① 11/5/08

תורת המספרים וקריפטוגרפיה

מדוע? - אבי ויגדרזון מפרינסטון

"זו הדרך הטובה ביותר לקבל הקדמה לקורס" (לובוצקי)

המטרה: להסתיר מידע מאחרים. זה משהו שהיה רלוונטי כבר לפני 3000 שנה. אז ההנחה תמיד הייתה שלצד שרוצה לתקשר יש איזשהו מידע משותף סודי ומי שמאזין לתקשורת אין לו המידע הזה. בקריפטוגרפיה המודרנית נקודת המוצא היא שונה.

יש קונפליקט בין שתי המטרות:
- סודיות ופרטיות
- עמידות בפני תקלות ותפסות

כמובן נרצה לעשות את כל המשימות שלנו (הצבעה, זיהוי, חתימת חוזים, העברת כספים וכן הלאה) באופן דיגיטלי, ללא שימוש בשום עזר פיסי וללא צורך לבטוח באף אחד.

דיפי והלמן, במאמר מ-1976 עשו פריצת דרך עם שתי ההנחות שלהם:
- לכל המשתתפים יכולת חישוב מוגבלת
- יש בעיות שמאוד קשה לפתור (חישובית) (מדידה של קושי של בעיה נעשית ע"י הסתכלות אסימפטוטית כאשר גודל הנתונים גדל - למשל חיבור שני מספרים באורך 3 ספרות מול 3-מיליון ספרות)

דוגמאות לבעיות:
- כפל מספרים - בעיה קלה. אפשר להכפיל בשניה מספרים בני אלפי ספרות. מספר הצעדים לכפל

מספרים בני n ספרות הוא n^2. זה לא נחשב הרבה.

- הבעיה ההפוכה לרפל: פירוק מספרים לגורמים ראשוניים. האלגוריתם הטוב ביותר שקיים היום מבצע $e^{\sqrt{n}}$ צעדים על קלטים בני n ספרות. זאת בעיה קשה!!! לפחות נכון לזמן כתיבת סיכום זה. אבל מעתה נניח שזו בעיה קשה.

⇐ **אקסיומה: קשה לפרק מספרים**

⇐ **אקסיומה: המשתתפים מוגבלים חישובית**

איך האקסיומות האלה עוזרות לנו? ישנן שתי קופסאות:

| p·q | | (p, q) |

מבחינת אינפורמציה הן שקולות. מכל אחת ניתן לעבור לשנייה. אבל ברגע שמכניסים פנימה שיקולים של חישוביות מדובר בשני דברים מאוד שונים. קל לעבור מ-(p,q) ל-pq אבל קשה לעבור מ-pq ל-(p,q). חוסר הסימטריה הזה ישרת אותנו.

האמת היא שלא חייבים להסתמך על פירוק מספרים. מספיק להניח שקיימת פונקציה חד-כיוונית E. כלומר להשתמש בה היא פעולה קלה, אבל קשה להפוך אותה. יש כל מיני דוגמאות לפונקציות כאלה (למשל הכנת חביתה מביצה. אם כי אנחנו נתעניין בפונקציות מתמטיות ולא פיסיקליות...)

של הפונקציה E יש כמה הנחות:

- אפשר להכניס פנימה כל תוכן X
- קל לחשב את הערך E(X)
- בלתי אפשרי לשנות את התוכן - כלומר E(X) מגדיר את X
- קל לוודא ש-X הוא "תוכן המעטפה".
- מהידיעת E(X) קשה למצוא את X.

דוגמאות

• מכרז פומבי: יש אנשים שרוצים לקנות מחשב ורק אחד ויש מחיר שהוא מוכן לתת. בעל המחשב לא רוצה שהם ידעו את ההצעות האחרות כי אז הם עלולים להציע פחות. אז נעשה משני שלבים:
  - התחייבות: כל אחד רושם במעטפה את הערך E(X) כאשר X הסכום שהוא מציע
  - גילוי: פותחים את המעטפות ואז כל אחד אומר מה ה-X שלו ואפשר לוודא שהוא לא שיקר

• הגרלה דיבורית: אליס ובוב מדברים בטלפון ויש הגרלה על מכונית והם מחליטים להטיל מטבע. אבל מכיוון שהם לא באותו מקום אי אפשר לדעת שמי שהטיל את המטבע לא משקר.
אז הפרוטוקול הבא עושה את העבודה.
אליס: אם E(X) אני מקבלת את המכונית
בוב: מטיל מטבע ... מה בחרת?
במקרה שאליס התחייבה על X היא לא יכולה לרמות...

• זיהוי סיסמאות: יש שמות משתמש ולכל משתמש
יש סיסמה. לא חכם לשמור במחשב את הסיסמאות
כי אפשר לפרוץ אליו. אז אם שומרים $E(x)$ במקום
את x לא נורא אפילו אם הקובץ פומבי. בעת
כניסה של משתמש המחשב בודק אם הקלט שלו
אחרי הפעלת E מתאים למה ששמור.
לכאורה השיטה הזאת טובה. אבל יש כאן בעיה
קשה של ציטוט ושימוש חוזר.
אז צריך להיות נחמד אם אפשר היה לשכנע את המחשב
שאני יודע את הסיסמה גם בלי לתת לו אותה.
כלומר מחפשים הוכחת אפס-ידיעה. - הוכחות
משכנעות אך לא מספקות מידע.

• זכויות יוצרים:

ד"ר אליס: הוכחתי את השערת רימן
פרופ' בוב: לא אפשרי. מה ההוכחה?
ד"ר אליס: משפט... למה... משפט... למה.
פרופ' בוב: מדהים! אמליץ על קביעות.
(חושב לעצמו: מדהים! אפרסם ראשון...)

איך אליס יכולה להגן על עצמה מפני בוב הרשע?

מה אנחנו רוצים מהוכחת אפס ידיעה?
- אם הטענה נכונה נרצה שבוב יקבל אותה אבל לא ילמד דבר
- אם הטענה לא נכונה בוב ידחה אותה בהסתברות גבוהה.

זה מה שאליס צריכה היתה לעשות במקום פשוט
לספר לבוב את כל ההוכחה שלה.

נשמע קצת מוזר כל העסק הזה, אבל למעשה יש משפט
שאומר שכל מה שניתן להוכיח, ניתן להוכיח באפס-מידע.

הוכחת אפס-ידיעה של צביעת מפות:

קלט: מפה מישורית M

פלט: האם M היא 3-צביעה?

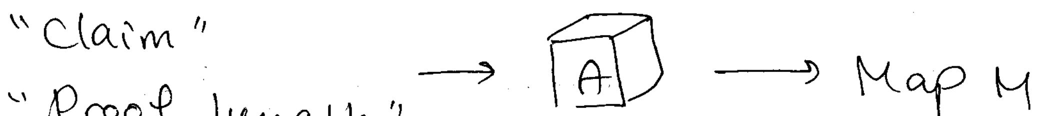
השאלה היא איך להוכיח שהיא 3-צביעה או לא מבלי לתת שום אינפורמציה על הצביעה עצמה.

(עשינו את ההוכחה שמפת אפריקה היא 3-צביעה)

הרעיון היא כזה: יש לנו 6 מיני צביעות אפשריות. בכל שלב מגרילים צביעה אחת ומקבלים אתגר: לפתוח שני איזורים שכנים ולבדוק אם הצביעה שלהן חוקית.
המידע שמתגלה כאן הוא כמובן חסר ערך כי כל פעם מקבלים זוג צבעים אקראיים ובשביל זה לא צריך לנו מפה בכלל.

למה זו הוכחה משכנעת? אם המפה 3-צביעה אז אף פעם לא נמצא עדות נגדית לכך. לכן הסיכוי שבוב יקבל את הטיעון של אליס הוא 1.
אבל אם המפה אינה 3-צביעה אז איפשהו יש טעות בצביעה ולכן יש סיכוי שהטעות תימצא. ע״י חזרות מרובות של המבחן הסיכוי הזה גדל.

למה הסתכלנו על הבעיה הזאת? מסתבר שכל טענה מתמטית אפשר לעשות רדוקציה לבעיה של המפה. קיים אלגוריתם ועוד A שפועל כך:



"Claim" true ⟷ M 3-colorable

Proof ⟶ 3-coloring of M

אז בכך שיש הוכחה קצרה אפשר להוכיח ביעילות גם באפס-ידיעה.

ולכן אפשר לשבור פרוטוקולים קריפטוגרפיים עמידים בפני ועקלט - כי תמיד אפשר לדרוש הורדה...

עד עכשיו ראינו איך אפשר להכריח שחקנים להתנהג כראוי. עכשיו נדבר על פרטיות מידע.

גם כשכל השחקנים אמינים לא תמיד אפשר לשמור על סודות. אליס ובוב רוצים לקיים שיחה לגמרי פרטית בלי להיפגש מראש ולתאם סודות.
כיום עושים את זה כל הזמן בהרבה מקומות - למשל, אנחנו קונים דברים באינטרנט ומוסרים את מספר כרטיס האשראי ובכל זאת לא קורה לנו כלום.
האמת היא שמה שדיברנו עליו עד כה לא מספיק. בשביל זה צריך קריפטוגרפיה אסימטרית: לכל משתתף יש פונקציה פרטית משלו. לאליס יש E_a ולבוב יש E_b. אז כולם יכולים לשלוח דברים אליהם אבל רק הם יכולים לפענח את המוצפן (לא נדבר על המימוש של זה). זה בדיוק מה שקורה כשאנחנו קונים באינטרנט. אנחנו שולחים את מספר כרטיס האשראי מוצפן בצורה שרק Amazon יכולים לפענח...

ספרים:
1) Hardy & Wright, Introduction to Number Theory
2) Ireland & Rosen
3) Koblitz (??), Number theory and Cryptography

מטרת הקורס: תורת המספרים והמחשה בעזרת שימושים מקריפטוגרפיה.

רצוי מאוד שמי שכאן יידע מבנים אלגבריים. זה קורס נחמד אבל השכלה משמעותית לא תהיה כאן.

(4)

יהיה מבחן!

יהיו בו הרבה תרגילי חשבון. ומשם תהיה הבחינה.

שבוע הבא- יכול להיות שאלות ואחר כך.

נתחיל ב- $17^{\underline{15}}$

תגיע הודעה לגבי המיקום.

(5) 18.05.08

תורת המספרים

אנחנו עוסקים בקבוצות $\mathbb{N}=\{1,2,3,\dots\}$

$\mathbb{Z}=\{0,\pm1,\pm2,\pm3,\dots\}$

תכונה מאוד חשובה של $\mathbb{Z}$ היא שהיא חוג אוקלידי - כלומר

$\forall a,b\in\mathbb{Z}\quad b\neq0 \Rightarrow \exists q,r\in\mathbb{Z}: a=qb+r$

כאשר $r=0$ (כלומר ש- $b|a$) או $|r|<|b|$.

<u>טענה</u>: כל אידיאל ב- $\mathbb{Z}$ הוא ראשי.

<u>הוכחה</u>: אם $I\lhd\mathbb{Z}$ אידיאל (כלומר לכל $a,b\in I$ $a+b\in I$ ולכל $r\in\mathbb{Z}$ ולכל $a\in I$ $ar,ra\in I$). צריך להראות שקיים $a\in\mathbb{Z}$ כך ש- $I=a\mathbb{Z}$.

אם $I=\{0\}$ ניקח $a=0$ וסיימנו.

אחרת, יהי $a\in I$ עם $|a|$ מינימלי ונראה שלכל $c\in I$, $a|c$. אכן: $c=aq+r$ כאשר $r=0$ או $|r|<|a|$. אבל $|a|$ מינימלי ולכן לא ייתכן להיות שהרי $r=c-aq\in I$. לכן נותרת רק האפשרות $r=0$ ואז $a|c$ וסיימנו.

☺

<u>הגדרה</u>: $p\in\mathbb{Z}$ נקרא ראשוני אם $p\neq\pm1$ ואם $p=ab$ כאשר $a,b\in\mathbb{Z}$ אז $a=\pm1$ או $b=\pm1$.

<u>המשפט המרכזי של האריתמטיקה</u>: כל $n\in\mathbb{Z}$ ניתן לכתיבה כ- $n=p_1p_2\cdots p_\ell$ כאשר $p_1,\dots,p_\ell$ ראשוניים וכתיבה זו במובן הבא: אם $n=q_1\cdots q_m$ מכפלה של ראשוניים אזי $m=\ell$ ולאחר שינוי סדר מתקיים ש- $p_i=\pm q_i$ לכל $i=1,\dots,\ell$.

<u>הוכחה</u>: הקיום פשוט - אינדוקציה על n (כ- n חיובי ונסיק גם כ- n שלילי)

לצורך היחידות נפתח את מושג הממ"מ (מחלק משותף מקסימלי) (gcd) - בהינתן $a,b\in\mathbb{Z}$ נאמר ש- d הוא ממ"מ

שהם גם: $d|a$, $d|b$ אם $d'|b$ ו- $d'|a$ אז $d'|d$.

למה: לכל $a,b\in\mathbb{Z}$ קיים ממ"מ והוא יחיד עד כדי סימן.

הוכחה: נסתכל באידיאל הנוצר ע"י a ו-b, כלומר הקבוצה $I=\{xa+yb \mid x,y\in\mathbb{Z}\}$ (קל לראות שזה אכן אידיאל). אבל ב-$\mathbb{Z}$ כל אידיאל הוא ראשי לכן קיים d רק ש- $I=d\mathbb{Z}$.

ברור ש- $d|a$ ו- $d|b$ כי $I=d\mathbb{Z}$. נראה שאם $c|a$ ו- $c|b$ אז $c|d$ אבל זה ברור כי $d=x_0a+y_0b$ ל- $x_0,y_0\in\mathbb{Z}$. $\Leftarrow$ אם $c|a$ ו- $c|b$ אז הוא מחלק גם כל צירוף לינארי שלהם ולכן את d.

נשים לב שקיבלנו: מראין שאם $d=\gcd(a,b)$ אז קיימים $x,y\in\mathbb{Z}$ רק ש- $ax+by=d$.

הוכחה ב: (האלגוריתם של אוקלידס) מציאת $d=\gcd(a,b)=(a,b)$

מתחילים עם שארית:

$$a=q_1b+r_1 \qquad |r_1|<|b|$$
$$b=q_2r_1+r_2 \qquad |r_2|<|r_1|$$
$$r_1=q_3r_2+r_3 \qquad |r_3|<|r_2|$$
$$\vdots$$
$$r_{m-2}=q_mr_{m-1}+r_m$$
$$r_{m-1}=q_{m+1}r_m+0$$

הטענה היא ש- $r_m=\gcd(a,b)$. (נשים לב שבגלל שהנורמה של השארית יורדת ממש התהליך נגמר בזמן סופי).

נראה $r_m|a$ ו- $r_m|b$. מהמשוואה האחרונה נקבל ש- $r_m|r_{m-1}$. לכן מחלק את r_{m-2} וכך הלאה הוא מחלק את b ואת r_1 ולבסוף את a.

באופן דומה, אם $c|a$ ו- $c|b$ קל לראות ש- $c|d$.

תרגיל: מצא הערכה "טובה" למספר הפעולות הנדרשות כדי לחשב את $\gcd(a,b)$. דוגמה: $a=35, b=20$

$$35=1\cdot 20+15 \qquad 35=2\cdot 20-5$$

אז רואים להשתמש במשולים כי לפעמים זה מקצר את התהליך.

תרגיל: הוכח יחידות של $\gcd$ עד כדי $\pm$.

למה: אם p ראשוני ו- $p|ab$ אזי או $p|a$ או $p|b$.

הוכחה: נסמן ב- $d=\gcd(a,b)$. אז $d|p$ ולכן או $d=\pm1$ ואז הם זרים או $d=\pm p$ ואז $p|a$ וסיימנו. לכן נניח שהם זרים. נסמן $1=x_0a+y_0b$.
$\Leftarrow$ $b=x_0ab+y_0pb$. לפי ההנחה $p|ab$ ולכן $p|x_0ab$ ו- $p|y_0pb$ $\Leftarrow$ $p|b$ וסיימנו.

עכשיו אנחנו יכולים לעבור להוכחת היחידות במשפט המרכזי. נניח

$$p_1p_2\dots p_l = q_1q_2\dots q_m$$

נוכיח באינדוקציה על l:
$p_1 | q_1\dots q_m$ ולכן (באינדוקציה על m) $p_1|q_i$ לאיזה $1\le i\le m$ ואחרי שינוי סדר אפשר לקבל $p_1|q_1$ $\Leftarrow$ $p_1=\pm q_1$. אפשר לצמצם ב- p_1 ונשנה את הסימן של q_1 אם יש צורך. עכשיו נותרנו עם מכפלה של $l-1$ ראשוניים ובאינדוקציה סיימנו. ☺

משפט אוקלידס: יש אינסוף מספרים ראשוניים.

הוכחה: נניח שלא. אזי נניח ש- $p_1,p_2,\dots,p_l$ הם כל הראשוניים. נתבונן ב- $N=p_1\dots p_l+1$. אם N ראשוני אזי הוא ראשוני מחוץ לרשימה. בכל מקרה N מתפרק למכפלה של ראשוניים, אבל אף אחד מהם לא ברשימה $p_1,\dots,p_l$ כי החלוקה ב- p_i משאירה שארית 1. בכל מקרה הגענו לסתירה. ☺

טענה: יש אינסוף ראשוניים מהצורה $4n+3$.

הוכחה: נניח שיש רק מספר סופי של ראשוניים מהצורה הזו, $p_1,\dots,p_l$. נתבונן ב- $N=4p_1p_2\dots p_l-1$. אזי $N\equiv 3 \pmod 4$ והוא מכפלת ראשוניים. לא ייתכן שכולם מהצורה $p\equiv 1 \pmod 4$ כי אז גם המכפלה הזו נותנת שארית 1 בחלוקה ב-4. לכן יש ראשוני $q|N$ כך ש- $q\equiv 3 \pmod 4$, אבל $q\neq p_1,\dots,p_l$ כי $N\equiv -1 \pmod{p_i}$ לכל $i=1,\dots,l$. ☺

הערה: אם $\gcd(a,b)=\pm1$ אומרים ש- a,b זרים.

משפט דיריכלה: אם $n,a\in\mathbb{Z}$ ו- $gcd(n,a)=1$ אז יש אינסוף ראשוניים רק ש- $p\equiv a \pmod n$

(אין למשפט הזה הוכחה אלמנטרית. ההוכחה משתמשת בפונקציות יוצרות.)

הערה: יש גם הוכחה אלמנטרית (אם כי לא כל כך קלה) שיש אינסוף מספרים ראשוניים $\equiv 1 \pmod 4$

תרגיל: (שאולי מתאים למבחן) יש אינסוף ראשוניים p רק ש- $p\equiv 5 \pmod 6$.

הוכחה טופולוגית למשפט אוקלידס (פירסטנברג - 1955)

נגדיר טופולוגיה על $\mathbb{Z}$: קבוצה $A\subseteq\mathbb{Z}$ תיקרא פתוחה אם לכל $a\in A$ קיים $0\neq d\in\mathbb{Z}$ רק ש- $a+d\mathbb{Z}\subseteq A$

קל לראות שזה אכן מגדיר טופולוגיה. כל סדרה חשבונית היא פתוחה. אבל היא גם סגורה כי אם $A=a+d\mathbb{Z}$ אז המשלים של A הוא איחוד (סופי!) של סדרות אריתמטיות.

בפרט, לכל ראשוני p, $p\mathbb{Z}$ היא פתוחה וסגורה. נתבונן ב-

$$X=\mathbb{Z}\setminus\bigcup_{p\ \text{ראשוני}} p\mathbb{Z}$$

כל $p\mathbb{Z}$ סגורה לכן אם יש מספר סופי של ראשוניים אז $\bigcup_{p\ \text{ראשוני}} p\mathbb{Z}$ סגורה לכן X פתוחה. אבל $X=\{\pm 1\}$ אינה פתוחה! ☺

עוד הוכחה: נניח שיש מספר סופי l של ראשוניים. נשים לב שכל מספר טבעי n ניתן להצגה כ- $n=a\cdot b^2$ כאשר a חופשי מריבועים (ז"א לכל p ראשוני $p^2\nmid a$).

נקבע N גדול מאוד; לכל $n\le N$ אפשר להציג $n=ab^2$ כאשר $b\le\sqrt{N}$. a מכפלה של ראשוניים שונים, לכן מספר האפשרויות ל-a הוא לכל היותר 2^l לכן $2^l\sqrt{N}\ge N$ אבל אם l קבוע זה לא יכול להיות! ☺

מסקנה: נסמן $\pi(x)$ = מספר הראשוניים (החיוביים) הקטנים מ-x, $x\in\mathbb{R}$.
אזי $\pi(x)\ge\frac{\log_2 x}{2}=\frac{\ln x}{2\ln 2}$.

<u>הוכחה</u>: אותו ארגומנט בדיוק כמו בהוכחה אומר ש-

$$2^{\pi(x)}\cdot\sqrt{x} \ge x$$

$$\Rightarrow \quad 2^{\pi(x)} \ge x^{\frac{1}{2}}$$

$$\Rightarrow \quad \pi(x)\ln 2 \ge \tfrac{1}{2}\ln x$$

$$\Rightarrow \quad \pi(x) \ge \ln x / 2\ln 2$$

☺

ההוכחה הזאת נותנת גם חסם כמותי אבל היא קשה יותר מהקודמות.

<u>טענה</u>: $\sum_{p \text{ ראשוני}} \frac{1}{p}$ מתבדר

<u>הוכחה</u>: אם הטור מתכנס אזי קיים ℓ כך ש-

$$\frac{1}{p_1}+\dots+\frac{1}{p_\ell}+\sum_{p>p_\ell}\frac{1}{p} = \sum_{p \text{ ראשוני}}\frac{1}{p}$$

ו- $\sum_{p>p_\ell}\frac{1}{p} < \frac{1}{2}$. ניקח $x\in\mathbb{N}$ גדול. מספר המספרים השלמים הקטנים מ-x ומתחלקים בראשוני p הוא לכל היותר $\frac{x}{p}$
לכן אם נסמן $N(x)$ = מספר המספרים השלמים החיוביים הקטנים מ-x ומתחלקים באחד או יותר מבין הראשוניים מ- p_ℓ
אז $N(x) \le \sum_{p>p_\ell}\frac{x}{p} = x\sum_{p>p_\ell} p \le \frac{1}{2}x$

$\Leftarrow$ $x - N(x) \ge \frac{x}{2}$, כלומר לפחות מחצית השלמים בין 1 ל-x מתחלקים רק ב- $p_1,\dots,p_\ell$ (ℓ קבוע!). ז"א לפחות מחצית $[1,\dots,x]$ מתפרקים לראשוניים שכולם מ- $p_1,\dots,p_\ell$. ארגומנט דומה לקודם מראה שמספרם של אלו הוא לכל היותר $2^\ell\cdot\sqrt{x}$ $\Leftarrow$ $2^\ell\sqrt{x} \ge \frac{x}{2}$
וזו סתירה כאשר x מספיק גדול.

☺

משפט המספרים הראשוניים:

נסמן $\pi(x) = \#\{p \le x : p \text{ ראשוני}\}$ $x \in \mathbb{R}$

אז $\pi(x) \sim \frac{x}{\ln x}$ כלומר $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$

זה משפט מאוד עמוק. אנחנו נראה משהו חלש יותר.

משפט 1: (צ'בישב) קיימים קבועים $0 < a, b$ כך שלכל $2 \le x \in \mathbb{R}$

$$a\frac{x}{\ln x} \le \pi(x) \le b\frac{x}{\ln x}$$

סיפור: אם נסמן $E(x) = |\pi(x) - \frac{x}{\ln x}|$, כלומר זו השגיאה של הקירוב $\frac{x}{\ln x}$ אז השערת רימן אומרת שקיים קבוע $c \in \mathbb{R}$ כך ש- $E(x) \le c \cdot x^{\frac{1}{2}} \cdot \ln x$

(בד"כ מנסחים את השערת רימן אחרת, בעזרת פונקציית ζ. האמנם $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. עבור s ממשי ברור במה מדובר. אבל יש לה הרחבה יחידה אנליטית (הולומורפית פרט למספר נקודות ובהן יש קוטב) השערת רימן אומרת שאם $z \in \mathbb{C}$ שורש של ζ !: אז $0 \le Re z \le 1$, $Re z = \frac{1}{2}$, כלומר כל האפסים נמצאים על הישר $x = \frac{1}{2}$).

תרגיל: הוכח שכטורים פורמליים (כלומר בלי לדאוג להתכנסות) $\zeta(s) = \prod_{p \text{ ראשוני}} (1 - \frac{1}{p^s})^{-1}$ $\left((1-q)^{-1} = \sum_{i=0}^{\infty} q^i\right)$ ושוויון הזה שקול למשפט היסודי של האריתמטיקה.

משפט 2: נסמן $\theta(x) = \sum_{\substack{p \le x \\ \text{ראשוני}}} \ln p$ $0 < x \in \mathbb{R}$

אז קיימים $0 < a', b'$ כך ש- $a'x \le \theta(x) \le b'x$

(ראו גם ש- $\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$).

למה 1: קיים קבוע b' כך ש- $\theta(x) \le b'x$

הוכחה: מתקיים

$$\binom{2n}{n} = \frac{(2n)!}{n!\,n!} = \frac{(n+1)}{1} \cdot \frac{(n+2)}{2} \cdot \ldots \cdot \frac{(n+n)}{n}$$

ברור ש- $\binom{2n}{n}$ מתחלק בכל ראשוני p כך ש- $n<p\le 2n$
(ה-p הזה בטוח מופיע במונה אבל לא במכנה ולכן לא מצטמצם
בחלוקה ולכן המספר כולו מתחלק בו).
מצד שני, נקבל ש-

$$2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n}\binom{2n}{i} > \binom{2n}{n} > \prod_{n<p\le 2n} p$$

נפעיל $\ln$ משני האגפים ונקבל

$$2n\ln 2 > \sum_{n<p\le 2n}\ln p = \theta(2n)-\theta(n)$$

כעת נתבונן בטור הבא

$$\theta(2^m) = \left(\theta(2^m)-\theta(2^{m-1})\right) + \left(\theta(2^{m-1})-\theta(2^{m-2})\right) + \dots + \left(\theta(4)-\theta(2)\right) + \left(\theta(2)-\theta(1)\right)$$
$$\le 2\ln 2\left(2^{m-1}+2^{m-2}+\dots+2^2+2+1\right) = 2\ln 2\cdot\frac{2^{m-1}}{2-1} \le 2\ln 2\cdot 2^m$$

זה מוכיח את המשפט לכל x מהצורה $x=2^m$ וזה נכון
מוכיח לכל המספרים, שהרי לכל x יש m מינימאלי שעבורו
$2^{m-1}\le x\le 2^m$ ולכן

$$\theta(x)\le\theta(2^m)\le 2\ln 2\cdot 2^m\le 2\cdot\ln 2\cdot 2x = b'x$$

$b'=4\ln 2$.

☺

<u>מסקנה</u> 2: קיים b כך ש- $\pi(x)\le b\frac{x}{\ln x}$

<u>הוכחה</u>:

$$b'x \ge \theta(x) \ge \sum_{\sqrt{x}<p\le x}\ln p \ge$$
$$\ge \sum_{\sqrt{x}<p\le x}\ln\sqrt{x} = \frac{1}{2}\ln x\sum_{\sqrt{x}<p\le x}1 =$$
$$= \frac{1}{2}\ln x\left(\pi(x)-\pi(\sqrt{x})\right)$$

סה"כ קיבלנו $\frac{1}{2}\ln x\left(\pi(x)-\pi(\sqrt{x})\right)\le b'x$

$$\Rightarrow \pi(x)\le 2b'\frac{x}{\ln x}+\pi(\sqrt{x})\le 2b'\cdot\frac{x}{\ln x}+\sqrt{x}\le$$

(מספיק $\sqrt{x}\le 2\frac{x}{\ln x}$ לכל $2\le x$)

$$\le (2b'+2)\frac{x}{\ln x} = b\frac{x}{\ln x}$$

$b=2(b'+1)$

☺

<u>מסקנה</u>: $\frac{\pi(x)}{x} \longrightarrow 0$

נסיים הוכחת החסמים התחתונים נזכיר:

עבור p ראשוני, m-ו שלם חיובי נסמן

$Ord_p(m) = t \in \{0,1,2,\dots\}$ אם $p^t | m$ אבל $p^{t+1} \nmid m$

<u>תרגיל 1</u>: $Ord_p(n!) = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \dots$

(הסכום לא מגיע לאינסוף!!!) כאשר $[x] = \max_{n\in\mathbb{N}}\{n \le t\}$

למעשה המחובר האחרון הוא $\frac{n}{p^{t_p}}$, $t_p = [\frac{\ln n}{\ln p}]$

<u>תרגיל 2</u>: ברור כי $\binom{2n}{n} \ge 2^n$

$$\binom{2n}{n} = \frac{(n+1)}{1}\frac{(n+2)}{2}\cdots\frac{(n+n)}{n}$$

<u>תרגיל 3</u>:

$$Ord_p\left(\binom{2n}{n}\right) = Ord_p\left(\frac{(2n)!}{n!n!}\right) =$$

$$= Ord_p((2n)!) - 2\cdot Ord_p(n!) =$$

$$= \sum_{j=1}^{s_p}\left(\left[\frac{2n}{p^j}\right] - 2\cdot\left[\frac{n}{p^j}\right]\right) \le \sum_{j=1}^{s_p} 1 = s_p = \left[\frac{\ln 2n}{\ln p}\right]$$

$s_p = \left[\frac{\ln 2n}{\ln p}\right]$

לכל $x \in \mathbb{R}$
$[2x] - 2[x] \in \{0,1\}$
(בדקו!)

<u>חישוב</u>:

$$(*) \quad 2^n \underset{\text{2 תרגיל}}{\le} \binom{2n}{n} = \prod_{\substack{p \le 2n \\ \text{ראשוני}}} p^{ord_p\left(\binom{2n}{n}\right)} \le \prod_{\substack{p \le 2n \\ \text{ראשוני}}} p^{\left[\frac{\ln 2n}{\ln p}\right]}$$

<u>מסקנה 4</u>: יש קבוע a כך ש- $\pi(x) \ge a\cdot\frac{x}{\ln x}$

<u>הוכחה</u>: נוציא $\ln$ משני אגפי $(*)$ ונקבל

$$n\ln 2 \le \sum_{p\le 2n}\left(\left[\frac{\ln 2n}{\ln p}\right]\cdot\ln p\right) \le \sum_{p \le 2n}\left(\frac{\ln 2n}{\ln p}\cdot\ln p\right) =$$

$$= \ln 2n \sum_{p\le 2n} 1 = (\ln 2n)\,\pi(2n)$$

$$\Rightarrow \pi(2n) \ge \ln 2\cdot\frac{n}{\ln 2n} = \frac{\ln 2}{2}\cdot\frac{2n}{\ln 2n}$$

ועכשיו הוכחנו את מה שצריך לכל x מהצורה $x = 2n$

ומכאן אפשר לעבור להוכחה לכל x.

טענה 2: קיים a' כך ש- $\theta(x) \geq a'x$

הוכחה: $\theta(x) = \sum_{p<x} \ln p \geq (\pi(x) - \pi(\sqrt{x})) \ln \sqrt{x} \geq$

(רצים רק על הראשוניים שגדולים מ- $\sqrt{x}$ - מספרם $\pi(x) - \pi(\sqrt{x})$ וחוסמים אותם מלמטה ע"י $\sqrt{x}$.)

$$\geq \left(a \cdot \frac{x}{\ln x} - b\frac{\sqrt{x}}{\frac{1}{2}\ln x}\right)\frac{1}{2}\ln x = \frac{1}{2}(ax - 2b\sqrt{x}) \geq$$

$$\geq a'x$$

עבור a' מתאים.

עד כאן הראנו שיש אינסוף מספרים ראשוניים ואפילו נתנו הערכה מספרית.

בע"ת הראשוניים התאומים.

הגדרה: שני מספרים ראשוניים p, q נקראים תאומים אם $|p - q| = 2$.

דוגמאות - $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$

תרגיל: אם $a^n - 1$ ראשוני אז $a = 2$ ו- n ראשוני.

בעיה פתוחה: האם יש ∞ ראשוניים - תאומים?

בעיה פתוחה: האם תמיד יש ראשוני בין n^2 ל- $(n+1)^2$?

בעיה פתוחה: האם יש אינסוף ראשוניים מהצורה n^2+1?

בעיה פתוחה (השערת גולדבך): כל מספר זוגי הוא סכום של שני ראשוניים

בעיה פתוחה: האם יש ∞ ראשוניים של פרמה (מהצורה 2^n+1)?

בעיה פתוחה: האם יש ∞ ראשוניים של מרסן (מהצורה $2^{2^n}-1$)?

⑩ 1/6/08
תורת המספרים

קונגרואנציות

<u>הגדרה</u>: יהי $n\in\mathbb{Z}$. נאמר ש- $a,b\in\mathbb{Z}$
מקיימים $a\equiv b\pmod n$ (ולפעמים אם $a\equiv b(n)$)
אם $n\mid b-a$ (נאמר: a שקול ל-b מודולו n)

<u>תרגיל</u>: זהו יחס שקילות.

ומעשה, נתבונן בחוג $\mathbb{Z}$ ובאידיאל $I=n\mathbb{Z}$.
נסמן ב- $\bar{k}$ את מחלקת השקילות של k תחת $\equiv(\bmod n)$.
אז $\mathbb{Z}/I\cong\{\bar{0},\bar{1},\bar{2},\dots,\overline{n-1}\}$
וישנו הומומורפיזם $\pi:\mathbb{Z}\to\mathbb{Z}/I\cong\mathbb{Z}/n\mathbb{Z}$ ו- $a,b\in\mathbb{Z}$
מקיימים $a\equiv b\pmod n$ אמ"מ $\pi(a)=\pi(b)$.

<u>הערה</u>: $a\equiv b\pmod n$ אמ"מ $a\equiv b(\bmod(-n))$ וכן $n\mathbb{Z}=(-n)\mathbb{Z}$

<u>טענה</u>: $\mathbb{Z}/n\mathbb{Z}$ שדה אמ"מ n ראשוני.
<u>הוכחה</u>: בה"כ $n>0$.
(⇐) נניח ש- n אינו ראשוני. אזי $n=ab$ כאשר
$1<a,b<n$ ואז $0=\pi(n)=\pi(a)\pi(b)$. לעומת
זאת, $\pi(a),\pi(b)\neq 0$ וזו סתירה לכך ש- $\mathbb{Z}/n\mathbb{Z}$ שדה
(בשדה אין מחלקי אפס).
(⇒) צריך להוכיח שלכל $\bar{a}\in\mathbb{Z}/n\mathbb{Z}$ כך ש- $\bar{a}\neq\bar{0}$
יש ל- $\bar{a}$ הופכי ב- $\mathbb{Z}/n\mathbb{Z}$ ביחס לכפל (ברור שזה
חוג). נראה שתי הוכחות:
הוכחה א: נסמן $f:(\mathbb{Z}/n\mathbb{Z}\setminus\{0\})\to(\mathbb{Z}/n\mathbb{Z}\setminus\{0\})$ המוגדרת
ע"י $f(\bar{x})=\bar{a}\bar{x}$. נשים לב ש- f אכן לוקחת
את $\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ לעצמו כי $\bar{a}\cdot\bar{x}\neq\bar{0}$ כי אם
a,x לא מתחלקים ב- n אז $n\nmid ax$ (כי n ראשוני).

נראה ש- f חח"ע - נניח ש- $\bar{a}\bar{x} = \bar{a}\bar{y}$.
$\Leftarrow$ $\bar{a}(\bar{x}-\bar{y}) = 0$. אבל $\bar{a} \neq 0$ ולכן
שוב מהראשוניות של n נובע ש- $\bar{x}-\bar{y}=0$, כלומר
$\bar{x}=\bar{y}$. מאחר שהקבוצה סופית, f הוא גם על
ולכן יש $\bar{x}$ רק ש- $\bar{a}\bar{x} = \bar{1}$. אז $\bar{x}$ הוא
ההופכי של $\bar{a}$.

הוכחה ב: צריך להראות שאם $a \in \mathbb{Z}$; $(a,n)=1$
אז קיים $x \in \mathbb{Z}$ רק ש- $ax \equiv 1 \pmod{n}$.
ראינו שאם a,n זרים (הם אכן זרים במקרה
זה!) אזי יש $x,y \in \mathbb{Z}$ רק ש- $ax+ny=1$
אבל זה בדיוק אומר ש- $\bar{a}\bar{x} = \bar{a}\bar{x} \equiv 1 \pmod{n}$
(נשים לב הוכחה קונסטרוקטיבית, כי בעזרת אלגוריתם
אוקלידס המורחב אפשר למצוא את x,y הדרושים).

(ii)

<u>דוגמה:</u> $(17 \pmod{53})^{-1} = ?$

$$53 = 3\cdot 17 + 2$$
$$17 = 8\cdot 2 + 1$$
$$2 = 2\cdot 1$$
$$\Rightarrow 1 = 17 - 8\cdot 2 =$$
$$= 17 - 8(53 - 3\cdot 17) =$$
$$= (1+8\cdot 3)17 + 8\cdot 53$$
$$\Rightarrow (17 \pmod{53})^{-1} = \overline{25} \equiv 25 \pmod{53}$$
(אפשר גם לבדוק את זה בקלות).

במבחן - יהיו גם שאלות חישוביות!!
(א להתאמן!)

<u>מסקנה</u>: נסמן ב- $(\mathbb{Z}/n\mathbb{Z})^*$ את קבוצת האיברים ב- $\mathbb{Z}/n\mathbb{Z}$ שיש להם הפכי בחוג. כלומר

$$(\mathbb{Z}/n\mathbb{Z})^* = \{t \in \mathbb{Z}/n\mathbb{Z} : \exists s \in \mathbb{Z}/n\mathbb{Z} : ts = 1\}$$

אזי $(\mathbb{Z}/n\mathbb{Z})^*$ חבורה ביחס לכפל.

<u>הוכחה</u>: צריך רק לבדוק סגירות לכפל וזה ברור כי באופן כללי $(t_1 t_2)^{-1} = t_2^{-1} t_1^{-1}$ ואם קיימים t_1^{-1}, t_2^{-1} אז קיים גם $(t_1 t_2)^{-1}$. ☺

<u>הגדרה</u>: עבור $n \in \mathbb{N}$ נסמן פונקציית φ של אוילר

$$\varphi(n) = \#\{1 \le a < n : (a,n) = 1\}$$

<u>טענה</u>: $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$

<u>הוכחה</u>: איברי החוג $\mathbb{Z}/n\mathbb{Z}$ הם $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$ ו- $\bar{i}$ ב- $\mathbb{Z}/n\mathbb{Z}$ הפיך אמ"מ $(i,n)=1$:
אם $(i,n)=1$ ראינו שלה גורר ש- $\bar{i}$ הפיך. מצד שני, אם $\bar{i}$ הפיך אז יש x כך ש- $\overline{ix} = \bar{i}\cdot\bar{x} = \bar{1}$ ⇐ $ix \equiv 1 \pmod{n}$ ⇐ יש y כך ש- $ix + ny = 1$ וזה אומר ש- $(i,n)=1$. ☺

<u>משפט לגרנז'</u>: אם G חבורה סופית אז $g \in G$:
(תרגיל נחמד)

$$g^{|G|} = e_G$$

← איבר היחידה של G.

<u>מסקנה</u>: אם $(a,n)=1$ אז $a^{\varphi(n)} \equiv 1 \pmod{n}$

<u>הוכחה</u>: $(a,n)=1$ פירושו $a \in (\mathbb{Z}/n\mathbb{Z})^*$ והרי $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. ☺

<u>דוגמה</u>: $n=12$ מהם המספרים זרים ל- n?

1, ~~2~~, ~~3~~, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11

$\Rightarrow \varphi(12) = 4 \Rightarrow 7^{29} \pmod{12} = ?$

$7^{29} = 7^{4\cdot 7+1} = (7^4)^7 \cdot 7 \equiv 1^7 \cdot 7 \pmod 7 \equiv$

$\equiv 7 \pmod 7$

אז המשפט הזה מאוד מקל על חישובים של שאריות.

<u>טענה</u>: לכל n
$$\sum_{d|n} \varphi(d) = n$$

<u>הוכחה תמצה</u>: נתבונן במספרים

$$\frac{1}{n} \quad \frac{2}{n} \quad \frac{3}{n} \quad \frac{4}{n} \quad \cdots \quad \frac{n}{n}$$

יש פה n שברים. ניקח את n השברים האלה ונצמצם אותם. אז יש בדיוק $\varphi(n)$ כאלה שאי אפשר לצמצם. את אלה שאפשר לצמצם, מקבלים שהם יופיעו מחלקי n. כמה פעמים יופיע מחלק נתון d? הוא יופיע $\varphi(d)$ פעמים. אם d במכנה אז המונה המתאים הוא מספר קטן מ-d וזר לו. לכן d יופיע לכל היותר $\varphi(d)$ פעמים. מצד שני, אם $j<d$ וזר לו אז $\frac{j\cdot n/d}{n} = \frac{j}{d}\cdot\frac{n/d}{n/d}$ מופיע ברשימה. לכן יש בדיוק $\varphi(d)$ מופעים של d. לכן בסה"כ נקבל ש- $\sum_{d|n}\varphi(d) = n$. ☺

<u>תכונות של פונקציית אוילר</u>:

① $\varphi(p) = p-1$ לכל p ראשוני (ברור!)

② $\varphi(p^r) = p^{r-1}(p-1)$

<u>הוכחה</u>: מבין המספרים $1,\dots,p^r$ הזרים ל-p^r הם בדיוק הזרים ל-p. הזרים ל-p, מספרם $p^r - $ (מספר המתחלקים ב-p) וזה $p^{r-1}(p-1) = p^r - p^{r-1} = p^r - \left(\frac{p^r}{p}\right)$ ☺

[$(a,p^r)=1$ אמ"מ $(a,p)=1$ לכן
$(\mathbb{Z}/p^r\mathbb{Z})^* = \{1 \le a \le p^r : p \nmid a\}$]

③ $\varphi(n) = n \cdot \prod_{p|n}\left(1-\frac{1}{p}\right)$

<u>משפט השאריות הסיני</u>: אם $(m,n)=1$ ו- $a,b\in\mathbb{Z}$

אזי יש פתרון למערכת

$$x \equiv a \pmod m$$
$$y \equiv a \pmod n$$

והפתרון הזה יחיד מודולו $m\cdot n$.

<u>הערה</u>: <u>טענת עזר</u>: אם $(m,n)=1$ אזי

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

<u>הוכחה</u>: יש הומומורפיזמים

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}/m\mathbb{Z}$$

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\pi_2} \mathbb{Z}/n\mathbb{Z}$$

$\Leftarrow$ $(\pi_1,\pi_2): \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

הומומורפיזם של חוגים.

$$a \mapsto (a \bmod m,\ a \bmod n)$$

ההומומורפיזם הזה הוא חח"ע כי אם $a \mapsto (0,0)$

אז $n|a$ וגם $m|a$ אבל $(m,n)=1$

$\Leftarrow$ $mn|a$, כלומר $a \equiv 0 \pmod{mn}$.

זה הומומורפיזם שגרעינו טריוויאלי. לכן הוא חח"ע ומאחר שהחוגים סופיים ומאותו סדר הוא גם על, כלומר קיבלנו איזומורפיזם וזה מה שרצינו.

נוכיח עכשיו את משפט השאריות ה- כי

קיים $x\in\mathbb{Z}/mn\mathbb{Z}$ שתמונתו $(a \bmod m,\ b \bmod n)$

ו- x זה מקיים

$$x \equiv a \pmod m$$
$$x \equiv b \pmod n$$

הפתרון יחיד כי אם יש $y\in\mathbb{Z}$ שגם הוא פתרון אז

$y \equiv x \pmod{mn}$.

מסקנה: (מאינדוקציה) אם $n_1,\dots,n_k$ מספרים זרים בזוגות אז למשוואות

$$x\equiv a_1 \pmod{n_1}$$
$$\vdots$$
$$x\equiv a_k \pmod{n_k}$$

יש פתרון והוא יחיד מודולו $n_1\cdots n_k$

מסקנה: אם $n=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$ פירוק לראשוניים אז

$$\mathbb{Z}/n\mathbb{Z}\cong\prod_{i=1}^{l}\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

(וזו בעצם הטענה שהחבורה החיבורית $\mathbb{Z}/n\mathbb{Z}$ איזומורפית למכפלה הישרה של חבורות p-סילו שלה).

מסקנה: אם $n=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$

$$(\mathbb{Z}/n\mathbb{Z})^*=(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^*\times\dots\times(\mathbb{Z}/p_l^{\alpha_l}\mathbb{Z})^*$$

$$\Rightarrow\quad \varphi(n)=\prod_{i=1}^{l}\varphi(p_i^{\alpha_i})=\prod_{i=1}^{l}(p_i-1)p_i^{\alpha_i-1}$$

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

דוגמה:

$$\varphi(12)=12\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{3}\right)=12\cdot\tfrac{1}{2}\cdot\tfrac{2}{3}=4$$

$$\varphi(100)=100\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{5}\right)=100\cdot\tfrac{1}{2}\cdot\tfrac{4}{5}=40$$

קל מאוד לחשב את $\varphi(n)$ (אם יודעים את הפירוק לראשוניים).

הגדרה: פונקציה $f:\mathbb{N}\to\mathbb{N}$ נקראת פונקציה של תורת המספרים אם מקיימת $f(mn)=f(m)f(n)$ לכל $m,n\in\mathbb{N}$ רק כש- $(m,n)=1$.

דוגמא: פונקציית φ של אוילר היא פונקציה של תורת המספרים. (נובע באופן ישיר מהנוסחה של $\varphi(n)$).

הגדרה: עבור $n\in\mathbb{N}$ נסמן $\sigma(n)=\sum_{d|n}d$

דוגמה: $\sigma(1)=1$ $\sigma(2)=3$ $\sigma(4)=7$ $\sigma(p)=1+p$
$\sigma(6)=12$ $\sigma(28)=56$

הגדרה: מספר $n \in \mathbb{N}$ נקרא מושלם (perfect) אם $\sigma(n) = 2n$

למשל, 6 ו- 28 מספרים מושלמים. המספר המושלם הבא הוא גדול הרבה יותר! משהו מעניין

$$6 = 2 \cdot 3 = 2^1(2^2-1)$$

$$28 = 2^3 \cdot 7 = 2^2(2^3-1)$$

היינו רוצים לנחש שגם $2^3(2^4-1)=120$ מושלם. אבל הוא לא! ואולי $2^4(2^5-1)=496$ הוא כן מושלם. מהם המחלקים של $2^4(2^5-1)$?

$$1,\ 2,\ 4,\ 8,\ 16,\ 31\cdot 1,\ 31\cdot 2,\ 31\cdot 4,\ 31\cdot 8,\ 31\cdot 16$$

וסכומם $31+31\cdot 31 = 32\cdot 31 = 2\cdot 16\cdot 31 = 2\cdot 496$

טענה: אם 2^n-1 ראשוני אזי $k=2^n(2^{n-1}-1)$ מושלם.

הוכחה: אם זה ראשוני אז המחלקים של k הם

$$1, 2, \ldots, 2^{n-1},\ (2^n-1)\cdot 1,\ (2^n-1)\cdot 2,\ \ldots,\ (2^n-1)2^{n-1}$$

וסכומם

$$\sum_{i=0}^{n-1} 2^i + (2^n-1)\sum_{i=0}^{n-1} 2^i = 2^n \cdot \sum_{i=0}^{n-1} 2^i =$$

$$= 2^n \cdot 2(2^{n-1}-1) = 2k$$

למה: אם 2^n-1 ראשוני אזי n ראשוני. (תרגיל)

אוילר הוכיח שכל מספר מושלם זוגי הוא מהצורה $2^{p-1}(2^p-1)$ כאשר p ראשוני ו- 2^p-1 ראשוני.

בעיות פתוחות:

1. האם יש בכלל איזשהו מספר מושלם אי-זוגי?
2. האם יש אינסוף מספרים מושלמים זוגיים? (זה שקול לשאלה אם יש אינסוף ראשוניים מרסן)

הגדרה: מספר מושלם כפלי הוא מספר n שמכפלת כל מחלקיו היא n^2.

איהם המספרים המושלמים כפלית?

אם n לא ראשוני ולא $n=p^2$ אז יש ל-n מחלק d רק ש- $d \neq \frac{n}{d}$. אז המחלקים הם

$$1, d, \frac{n}{d}, n, \ldots$$

אם מכפלת אלה שרשמנו היא n^2. אז גם המספר מושלם כפלי אז אלו כל מחלקיו. אז ל-n יש בדיוק ארבעה מחלקים וזה קורה בדיוק כאשר $n = pq$ עבור p, q ראשוניים, או כאשר $n = p^3$ עבור p ראשוני.

(14) 15.6.08

תורת המספרים

יהי $0 \neq n \in \mathbb{Z}$. נתבונן בהעתקה הטבעית

$$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

$$\pi(a) = \pi(b) \Leftrightarrow a \equiv b \pmod{n}$$

טענה: $b, a, n \in \mathbb{Z}$. אז למשוואה $ax \equiv b \pmod{n}$ יש פתרון אמ"מ $d := (a,n) \mid b$

במקרה שיש פתרונות אזי מספר הפתרונות (מודולו n) הוא d. ואם x_0 פתרון אז קבוצת הפתרונות הם

$$x_0, \quad x_0 + n', \quad x_0 + 2n', \quad \dots, \quad x_0 + (d-1)n'$$

כאשר $n' = \frac{n}{d}$.

הוכחה: נניח ש- $d = (a,n) \mid b$. כזכור, d הוא היוצר של האידיאל $\mathbb{Z}a + \mathbb{Z}n$. אם $d \mid b$ אז b נמצא באידיאל זה. $\Leftarrow$ קיימים $x_0, y_0 \in \mathbb{Z}$ כך ש- $ax_0 + y_0 n = b$

זה אומר ש- $ax_0 \equiv b \pmod{n}$, כלומר יש פתרון למשוואה.

להפך, נניח שיש x_0 כך ש- $ax_0 \equiv b \pmod{n}$ $\Leftarrow$ קיים $y_0 \in \mathbb{Z}$ כך ש- $ax_0 = b + ny_0$ ולכן $b = ax_0 - ny_0 \in a\mathbb{Z} + n\mathbb{Z}$ ולכן $d = (a,n) \mid b$ כי d יוצר את האידיאל.

כעת, נשים לב שאם x_0 אזי $x_0 + in'$ פתרון עבור $0 \le i \le d-1$ שהרי:

$$a(x_0 + in') = ax_0 + ian' = ax_0 + ia\frac{n}{d} =$$

$$= ax_0 + i \cdot \frac{a}{d} \cdot n \equiv ax_0 \pmod{n}$$

$$\equiv b \pmod{n}$$

$\frac{a}{d} \in \mathbb{Z}$ כי d מחלק את a

קל לראות ש- d פתרונות אלו שונים זה מזה מודולו n.

נראה עכשיו שכל פתרון הוא מהרשימה הנ"ל (מודולו n)

נניח ש- y פתרון. אז $ay \equiv b \pmod{n}$. אבל גם $ax_0 \equiv b \pmod{n}$

ונחסר ונקבל $a(y - x_0) \equiv 0 \pmod{n}$ $\Leftarrow$ $a(y - x_0) = zn$

ל- $z \in \mathbb{Z}$ כלשהו. נחלק ב- d ונקבל

$$\frac{a}{d}(y-x_0) = z\cdot\frac{n}{d} = zn'$$
$\in \mathbb{Z}$

$\Leftarrow \quad y \equiv x_0 \pmod{n'}$

$\Leftarrow$ וזה בדיוק אומר ש-y (מודולו n) הוא אחד מהרשימה שלנו. ☺

$(\mathbb{Z}/n\mathbb{Z})^*$ מבנה

תזכורת:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a\in \mathbb{Z}/n\mathbb{Z} : \exists b\in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } ab=1\}$$

זאת חבורה כפלית שהסדר שלה $\varphi(n)$ פונקציית אוילר.

דוגמה:

$n=p$ ראשוני. אז $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ שדה מסדר p.

מה המבנה של $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$?

- הסדר שלה הוא $p-1$
- היא ציקלית, כלומר $((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +)$

(זה לא התחלנו להבין הפעולות - זה לא ש-$\mathbb{Z}/(p-1)\mathbb{Z}$ מתנהגת תחבורה חיבורית משכנת ב-$\mathbb{Z}/p\mathbb{Z}$.)

למשל, 2 יוצר את $(\mathbb{Z}/11\mathbb{Z})^*$:

$$\langle 2\rangle = \{2,4,8,5,10,9,7,3,6,1\}$$

ויש איזומורפיזם $(\mathbb{Z}/10\mathbb{Z},+) \longrightarrow ((\mathbb{Z}/11\mathbb{Z})^*, \cdot)$

$$i \longmapsto 2^i$$

3 דווקא לא יוצר כי $\langle 3\rangle = \{3,9,5,4,1\}$

הגדרה: $a\in\mathbb{Z}$ יקרא פרימיטיבי מודולו p-ראשוני אם a יוצר את $(\mathbb{Z}/p\mathbb{Z})^*$.

אז 2 פרימיטיבי מודולו 11 אבל 3 לא!

דוגמה: $n=8$. אז $(\mathbb{Z}/n\mathbb{Z})^* = \{1,3,5,7\}$

$3^2=1 \quad 5^2=1 \quad 7^2=1$

$\Leftarrow$ $(\mathbb{Z}/8\mathbb{Z})^* \cong C_2\times C_2$ כאשר C_m חבורה ציקלית מסדר m.

תזכורת: אם A חבורה אבלית סופית אז $A \cong C_{m_1}\times\dots\times C_{m_r}$ כאשר $m_1|m_2|\dots|m_r$.

הגדרה: תהא G חבורה סופית. נסמן

$$\exp(G) = \min\{m : \forall x\in G \ x^m=1\}$$

ממשפט לגרנז' ($x^{|G|}=e$) נובע ש- $\exp(G)\le|G|$.

תרגיל: הוכח ש- $\exp(G) \mid |G|$

טענה: אם A חבורה אבלית, אזי A ציקלית אמ"מ $\exp(A)=|A|$

הוכחה: אם A ציקלית אזי $\exp(A)=|A|$ כי יש איבר מסדר $|A|$ ($\Leftarrow \exp(A)\ge|A|$). אם A חבורה אבלית כלשהי אזי נטען $A \cong C_{m_1}\times\dots\times C_{m_r}$ -

$2\le m_1|\dots|m_r$ אז $|A|=m_1\cdot\dots\cdot m_r$ -

$\exp(A)=m_r$ (זו הכפולה המשותפת המינימלית של כולם).

לכן, אם $m_r=\exp(A)=|A|=m_1\cdot\dots\cdot m_r$ $\Leftarrow$ $r=1$ $\Leftarrow$ A חבורה ציקלית מסדר m_r. ☺

תזכורת מתורת השדות: F שדה. אזי

1) אם $f(x)\in F[X]$ אזי $\alpha\in F$ שורש של $f(x)$ אמ"מ $x-\alpha \mid f(x)$

2) אם $\deg f(x)=n$ אזי ל- $f(x)$ יש לכל היותר n שורשים ב- F.

3) אם $f(x),g(x)\in F[X]$ פולינומים ממעלה n רק ש- $f(\alpha_i)=g(\alpha_i)$ עבור איברים שונים $\alpha_1,\dots,\alpha_n,\alpha_{n+1}$ אז $f(x)=g(x)$.

(ונובע מכאן שאם f,g מתוקנים ממעלה n ומזדהים על $\alpha_1,\dots,\alpha_n$ אז $f(x)=g(x)$ - כי ההפרש ממעלה $n-1$).

שימוש נחמד: $X^{p-1}-1 \in \mathbb{F}_p[X]$. שורשיו הם $1,2,3,\dots,p-1$

(ממשפט לגרנז') אז כפולינומים ב- $\mathbb{F}_p[X]$

$$X^{p-1}-1=(X-1)(X-2)(X-3)\dots(X-(p-1))$$

כי שניהם מתוקנים ושניהם ממעלה $p-1$ עם אותם $p-1$ שורשים.

משפט: לכל p ראשוני $(p-1)! \equiv -1 \pmod p$

הוכחה: עבור $p=2$ זה ברור. ל- $p>2$ נציב 0 בפולינומים ונקבל $-1\equiv(-1)(-2)\dots(-(p-1)) \pmod p$

$$\Rightarrow -1 \equiv \underbrace{(-1)^{p-1}}_{=1}(p-1)! \pmod p$$

$$\Rightarrow -1\equiv (p-1)! \pmod p$$

☺

תרגיל: אם n לא ראשוני ולא מהצורה $n=p^2$ עבור p ראשוני אז $(n-1)!\equiv 0 \pmod n$

טענה: $\exp(\mathbb{F}_p^*)=p-1$ ואז ציקלית לפי טענה קודמת.

הוכחה: אחרת, $\exp(\mathbb{F}_p^*)=m \lneq p-1$ ואז יש $p-1$ איברים שונים המקיימים $X^m=1$. לכן לפולינום X^m-1 יש $p-1$ ($> m$) שורשים וזו סתירה.

☺

תרגיל: אם F שדה כלשהו ו- A תת חבורה סופית של F^*, אזי A ציקלית.

משפט: אם $p>2$ ראשוני אז לכל $r\in\mathbb{N}$ $(\mathbb{Z}/p^r\mathbb{Z})^*$ ציקלית.

הוכחה: $|(\mathbb{Z}/p^r\mathbb{Z})^*|=\varphi(p^r)=(p-1)p^{r-1}$. יהי a פרימיטיבי מודולו p (יש כזה לפי הטענה הקודמת). נתבונן ב- a^{p-1}. ידוע ש- $a^{p-1}\equiv 1 \pmod p$.

למה: יש $a\in\mathbb{Z}$ פרימיטיבי מודולו p. אבל $a^{p-1}\not\equiv 1 \pmod{p^2}$

הוכחה: יהי $a\in\mathbb{Z}$ פרימיטיבי מודולו p. אם הוא מקיים את הדרוש סיימנו. אחרת, נתבונן ב- $a+p$. צריך

$a+p$ פרימיטיבי מודולו p. מצד שני,

$$(a+p)^{p-1} = a^{p-1} + \binom{p-1}{1}a^{p-2}p + p^2\cdot y \quad , y\in\mathbb{Z}$$

$$\Rightarrow \quad (a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}\cdot p \pmod{p^2}$$

נראה ש- $a^{p-1}+(p-1)a^{p-2}p \not\equiv 1$ וזה נובע משום ש- $a^{p-1}\equiv 1 \pmod{p^2}$ אבל $(p-1)a^{p-2}p \equiv 0 \pmod{p^2}$.

מסקנה: $(\mathbb{Z}/p^2\mathbb{Z})^*$ ציקלית. כי ניקח a כמו בלמה רק ש- $a^{p-1}\not\equiv 1 \pmod{p^2}$.

נסתכל בה העתקה $\pi: (\mathbb{Z}/p^2\mathbb{Z})^* \xrightarrow[\text{מסדר } p-1]{\text{על}} (\mathbb{Z}/p\mathbb{Z})^*$ (מסדר $(p-1)p$)

זה על כי איבר שזר ל- p בוודאי זר ל- p^2.

יש לנו $a\in\mathbb{Z}/p^2\mathbb{Z}$ שהוא פרימיטיבי מודולו p, כ"א תמונת a ב- $(\mathbb{Z}/p\mathbb{Z})^*$ יוצרת את $(\mathbb{Z}/p\mathbb{Z})^*$.

אבל $a^{p-1}\in\ker\pi$ ולא הוא איבר היחידה שם כי בחרנו את a רק ש- $a^{p-1}\not\equiv 1 \pmod{p^2}$. אבל הגרעין מסדר p אז a^{p-1} יוצר אותו. לכן $o(a)=p(p-1)$

$\Leftarrow$ מצאנו איבר שהוא מסדר החבורה אז היא ציקלית.

למה: יהא $b\in\mathbb{Z}$ רק ש- $b\equiv 1 \pmod p$ ו- $b\not\equiv 1 \pmod{p^2}$. אזי הסדר של b מודולו p^l הוא בדיוק p^{l-1}.

שימוש: נייש את הלמה עבור $b=a^{p-1}$ שמצאנו קודם ונסיק שהסדר שלו הוא $(p-1)p^{l-1}$ וזה משלים את הוכחת המשפט.

הוכחת הלמה: $b=1+xp$ ו- $p\nmid x$. אז

$$(1+xp)^{p^{l-1}} = 1+\binom{p^{l-1}}{1}\cdot 1\cdot x\cdot p+\dots \equiv 1 \pmod{p^l}$$

אז מספיק להוכיח ש- $(1+xp)^{p^{l-2}}\not\equiv 1 \pmod{p^l}$.

ואכן $1+\binom{p^{l-2}}{1}xp+p^l\{\} = 1+p^{l-2}xp \pmod{p^l} \not\equiv 1 \pmod{p^l}$.

חוק ההדדיות הריבועית של גאוס

p ראשוני שאינו 2.

מסמנים $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ שדה השאריות מודולו p. זה שדה.

$\mathbb{F}_p^*$ חבורה ציקלית כפלית מסדר $p-1$. למשל

$$\mathbb{F}_{11}^* = \langle 2 \rangle = \{1,2,4,8,5,10,9,7,3,6\}$$

ראשית, לא תמיד קל לנחש מי היוצר. ומה לגבי הריבועים?

נשאל מתי המשוואה $a \equiv x^2 \pmod p$ פתירה?

למשל ב- $\mathbb{F}_{11}^*$ הריבועים הם $1,3,4,5,9$ (לא רואים לעין שום חוקיות...)

<u>הגדרה</u>: a ייקרא <u>שארית ריבועית</u> מודולו הראשוני p אם למשוואה $a \equiv x^2 \pmod p$ יש פתרון.

היות ש- $\mathbb{F}_p^*$ ציקלית מסדר זוגי, מחצית איבריה ($\frac{p-1}{2}$) הינם שאריות ריבועיות ומחציתם אינם שאריות ריבועיות.

<u>הסמל של לז'נדר</u>:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \equiv x^2 \pmod p \\ -1 & a \not\equiv x^2 \pmod p \end{cases}$$

מאחר שהסמל תלוי רק בשארית של a אפשר להרחיב אותו לכל השלמים וגם יש לו מחזור p.

<u>חוק ההדדיות הריבועית של גאוס</u>:

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

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

אם p,q ראשוניים אי-זוגיים אז

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

למה: תהי H חבורה ציקלית מסדר זוגי m. אזי בדיוק מחצית מאיבריה הם ריבועיים.

כמובן, $a=x^2$ אזי $a^{\frac{m}{2}}=1$ שום תנאי לה לא מתקיים אם $a^{\frac{m}{2}}$ הינו האיבר היחיד מסדר 2 בחבורה.

הוכחה: H ציקלית ולכן $H=\{1,g,g^2,\dots,g^{m-1}\}$ כאשר g יוצר של H ו- $g^m=1$. ברור שהריבועים הם בדיוק $1,g^2,g^4,\dots,g^{m-2}$ (חצי מהאיברים).

אם $a=x^2$ אזי כמובן $a^{\frac{m}{2}}=x^m=1$.

אם $a\neq x^2$ אזי $a=g^k$ עבור k אי-זוגי ואז $a^{\frac{m}{2}}=g^{\frac{km}{2}}\neq 1$ כי $m\nmid\frac{km}{2}$. אבל $a^m=1$ ולכן $a^{\frac{m}{2}}$ הינו איבר שריבועו 1 והוא עצמו אינו 1, ולכן הוא האיבר היחידי מסדר 2 בחבורה (בחבורה ציקלית יש איבר יחיד מסדר 2). ☺

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

הוכחה: אם a שארית ריבועית אז מהלמה $a^{\frac{p-1}{2}}\equiv 1\pmod p$ וזו ההגדרה של $\left(\frac{a}{p}\right)$.

אם a אינו שארית ריבועית אזי $a^{\frac{p-1}{2}}\neq 1$ אבל הוא האיבר היחידי של $\mathbb{F}_p^*$ מסדר 2 והאיבר הזה הוא -1 וזו ההגדרה של $\left(\frac{a}{p}\right)$.

וכמובן גם אם $a|p$ יש שוויון. $(0=0)$. ☺

מסקנה מן המסקנה:

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

2) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1 & p\equiv 1\pmod 4\\ -1 & p\equiv 3\pmod 4\end{cases}$

דוגמה: $\left(\frac{365}{101}\right)=\left(\frac{62}{101}\right)$ (מכיוון שזה תלוי רק בשארית).

עכשיו אפשר מהר עם מחשב להעלות 100 מספרים בריבוע ולבדוק אם 62 ריבוע או לא. אבל אפשר לעשות יותר טוב:

$$\left(\frac{62}{101}\right)=\left(\frac{2}{101}\right)\left(\frac{31}{101}\right)=-1\cdot\left(\frac{101}{31}\right)(-1)^{\frac{100}{2}\cdot\frac{30}{2}}=-1\cdot\left(\frac{101}{31}\right)=$$

(יז)

$= -1\cdot\left(\frac{8}{31}\right) = -1\cdot\left(\frac{2}{31}\right)^3 = -1\cdot 1 = -1$

$\Leftarrow$ 365 איננו שארית ריבועית מודולו 101.

טוב למה: תהי H חבורה סופית ויהי $\chi: H \to \mathbb{C}^*$ קרקטר כפלי (הומומורפיזם $\chi(h_1h_2) = \chi(h_1)\chi(h_2)$ לתוך $\mathbb{C}^*$). אם $\chi \neq 1$ אז $S = \sum_{h\in H}\chi(h) = 0$

הוכחה: נסמן ב-S את הסכום. $\chi \neq 1 \Leftarrow$ ישנו $g \in H$ שעבורו $\chi(g)\neq 1$. אז

$$\chi(g)S = \sum_{h\in H}\chi(g)\chi(h) = \sum_{h\in H}\chi(gh) = S$$

כי כפל ב-g זו פרמוטציה.

אבל $\chi(g)\neq 1$ לכן $S=0$. ☺

שתי דוגמאות מתוך $\mathbb{F}_p$:

א) אם נסמן $\zeta = e^{\frac{2\pi i}{p}}$ אז $\sum_{a=0}^{p-1}\zeta^a = 0$

כי $a \mapsto \zeta^a$ הינו קרקטר של $(\mathbb{F}_p,+)$:

$$a+b \mapsto \zeta^{a+b} = \zeta^a\zeta^b$$

ב) $(\mathbb{F}_p^*,\cdot)$ $0\neq a \mapsto \left(\frac{a}{b}\right) = \pm 1$. אז $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$

נתבונן בחוג $\mathbb{Z}[\zeta]$ כאשר $\zeta = e^{\frac{2\pi i}{q}}$ (q ראשוני)

אז $0 = \zeta^q - 1 = (\zeta-1)(\zeta^{q-1}+\dots+\zeta+1)$. ומכיוון שאין מחלקי אפס נובע ש- $\zeta^{q-1}+\zeta^{q-2}+\dots+\zeta+1 = 0$ לכן

$$\zeta^{q-1} = -1-\zeta-\zeta^2-\dots-\zeta^{q-2}$$

לכן למעשה $\mathbb{Z}[\zeta] = \mathbb{Z}+\mathbb{Z}\zeta+\dots+\mathbb{Z}\zeta^{q-2}$ (כי למעשה לפחות הכל בחזקות ζ לכל היותר $q-2$. זה חוג קומוטטיבי. למעשה, אפשר להראות שהסכום ישר: $1,\zeta,\dots,\zeta^{q-2}$ הם מוכללים מעל $\mathbb{Z}$.

$1,\zeta,\zeta^2,\dots,\zeta^{q-2}$ בלתי תלויים מעל $\mathbb{Q}$ כאשר הפולינום $f(x) = x^{q-1}+\dots+x+1$ הוא הפולינום המינימלי של ζ מעל $\mathbb{Q}$, וזה מוכיחים בקורס בתורת השדות.

תוך שימוש בקריטריון אי הפריקות של אייזנשטיין.

<u>מסקנה</u>: $\mathbb{Z}[\zeta] \cap \mathbb{Q} = \mathbb{Z}$

<u>סכום גאוס</u>: $G = \sum_{a=1}^{q-1} \left(\frac{a}{q}\right)\zeta^a \qquad \zeta = e^{2\pi i/q}$

לפעמים לוקחים ביטוי מהצורה $\sum_{a\in\mathbb{F}_q^*} \chi(a)\psi(a)$ כאשר

$\psi(a+b)=\psi(a)\psi(b)$ ו- $\chi(ab)=\chi(a)\chi(b)$ קוראים סכום גאוס.

אז $G\in\mathbb{Z}[\zeta]$. ומתקיים

$$G^2 = \sum_{a=1}^{q-1}\sum_{b=1}^{q-1}\left(\frac{a}{q}\right)\left(\frac{b}{q}\right)\zeta^{a+b} =$$

(כפל ב-a פרמוטציה)

$$= \sum_{a=1}^{q-1}\sum_{b=1}^{q-1}\left(\frac{a}{q}\right)\left(\frac{ab}{q}\right)\zeta^{a+ab} = \sum_{b=1}^{q-1}\left(\frac{b}{q}\right)\sum_{a=1}^{q-1}\zeta^{(1+b)a} =$$

$$\left(\frac{a}{q}\right)\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)^2\left(\frac{b}{q}\right) = \left(\frac{b}{q}\right)$$

$$= \sum_{b=1}^{q-1}\left(\frac{b}{q}\right)\cdot\begin{cases} q-1 & b=q-1 \\ -1 & b\neq q-1\end{cases} = \left(\frac{-1}{q}\right)q - \sum_{b=1}^{q-1}\left(\frac{b}{q}\right)$$

(הסכום האחרון $=0$, מהלמה)

$\eta = \zeta^{1+b}$ שורש יחידה $\neq 1$ מסדר q
לפי הלמה $\sum_{a=0}^{q-1}\eta^a = 0$.

מסק': $G^2 = (-1)^{\frac{q-1}{2}}\cdot q$

<u>הערה</u>: (למי שמבין בשדות) $\mathbb{Q}\left(\sqrt{(-1)^{\frac{q-1}{2}}q}\right) \subseteq \mathbb{Q}(\zeta)$

בחוג $\mathbb{Z}[\zeta]$ הקונגרואנציה $x\equiv y \pmod p$ פירושה, $x-y\in p\mathbb{Z}[\zeta]$. אם $x,y\in\mathbb{Z}$ אז $\frac{x-y}{p}\in\mathbb{Z}[\zeta]\cap\mathbb{Q}=\mathbb{Z}$ ולכן $x-y\in p\mathbb{Z}$ ולכן $x\equiv y\pmod p$ מתלכד עם המשמעות הישנה.

(19)

ידוע ש- $(x+y)^p \equiv x^p + y^p \pmod p$. לכן
נפעיל את זה על G ונקבל

$$G^p \equiv \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta^{ap} \pmod p$$

תהי $\bar p$ שארית מודולו q כך ש- $p\bar p = 1 \bmod q$. לכן

$$G^p \equiv \sum_{a=1}^{q-1} \left(\frac{a\bar p}{q}\right) \zeta^{a} = \left(\frac{\bar p}{q}\right) G =$$

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

$$\Rightarrow G^p \equiv \left(\frac{p}{q}\right) G \pmod p$$

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

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

$$\Rightarrow (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{q}{p}\right) G \equiv \left(\frac{p}{q}\right) G$$

נכפיל ב- G (כאשר $G\bar G = q$) ונקבל

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

$$\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p \Leftarrow (q,p)=1$$

שני הצדדים הם ± 1 ולכן הם גם שווים.

נותר לחשב את $\left(\frac{2}{p}\right)$. (נשתמש בחוג $\mathbb{Z}[i]$):

$$(1+i)\left[(1+i)^2\right]^{\frac{p-1}{2}} = (1+i)^p \equiv 1 + i^p \bmod p$$

$$(1+i)(2i)^{\frac{p-1}{2}} \equiv (1+i)\, i^{\frac{p-1}{2}} \left(\frac{2}{p}\right)$$

$$\Rightarrow \left(\frac{2}{p}\right) \equiv \frac{1+i^p}{(1+i)\, i^{\frac{p-1}{2}}} = \begin{cases} 1 & p = 1,7 \pmod 8 \\ -1 & p = 3,5 \pmod 8 \end{cases}$$

בזאת הוכחנו את חוק ההדדיות.

סקיצה של הוכחה נוספת ש- $\mathbb{Z}[\zeta]\cap\mathbb{Q}=\mathbb{Z}$:

נתבונן ב- $\mathbb{Z}+\mathbb{Z}\zeta+\dots+\mathbb{Z}\zeta^{q-2}=\mathbb{Z}[\zeta]\subseteq\mathbb{Q}[\zeta]=\mathbb{Q}+\mathbb{Q}\zeta+\dots+\mathbb{Q}\zeta^{q-2}$
$\mathbb{Q}+\dots+\mathbb{Q}\zeta^{q-2}$ מרחב וקטורי ממימד סופי מעל $\mathbb{Q}$ (אפילו אם
זה לא סכום ישר). נניח ש- $\alpha_1,\dots,\alpha_d$ בסיס. בה"כ
$\alpha_1=1$. יהי N טבעי המשמש מכנה משותף לכל
המכנים המופיעים בפיתוחים של $1,\zeta,\dots,\zeta^{q-2}$
כצירופים לינאריים של $\alpha_1,\dots,\alpha_d$. ברור ש-

$$\mathbb{Z}[\zeta]\subseteq\frac{1}{N}\left(\mathbb{Z}\underbrace{\alpha_1}_{=1}\oplus\mathbb{Z}\alpha_2\oplus\dots\oplus\mathbb{Z}\alpha_d\right)$$

בפרט, $\mathbb{Z}[\zeta]\cap\mathbb{Q}\subseteq\frac{1}{N}\mathbb{Z}$ ולכן $\mathbb{Z}[\zeta]\cap\mathbb{Q}$
סגור לכפל ותת החוג היחיד של $\frac{1}{N}\mathbb{Z}$ הוא $\mathbb{Z}$.

(20) 29.06.08

תורת המספרים

משפט: תהא $G=(\mathbb{Z}/p^n\mathbb{Z})^*$ כאשר p ראשוני.

① אם p אי-זוגי אזי G חבורה ציקלית מסדר $p^{n-1}(p-1)$

② אם $p=2$ אזי $(\mathbb{Z}/2^n\mathbb{Z})^* \cong C_2\times C_{2^{n-1}}$ (כמעט ציקלית!)

עובדות מתורת החבורות:

בחבורה ציקלית כפלית מסדר n מתקיים

① אם n אי-זוגי אזי כל איבר הוא ריבוע

② אם n זוגי אזי בדיוק מחצית מאיברי החבורה הם ריבועים

* כדי לקבוע אם איבר הוא ריבוע ב- $(\mathbb{Z}/p^n\mathbb{Z})^*$ מספיק להסתכל ב- $(\mathbb{Z}/p\mathbb{Z})^*$ כי יש הומומורפיזם על $\mathbb{Z}_{p^n}^* \longrightarrow \mathbb{Z}_p^*$. אם איבר ריבוע ב- $\mathbb{Z}_{p^n}^*$ אז תמונתו כמובן ריבוע ב- $\mathbb{Z}_p^*$.

טענה: נניח $m=2^e p_1^{e_1}\cdots p_l^{e_l}$ כאשר p_i ראשוניים אי-זוגיים שונים. ויהי $a\in\mathbb{Z}$ כך ש- $(a,m)=1$. אזי למשוואה $x^2\equiv a \pmod m$ יש פתרון אמ"מ מתקיים:

(א) לכל $i=1,\dots,l$ a ריבוע מודולו p_i

(ב) אם $e=2$ אז $a\equiv 1 \pmod 4$

אם $e\geq 3$ אז $a\equiv 1 \pmod 8$

תזכורת: p ראשוני! $(a,p)=1$. אזי a ריבוע מודולו p אמ"מ $a^{\frac{p-1}{2}}=1$.

סימון: יהי p ראשוני. אז

$$\left(\frac{a}{p}\right)=\begin{cases}0 & p\mid a\\ +1 & a \text{ ריבוע מודולו } p\\ -1 & a \text{ לא ריבוע מודולו } p\end{cases}$$

למת גאוס: p ראשוני אי-זוגי. נסתכל ברשימת המספרים

$$Y=\left\{-\frac{p-1}{2},\ -\frac{p-1}{2}+1,\ \dots,\ -2,\ -1,\ 1,\ 2,\ \dots,\ \frac{p-1}{2}\right\}$$

אז נציג כל מחלקות הקונגרואנציה מודולו p הזרות ל- p.

יהי $a\in\mathbb{Z}$ כך ש- $(a,p)=1$.

נתבונן בשאריות של החלוקה ב- p בתוך Y של הקבוצה הבאה:

$$X=\{1\cdot a, 2\cdot a, \dots, \tfrac{p-1}{2}a\}$$

נסמן ב- μ את מספר השאריות השליליות בקבוצה זו.

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

<u>הוכחה</u>: נסמן ב- $m_1,m_2,\dots,m_{\frac{p-1}{2}}$ את שאריות החלוקה של X מתוך הקבוצה Y (כלומר, בוחרים את השארית עם הערך המוחלט הקטן ביותר).

דוגמא: $p=11$, $a=3$

$$X=\{3,6,9,12,15\}$$

אז השאריות הן $\{3,-5,-2,1,4\}$ לכן $\left(\frac{3}{11}\right)=(-1)^2=1 \Rightarrow$ 3 הוא ריבוע מודולו 11.

אכן $5^2=25\equiv 3 \pmod{11}$.

המשפט יראה רק קיום אבל לא יגיד איך למצוא אותו.

ראשית נציין שאם $i\neq j$ אז $m_i\neq m_j$ כי $(a,p)=1$

אז הכפלה ב- a זו תמורה של המחלקות מודולו p.

יתר על כן גם לא אפשרי ש- $|m_i|=|m_j|$ עבור $i\neq j$

כי אם $m_i=-m_j$ כלומר $ia\equiv -ja \pmod p$

אז $(i+j)a\equiv 0 \pmod p$. $(a,p)=1 \Rightarrow i+j\equiv 0 \pmod p$

וזה לא ייתכן כי $1\le i,j\le \frac{p-1}{2}$ ולכן $2\le i+j\le p-1$

נסמן $n_i=|m_i|$. אז $n_1,\dots,n_{\frac{p-1}{2}}$ כולם שונים ובין 1 ל- $\frac{p-1}{2}$ לכן זו בדיוק הקבוצה $1,2,\dots,\frac{p-1}{2}$

אך בסדר אחר. כעת מההגדרה של μ נקבל

$$m_1\cdot m_2\cdot\ldots\cdot m_{\frac{p-1}{2}}=(-1)^{\mu}n_1\cdot n_2\cdot\ldots\cdot n_{\frac{p-1}{2}}=(-1)^{\mu}\cdot 1\cdot 2\cdot\ldots\cdot\frac{p-1}{2}$$

נתבונן בשוויון הזה מודולו p: $m_i\equiv ia \pmod p$ לכן

$$a^{\frac{p-1}{2}}\prod_{i=1}^{\frac{p-1}{2}} i=\prod_{i=1}^{\frac{p-1}{2}}(ia)\equiv_p \prod m_i\equiv_p (-1)^{\mu}\left(\frac{p-1}{2}\right)!$$

אז $a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv(-1)^{\mu}\left(\frac{p-1}{2}\right)!$ ומכיוון ש- $\frac{p-1}{2}$ זר ל- p אפשר לצמצם ונקבל

(21) $a^{\frac{p-1}{2}} = (-1)^{\mu}$ אבל ראינו ש- $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ וסיימנו.
☺

טענה: 2 הוא שארית ריבועית מודולו p ראשוני (אי-זוגי)
אמ"מ $p \equiv \pm 1 \pmod 8$

הוכחה: μ בסימונים הקודמים הם למעשה מספר האיברים
$\{2\cdot 1, 2\cdot 2, \dots, 2\cdot j, \dots, 2\cdot \frac{p-1}{2}\}$ שגדולים מ- $\frac{p}{2}$
יהא m השלם המקיים $2m \le \frac{p-1}{2}$; $2(m+1) > \frac{p}{2}-1$ ואז ברור
ש- $\mu = \frac{p-1}{2} - m$. אם $p = 8k+1$ אז
$\frac{p-1}{2} = 4k$ ואז $m = 2k$ ולכן $\mu = 4k-2k = 2k$
זוגי. אם $p = 8k-1$ אז $\frac{p-1}{2} = 4k-1$!
לכן $m = 2k-1$ $\mu = (4k-1)-(2k-1) = 2k$ זוגי ולכן
2 שארית ריבועית לפי הלמה של גאוס.
אם $p = 8k+3$ אז $\frac{p-1}{2} = \frac{8k+2}{2} = 4k+1$ $\Leftarrow$
$m = 2k$ $\Leftarrow$ $\mu = 4k+1-2k = 2k+1$ אי-זוגי ולכן 2
אינו שארית ריבועית.
לבסוף, אם $p \equiv 8k+5$ אז $\frac{p-1}{2} = \frac{8k+4}{2} = 4k+2$ $\Leftarrow$
$m = 2k+1$ $\Leftarrow$ $\mu = 4k+2-(2k+1) = 2k+1$ אי-זוגי וסיימנו. ☺

משפט ההדדיות הריבועית: אם p,q ראשוניים אי-זוגיים אז
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

למה: p ראשוני אי-זוגי ; a שלם אי-זוגי כך ש- $p \nmid a$. נסמן
$\nu = \sum_{m=1}^{\frac{p-1}{2}} \left\lfloor \frac{ma}{p} \right\rfloor$. אזי $\left(\frac{a}{p}\right) = (-1)^{\nu}$

הוכחה: צריך להראות ש- $\nu \equiv \mu \pmod 2$ (μ מהסימונים הקודמים)
מתקיים $ma = \left\lfloor \frac{ma}{p} \right\rfloor p + r$ כאשר $1 \le r \le p-1$ השארית
של חלוקת ma ב- p.
$$\sum_{m=1}^{\frac{p-1}{2}} ma = \sum_{m=1}^{\frac{p-1}{2}} \left\lfloor \frac{ma}{p} \right\rfloor p + \underbrace{\sum_{j=1}^{\mu} b_j}_{\text{שאריות מהחלק הימני}} + \underbrace{\sum_{j=1}^{t} l_j}_{\text{שאריות מהחלק השמאלי}} \qquad t+\mu = \frac{p-1}{2}$$

המספרים $l_1, l_2, \ldots, l_t, p-b_1, p-b_2, \ldots, p-b_\mu$ נמצאים בין 1

ל- $\frac{p-1}{2}$ וכמו בהוכחה הקודמת מהווים סידור אחר של הקבוצה

$\{1, 2, \ldots, \frac{p-1}{2}\}$. אז

$$a\cdot\frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2} = \sum_{m=1}^{\frac{p-1}{2}} ma = p\nu + \left(1+2+\ldots+\frac{p-1}{2}\right) - \mu p + 2\sum_{j=1}^{\mu} b_j$$

$$= p(\nu-\mu) + \frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2} + 2\sum_{j=1}^{\mu} b_j$$

$$\Rightarrow \underbrace{(a-1)}_{\text{זוגי}}\cdot\underbrace{\frac{p-1}{4}\left(\frac{p-1}{2}+1\right)}_{\text{שלם}} = p(\nu-\mu) + \underbrace{2\sum_{j=1}^{\mu} b_j}_{\text{זוגי}}$$

$\Leftarrow$ $p(\nu-\mu)\equiv 0 \pmod 2$ ומאחר ש- $p\neq 2$

$\nu \equiv \mu \pmod 2$.

(☺)

לשאול שבוע הבא מה השם האתיופי של הנכדה של אלכס

<u>הוכחת המשפט</u>: מספיק להוכיח ש-

$$\sum_{m=1}^{\frac{p-1}{2}}\left\lfloor\frac{mq}{p}\right\rfloor + \sum_{m=1}^{\frac{q-1}{2}}\left\lfloor\frac{mp}{q}\right\rfloor = \frac{(p-1)(q-1)}{4}$$

נסתכל במלבן $Z=\{1\le x\le \frac{p-1}{2},\ 1\le y\le \frac{q-1}{2}\}$

מספר הנקודות שבו הוא $\frac{p-1}{2}\cdot\frac{q-1}{2}$

תהא A הקבוצה החלקית של Z של הזוגות (x,y)

עם $yp<xq$ ו- B הקבוצה החלקית שעבורה

$yp>xq$. [לא ייתכן ש- $yp=xq$]. רעיון

$Z=A\cup B$. אז נספור את איברי Z ע"י ספירת

איברי A ו- B. בהינתן (x,y), אם x קבוע, די

ש- (x,y) יהיה ב-A צריך $yp<xq$ כלומר

$y<\frac{xq}{p}$ כלומר $1\le y\le\left\lfloor\frac{xq}{p}\right\rfloor$. לכן $|A|=\sum_{x=1}^{\frac{p-1}{2}}\left\lfloor\frac{xq}{p}\right\rfloor$

ובדיוק באותו אופן $|B|=\sum_{y=1}^{\frac{q-1}{2}}\left\lfloor\frac{yp}{q}\right\rfloor$ וסיימנו!

(☺)

(22) 6/7/8

תורת המספרים

דוגמה 8 659 ראשוני (תאמינו לי).

$$\left(\frac{561}{659}\right) = \left(\frac{3}{659}\right)\left(\frac{11}{659}\right)\left(\frac{17}{659}\right) =$$

$$= \left(\frac{659}{3}\right)(-1)^{\frac{659-1}{2}\cdot\frac{3-1}{2}}\left(\frac{659}{11}\right)(-1)^{\frac{659-1}{2}\cdot\frac{11-1}{2}}\left(\frac{659}{17}\right)(-1)^{\frac{659-1}{2}\cdot\frac{17-1}{2}} =$$

$$= \left(\frac{2}{3}\right)(-1)\left(\frac{-1}{11}\right)(-1)\left(\frac{13}{17}\right) = (-1)(-1)(-1)(-1)\left(\frac{17}{13}\right)(-1)^{\frac{17-1}{2}\cdot\frac{13-1}{2}} =$$

$$= (-1)(-1)(-1)(-1)\left(\frac{3}{4}\right)(+1) = +1$$

כלומר 561 שארית ריבועית מודולו 659.

הערה: אם יודעים לפרק מספר לגורמים אז חוק ההדדיות הריבועית נותן לנו אלגוריתם לבדיקה אם מספר הוא שארית ריבועית או לא.

תזכורת: -1 שארית ריבועית מודולו p ראשוני (אי-זוגי) אמ"מ $p \equiv 1 \pmod 4$.

טענה: p ראשוני אי-זוגי. אז $\left(\frac{3}{p}\right) = 1$ אמ"מ $p \equiv \pm 1 \pmod{12}$.

הוכחה: לפי משפט ההדדיות:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

מתי $\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = 1$? זה קורה אמ"מ

(א) $\frac{p-1}{2} =$ זוגי וגם $\left(\frac{p}{3}\right) = 1$

או

(ב) $\frac{p-1}{2} =$ אי-זוגי וגם $\left(\frac{p}{3}\right) = -1$

במקרה (א) $p \equiv 1 \pmod 3$ וגם $p \equiv 1 \pmod 4$
וזה שקול לכך ש- $p \equiv 1 \pmod{12}$ (משפט השאריות הסיני)

במקרה (ב) $p \equiv 2 \pmod 3$ וגם $p \equiv 3 \pmod 4$ וזה
שקול לכך ש- $p \equiv -1 \pmod{12}$

טענה: $\left(\frac{5}{p}\right)=1$ אמ"מ $p\equiv 1,3,7,9 \pmod{20}$

טענה: יהי $0\neq a\in\mathbb{Z}$. אזי a שארית ריבועית ל-∞ ראשוניים.

הגדרה: סמל יעקובי (Jacobi) בהינתן a,b רק ש-b שלם חיובי אי-זוגי ו-a שלם כלשהו נכתוב $b=p_1\cdots p_l$ מכפלת ראשוניים (לאו דווקא שונים) ונגדיר

$$\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_l}\right)$$

תכונות סמל יעקובי:

1. אם $a_1\equiv a_2 \pmod b$ אז $\left(\frac{a_1}{b}\right)=\left(\frac{a_2}{b}\right)$

2. $\left(\frac{a_1a_2}{b}\right)=\left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$

3. $\left(\frac{a}{b_1b_2}\right)=\left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$

הערה + אזהרה: אם $\left(\frac{a}{b}\right)=-1$ אזי a איננו שארית ריבועית מודולו b (כי אין פתרון למשוואה $x^2\equiv a \pmod b$). **אבל** ייתכן ש-$\left(\frac{a}{b}\right)=+1$ ובכל זאת a לא שארית ריבועית מודולו b. למשל $\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)(-1)=+1$ אבל 2 אינו שארית ריבועית מודולו 15.

משפט: אם a,b שלמים חיוביים אי-זוגיים אזי

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

רמז להוכחה: לפרק את $\left(\frac{a}{b}\right)$ ואת $\left(\frac{b}{a}\right)$ ולהשתמש במשפט ההדדיות הריבועית ובכך ש-$\frac{rs-1}{2}\equiv\frac{r-1}{2}+\frac{s-1}{2} \pmod 2$ עבור r,s אי-זוגיים.

דוגמה: קודם חישבנו את $\left(\frac{561}{659}\right)$ ע"י פירוק 561 לגורמים. אבל באופן כללי פירוק לגורמים זו בעיה קשה מאוד. סמל יעקובי מאפשר לנו להתחיל לחשב בלי לפרק לגורמים.

(23) $\left(\frac{561}{659}\right) = \left(\frac{659}{561}\right)(-1)^{\frac{561-1}{2}\cdot\frac{659-1}{2}} =$

$$= \left(\frac{98}{561}\right)(-1)^{m} = \left(\frac{2\cdot 49}{561}\right)(-1)^{m} = \left(\frac{2}{561}\right)\left(\frac{49}{561}\right)(-1)^{m}$$

את $\left(\frac{2}{p}\right)$ אנחנו יודעים לחשב ואת $\left(\frac{49}{561}\right)$ נמשיך לחשב באותו אופן...

טענה: יהא $0\neq a\in\mathbb{Z}$. אזי a שארית ריבועית ל-∞ ראשוניים.

הוכחה: צריך למצוא אינסוף ראשוניים q כך ש- $\left(\frac{a}{q}\right)=1$.

נכתוב $a=2^{e}p_1^{e_1}p_2^{e_2}\cdots p_\ell^{e_\ell}$. אז

$$\left(\frac{a}{q}\right)=\left(\frac{2}{q}\right)^{e}\left(\frac{p_1}{q}\right)^{e_1}\cdots\left(\frac{p_\ell}{q}\right)^{e_\ell}$$

לכן אפשר להניח ש-a הוא מהצורה $a=2^{e}l_1\cdots l_s$ כאשר $l_1,\dots,l_s$ ראשוניים ! - $e\in\{0,1\}$.

צריך אינסוף q-ים כך ש- $\left(\frac{2}{q}\right)^{e}\left(\frac{l_1}{q}\right)\cdots\left(\frac{l_s}{q}\right)^{e}=1$

נניח ש- $q\equiv 1 \pmod 8$. אז

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

$\frac{q-1}{2}$ זוגי כי $q\equiv 1 \pmod 8$

לכן נדרוש גם ש- $q\equiv 1 \pmod{l_i}$ לכל $i=1,\dots,s$

ובסה"כ $q\equiv 1 \pmod{8l_1\cdots l_s}$.

לפי משפט דיריכלה יש ∞ q-ים שמקיימים זאת. ☺

תרגיל: אם 2^N+1 ראשוני אזי קיים $n\in\mathbb{N}$ כך ש- $N=2^n$.

מספרים מהצורה $F_n=2^{2^n}+1$ נקראים מספרי פרמה.

הראשונים הם $(3, 5, 17, 257, 65537, \dots)$

בעיה פתוחה? האם בסדרה F_n יש אינסוף ראשוניים?

משפט: קריטריון הראשוניות של Pepin.

$F_n=2^{2^n}+1$. אז F_n ראשוני אמ"מ $3^{\frac{F_n-1}{2}}\equiv -1 \pmod{F_n}$

הוכחה: עבור $n\geq 1$ נניח ש- $q=F_n$ ראשוני. נזכור שלכל $(a,q)=1$ מתקיים $a^{\frac{q-1}{2}} = \left(\frac{a}{q}\right)$

לכן

$$3^{\frac{F_n-1}{2}} = \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)(-1)^{\frac{F_n-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$F_n = 2^{2^n}+1 \equiv 2 \pmod 3$$

להפך, נניח ש- $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$

יהי p מחלק ראשוני של F_n. אז $3^{\frac{F_n-1}{2}} \equiv -1 \pmod p$

נעלה בריבוע ונקבל $3^{F_n-1} \equiv 1 \pmod p$.

אבל $F_n-1 = 2^{2^n}$. $3^{2^{2^n}} \equiv 1 \pmod p$.

אם m הסדר של 3 בחבורה $(\mathbb{Z}/p\mathbb{Z})^*$ אזי $m \mid 2^{2^n}$

לכן $m=2^r$ לאיזשהו $1\le r\le 2^n$.

נסמן $s = 2^n - r$. אם $s>0$ אז

$$3^{\frac{F_n-1}{2}} = 3^{\frac{2^{2^n}}{2}} = 3^{2^{2^n-1}} = 3^{2^{r+s-1}} = 3^{2^r\cdot 2^{s-1}} = \left(3^{2^r}\right)^{2^{s-1}} \equiv 1^{2^{s-1}} \pmod p \equiv 1 \pmod p$$

$\Leftarrow s=0 \Leftarrow r=2^n$.

כלומר הסדר של 3 מודולו p הוא 2^{2^n}. זה חייב להיות $\le p-1$. כלומר $2^{2^n}\le p-1$. $\Leftarrow p \ge 2^{2^n}+1 = F_n$

אבל $p \mid F_n$ $\Leftarrow$ $p=F_n$ ראשוני! ☺

יהי n כלשהו. מתי n ראשוני? ברור שיש אלגוריתם לבדיקה. נחלק בכל המספרים עד $\sqrt{n}$ ונבדוק אם יוצא מספר שלם. זה אפשרי תיאורטית אבל לא מעשי בפרקטיקה.

תנאי הכרחי לראשוניות: אם n ראשוני אז לכל $(a,n)=1$
$a^{n-1}\equiv 1 \pmod n$ [המשפט הקטן של פרמה]

אבל יש מספרים לא ראשוניים שבכל זאת מקיימים זאת.

למשל $n=561=3\cdot 11\cdot 17$. מספיק להוכיח שלכל $p=3,11,17$
$a^{560}\equiv 1 \pmod p$ (לפי משפט השאריות הסיני). כאן $n=p_1p_2p_3$
ו- $p_i-1 \mid n-1$. לכן $a^{n-1} = a^{(p_i-1)r_i} \pmod{p_i} = 1^{r_i} \pmod{p_i} = 1\ (p_i)$

לכן המבחן הזה לא מספיק טוב. מספרים כאלה נקראים מספרי Carmichael.

<u>טענה</u>: אם p ראשוני אז לכל $1 \le a \le p-1$ מתקיים
$$a^{p-1} \equiv 1 \pmod p$$
(זה המשפט הקטן של פרמה).

<u>הערה</u>: נניח n כלשהו. נתבונן ב- $\{a \in \mathbb{Z}_n^* : a^{n-1} \equiv 1 \pmod n\}$
ברור שזו ת"ח של $\mathbb{Z}_n^*$ (תרגיל!) ומכאן או שכולם מקיימים זאת
או שמחצית מתוך איברי $\mathbb{Z}_n^*$ אינם מקיימים זאת (כי אינדקס
של תת חבורה ממש הוא לפחות 2).

<u>הגדרה</u>: מספר טבעי <u>אי-זוגי</u> נקרא מספר קרמייקל (Carmichael)
אם לכל $a \in \mathbb{Z}_n^*$ מתקיים $a^{n-1} \equiv 1 \pmod n$

<u>טענה</u>: $n \in \mathbb{N}$ אי-זוגי הוא מספר קרמייקל אמ"מ הוא מכפלה של
ראשוניים שונים ולכל $p|n$ מתקיים $p-1 \mid n-1$

<u>הערה</u>: מספר קרמייקל הקטן ביותר הוא $561 = 3 \cdot 11 \cdot 17$ שהרי
$2|560$ $10|560$ $16|560$

<u>טענת עזר</u>: אם n מספר קרמייקל אז לכל p ראשוני $p^2 \nmid n$.
(כלומר n הוא חופשי מריבועים square-free)

<u>הוכחת טענת העזר</u>: נניח $p^2 | n$ עבור p ראשוני אי-זוגי. אזי
יש מספר g כלשהו שיוצר את החבורה $(\mathbb{Z}/p^2\mathbb{Z})^*$, כלומר יש ל- g
סדר $|\mathbb{Z}_{p^2}^*| = p(p-1)$.
n מספר קרמייקל. לכן $g^{n-1} \equiv 1 \pmod n$ בפרט $g^{n-1} \equiv 1 \pmod{p^2}$
ולכן $o(g) = p(p-1) \mid n-1$ [$o(g)$ הסדר של g] כלומר $p|n$
$p \mid n-1 \Rightarrow p|1$ וזו סתירה. !
☺

<u>הוכחת הטענה</u>: נניח n מספר קרמייקל. לפי טענת העזר $n = p_1 \cdots p_t$
מכפלה של ראשוניים שונים. צריך להראות שלכל $i = 1, \dots, t$ $p_i - 1 \mid n-1$
ואכן, יהי $g \in \mathbb{N}$ איבר פרימיטיבי מודולו p_i, ר"ל איבר שיוצר את $\mathbb{Z}_p^*$

אז $g^{p-1}\equiv 1 \pmod p$ ו- $ord_{\mathbb{Z}_p^*}(g) = p-1$. מתקיים

ש- $g^{n-1}\equiv 1 \pmod n$ ולכן $p-1 | n-1$ כנדרש.

להפך, נניח ש- n מכפלה של ראשוניים שונים וגם לכל $p|n$ מתקיים $p-1 | n-1$. צריך להראות ש- n קרמייקל. יהי $1\le a<n$ כך ש- $(a,n)=1$. צריך להראות ש- $a^{n-1}\equiv 1 \pmod n$. נסמן $n=p_1\cdots p_t$. אנחנו יודעים שלכל $i=1,\dots,t$ מתקיים $a^{n-1}\equiv a^{(p_i-1)s_i}\equiv 1^{s_i}\equiv 1 \pmod{p_i}$ כאשר $n-1=(p_i-1)s_i$.

$b=a^{n-1}$ הוא פתרון למערכת המשוואות

$$x\equiv 1 \pmod{p_1}$$
$$\vdots$$
$$x\equiv 1 \pmod{p_t}$$

לכן $b\equiv 1 \pmod{p_1\cdots p_t}$ כלומר $b\equiv 1 \pmod n$. ☺

אלגוריתם שגוי למציאת מספר ראשוני:

- בחר n אי-זוגי גדול מאוד.
- בחר מקרית $1\le a<n$ ותחשב את a^{n-1} (זאת לא בעיה קשה במחשב).

אם $a^{n-1}\not\equiv 1 \pmod n$ אז n בטוח לא ראשוני.

אחרת נחזור

(הגרלה תלויה)

- נכריז ש- n ראשוני בהסתברות גבוהה.

למה זה שגוי? כי יכול להיות ש- n מספר קרמייקל...

משפט: $n\in\mathbb{N}$. תיזוגי אי-זוגי הוא ראשוני אמ"מ לכל $(a,n)=1$

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

הוכחה: $(\Leftarrow)$ כבר ראינו.

$(\Rightarrow)$ נניח שמתקיים $a^{\frac{n-1}{2}}\equiv \left(\frac{a}{n}\right) \pmod n$ לכל $(a,n)=1$.

זה אומר ש- n מספר קרמייקל כי אז

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

לכן n מכפלה של ראשוניים שונים זה מזה: $n=p_1\cdots p_t$

! $p_i-1 \mid n-1$ לכל $i=1,\dots,t$. ניקח $p=p_1$.

ונסמן $n-1=(p-1)\ell$ (לא בהכרח זוגי! $\frac{\text{זוגי}}{\text{זוגי}}$)

נניח ש- $1<t$. נניח ש- ℓ אי-זוגי. נבחר $b_1 \pmod p$ רק

ש- $\left(\frac{b_1}{p}\right)=-1$ ונבחר $b_2 \pmod{\frac{n}{p}}$ רק ש- $\left(\frac{b_2}{n/p}\right)=-1$

[אפשר כי $\frac{n}{p}=p_2\cdots p_t$. נבחר מספר c_2 שאינו שארית

ריבועית מודולו p_2. לכל $i=3,\dots,t$ נבחר c_i שהוא כן

שארית ריבועית מודולו p_i ואז נפתור

$$X\equiv c_2 \pmod{p_2}$$
$$X\equiv c_3 \pmod{p_3}$$
$$\vdots$$
$$X\equiv c_t \pmod{p_t}$$

הפתרון b_2 מקיים

$$\left(\frac{b_2}{n/p}\right)=\left(\frac{b_2}{p_2\cdots p_t}\right)=\left(\frac{b}{p_2}\right)\left(\frac{b}{p_3}\right)\cdots\left(\frac{b}{p_t}\right)=\left(\frac{c_2}{p_2}\right)\left(\frac{c_3}{p_3}\right)\cdots\left(\frac{c_t}{p_t}\right)=$$
$$=(-1)\cdot 1\cdot 1\cdot\ldots\cdot 1=-1$$
[

אחרי שבחרנו b_1, b_2 כנ"ל, נבחר לפי משפט השאריות הסיני

$1\le b\le n$ רק ש- $b\equiv b_1 \pmod{p_1}$

$b\equiv b_2 \pmod{n/p_1}$

ונחשב:

$$\left(\frac{b}{n}\right)=\left(\frac{b}{p\cdot\frac{n}{p}}\right)=\left(\frac{b}{p}\right)\left(\frac{b}{n/p}\right)=\left(\frac{b_1}{p}\right)\left(\frac{b_2}{n/p}\right)=(-1)(-1)=1$$

מצד שני, $n-1=(p-1)\ell$ ולכן $\frac{n-1}{2}=\frac{p-1}{2}\cdot\ell$. לכן

$$b^{\frac{n-1}{2}}=b^{\frac{p-1}{2}\cdot\ell}\equiv\left(\frac{b}{p}\right)^{\ell} \pmod p\equiv\left(\frac{b_1}{p}\right)^{\ell} \pmod p=$$
$$\equiv(-1)^{\ell} \pmod p=-1 \pmod p$$

$\downarrow$ ℓ אי-זוגי

אבל $\left(\frac{b}{n}\right)\equiv 1 \pmod n$ ולכן $\left(\frac{b}{n}\right)\equiv 1 \pmod p$. לכן

$b^{\frac{n-1}{2}}\not\equiv\left(\frac{b}{n}\right) \pmod n$ וזו סתירה לנתון. לכן במקרה ש- ℓ אי-זוגי

לא ייתכן להיות $1<t$. [אפשר להראות ש- b זר ל- n (וצריך!) גם אם לא, אז זר או ל- n או ל- n/p ואז [illegible] b_2 וזה יוצא]

כעת נניח ש- ℓ זוגי. נבחר b_1 רק ש- $\left(\frac{b_1}{p}\right)=-1$; נבחר b_2

רק ש- $\left(\frac{b_2}{n/p}\right)=1$ (זה אפשרי בדומה לקודם)

אז נבחר b רק ש: $b \equiv b_1 \pmod p$

$b \equiv b_1 \pmod{n/p}$

ואז

$$b^{\frac{n-1}{2}} = b^{\frac{p-1}{2}\ell} \equiv_p \left(\frac{b}{p}\right)^{\ell} = 1 \pmod p$$

$$\Rightarrow \left(\frac{b}{n}\right) = \left(\frac{b}{p\cdot\frac{n}{p}}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{n/p}\right) = \left(\frac{b_1}{p}\right)\left(\frac{b_2}{n/p}\right) = (-1)\cdot 1 = -1$$

$$\Rightarrow b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod p$$

ולכן גם $b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod n$ כי $p|n$. שוב סתירה.

$\Leftarrow t=1$ וסיימנו. ☺

אלגוריתם Solovay-Strassen יהי n שלם חיובי אי-זוגי

צעד 1. הגרל b אקראי וחשב $\left(\frac{b}{n}\right)$ (ע"י חוק ההדדיות הריבועית)

[תרגיל: מספר פעולות החישוב שנוהם הוא $O(\log^3 n)$]

אם $b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod n$ הכרז על n כפריק.

אחרת, הגדל מונה ב-1. אם המונה קטן מ-100 חזור לצעד 1

ואם המונה = 100 הכרז על n כראשוני בהסתברות לפחות $1-\frac{1}{2^{100}}$.

הצדקה: $H = \{b \in \mathbb{Z}_n^* : b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \pmod n\}$

מהווה תת חבורה של $\mathbb{Z}_n^*$ ולכן אם n לא ראשוני, עפ"י המשפט לפחות 50% מהמספרים בין 1 ל-n לא מקיימים את המשוואה. שהרי, זה בוודאי נכון לאלו שאינם זרים ל-n. והמקרה שזרים מכיוון שמדובר בתת חבורה ממש והאינדקס לפחות 2 אז זה גם נכון.

איך לחסכון חישובי: $a_i \in F$; $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\Rightarrow f(x) = \dots x(x((a_n x + a_{n-1})x + a_{n-2}) + a_{n-3})\dots$$

אם רוצים לחשב $a^m \pmod n$ (כאשר) $m = \sum_{i=0}^{r} b_i 2^i$ ו-$b_i = 0,1$. ואז

$$a^m = a^{\sum b_i 2^i} = \prod_{i=1}^{r} (a^{2^i})^{b_i}$$

וזה חוסך פעולות.

(26) 20/7/08
תורת המספרים

משפט: $n\in\mathbb{N}$ אי-זוגי. אז n ראשוני אמ"מ לכל $1\le a\le n$ עם $(a,n)=1$ מתקיים $(*)\quad \left(\frac{a}{n}\right)=a^{\frac{n-1}{2}} \pmod n$

יתר על כן, אם n לא ראשוני אז לפחות 50% מהמספרים $1\le a\le n$ מקיימים $a^{\frac{n-1}{2}}\not\equiv\left(\frac{a}{n}\right) \pmod n$

אלגוריתם Soloway-Strassen:

רוצים להחליט אם n ראשוני.

בחר a מקרי. אם $(*)$ לא מתקיים אזי הכרח ש-n לא ראשוני. אם מתקיים, המשך לסיבוב נוסף.

אם מתקיים ל-k סיבובים אזי n ראשוני בהסתברות $\ge 1-\frac{1}{2^k}$.

אלגוריתם Rabin-Miller:

נניח ש-n מספר אי-זוגי חיובי גדול; $b\in(\mathbb{Z}/n\mathbb{Z})^*$ המקיים $b^{n-1}\equiv 1 \pmod n$. הרעיון הוא להתחיל להסתכל בשורשים ריבועיים $b^{\frac{n-1}{2}}, b^{\frac{n-1}{4}}, \ldots, b^{\frac{n-1}{2^t}}$

כאשר $\frac{n-1}{2^t}$ אי-זוגי. אם n ראשוני אזי אם $b^{\frac{n-1}{2^{s-1}}}\equiv 1 \pmod n$ ו- $b^{\frac{n-1}{2^s}}\not\equiv 1 \pmod n$ אזי בהכרח $b^{\frac{n-1}{2^s}}\equiv -1 \pmod n$ (כי בשדה יש ל-1 רק שני שורשים - ±1).

לעומת זאת, אם n מכפלה של ראשוניים $b^{\frac{n-1}{2^s}}$ יכול להיות "כל מיני דברים".

נאמר ש-b עד תקף לראשוניות של n אם בסדרה $b^{\frac{n-1}{2^s}} \pmod n$ מופיע -1. אלגוריתם רבין-מילר מתבסס על כך שאם n לא ראשוני אזי לכל היותר ב-25% מהמספרים בין 1 ל-n הם עדים תקפים.

הערה: מבין כל ה-n-ים עד 25×10^{10} רק מספר אחד $m=3215031751$ עבר את מבחן רבין-מילר עבור $b=2,3,5,7$ והוא לא ראשוני.

הערה: אם מניחים את נכונות של השערת רימן, אפשר להראות שאפשר לבדוק ראשוניות של n בזמן פולינומיאלי. כמה חברה הודים מצאו אלגוריתם פולינומיאלי דטרמיניסטי לבדיקת ראשוניות אבל הקבועים שלו הם גדולים שעדיין משתמשים באלגוריתמים ההסתברותיים.

שדות סופיים

אם F שדה סופי אז $0 = 1 + \dots + 1$ פעם ראשונה לאחר p צעדים עבור p ראשוני. p זה הוא המציין של F. מכאן נובע ש-F מכיל את $\mathbb{Z}/p$, $\mathbb{F}_p = \{0,1,\dots,p-1\}$. F הוא מ"ו מעל $\mathbb{F}_p$ ולכן $|F| = p^n$ לאיזשהו n.

משפט: לכל p ראשוני ולכל $n \in \mathbb{N}$ קיים שדה מסדר p^n. שדה זה יחיד עד כדי איזומורפיזם.

"הוכחה": ב-$\mathbb{F}_p[x]$ לכל n יש פולינום מתוקן ראשוני (= אי-פריק) ממעלה n. ניקח $f(x)$ פולינום כזה ונסתכל ב- $F = \mathbb{F}_p[x]/(f(x))$ מאחר ש-$f(x)$ אי-פריק האידיאל $(f(x))$ הוא מקסימלי ולכן F שדה. קל לראות ש-$|F| = p^n$. צריך גם להראות יחידות...

בניית שדה מסדר p^2: ניקח $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ כך ש- $\left(\frac{a}{p}\right) = -1$ כלומר a לא ריבוע. נסתכל בפולינום $f(x) = x^2 - a$. זה פולינום אי-פריק. $F = \mathbb{F}_p[x]/(f(x))$ שדה שבו יש שורש ל-f (הוא התמונה של x תחת ההטלה הטבעית, כלומר $x + (f(x))$). באופן יותר קונקרטי $F = \{x + y\sqrt{a} : x, y \in \mathbb{F}_p\}$ וזה שדה מסדר p^2.

נניח עתה ש- $|F| = p^2$ ו- $\mathbb{F}_p \subseteq F$. אם φ אוטומורפיזם של F אז $\varphi(b) = b$ לכל $b \in \mathbb{F}_p$. ובפרט $\varphi(a) = a$. לכן $\varphi(a) = \pm\sqrt{a}$. אם $\varphi(\sqrt{a}) = \sqrt{a}$ אז $\varphi = id$ כי

$$\varphi(x + y\sqrt{a}) = \varphi(x) + \varphi(y)\varphi(\sqrt{a}) = x + y\sqrt{a}$$

לכן יש רק אוטומורפיזם אחד יחיד לא טריוויאלי
$\varphi(x+y\sqrt{a}) = x-y\sqrt{a}$.

גם ההעתקה $Fr: F \to F$, $h \mapsto h^p$ הוא אוטומורפיזם כי

הוא בוודאי שומר על כפל: $Fr(h_1h_2) = (h_1h_2)^p = h_1^p h_2^p = Fr(h_1)Fr(h_2)$

אבל הוא גם שומר על חיבור:

$$(h_1+h_2)^p = h_1^p + \binom{p}{1}h_1^{p-1}h_2 + \dots + \binom{p}{p-1}h_1h_2^{p-1} + h_2^p \equiv h_1^p + h_2^p$$

$\downarrow$

$p \mid \binom{p}{i}$ לכל $1 \le i \le p-1$

לכן Fr הומומורפיזם. הוא אוטומורפיזם כי הגרעין אפס והומומורפיזם של שדות הוא תמיד חח"ע. מאחר שאלה שדות סופיים הוא גם על. (למה הוא לא טריוויאלי? כי אם היה טריוויאלי אז לפולינום $x^p - x$ היו p^2 שורשים וזה בלתי אפשרי).

אלגוריתם להוצאת שורש ריבועי ב- $\mathbb{F}_p$

יהי $b \in \mathbb{F}_p$ כך ש- $\left(\frac{b}{p}\right)=1$, כלומר יש לו שורש ריבועי ואנחנו רוצים למצוא אותו.

נגריל t מקרי ב- $\mathbb{F}_p$ עד שנקבל כזה ש- $\alpha = t^2 - b$ אינו ריבוע. נסמן $\beta = \sqrt{\alpha}$ ונסתכל בשדה $F = \{x + y\beta : x,y \in \mathbb{F}_p\}$ זה שדה מסדר p^2. נתבונן ב- $\gamma = (\beta+t)^{\frac{p+1}{2}}$.

טענה: (א) $\gamma \in \mathbb{F}_p$

(ב) $\gamma^2 = b$

הוכחה: נציין ש- (ב $\Leftarrow$ א) כי התנאי- b שיש לו שורש ב- $\mathbb{F}_p$ אומר יש לו בדיוק שני שורשים ב- F ושניהם ב- $\mathbb{F}_p$ (והם הנגדיים אחד של השני). לכן מספיק להוכיח את (ב).

$\gamma^2 = (\beta+t)^{p+1} = (\beta+t)^p(\beta+t)^1 =$

$= Fr(\beta+t)(\beta+t) = \varphi(\beta+t)(t+\beta) =$

מלמעלה $\swarrow$

$$= (t-\beta)(t+\beta) = t^2 - \beta^2 = t^2 - \alpha =$$
$$= t^2 - (t^2 - b) = b$$

(ש)

Public Key Cryptography

מאז ומעולם אנשים רצו להסתיר סודות ולהעביר מסרים בסוד. אפילו בתנ"ך יש שימוש בקוד אתב"ש (א ↔ ת, ב ↔ ש וכו') ומופיעה המילה ששך שהיא למעשה בבל. זו דוגמה לצופן החלפה. צפני החלפה קל מאוד לשבור ע"י ניתוח שכיחות של האותיות בטקסט המוצפן.
הבעיה בכל השיטות הקודמות היא שהיה צורך בסוד משותף שנקבע קודם להתכתבות.
נקודת מפנה הייתה מאמר של דיפי והלמן שהתחיל לבסס את ההצפנה הציבורית. הרעיון הוא שיש פונקציה חד-כיוונית (בהינתן x קל לחשב את $f(x)$ אבל בהינתן y קשה מאוד לחשב את $f^{-1}(y)$, אלא אם יודע סוד כלשהו).

הנה אנלוגיה תמימה: יש שני אנשים שרוצים לדבר - אליס ובוב. הם ממציאים שפות A ו-B בהתאמה. אליס נותנת לבוב מילון עברית-A ובוב נותן לאליס מילון עברית-B. לאליס יש גם מילון A-עברית ולבוב יש מילון B-עברית. עכשיו אליס יכולה לשלוח לבוב הודעה מוצפנת - היא תתרגם את ההודעה שלה מעברית ל-B. בוב יוכל לפענח את ההודעה חזרה לעברית בעזרת המילון B-עברית.
אבל בגלל שעבר המון זמן לקחת מילון עברית-B ולהפוך אותו ל-B-עברית, אפקטיבית ההודעות סודיות ואף אחד לא יוכל בזמן סביר לפענח אותן.

שיטת RSA

אבחר p ו- q ראשוניים גדולים ונסמן ב- $n=pq$.

אחשב $\varphi(n)=|\mathbb{Z}_n^*|=\varphi(p)\varphi(q)=(p-1)(q-1)$

אבחר e אקראי בין $1\le e\le\varphi(n)$ רק ש- $(e,\varphi(n))=1$

ואפרסם בציבור את (n,e).

מי שרוצה לשלוח לי הודעה $1\le x<n$ ישלח במקום זה את $x^e \pmod n$. לי יש את $\varphi(n)$ ולכן יכול למצוא $1\le f<\varphi(n)$ רק ש- $ef\equiv 1 \pmod{\varphi(n)}$ (בעזרת אלגוריתם אוקלידס המורחב). אז $ef=1+r\varphi(n)$ ולכן הפענוח הוא

$$(x^e)^f=x^{ef}=x^{1+r\varphi(n)}=x\cdot x^{r\varphi(n)}=x\cdot 1^r=x$$

האמת היא שיש כאן הנחה מוסווית ש- $(x,n)=1$ אבל הסיכוי שזה יקרה הוא מאוד נמוך כשמדובר במספרים עם 200 ביטים...

"<u>אקסיומה" (מפוקפקת)</u>: אין אלגוריתם יעיל לפירוק לגורמים.

<u>הערה</u>: ידיעת $\varphi(n)$ נותנת פירוק של n (כאשר $n=pq$) שהרי $\varphi(n)=(p-1)(q-1)=pq-(p+q)+1$

ולכן ידיעת $n=pq$ ו- $\varphi(n)$ נותנת את ידיעת $p+q$ ואז אפשר לפתור את המערכת

$$\begin{cases} pq=n \\ p+q=S \end{cases}$$

(29) 27.07.08
תורת המספרים

RSA

בוב בוחר p,q ראשוניים ; e רק ש- $(e,\varphi(n))=1$

כאשר $n=pq$; $\varphi(n)=(p-1)(q-1)$. אז המפתח הציבורי שלו הוא (n,e).

אליס רוצה לשלוח לבוב את ההודעה x. אז היא שולחת אליו את $x^e \pmod n$.

בוב יודע את $\varphi(n)$ ולכן יכול בקלות למצוא f רק ש- $ef\equiv 1 \pmod{\varphi(n)}$ (בעזרת אלגוריתם אוקלידס). אז $ef = 1+r\varphi(n)$ עבור $r\in\mathbb{Z}$ ולכן

$$x^{ef}\equiv_n x^{1+r\varphi(n)} \equiv_n x(x^{\varphi(n)})^r \equiv_n x\cdot 1^r \equiv_n x$$

זה במקרה ש- $(x,\varphi(n))=1$. הסיכוי שהם לא זרים הוא מאוד מאוד קטן אז נתעלם מזה...

הערות:

1) ידיעת $\varphi(n)$ שקולה לפירוק (ראינו בשבוע שעבר)

2) אם איב יודעת למצוא m רק ש- $a^m\equiv 1 \pmod n$ (*) לכל $a\in\mathbb{Z}_n^*$, אזי היא יודעת לפרק את n כי:

(i) m כזה חייב להיות זוגי (כי מתחלק ב- $p-1$ וב- $q-1$)

(ii) נבדוק אם גם ל- $\frac{m}{2}$ יש את התכונה (*). אפשר לבדוק את זה באופן הסתברותי מהר כי אוסף ה-a-ים שמקיימים (*) זו חבורה חלקית.

אם $\frac{m}{2}$ מקיים (*) נמשיך לבדוק את $\frac{m}{4}$ וכן הלאה עד שנגיע ל- m כזה שהוא מקיים (*) אבל $\frac{m}{2}$ לא מקיים.

למה $\frac{m}{2}$ לא מקיים? זה אומר שלא נכון שלכל a, $a^{\frac{m}{2}}\equiv 1 \pmod p$ או שלא לכל a, $a^{\frac{m}{2}}\equiv 1 \pmod q$. זה אומר ש-(א) $p-1 \nmid \frac{m}{2}$ או (ב) $q-1 \nmid \frac{m}{2}$.

נניח שקורה (א) ולא (ב), כלומר $q-1 \mid \frac{m}{2}$ אז לכל a, $a^{\frac{m}{2}}\equiv 1 \pmod q$

ולפעמים מתקיים $a^{\frac{m}{2}} \not\equiv 1 \pmod p$. לכן בהסתברות לפחות ½, a אקראי יקיים ש- $a^{\frac{m}{2}}-1$ מתחלק ב-q ולא ב-p.
כלומר $q = (a^{\frac{m}{2}}-1, n)$ ולכן נמצא בקלות את q ומכאן פירוק ל-n. אם מתקיים (ב) ולא (א) זה סימטרי.
אם מתקיים גם (א) וגם (ב) אז $q-1 \mid \frac{m}{2}$; $p-1 \nmid \frac{m}{2}$
אז יש חלוקה ל-4 מצבים לפי אחד מהמצבים:

$$a^{\frac{m}{2}} \equiv \pm 1 \pmod p$$

$$a^{\frac{m}{2}} \equiv \pm 1 \pmod q$$

אם נסתכל ב- $a^{\frac{m}{2}}-1$ יש לו סכוי $\frac{1}{2}$ שיהיה לו גורם משותף עם n.

שיטת רבין

p,q ראשוניים. $n=pq$. והמפתח הציבורי הוא n.
אז במקום לשדר את x משדרים את $m = x^2 \pmod n$
מי שיודע את p,q יחשב את r_p, r_q כך ש-

$$r_p^2 \equiv m \pmod p$$

$$r_q^2 \equiv m \pmod q$$

כזכור: יש אלגוריתם מהיר להוצאת שורש מודולו ראשוני.
(הערה: אם נדאג לבחור את p ו-q להיות שניהם $p \equiv q \equiv 3 \pmod 4$ אז יש אלגוריתם מאוד מהיר להוצאת שורש ל-m: $m^{\frac{p+1}{4}}$:

$$(m^{\frac{p+1}{4}})^2 = m^{\frac{p+1}{2}} = m^{\frac{p-1}{2}+\frac{2}{2}} = m^{\frac{p-1}{2}} \cdot m \equiv_p \left(\frac{m}{p}\right) m \equiv 1 \cdot m = m$$

(m ריבוע ←)

מתוך r_p ו-r_q ע"י משפט השאריות הסיני מקבלים a יחיד כך ש- $a \equiv r_p \pmod p$, $a \equiv r_q \pmod q$ (קל)
(מוצא y,z כך ש- $yp+zq=1$ ולוקח $a = r_q y p + r_p z q$)
לכן $a^2 \equiv r_p^2 \equiv m \pmod p$, $a^2 \equiv r_q^2 \equiv m \pmod q$

אם $a^2 \equiv m \pmod n$, אז מצאנו פתרון.
אלא שהבעיה היא ש- r_p, r_q לא נקבעים באופן יחיד. לכל
אחד מהם יש 2 אפשרויות אלא סה"כ יש 4 a-ים אפשריים...
אפשר לפתור את הפרקטיקה ע"י קביעת תבנית מסוימת לחלק
מהביטים (אבל במקרה זה יש גם חשש שזה יעזור לשבירה של
הצופן איכשהו...).

<u>טענה</u>: אם יש אלגוריתם יעיל שבהינתן $n \geq m \geq 1$ שהוא
שארית ריבועית, נותן את אחד משורשיו הריבועיים (נזכור
יש 4 כאלה), אזי ניתן לפרק את n

<u>הוכחה</u>: נגריל באופן מקרי y-ים $n \geq y \geq 1$ ונכניס
לאלגוריתם את $y^2 \bmod m$. האלגוריתם יחזיר שורש
משהו של y^2. ב- 50% מהמקרים יחזור y או $\pm y$ ואז
אין שם תועלת. אבל ב- 50% מהמקרים יהיה שורש $z \neq \pm y$
במקרה כזה. $0 \equiv_n y^2 - z^2 = (y-z)(y+z)$
אבל $y - z \not\equiv 0 \pmod n$ וגם $y + z \not\equiv 0 \pmod n$.
לכן בהכרח $p | y-z$ וגם $q | y+z$ או להפך
אז נחשב את $(y-z, n)$ ונפרק את n.

כאן הוכחה לחוזק של האלגוריתם: אם מישהו יודע לפצח אותו
אז הוא גם יודע לפרק מספרים. ומאחר שמאמינים
שזו בעיה קשה אז גם קשה לפצח את השיטה.

חתימה דיגיטלית

$n = pq$ ידוע לכל. פורסם x^2 ומטרתי לשכנע
שאני יודע את x בלי שאחשוף אותו.
אגריל y ואשלח אליכם את y^2. אתם רשאים לדרוש
ממני (אחרי שקיבלתם את y^2) לפרסם או את y או את
$xy \bmod n$. כל זה חוזרים הרבה פעמים ואחוז מספיק

תכונות — אין ברירה אלא להאמין לו..

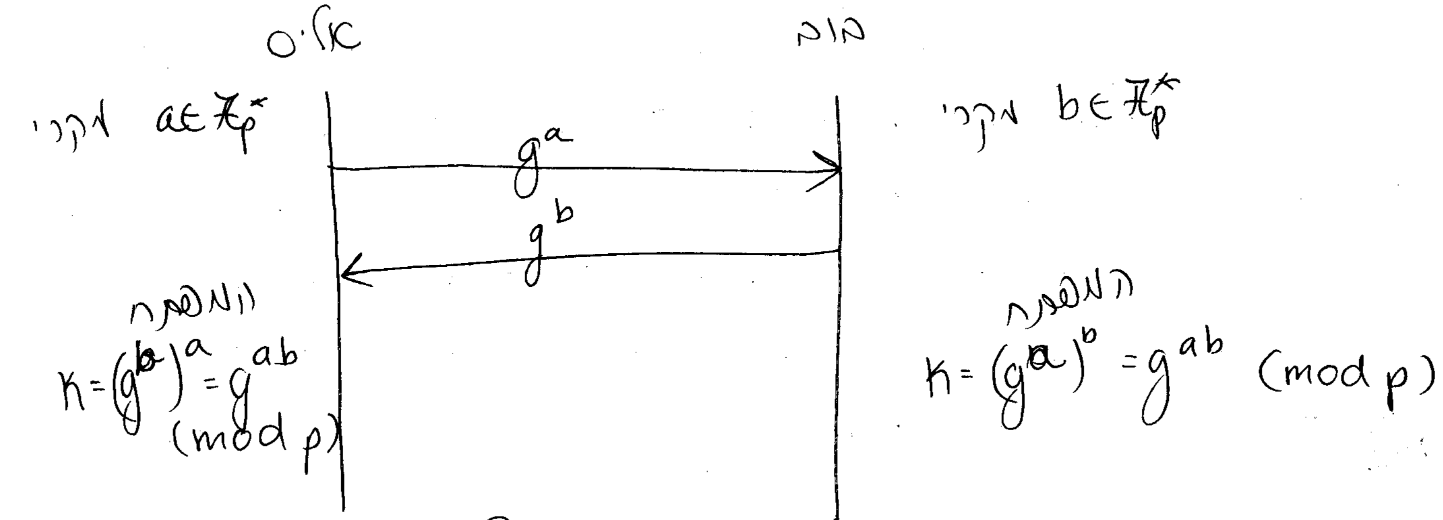
אפשר להוכיח שהשיטה הזאת לא מסגירה שום דבר על x (זה נקרא zero-knowledge proof).

(כמעט בטוח שזה נכון - אלרון משה את זה מהזיכרון).

הפצת מפתחות / לוגריתם דיסקרטי

- p ראשוני גדול ידוע
- נמצא g שיוצר את $\mathbb{Z}_p^*$ (g פרימיטיבי)

אליס מגרילה מספר מקרי $1 \le a \le p-1$ ובוב מגריל מספר מקרי $1 \le b \le p-1$.



והנה לאליס ולבוב יש מפתח משותף $K=g^{ab} \bmod p$ וזה יכול לשמש כמפתח לשימוש בהצפנה סימטרית.

נניח שאיב מאזינה לתקשורת - היא יודעת את g, g^a, g^b אבל לא את g^{ab}. עד כמה שידוע, להוציא לוג זו בעיה קשה ולכן היא לא יכולה לפענח את a,b.

(31) 3.8.08

תורת המספרים

<u>משפט פרמה</u>: לא קיים פתרון בשלמים ל- $x^n+y^n=z^n$ עבור $n\geq 3$.

<u>הערה</u>: אם למשוואה פולינומיאלית $f(x_1,\dots,x_n)=0$ יש פתרון ב- $\mathbb{Z}$ אזי יש פתרון למשוואה $f(x_1,\dots,x_n)\equiv 0 \pmod m$ לכל $m\in\mathbb{N}$. ההיפך הוא בד"כ לא נכון.

<u>טענה</u>: למשוואה $f(x_1,\dots,x_n)\equiv 0 \pmod m$ יש פתרון לכל $m\in\mathbb{N}$ אמ"מ לכל p ראשוני ולכל r יש פתרון למשוואה $f(x_1,\dots,x_n)\equiv 0 \pmod{p^r}$ (ממשפט השאריות הסיני).

השלמים ה-p-אדיים

יהי p ראשוני. נתבונן בסדרות $\{a_i\}_{i=0}^{\infty}=(a_0,a_1,a_2,\dots)$ רק ש- $a_n\equiv a_{n-1} \pmod{p^n}$.

נאמר שסדרות כאלו $\{a_i\}$; $\{b_i\}$ שקולות אם לכל n $a_n\equiv b_n \pmod{p^{n+1}}$.

<u>הגדרה</u>: מספר שלם p-אדי זו מחלקת שקילות של סדרות כאלה.

כל מספר p-אדי מיוצג ע"י סדרה $\{a_i\}$ רק ש- $0\leq a_n<p^{n+1}$

<u>הגדרת חיבור וכפל</u>:

$$\{a_i\}+\{b_i\}=\{a_i+b_i\}$$
$$\{a_i\}\{b_i\}=\{a_ib_i\}$$

צריך להראות שזה מוגדר היטב (תרגיל)

<u>טענה</u>: השלמים ה-p-אדיים עם החיבור והכפל שהגדרנו הם חוג עם יחידה;

$0=(0,0,0,\dots)$

$1=(1,1,1,\dots)$

נסמן חוג זה ב- $\hat{\mathbb{Z}}_p$ - חוג השלמים ה-p-אדיים.

טענה: יש שיכון $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}_p$

$n \longmapsto (n, n, n, \ldots)$

(נזכור שהשקילות היא $a_n = b_{n+1} (\mod p^{n+1})$ אבל גם בצורה המצומצמת הסדרה מסתיימת באינסוף מופעים של n).

איך נראה מספר p-אדי? תמיד אפשר להניח ש- $0 \le a_0 < p$.

$\Leftarrow$ $a_1 \equiv a_0 (\mod p)$, $0 \le a_1 < p^2$

$\Leftarrow$ $a_1 = a_0 + b_1 p$ כאשר $0 \le b_1 < p$

$a_2 \equiv a_1 (\mod p^2)$, $0 \le a_2 < p^3$

$\Leftarrow$ $a_2 = a_1 + b_2 p^2$, $0 \le b_2 < p$

$\Leftarrow$ $a_2 = a_0 + b_1 p + b_2 p^2$, $0 \le b_1, b_2 < p$

וכן הלאה. לשם האסתטיות נסמן: $a_0 = b_0$ ואז

$$a_n = b_0 + b_1 p + b_2 p^2 + \ldots + b_n p^n \qquad 0 \le b_i < p$$

$$a_{n+1} = a_n + b_{n+1} p^{n+1} \qquad 0 \le b_{n+1} < p$$

אז המספרים הם למעשה תחיליות של טור אינסופי פורמלי במשתנה p. לכן ניתן לכתוב את השלם ה- p-אדי $\alpha = \{a_i\}$ עם הטור הפורמלי $\sum_{i=0}^{\infty} b_i p^i$.

למשל עבור $n \in \mathbb{N}$

$$(n, n, n, \ldots) = (n \mod p, n \mod p^2, \ldots) = (a_0, a_1, a_2, \ldots)$$

בכתיבה כטור זה יוצא $n = \sum_{i=0}^{r} b_i p^i$. $r \sim \log_p n$

אז מה שמייצג את הטבעיים כאן זה הפיתוח ה- p-אדי שלהם.

טענה: נניח ש- $\alpha = \{a_i\} = \sum_{i=0}^{\infty} b_i p^i \in \hat{\mathbb{Z}}_p$. α הפיך ב- $\hat{\mathbb{Z}}_p$ אמ"מ $a_0 (= b_0) \not\equiv 0 (\mod p)$.

הערה: החיבור במונחי טורים הוא חיבור עם נשא (carry) (כמו חיבור ארוך) וכפל הוא הכפל הפורמלי של שני טורים ב- p (שוב עם נשא). זה מבדיל את $\hat{\mathbb{Z}}_p$ מ- $\mathbb{F}_p[[X]]$ (: טורי חזקות פורמליים מעל $\mathbb{F}_p$).

הוכחת הטענה:

אם $\alpha=(a_0,a_1,\dots)$ הפיך פירושו שקיים $\gamma=(c_0,c_1,\dots)$ כאשר $0\le c_i\le p^{i+1}$ כך ש- $a_i c_i\equiv 1 \pmod{p^{i+1}}$.
בפרט, אם α הפיך אז $a_0 c_0\equiv 1 \pmod p$ ולכן $a_0\not\equiv 0 \pmod p$.

מצד שני, נניח ש- $a_0\not\equiv 0 \pmod p$. אזי מאחר ש- $a_n\equiv a_{n-1} \pmod{p^n}$ נובע ש- $a_i\equiv a_0 \pmod p$ לכל i והרי $a_i\not\equiv 0 \pmod p$ לכל i ולכן הפיך בחוג $\mathbb{Z}_{p^{i+1}}$ ולכן יש c_i כך ש- $a_i c_i\equiv 1 \pmod{p^{i+1}}$, צריך להראות ש- $(c_0,c_1,\dots)$ אכן שלם p-אדי.

☺

דוגמה: למספרים שליליים יש "ייצוג" p-אדי אינסופי (רטור) למשל,

$$-1=(p-1,\,p^2-1,\,p^3-1,\,\dots)=$$
$$=(p-1)+(p-1)p+(p-1)p^2+\dots=$$
$$=\sum_{i=0}^{\infty}(p-1)p^i$$

$$\sum_{i=0}^{n}(p-1)p^i=(p-1)\frac{p^{n+1}-1}{p-1}=p^{n+1}-1\equiv -1 \pmod{p^{n+1}}$$
$$\sum_{i=0}^{\infty}(p-1)p^i=(p-1)\sum_{i=0}^{\infty}p^i=(p-1)\frac{1}{1-p}=-1$$

מסקנה: כל איבר α ב- $\hat{\mathbb{Z}}_p$ ניתן לכתיבה כ- $\varepsilon\cdot p^m$ כאשר ε הפיך ב- $\hat{\mathbb{Z}}_p$.

הוכחה: נסמן $\alpha=\sum b_i p^i$ ויהי m הראשון כך ש- $b_m\neq 0$. אז מתקיים $\alpha=p^m\left(\sum_{i=0}^{\infty} b_{m+i}p^i\right)$ ו- $\sum b_{m+i}p^i$ הפיך כי $b_m\not\equiv 0 \pmod p$.

☺

טענה: ב- $\hat{\mathbb{Z}}_p$ אין מחלקי אפס. כלומר, הוא תחום שלמות. לכן יש לו שדה שברים שסימונו $\mathbb{Q}_p$ (שדה המספרים

ה-p-אדיים).

טענה: $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}_p$ ולכן $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$

מסקנה: כל איבר של $\mathbb{Q}_p$ ניתן להצגה כ- $\sum_{i=v}^{\infty} b_i p^i$ עבור $v \in \mathbb{Z}$. אז $\mathbb{Q}_p$ = טורי לורן פורמליים ב- p.

הגדרה: עבור $\gamma = \sum_{i=v}^{\infty} b_i p^i$ כאשר $b_v \neq 0$ ו- $0 \le b_i < p$ נגדיר את הנורמה $|\gamma| = \frac{1}{p^v}$, $|0| = \infty$ (?)
ונגדיר מטריקה על $\mathbb{Q}_p$ ע"י $d(\alpha,\beta) = |\alpha - \beta|$

טענה: זו מטריקה, כלומר:
1) $d(\alpha,\beta) = 0$ אמ"מ $\alpha = \beta$
2) $d(\alpha,\beta) = d(\beta,\alpha)$
3) $d(\alpha,\gamma) \le d(\alpha,\beta) + d(\beta,\gamma)$

דוגמה: $p^i \longrightarrow 0$ שהרי
$$d(p^i,0) = |p^i - 0| = |p^i| = \frac{1}{p^i} \longrightarrow 0$$
באופן דומה: (תרגיל) $n! \longrightarrow 0$

משפט: (א) $\mathbb{Q}_p$ שדה שלם (כלומר כל סדרת קושי מתכנסת)
(ב) $\mathbb{Q}_p$ מכיל את $\mathbb{Q}$ כתת שדה צפוף
(כלומר כל מספר p-אדי אפשר להתקרב ע"י רציונליים).

הוכחה:
(ב) נוכיח ש- $\mathbb{N}$ צפופים ב- $\hat{\mathbb{Z}}_p$: נניח $\beta = \sum_{i=0}^{\infty} b_i p^i$ ונקרב אותו ע"י המספרים הטבעיים $\beta_n = \sum_{i=0}^{n} b_i p^i$:
$$d(\beta - \beta_n) = \left| \sum_{i=n+1}^{\infty} b_i p^i \right| \le \frac{1}{p^{n+1}} \longrightarrow 0$$
ועושים מאריתמטיקה של גבולות נקבל ש- $\mathbb{Q}$ צפוף ב- $\mathbb{Q}_p$:
ומעשה, אם $\beta \in \mathbb{Q}_p$ כללי (לאו דווקא שלם) אז ניקח $\beta = \sum_{i=v}^{\infty} b_i p^i$ ונקבל $\beta_n = \sum_{i=v}^{n} b_i p^i$, $\beta_n \to \beta$
☺

משפט Ostrowski: אם F שדה שלם המכיל את $\mathbb{Q}$ כתת שדה צפוף אז $F \cong \mathbb{R}$ או $F \cong \mathbb{Q}_p$ לאיזה p.

טענה: אם $\alpha_i \in \mathbb{Q}_p$ הטור $\sum_{i=1}^{\infty} \alpha_i$ מתכנס אמ"מ $\alpha_i \longrightarrow 0$ (בניגוד לממשיים!!)

מה זה נותן לנו? רוצים לפתור את $f(x) \equiv 0 \pmod{p^n}$ $\forall n$ לכל
זה שקול לפתרון עם השלמים ה-p-אדיים ושם זה יותר קל הרבה פעמים וזה יכול לעזור המון.

המבחן

שנצטרך לעבוד עם החומרים (למשל ההופכי של 7 מודולו 13). בעיקר יהיו שאלות פרקטיות - מהתרגולים ודומיהם. למשל, לכתוב את $\frac{2}{3}$ ב- $\hat{\mathbb{Z}}_5$, להשתמש במשפט השאריות הסיני.
שאלות תיאורטיות יכולות להיות מההתחלה של החומר - אולי יש אינסוף ראשוניים מהצורה $4n+1$ וכן $\pi(x) \leq \frac{x}{\ln x}$, וכו'.