תנאי הכרחי לכך ש־a ־ שארית ריבועית. למעשה זה גם תנאי מספיק: בשביל זה צריך לשים לב שבקבוצת השאריות ההפיכות ${Z_p}^*$, ההעתקה $x \mapsto x^2$ היא שתיים לאחת (תרגיל: הוכיחו זאת). כלומר בדיוק חצי מכל השאריות הן שאריות ריבועיות. לפולינום $x^{(p-1)/2}-1 \equiv 0 \mod p$ יכולים להיות לכל היותר $(p-1)/2$ שורשים שונים, וכבר הוכחנו שכל שארית ריבועית היא שורש של הפולינום. לכן רק השאריות הריבועיות פותרות אותו.

שאלה 7: להוכיח שיש אינסוף ראשוניים מהצורה $4k+1$
הוכחה: נניח שיש מספר סופי: $p_1,...,p_n$. נתבונן ב־ $Q=4p_1^2...p_n^2+1$. יש לו מחלק ראשוני מהצורה $p=4k+3$, ואז $x^2 \equiv -1 \mod p$ ובפרט $1 \equiv (-1)^{(p-1)/2}=(-1)^{2k+1}=-1$. וזו סתירה.

שאלה 8: להוכיח שאם $1+1/2+1/3+..+1/(p-1)=m/n$, $p \neq 2,3$, אז $p^2|m$.
הוכחה: נשים לב ש־

$$\frac{1}{k}+\frac{1}{p-k}=\frac{p}{k(p-k)}$$

מכאן שאם נסמן $h=(p-1)/2$,

$$1+1/2+1/3+..+1/(p-1)=p\left(\frac{1}{p-1}+\frac{1}{2(p-2)}+...+\frac{1}{h(p-h)}\right)$$

לכן מספיק להראות

$$\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+...+\frac{1}{h(p-h)} \equiv 0 \mod p$$

במכנה מופיעים כל הריבועים הלא אפסיים עם סימן מינוס:

$$\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+...+\frac{1}{h(p-h)} \equiv -\frac{1}{1^2}-...-\frac{1}{h^2} \mod p$$

כל שארית לא אפסית מופיעה פעם אחת בדיוק (כמו כן, לקיחת הפכי כפלי מעבירה את קבוצת השאריות הריבועיות לעצמה). אם נכפיל ב־ (-2) (זה לא ישנה התאפסות מודולו p), נקבל את סכום כל ריבועי כל השאריות מודולו p:

$$1^2+...+(p-1)^2=\frac{(p-1)p(2p-1)}{6} \equiv 0 \mod p$$

כי $p \neq 3$.

2.2 סימני חלוקה

סימני חלוקה זו דרך פשוטה לדעת מהצגה עשרונית של מספר, אם הוא מתחלק במספר נתון. לכן חשוב לדעת מה שאריות החלוקה של חזקות של 10. לפי משפט פרמה הקטן, יש סימן חלוקה מהצורה הבאה:
$p|\overline{a_1...a_n}$ אם ורק אם המספר $\overline{a_1...a_n}$ מורכב מבלוקים באורך $p-1$ עבורם הסכום המשוקלל $w_1a_1+...+w_{p-1}a_{p-1} \equiv 0 \mod p$, כאשר $w_j \equiv 10^j \mod p$.
העובדה הבאה שימושית: $10^k \equiv 1 \mod p \Leftrightarrow 111...1 \equiv 0 \mod p$.
לכן בכל פעם ש־$11..1$ מתחלק במספר ראשוני מסויים, יש בשבילו סימן חלוקה פשוט. למשל:
$3 \cdot 37=111$ ־ סימן חלוקה ל־37 מאורך 3.
$11 \cdot 101=1111$ ־ סימן חלוקה ל־101 מאורך 4.
$41 \cdot 271=11111$ ־ סימן חלוקה ל־41, 271 מאורך 5
$7 \cdot 11 \cdot 13=111111$ ־ ...
תרגיל: הוכיחו: $123|\overline{abcde}$ אם ורק אם $123|\overline{eabcd}$

2.3 מחזור של שברים עשרוניים

מה אורך המחזור של השבר $1/p$? ננסה מספר דוגמאות:
$1/7 = 0.142857142857...$ ־ אורך מחזור מינימלי = 6,
$1/13 = 0.076923076923...$ ־ אורך מחזור מינימלי = 6.
באופן כללי, אורך המחזור נקבע ע"י הסדר של 10 מודולו p:
משפט: אורך המחזור של $1/p$ הוא $ord_p(10)$.
הוכחה: נרשום $1/p = 0.a_1a_2...a_ka_{k+1}...$. אז $10^k/p = \overline{a_1...a_k} + 0.a_{k+1}a_{k+2}...$. אם $10^k = pA + 1$, נקבל ש־$A + 1/p = \overline{a_1...a_k} + 0.a_{k+1}a_{k+2}...$ ומכאן $1/p = 0.a_{k+1}a_{k+2}...$. כלומר $10^k \equiv 1 \mod p$ (k מינימלי נקרא $ord_p(10)$) אם ורק אם k־מחזור של השבר העשרוני.

מסקנה: אורך המחזור של $1/p$ מחלק את $p-1$.

תרגיל: נניח ש־$ord_p(10) = p - 1$, ו־ $1/p = 0.\overline{a_1...a_{p-1}}$. הוכיחו שעבור $j = 1, ..., p - 1$, הכפלה ב־ j של המספר $\overline{a_1...a_{p-1}}$ מביאה לתמורה של הספרות.