תורת המספרים ושימושים בקריפטוגרפיה

יובל קפלן

סיכום הרצאות פרופ' אלכס לובוצקי (የለምለም፡አያት) בקורס "תורת המספרים ושימושים בקריפטוגרפיה" (80611) באוניברסיטה העברית, 2007-8.

תוכן מחברת זו הוקלד ונערך על־ידי יובל קפלן. אין המרצה אחראי לכל טעות שנפלה בו. סודר באמצעות LaTeX 2ε ב־22 באוגוסט 2008.
עדכונים ותיקונים יופיעו ב־http://www.limsoup.net/. לתגובות, לתיקונים ובכל עניין אחר, אנא כתבו ל־yuvak@gmx.net.

סיכומים נוספים בסדרה:

2006–7	חשבון אינפיניטסימלי 1	אלגברה לינארית 1
	חשבון אינפיניטסימלי 2	אלגברה לינארית 2
	תורת הקבוצות	
2007–8	מבנים אלגבריים 1	תורת ההסתברות 1
	חשבון אינפי׳ מתקדם 1	
בקרוב	חשבון אינפי׳ מתקדם 2	מבוא לטופולוגיה
	תורת המספרים וקריפטו׳	מבנים אלגבריים 2
	תולדות המתמטיקה	

תוכן עניינים

1 תורת המספרים 5
1.1 תכונות של $\mathbb{Z}$ 5
1.2 מניית המספרים הראשוניים 6
1.3 בעיות פתוחות לגבי ראשוניים 9
1.4 קונגרואנציות 9
1.5 פונקציית φ של אוילר 11
1.6 מספרים מושלמים 12
1.7 מבנה $(\mathbb{Z}/n\mathbb{Z})^*$ 13
1.8 חוק ההדדיות הריבועית של גאוס 15
1.9 מבחני ראשוניות 21
1.10 שדות סופיים 24
2 קריפטוגרפיה: הצפנה ציבורית 26
2.1 שיטת RSA 26
2.2 שיטת רבין 27
2.3 חתימה דיגיטלית / zero-knowledge proofs 28
2.4 הפצת מפתחות / לוגריתם דיסקרטי 28
3 המספרים ה־p־אדיים 29
4 תרגילים 31
4.1 12.6.2008 31
4.2 6.7.2008 32
4.3 3.8.2008 33

1 תורת המספרים

1.1 תכונות של $\mathbb{Z}$

18.5.2008 הקבוצות בהן נעסוק: $\mathbb{Z} = \{0, \pm1, \pm2, \ldots\}$, $\mathbb{N} = \{1, 2, \ldots\}$.

$\mathbb{Z}$ הוא חוג אוקלידי: $\forall a, b \in \mathbb{Z} \quad \exists q, r \in \mathbb{Z} \ : \ a = qb + r$, כאשר $r = 0$ (ואז נאמר ש־a | b) או $|r| < |b|$.

טענה 1: כל אידיאל ב־$\mathbb{Z}$ הוא ראשי.

הוכחה. אם $I \lhd \mathbb{Z}$ אידיאל (כלומר, לכל $a, b \in I$, $a \pm b \in I$, ולכל $r \in \mathbb{Z}$ ו־$a \in I$, $ra \in I$), צריך להראות שקיים $a \in \mathbb{Z}$ כך ש־$I = a\mathbb{Z}$. אם $I = \{0\}$, ניקח $a = 0$. אחרת, נבחר $a \in I$ עם $|a|$ מינימלי ונוכיח שלכל $c, a \in I$ | a: ואכן, $c = aq + r$ כאשר $r = 0$ (ואז $a \mid c$ וגמרנו) או $r = c - aq \in I$ אבל $|r| < |a|$, בסתירה לבחירת a.

מספר ראשוני **הגדרה.** $p \in \mathbb{Z}$ נקרא **ראשוני** אם $p \neq \pm1$ וכאשר $p = ab$ עם $a, b \in \mathbb{Z}$, אזי $a = \pm1$ או $b = \pm1$.

משפט 2 (היסודי של האריתמטיקה): כל $n \in \mathbb{Z}$ ניתן לכתיבה כ־$n = p_1 p_2 \cdot \ldots \cdot p_l$ כאשר $p_1, \ldots, p_l$ ראשוניים, וכתיבה זו יחידה: אם $n = q_1 \cdot \ldots \cdot q_m$, אזי $m = l$ ולאחר שינוי סדר $p_i = \pm q_i$ לכל $i = 1, \ldots, l$.

הוכחה. קיום – באינדוקציה על n (ל־n חיובי, ונסיק גם ל־n שלילי).

מחלק משותף מקסימלי לצורך היחידות, נשתמש ב**מחלק המשותף המקסימלי**: בהינתן $a, b \in \mathbb{Z}$, d הוא מחלק משותף מקסימלי שלהם אם $d \mid a$ ו־$d \mid b$ ואם $c \mid a$ וגם $c \mid b$, אזי $c \mid d$. (אם $\gcd(a, b) = 1$, נאמר ש־a ו־b **זרים**.)

למה 1.2: לכל $a, b \in \mathbb{Z}$ קיים מחלק משותף מקסימלי d, והוא יחיד עד־כדי סימן.

הוכחה (דרך א'). נסתכל באידיאל הנוצר על־ידי a ו־b, כלומר ב־$I = \{xa + yb \ : \ x, y \in \mathbb{Z}\}$. זה אידיאל, לכן קיים d כך ש־$I = d\mathbb{Z}$. ברור ש־$d \mid a$ ו־$d \mid b$, כי $a, b \in I$; אם $c \mid a, b$, אזי $c \mid d$ כי $d = x_0 a + y_0 b$ ל־$x_0, y_0 \in \mathbb{Z}$ כלשהם.

מההוכחה לעיל נובע שהמחלק המשותף המסימלי של a ו־b ניתן לכתיבה כ־$d = x_0 a + y_0 b$.

הוכחה (דרך ב'). באמצעות האלגוריתם של אוקלידס[1] למציאת $d = \gcd(a, b) = (a, b)$: נכתוב

[1] תרגיל: מצאו הערכה טובה על מספר הפעולות הנדרשות לחישוב $\gcd(a, b)$ באמצעות האלגוריתם של אוקלידס.

$$\begin{aligned} a &= q_1 b + r_1 \quad |r_1| < |b| \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

ונטען כי $r_n = \gcd(a,b)$.

הוכחת יחידות ה־gcd – כתרגיל.

למה 2.2: אם p ראשוני ו־$p \mid ab$ אז $p \mid a$ או $p \mid b$.

הוכחה. נסתכל ב־$d = \gcd(p,a)$. $d \mid p$ ולכן $d = \pm 1$ והם זרים, או $d = \pm p$ ואז $p \mid a$ וגמרנו. לכן נניח שהם זרים. אז $1 = x_0 a + y_0 p$ ואז $b = x_0 ab + y_0 pb$. $p \mid ab$ ולכן $p \mid b$, וגמרנו.

נוכיח עכשיו את היחידות: $p_1 \mid q_1 \dots q_m$. באינדוקציה על l: $p_1 p_2 \cdot \ldots \cdot p_l = q_1 q_2 \cdot \ldots \cdot q_m$ ולכן (באינדוקציה על m) p_1 מחלק את אחד הראשוניים q_i. לאחר שינוי סדר, $p_1 \mid q_1$ ולכן נקבל $p_1 = \pm q_1$. נצמצם ב־p_1 ונמשיך.

1.2 מניית המספרים הראשוניים

משפט 3 (אוקלידס): יש אינסוף מספרים ראשוניים.

הוכחה (דרך א'). נניח שלא; אזי כל המספרים הראשוניים הם $p_1, p_2, \dots, p_l$ ($l \in \mathbb{N}$). נתבונן במספר $N = p_1 \cdot \ldots \cdot p_l + 1$. N מתפרק למכפלת גורמים ראשוניים שאף אחד מהם לא ברשימה.

ההוכחה הזו לא נותנת הערכה טובה על כמות הראשוניים. עם זאת, שיטת ההוכחה שימושית גם לטענות דומות אחרות:

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

הוכחה. נניח שיש רק מספר סופי של ראשוניים מצורה זו, $p_1, p_2, \dots, p_l$ ($l \in \mathbb{N}$). נסתכל במספר $N = 4p_1 \cdot \ldots \cdot p_l - 1$. אזי $N \equiv 3 \pmod 4$ הוא מכפלת ראשוניים. לא ייתכן שכולם מהצורה $p \equiv 1 \pmod 4$ ולכן יש ראשוני $q \mid N$, $q \equiv 3 \pmod 4$, $q \neq p_1, \dots, p_l$, כי $N \equiv -1 \pmod{p_i}$ לכל $i = 1, \dots, l$.

באופן כללי יותר:

משפט 5 (דיריכלה): אם $n, a \in \mathbb{Z}$ ו־$\gcd(n,a) = 1$, אזי יש אינסוף ראשוניים p כך ש־$p \equiv a \pmod n$.

למשפט זה אין הוכחה אלמנטרית (כלומר, הוכחה ללא פונקציות מרוכבות).

ברוח דומה, תרגיל: הוכח שיש אינסוף ראשוניים p כך ש־$p \equiv 5 \pmod 6$.

הוכחה (פירסטנברג). נגדיר טופולוגיה על $\mathbb{Z}$: קבוצה $A \subseteq \mathbb{Z}$ תיקרא פתוחה אם לכל $a \in A$ קיים $0 \neq d \in \mathbb{Z}$ כך ש־$a + d\mathbb{Z} \subseteq A$. כל סדרה אריתמטית היא קבוצה פתוחה. נשים לב שסדרה אריתמטית היא גם סגורה, כי המשלים של סדרה אריתמטית הוא איחוד (סופי) של סדרות אריתמטיות. בפרט, לכל ראשוני p, $p\mathbb{Z}$ פתוחה וסגורה.

$X = \mathbb{Z} \setminus \bigcup_{p \text{ prime}} p\mathbb{Z}$. $p\mathbb{Z}$ סגורה, ולכן אם יש מספר סופי של ראשוניים גם $\bigcup_{p \text{ prime}} p\mathbb{Z}$ סגורה, ולכן X פתוחה. אבל $X = \{\pm 1\}$ לא פתוחה.

הוכחה זו לא נותנת הערכה כלל. ההוכחה הבאה טובה מעט יותר:

הוכחה (דרך ג'). נניח שיש מספר סופי l של ראשוניים. נשים לב שכל מספר טבעי n ניתן לכתיבה כ־$n = ab^2$ כאשר a חפשי מריבויים, כלומר לכל ראשוני p, $p^2 \nmid a$. נסתכל ב־N מאוד גדול; כל $n \leq N$ ניתן לכתיבה כ־ab^2 כנ"ל כאשר $b \leq \sqrt{N}$ ו־a מכפלת ראשוניים שונים. מספר האפשרויות ל־a הוא לכל היותר 2^l, לכן $2^k\sqrt{N} \geq N$ ולפיכך $2^l \geq \sqrt{N}$. זו סתירה כאשר N גדול מספיק.

נסמן ב־$\pi(x)$ את מספר הראשוניים (החיוביים) הקטנים מ־x. מההוכחה האחרונה ניתן להסיק את המסקנה הבאה:

מסקנה 6: $\pi(x) \geq \frac{\log_2 x}{2} = \frac{\ln x}{2 \ln 2}$

הוכחה. בפרט, $2^{\pi(x)} \geq \sqrt{x}$ ולכן $\pi(x) \ln 2 \geq \frac{1}{2} \ln x$.

טענה 7: $\sum_{p \text{ prime}} \frac{1}{p}$ מתבדר.

הוכחה. אם הטור מתכנס, קיים l כך ש־$\sum_p \frac{1}{p} = \sum_{p \leq p_l} \frac{1}{p} + \sum_{p > p_l} \frac{1}{p} < \frac{1}{2}$ ו־$\frac{1}{p_1} + \ldots + \frac{1}{p_l} + \sum_{p > p_l} \frac{1}{p}$. יהי $x \in \mathbb{N}$ גדול. מספר השלמים הקטנים מ־x ומתחלקים בראשוני p קטן מ־ או שווה ל־$\frac{x}{p}$. לכן אם נסמן ב־$N(x)$ את מספר השלמים (החיוביים) הקטנים מ־x ומתחלקים באחד או יותר מבין הראשוניים הגדולים מ־p_l, נקבל $N(x) \leq \sum_{p > p_l} \frac{x}{p} = x \sum_{p > p_l} \frac{1}{p} \leq \frac{1}{2}x$, ולפיכך $x - N(x) \geq \frac{x}{2}$. כלומר, למעלה ממחצית השלמים בין 1 ל־x מתחלקים רק ב־$p_1, \ldots, p_l$: יותר ממחצית השלמים ב־$[1, \ldots, K = x]$ מתפרקים לראשוניים שכולם מבין $p_1, \ldots, p_l$. ארגומנט דומה לקודם מראה שמספרם של אלו קטן מ־ או שווה ל־$2^l\sqrt{K}$. אם כן, $2^l\sqrt{K} \geq \frac{K}{2}$, ומתקבלת סתירה ל־$K$ מספיק גדול.

25.5.2008 **משפט 8 (המספרים הראשוניים):** $\pi(x) \sim \frac{x}{\ln x}$, כלומר $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.

למשפט זה הרבה עומק; אנחנו נראה תוצאות חלשות יותר.

משפט 9 (צ'ביצב): קיימים קבועים a ו־b כך שלכל $2 \leq x \in \mathbb{R}$, $a \cdot \frac{x}{\ln x} \leq \pi(x) \leq b \cdot \frac{x}{\ln x}$.

סיפור. נסמן $E(x) = |\pi(x) - \frac{x}{\ln x}|$. **השערת רימן**: קיים קבוע $c \in \mathbb{R}$ כך ש־$E(x) \leq cx^{\frac{1}{2}} \ln x$. למעשה, בדרך־כלל מנסחים את השערת רימן באמצעות פונקציית זיתא - $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. היא

מתכנסת כאשר $\operatorname{Re} s > 1$. יש לה הרחבה (יחידה) מרומורפית לפונקציה המוגדרת לכל s מרוכב. השערת רימן היא שאם $z \in \mathbb{C}$ שורש של $\zeta(s)$ ו־$0 \leq \operatorname{Re} z \leq 1$ אזי $\operatorname{Re} z = \frac{1}{2}$.

טענה 10: כטור פורמלי,[2] $\zeta(s) = \prod_p (1 - \frac{1}{1-p^s})$, וזה שקול למשפט היסודי של האריתמטיקה.[3]

משפט 11: ל־$0 \leq x \in \mathbb{R}$, נסמן $\theta(x) = \sum_{x \geq p \text{ prime}} \ln p$.[4] אזי קיימים $0 < a', b' \in \mathbb{R}$ כך ש־$a'x \leq \theta(x) \leq b'x$.[5]

למה 1.11: קיים קבוע b' כך ש־$\theta(x) \leq b'x$.

הוכחה. מתקיים $\binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{n+1}{1} \cdot \frac{n+2}{2} \cdot \ldots \cdot \frac{2n}{n}$. ברור ש־$\binom{2n}{n}$ מתחלק בכל ראשוני $n < p \leq 2n$.

מצד שני, $2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} > \binom{2n}{n} > \prod_{n<p\leq 2n} p$. נוציא לוגריתם ונקבל $2n \ln 2 > \sum_{n<p\leq 2n} \ln p = \theta(2n) - \theta(n)$. כעת,

$$\begin{aligned}
\theta(2^m) &= (\theta(2^m) - \theta(2^{m-1})) + \\
&\quad (\theta(2^{m-1}) - \theta(2^{m-2})) + \ldots + \\
&\quad (\theta(4) - \theta(2)) + (\theta(2) - \theta(1)) \\
&\leq 2\ln 2(2^{m-1} + 2^{m-2} + \ldots + 2^2 + 2 + 1) \\
&= 2\ln 2 \cdot \tfrac{2^m - 1}{2-1} \\
&\leq 2\ln 2 \cdot 2^m
\end{aligned}$$

עבור $2^{m-1} \leq x \leq 2^m$, נקבל $\theta(x) \leq \theta(2^m) \leq 2\ln 2 \cdot 2^m \leq 2\ln 2 \cdot 2x = b'x$ כאשר $b' = 4\ln 2$.

כבר מחלק זה של המשפט, נקבל

מסקנה 12: קיים b כך ש־$\pi(x) \leq b \cdot \frac{x}{\ln x}$.

הוכחה.

$$\begin{aligned}
b'x &\geq \theta(x) \\
&\geq \textstyle\sum_{\sqrt{x}<p\leq x} \ln p \\
&\geq \textstyle\sum_{\sqrt{x}<p\leq x} \ln \sqrt{x} \\
&= \tfrac{1}{2}\ln x \textstyle\sum_{\sqrt{x}<p\leq x} 1 \\
&= (\tfrac{1}{2}\ln x)(\pi(x) - \pi(\sqrt{x}))
\end{aligned}$$

כלומר, $\pi(x) \leq 2b' \cdot \frac{x}{\ln x} + \pi(\sqrt{x}) \leq 2b' \cdot \frac{x}{\ln x} + \sqrt{x} \leq 2(b'+1)\frac{x}{\ln x}$ (בדוק של־$x \geq 2$, $\sqrt{x} \leq 2 \cdot \frac{x}{\ln x}$.)

למה 1.12: ל־p ראשוני, $m \in \mathbb{N}$, נאמר $\operatorname{ord}_p(m) = t \in \{0, 1, \ldots\}$ אם $p^t \mid m$ אבל $p^{t+1} \nmid m$. אז $\operatorname{ord}_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots + \lfloor \frac{n}{p^{t_p}} \rfloor$, כאשר $t_p = \lfloor \frac{\ln n}{\ln p} \rfloor$.[6]

---

[2] בלי לדאוג להתכנסות.

[3] רמז: $(1-q)^{-1} = \sum_{i=0}^{\infty} q^i$.

[4] נעיר רק שגם את $\pi(x)$ ניתן להציג באופן דומה: $\pi(x) = \sum_{p\leq x} 1$.

[5] למעשה, $\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$.

[6] כזכור, $\lfloor t \rfloor = \max_{n\in\mathbb{N}}\{n \leq t\}$.

למה 2.12: $\binom{2n}{n} \geq 2^n$

למה 3.12: $\mathrm{ord}_p(\binom{2n}{n}) = \mathrm{ord}_p((2n)!) - 2\mathrm{ord}_p(n!) = \sum_{j=1}^{s_p}(\lfloor \frac{2n}{p^j} \rfloor - 2\lfloor \frac{n}{p^j} \rfloor) \leq s_p$, כאשר $s_p = \lfloor \frac{\ln 2n}{\ln p} \rfloor$.

מסקנה 13: יש קבוע a כך ש־$\pi(x) \geq a \cdot \frac{x}{\ln x}$.

הוכחה. נחשב: $2^n \leq \binom{2n}{n} = \prod_{p \leq 2n} p^{\mathrm{ord}_p(\binom{2n}{n})} \leq \prod_{p \leq 2n} p^{\frac{\ln 2n}{\ln p}}$. נוציא לוגריתם בשני האגפים ונקבל $n \ln 2 \leq \sum_{p \leq 2n} \frac{\ln 2n}{\ln p} \cdot \ln p = \ln 2n \sum_{p \leq 2n} 1 = \ln 2n \cdot \pi(2n)$. מכאן, $\pi(2n) \geq \ln 2 \cdot \frac{n}{\ln 2n} = \frac{\ln 2}{2} \cdot \frac{2n}{\ln(2n)}$.

מההוכחה ל־$x = 2n$ אפשר, כקודם, לעבור להוכחה ל־x כללי.

למה 1.13: קיים a' כך ש־$\theta(x) \geq a'x$.

הוכחה.

$$\begin{aligned}
\theta(x) &= \textstyle\sum_{p<x} \ln p \\
&\geq (\pi(x) - \pi(\sqrt{x}) \ln \sqrt{x} \\
&\geq (a \cdot \tfrac{x}{\ln x} - b \cdot \tfrac{\sqrt{x}}{\frac{1}{2}\ln x}) \cdot \tfrac{1}{2} \ln x \\
&= \tfrac{1}{2}(ax - 2b\sqrt{x} \\
&\geq a'x
\end{aligned}$$

ל־a' מתאים. ($a = \frac{\ln 2}{2}$, $b = 8 \ln 2 + 2$.)

1.3 בעיות פתוחות לגבי ראשוניים

כשמערבבים חיבור וכפל, מגיעים לבעיות הקשות באמת בתורות המספרים. למשל:

1. האם יש אינסוף ראשוניים מהצורה $n^2 + 1$?
2. **השערת גולדבאך:** כל מספר זוגי הוא סכום של שני ראשוניים.
3. האם יש אינסוף ראשוניים של פרמה, כלומר ראשוניים מהצורה $2^n + 1$?
4. האם יש אינסוף ראשוניים של מרסן, כלומר ראשוניים מהצורה $2^n - 1$?
5. ידוע שלכל n יש ראשוני בין n ל־$2n$, אך האם תמיד יש ראשוני בין n^2 ל־$(n+1)^2$?

ועוד בעיה מעניינת: p ו־$p+2$ ראשוניים נקראים **ראשוניים תאומים**. ידועים הזוגות $3, 5$, $5, 7$, $11, 13$, $17, 19$, $29, 31$ ועוד, אך האם יש אינסוף ראשוניים תאומים? לא ידוע. (ישנה שמועה, שאולי בקרוב תוכח, שקיים קבוע c כך שקיימים אינסוף זוגות ראשוניים שהמרחק ביניהם c.)

את הפתרונות יש לשלוח אלינו. את הכתובת ניתן לכם בשבוע הבא.

1.4 קונגרואנציות

1.6.2008

הגדרה. יהי $n \in \mathbb{Z}$. נאמר ש־$a \equiv b \pmod n$ ($a \equiv b \ (n)$) אם $n \mid b - a$.

זהו יחס שקילות.

נתבונן בחוג $\mathbb{Z}$, $I = n\mathbb{Z}$. $\mathbb{Z}/I \cong \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. יש הומומורפיזם $\pi : \mathbb{Z} \to \mathbb{Z}/I =$ $\mathbb{Z}/n\mathbb{Z}$ ו־$a, b \in \mathbb{Z}$ מקיימים $a \equiv b \pmod{n}$ אם"ם $\pi(a) = \pi(b)$.

טענה 14: $\mathbb{Z}/n\mathbb{Z}$ שדה אם"ם n ראשוני.

הוכחה. אם n אינו ראשוני, אזי $n = ab$, $1 < a, b < n$ 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.

מצד שני, צריך להראות שלכל $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ כך ש־$\overline{a} \neq 0$ יש הפכי ב־$\mathbb{Z}/n\mathbb{Z}$ ביחס לכפל:

הוכחה ראשונה. נגדיר $f : (\mathbb{Z}/n\mathbb{Z} \setminus \{0\}) \to (\mathbb{Z}/n\mathbb{Z} \setminus \{0\})$ על־ידי $f(\overline{x}) = \overline{a} \cdot \overline{x}$. נישם לב ש־$f$ אכן לוקחת את $\mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ לעצמו, כי $\overline{0} \neq \overline{a} \cdot \overline{x}$ כי a ו־x לא מתחלקים ב־n. לכן $n \nmid ax$, כי n ראשוני.

הוכחה שנייה (בנייתית). צריך להראות שאם $a \in \mathbb{Z}$ ו־$(a, n) = 1$ אזי קיים $x \in \mathbb{Z}$ כך ש־$ax \equiv 1 \pmod{n}$. ראינו שאם a ו־n זרים, וזה אכן המצב, אזי יש x ו־y ב־$\mathbb{Z}$ כך ש־$ax + ny = 1$, ו־$\overline{x}$ זה יהיה ההפכי של $\overline{a}$.

את x ו־y ניתן למצוא באופן קונסטרוקטיבי על־ידי האלגוריתם של אוקלידס.

דוגמה. נחשב את $(17)^{-1} \pmod{53}$:

$$\begin{aligned} 53 &= 3 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

אז $1 = 17 - 8 \cdot 2 = 17 - 8(53 - 3 \cdot 17) = (-8)53 + (25)17$ ולכן $(17)^{-1} = 25 \pmod{53}$.

טענה 15: $a, b, n \in \mathbb{Z}$. למשוואה $ax = b \pmod{n}$ יש פתרון אם"ם $(a, n) \mid b$. 15.6.2008

במקרה שיש פתרונות, אזי מספר הפתרונות (מודולו n) הוא d; אם x_0 פתרון, אזי רשימת הפתרונות היא $x_0, x_0 + n', x_0 + 2n', \ldots, x_0 + (d-1)n'$ כאשר $n' = \frac{n}{d}$.

הוכחה. נניח $d = (a, n) \mid b$. כזכור, d הוא היוצר של האידיאל $\mathbb{Z}a + \mathbb{Z}n$. אם $d \mid b$, אזי b באידיאל זה, כלומר קיימים $x_0, y_0 \in \mathbb{Z}$ כך ש־$ax_0 + ny_0 = b$, וזה אומר ש־$ax_0 \equiv b \pmod{n}$.

להיפך, נניח שיש פתרון, כלומר יש x_0 כך ש־$ax_0 \equiv b \pmod{n}$. אז $ax_0 = b + ny_0$ ל־$y_0 \in \mathbb{Z}$ כלשהו, ולכן $b = ax_0 + ny_0 \in \mathbb{Z}a + \mathbb{Z}n$ ולכן $d = (a, n) \mid b$ כי d יוצר את האידיאל.

נשים לב שאם x_0 פתרון, אזי גם $x_0 + in'$ פתרון:

$$a(x_0 + in') = ax_0 + ian' = ax_0 + i\frac{an}{d} = ax_0 + i\frac{a}{d}n \equiv ax_0 \pmod{n} \equiv b \pmod{n}$$

כי d מחלק את a ולכן $\frac{a}{d}$ שלם.

קל לראות ש־d פתרונות אלו שונים זה מזה מודולו n. נראה עכשיו שכל פתרון הוא מהצורה הזו (מודולו n): נניח ש־y פתרון. אזי $ay \equiv b \pmod{n}$. יודעים גם כי $ax_0 \equiv b \pmod{n}$, לכן

$a(y-x_0)\equiv 0 \pmod n$. אז $a(y-x_0)=zn$. נחלק ב־d ונקבל $\frac{a}{d}(y-x_0)=z\frac{n}{d}=zn'$.
זה בדיוק אומר ש־y (מודולו n) הוא אחד מהרשימה.

1.5 פונקציית φ של אוילר

1.6.2008 **טענה 16:** $(\mathbb{Z}/n\mathbb{Z})^*=\{t\in\mathbb{Z}/n\mathbb{Z}\mid \exists s\in\mathbb{Z}/n\mathbb{Z}\,:\,ts=1\}$ חבורה ביחס לכפל.

הוכחה. סגירות לכפל ברורה: $(t_1t_2)^{-1}=t_2^{-1}t_1^{-1}$.

פונקציית φ **הגדרה.** עבור n טבעי, נסמן $\varphi(n)=\#\{1\le a<n \mid (a,n)=1\}$ **פונקציית φ של אוילר**.

טענה 17: $|(\mathbb{Z}/n\mathbb{Z})^*|=\varphi(n)$.

הוכחה. איברי החוג $\mathbb{Z}/n\mathbb{Z}$ הם $\overline{0},\overline{1},\ldots,\overline{n-1}$ ($\bar i=i+n\mathbb{Z}$). האיבר $\bar i$ הפיך ב־$\mathbb{Z}/n\mathbb{Z}$ אם"ם $(i,n)=1$: את הכיוון ($\Rightarrow$) ראינו, ו־($\Leftarrow$) $\bar i$ הפיך פירושו קיום $\bar t$ כך ש־$\bar i\cdot\bar t=\overline{1}$. אם כן, נקבל $(i+rn)(t+sn)=1+rn$, כלומר $i\cdot t+n(rt+si+rsn-rt)$, כלומר $(i,n)=1$.

משפט 18 (לגראנז'): G חבורה סופית, $x\in G$. אזי $x^{|G|}=1$.

מסקנה 19: אם $(a,n)=1$ אזי $a^{\varphi(n)}\equiv 1 \pmod n$.

דוגמה. ל־$n=12$, $\varphi(12)=4$: מבין $1,\ldots,12$, רק $1,5,7,11$ זרים ל־12.
כעת נחשב את $7^{29} \pmod{12}$: $7^{29}=7^{4\cdot7+1}=(7^4)^77=1^77=7 \pmod{12}$.

טענה 20: לכל n, $\sum_{d|n}\varphi(d)=n$.

הוכחה. נסתכל במספרים $\frac{1}{n},\frac{2}{n},\ldots,\frac{n}{n}$ ונצמצם ככל יכולתנו. כשנגמור לצמצם, יופיעו במכנים מחלקי n. מחלק נתון d יופיע בדיוק $\varphi(d)$ פעמים, כי לכל $1\le j\le d$ ו־$(j,d)=1$, יופיע ברשימה המספר $\frac{j\cdot\frac{n}{d}}{d\cdot\frac{n}{d}}=\frac{j\cdot\frac{n}{d}}{n}$, ובכל מקום במכנה, מופיע במונה מספר קטן ממנו שזר לו. לכן בסך הכול $\sum_{d|n}\varphi(d)=n$.

טענה 21: לכל p ראשוני, $\varphi(p)=p-1$ ו־$\varphi(p^r)=p^{r-1}(p-1)$.

הוכחה. מבין המספרים $1,\ldots,p^r$, הזרים ל־p^r הם בדיוק הזרים ל־p. מספר הזרים ל־p הוא p^r פחות מספר המתחלקים ב־p, כלומר $p^r-\frac{p^r}{p}=p^r-p^{r-1}=p^{r-1}(p-1)$. $(a,p^r)=1$ אם"ם $(a,p)=1$, לכן $(\mathbb{Z}/p^r\mathbb{Z})^*=\{1\le a\le p^r \mid p\nmid a\}$.

משפט 22 (השאריות הסיני): אם $(m,n)=1$ ו־$a,b\in\mathbb{Z}$, אזי יש פתרון למערכת $x\equiv a \pmod m$, $x\equiv b \pmod n$ ופתרון זה יחיד מודולו $m\cdot n$.

למה 1.22: $(m,n)=1$ אז $\mathbb{Z}/mn\mathbb{Z}\cong\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$.

הוכחה. יש $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\pi_2} \mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}/m\mathbb{Z}$ הומומורפיזמים. לפיכך (π_1, π_2) : $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ הומומורפיזם של חוגים. הומומורפיזם זה חד־חד ערכי כי אם $a \mapsto (0,0)$ אזי $n \mid a$ וגם $m \mid a$, אבל $(m,n) = 1$ ולכן גם $mn \mid a$, כלומר $a \equiv 0 \pmod{mn}$. ההומומורפיזם החד־חד ערכי הוא גם על כיוון ש־$\mathbb{Z}/mn\mathbb{Z}$ ו־$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ מסדר mn. לכן קיים $x \in \mathbb{Z}/mn\mathbb{Z}$ שתמונתו $(a \pmod m, b \pmod n)$, כנדרש ; ברור שאם גם $y \in \mathbb{Z}$ פתרון אז $y \equiv x \pmod{mn}$.

מסקנה 23: אם $n_1, \ldots, n_k$ זרים בזוגות, אזי למשוואות $x \equiv a_i \pmod{n_i}$ יש פתרון והוא יחיד מודולו $n_1 \cdot \ldots \cdot n_k$.

מסקנה 24: אם $n = p_1^{\alpha_1} \cdot \ldots \cdot p_l^{\alpha_l}$ כאשר $p_1, \ldots, p_l$ ראשוניים זרים, $\alpha_i \in \mathbb{N}$, אז $\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{l} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

טענה 25: $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$.

הוכחה. אם $n = p_1^{\alpha_1} \cdot \ldots \cdot p_l^{\alpha_l}$, אז $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_l^{\alpha_l}\mathbb{Z})^*$. לכן נקבל $\varphi(n) = \prod_{i=1}^{l} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{l}(p_i - 1)p^{\alpha_i - 1} = n\prod_{i=1}^{l}(1 - \frac{1}{p_i})$.

דוגמה.
$$\varphi(12) = 12(1 - \tfrac{1}{2})(1 - \tfrac{1}{3}) = 12 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} = 4$$
$$\varphi(100) = 100(1 - \tfrac{1}{2})(1 - \tfrac{1}{5}) = 100 \cdot \tfrac{1}{2} \cdot \tfrac{4}{5} = 40$$

פונקציה של תורת המספרים

הגדרה. פונקציה $f : \mathbb{N} \to \mathbb{N}$ נקראת **פונקציה של תורת המספרים** אם לכל $m, n \in \mathbb{N}$ כך ש־$(m,n) = 1$ היא מקיימת $f(mn) = f(m)f(n)$.

דוגמה. פונקציית φ היא פונקציה של תורת המספרים.

1.6 מספרים מושלמים

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

דוגמה. $\sigma(p) = 1 + p$; $\sigma(1) = 1$; $\sigma(2) = 3$; $\sigma(4) = 7$; $\sigma(6) = 1 + 2 + 3 + 6 = 12$; $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$.

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

דוגמה. 6 ו־28 מספרים מושלמים.

נשים לב ש־$6 = 2 \cdot 3 = 2(2^2 - 1)$, $28 = 2^2 7 = 2^2(2^3 - 1)$. היה נחמד אם גם $120 = 2^3(2^4 - 1)$ היה מושלם, אבל $\sigma(120) \neq 240$. עם זאת, $496 = 2^4(2^5 - 1)$ מושלם ; מחלקיו הם $1, 2, 4, 8, 16, 31, 31 \cdot 2, 31 \cdot 4, 31 \cdot 8, 31 \cdot 16$ וסכומם הוא $31 + 31 \cdot 31 = 32 \cdot 31 = 2 \cdot 16 \cdot 31 = 2 \cdot 496$.

טענה 26: אם $2^n-1=p$ ראשוני, אזי $K=2^{n-1}(2^n-1)$ מספר מושלם.

הוכחה. המחלקים של k הם

$$\begin{aligned} 1+2+4+\ldots+2^{n-1}+ & \\ +p(1+2+\ldots+2^{n-1}) &= \tfrac{2^n-1}{2-1}+p(2^n-1) \\ &= p+p^2=p(p+1)=(2^n-1)2^n \\ &= 2\cdot 2^{n-1}(2^n-1)=2k \end{aligned}$$

למה 27: אם 2^n-1 ראשוני, אזי n ראשוני.

סיפור. אוילר הוכיח שכל מספר מושלם זוגי הוא מהצורה $2^{p-1}(2^p-1)$ כאשר p ראשוני ו־2^p-1 ראשוני (כלומר, ראשוני של מרסן). עם זאת, עדיין לא ידוע האם בכלל יש מספר מושלם אי־זוגי והאם יש אינסוף מספרים מושלמים זוגיים (או, באופן שקול, האם יש אינסוף ראשוני מרסן).

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

מיהם המספרים המושלמים כפלית? אם n איננו ראשוני ואיננו מהצורה $n=p^2$, יש ל־n מחלק d כך ש־$d\neq\frac{n}{d}$. אז $1,d,\frac{n}{d},n$ מחלקים אותו. אם המספר מושלם כפלית, אלו כל מחלקיו כי מכפלתם n^2. אם כן, המספרים המושלמים כפלית הם מהצורה $n=pq$ (p ו־q ראשוניים) או $n=p^3$ (p ראשוני).

אם כן, שאלת המספרים המושלמים כפלית הרבה יותר אלמנטרית, אך שהשאלה עצמה דומה מאוד.

1.7 מבנה $(\mathbb{Z}/n\mathbb{Z})^*$

15.6.2008 כזכור, $(\mathbb{Z}/n\mathbb{Z})^*=\{a\in\mathbb{Z}/n\mathbb{Z}\mid\exists b\in\mathbb{Z}/n\mathbb{Z}:\ ab\equiv 1\}$ חבורה ביחס לכפל מסדר $\varphi(n)$.

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

הגדרה. תהא G חבורה אבלית. נגדיר $\exp(G)=\min\{m\in\mathbb{N}\mid\forall x\in G\quad x^m=1\}$.
(למעשה, $\exp(G)\leq|G|$; $\exp(G)\mid|G|$ – תרגיל.)

טענה 28: אם A חבורה אבלית, אזי A ציקלית אם"ם $\exp(A)=|A|$.

הוכחה. אם A ציקלית אזי $\exp(A)=|A|$ כי יש איבר מסדר $|A|$.

במבנים אלגבריים הוכחנו כי אם A חבורה אבלית סופית, אזי $A\cong C_{m_1}\times C_{m_2}\times\ldots\times C_{m_r}$ כאשר $2\leq m_1\mid m_2\mid\ldots\mid m_r$. אז $|A|=m_1\cdot m_2\cdot\ldots\cdot m_l$ ו־$\exp(A)=m_l$. לכן אם $\exp(A)=|A|$, הרי $m_1\cdot\ldots\cdot m_l=m_l$ ולכן $l=1$, כלומר A חבורה ציקלית מסדר m_l.

תזכורת מתורת השדות: F שדה. (1) אם $f(X)\in F[X]$ אזי $\alpha\in F$ שורש של $f(X)$ אם"ם $X-\alpha\mid f(X)$. (2) אם $\deg f(X)=n$, אזי ל־$f(X)$ לכל היותר n שרשים. (3) אם $f(X),g(X)\in F[X]$ פולינומים מתוקנים ממעלה n כך ש־$f(\alpha_i)=g(\alpha_i)$ עבור i איברים שונים $\alpha_1,\ldots,\alpha_n$, אזי $f(X)=g(X)$.

דוגמה (שימוש נחמד). $X^{p-1}-1 \in \mathbb{F}_p[X]$ שרשיו הם $1,2,3,\ldots,p-1$, ולכן כפולינומים ב־$\mathbb{F}_p[X]$, $X^{p-1}-1=(X-1)(X-2)(X-3)\cdot\ldots\cdot(X-(p-1))$ כי שניהם מתוקנים ושניהם ממעלה $p-1$ עם אותם $p-1$ שרשים.

מסקנה 29 (וילסון): לכל p ראשוני, $(p-1)! \equiv -1 \pmod p$.

הוכחה. ל־$p=2$, הטענה ברורה; ל־$p>2$, נציב 0 בשני האגפים: $-(p-)\cdot\ldots\cdot(-2)(-1) \equiv -1 \pmod p$ ((1, כלומר $(p-1)! \equiv (-1)^{p-1} \equiv -1$. אך $p>2$ כש־$(-1)^{p-1} \equiv 1$ ראשוני, ולכן $(p-1)! \equiv -1 \pmod p$.

טענה 30: אם n לא ראשוני ולא מהצורה $n=p^2$, אזי $(n-1)! \equiv 0 \pmod n$.

טענה 31: $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ ציקלית מסדר $p-1$, כלומר $((\mathbb{Z}/p\mathbb{Z})^*,\cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z},+)$, ל־$p$ ראשוני.

דוגמה. ל־$(\mathbb{Z}/11\mathbb{Z})^*$ יש $\varphi(10)$ יוצרים.[7] מציאתם היא בעיה קשה. 2 הוא יוצר: מקבלים $\{2,4,8,5,10,9,7,3,6,1\}$; אך 3 אינו יוצר: $\{3,9,5,4,1\}$. כלומר, 2 פרימיטיבי מודולו 11, אך 3 לא.

דוגמה ($n=8$). $(\mathbb{Z}/n\mathbb{Z})^*=\{1,3,5,7\}$. בחבורה זו $3^2=1$, $5^2=1$ ו־$7^2=1$, לכן $(\mathbb{Z}/8\mathbb{Z})^* \cong C_2 \times C_2$ (כאשר C_m היא החבורה הציקלית מסדר m).

הוכחה. נטען ש־$\exp(\mathbb{F}_p^*)=p-1$ ואז ציקלית לפי טענה קודמת. אחרת, $\exp(\mathbb{F}_p^*)=m \lneq p-1$ ואז יש $p-1$ איברים שונים המקיימים $x^m=1$, כלומר לפולינום X^m-1 יש $p-1>m$ שרשים, בסתירה.

טענה חזקה יותר: אם F שדה כלשהו ו־A חבורה חלקית סופית של F^*, אזי A ציקלית.

משפט 32: אם p ראשוני גדול מ־2, אזי 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 טענה קודמת). נתבונן ב־a^{p-1}. יודעים ש־$a^{p-1} \equiv 1 \pmod p$. מה לגבי $a^{p-1} \pmod{p^2}$?

למה 1.32: יש $a \in \mathbb{Z}$ פרימיטיבי מודולו p (כלומר $a^{p-1} \equiv 1 \pmod p$ ולא קודם) אבל $a^{p-1} \not\equiv 1 \pmod{p^2}$.

הוכחה. אם a פרימיטיבי שבחרנו מקיים זאת – גמרנו. אם לא, נתבונן ב־$a+p$: הוא פרימיטיבי מודולו p, אבל $(a+p)^{p-1}=a^{p-1}+\binom{p-1,1}{a}^{p-2}p+p^2y$ כאשר $y \in \mathbb{Z}$. אם כן, נקבל $(a+p)^{p-1} \equiv a^{p-1}+(p-1)a^{p-2}p \mod p^2$. נטען ש־$a^{p-1}+(p-1)a^{p-2}p$ אינו 1 מודולו p^2: זאת כי $a^{p-1} \equiv 1 \pmod{p^2}$ ו־$(p-1)a^{p-2}p \not\equiv 0 \pmod{p^2}$.

למה 2.32: יהי $b \in \mathbb{Z}$ כך ש־$b \equiv 1 \pmod p$, $b \not\equiv 1 \pmod{p^2}$. אזי הסדר של b מודולו p^l הוא בדיוק p^{l-1}.

[7] בהינתן הטענה, נסתכל על החבורה הכפלית מסדר $p-1$; מספר היוצרים של חבורה מסדר $p-1$ הוא $\varphi(p-1)$.

הוכחה. $(1+xp)^{p^{l-1}} = 1+\binom{p^{l-1}}{1}1^*xp+\ldots \equiv 1 \pmod{p^l}$. אז $p \nmid x$ ו־$b = 1+xp$
לכן מספיק להראות ש־$(1+xp)^{p^{l-2}} \not\equiv 1 \pmod{p^l}$. ואכן,
$$\binom{p^{l-2}}{1}xp + p^l(*) = 1 + p^{l-2}xp \pmod{p^l} \not\equiv 1 \pmod{p^l}.$$ 1^*+

ניישם את הלמה עבור $b = a^{p-1}$ שמצאנו קודם. נסיק מכאן שהסדר של a^{p-1} ממקודם הוא $(p-1)p^{l-1}$, וזה מסיים את הוכחת המשפט.

מהלמה הראשונה, $(\mathbb{Z}/p^2\mathbb{Z})^*$ היא ציקלית: ניקח a כמו בלמה, ואז $a^{p-1} \not\equiv 1 \pmod{p^2}$. ההעתקה $\pi : (\mathbb{Z}/p^2\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ היא העתקה מחבורה מסדר $p(p-1)$ לחבורה מסדר $p-1$, והיא על כי איבר שזר ל־p זר גם ל־p^2. יש לנו $a \in \mathbb{Z}/p^2\mathbb{Z}$ שהוא פרימיטיבי מודולו p. כלומר, תמונת a ב־$(\mathbb{Z}/p\mathbb{Z})^*$ יוצרת את $(\mathbb{Z}/p\mathbb{Z})^*$.

$a^{p-1} \in \ker\pi$ אבל אינו איבר היחידה שם כי בחרנו את a כך ש־$a^{p-1} \not\equiv 1 \pmod{p^2}$. אבל הגרעין מסדר p, לכן a^{p-1} יוצר אותו. בסך הכול נובע ש־$o(a) = p(p-1)$.[8] מצאנו איבר מסדר החבורה, ולכן היא ציקלית.

1.8 חוק ההדדיות הריבועית של גאוס

גאוס גילה את חוק ההדדיות הריבועית ב־1801: זהו אחד משיאי המתמטיקה של כל הזמנים, שפתח פתח להרבה מאוד עבודה במאות ה־19 וה־20 ועד היום.

22.6.2008 p ראשוני גדול מ־2; $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ שדה השאריות מודולו p. הוכחנו ש־$\mathbb{F}_p^*$ ציקלית מסדר $p-1$.

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

לא תמיד קל למצוא יוצר ל־$\mathbb{F}_p^*$. שאלה נוספת, שבה נתמקד: מתי $a \equiv x^2 \pmod{p}$ פתיר?

הגדרה. a ייקרא **שארית ריבועית** ממודולו הראשוני p אם למשוואה $a \equiv x^2 \pmod{p}$ יש פתרון (אחרת, **אי־שארית**).

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

סמל לז׳נדר

הגדרה. סמל לז׳נדר:
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \equiv x^2 \pmod{p} \\ -1 & a \not\equiv x^2 \pmod{p} \end{cases}$$

משפט 33 (חוק ההדדיות הריבועית של גאוס):
א. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;
ב. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;
ג. אם p ו־q ראשוניים אי־זוגיים, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

[8] a^{p-1} בגרעין ואינו טריוויאלי; לכן הוא מסדר p, כי הגרעין ציקלי מסדר p.

למה 34: תהי H חבורה ציקלית מסדר זוגי m. אזי בדיוק מחצית מאיבריה הם ריבועים. $a = x^2 \iff a^{\frac{m}{2}} = 1$, ואם תנאי זה לא מתקיים, אזי $a^{\frac{m}{2}}$ הינו האיבר היחידי מסדר 2 בחבורה.

הוכחה. $H = \{1, g, g^2, \ldots, g^{m-1}\}$, $g^m = 1$ (עבור g יוצר). הריבועים הם איברים מהצורה $a = x^2 = (g^k)^2 = g^{2k}$ ולכן הריבועים הינם $1, g^2, g^4, \ldots, g^{m-2}$.

אם $a = x^2$, אזי $a^{\frac{m}{2}} = x^m = 1$. אם $a \neq x^2$, אזי $a = g^k$ עבור k אי־זוגי, ואז מתקיים $a^{\frac{m}{2}} = g^{\frac{km}{2}} \neq 1$ 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.

מסקנה 35: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod p$.

הוכחה. אם a שארית ריבועית, $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. אחרת, $a^{\frac{p-1}{2}} \neq 1$, אבל הוא האיבר היחידי של $\mathbb{F}_p^*$ מסדר 2, ואיבר זה הוא -1.

מסקנה 36 (מן המסקנה): $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$;

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

דוגמה. מהו $(\frac{365}{101})$? כלומר, מהם הפתרונות ל־$365 \equiv x^2 \pmod{101}$? ניעזר במה שהוכחנו:
$(\frac{365}{101}) = (\frac{62}{101}) = (\frac{2}{101})(\frac{31}{101}) = -1 \cdot (\frac{101}{31})(-1)^{\frac{100}{2} \cdot \frac{30}{2}} = -1 \cdot (\frac{8}{31}) = -1(\frac{2}{31})^3 = -1$

למה 37: תהי H חבורה סופית ויהי $\chi : H \to \mathbb{C}^*$ קרקטר כפלי[9]. אם $\chi \neq 1$, אזי $S = \sum_{h \in H} \chi(h) = 0$.

הוכחה. $\chi \neq 1$, לכן ישנו $g \in H$ עבורו $\chi(g) \neq 1$. נכפול בו את שני אגפי השוויון: נקבל $\chi(g) \cdot S = \sum_{h \in H} \chi(g)\chi(h) = \sum_{h \in H} \chi(gh) = S$. אבל $\chi(g) \neq 1$, ולכן $S = 0$.

דוגמה (מחיי $\mathbb{F}_p$). אם נסמן $\zeta = e^{\frac{2\pi i}{p}}$, אזי $\sum_{a=0}^{p-1} \zeta^a = 0$, כי $a \mapsto \zeta^a$ הינו קרקטר של $(\mathbb{F}_p, +)$: $a + b \mapsto \zeta^{a+b} = \zeta^a \zeta^b$.
ב־$(\mathbb{F}_p^*, \cdot)$, $1, 0 \neq a \mapsto (\frac{a}{p}) = \pm 1$, $\sum_{a=1}^{p-1} (\frac{a}{p}) = 0$.[10]

נתבונן בחוג $\mathbb{Z}[\zeta]$, כאשר $\zeta = e^{\frac{2\pi i}{q}}$.[11] מתקיים $0 = \zeta^q - 1 = (\zeta - 1)(\zeta^{q-1} + \ldots + \zeta + 1)$ ולכן $\zeta^{q-1} = -1 - \zeta - \zeta^2 - \ldots - \zeta^{q-2}$. לכן ניתן לכתוב $0 = 1 + \zeta + \ldots + \zeta^{q-1} + \zeta^{q-2}$, ומכאן $\mathbb{Z}[s] = \mathbb{Z} + \mathbb{Z} \cdot \zeta + \ldots + \mathbb{Z} \cdot \zeta^{q-2}$. זהו חוג קומוטטיבי וגם סכום ישר: $1, \zeta, \ldots, \zeta^{q-2}$ הם בסיס מעל $\mathbb{Z}$.

נעיר כי עובדת היות $1, \zeta, \zeta^2, \ldots, \zeta^{q-2}$ בלתי־תלויים מעל $\mathbb{Q}$ שקולה לעובדת היות הפולינום $f(x) = x^{q-1} + \ldots + x + 1$ הפולינום המינימלי של ζ מעל $\mathbb{Q}$ (ממבנים 2, תוך שימוש בקריטריון אי־הפריקות של אייזנשטיין).

[9] כלומר, הומומורפיזם ל־$\mathbb{C}^*$: $\chi(h_1 h_2) = \chi(h_1)\chi(h_2)$.
[10] זו הוכחה אחרת שמחצית האיברים הם שראיות והמחצית האחרת – אי־שאריות.
[11] הוכחה אלמנטרית לחלוטין ניתן למצוא בספר של Levesque.

מסקנה 38: $\mathbb{Z}[\zeta] \cap \mathbb{Q} = \mathbb{Z}$. (נובע מיחידות ההצגה.)

סכום גאוס: $G = \sum_{a=1}^{q-1}(\frac{a}{q})\zeta^a$, $\zeta = e^{\frac{2\pi i}{q}}$.[12]
$G \in \mathbb{Z}[\zeta]$. נחשב את G^2:

$$\begin{aligned} G^2 &= \sum_{a=1}^{q-1}\sum_{b=1}^{q-1}(\tfrac{a}{q})(\tfrac{b}{q})\zeta^{a+b} \\ &= \sum_{a=1}^{q-1}\sum_{b=1}^{q-1}(\tfrac{a}{q})(\tfrac{ab}{q})\zeta^{a+ab} \\ &= \sum_{b=1}^{q-1}(\tfrac{b}{q})\sum_{a=1}^{q-1}\zeta^{(1+b)a} \\ &= \sum_{b=1}^{q-1}(\tfrac{b}{q})\cdot\begin{cases} q-1 & b=q-1 \\ -1 & b\neq q-1 \end{cases} \end{aligned}$$

($\zeta^{1+b} = \eta$ שורש יחידה מסדר q שונה מ־1, ולפי הלמה, $\sum_{a=0}^{q-1}\eta^a = 0$.)
אם כן, $G^2 = (\frac{-1}{q})q - \sum_{b=1}^{q-1}(\frac{b}{q}) = (\frac{-1}{q})q = (-1)^{\frac{q-1}{2}}q$.[13]
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 $x - y \in p\mathbb{Z}$, ולכן $\frac{x-y}{p} \in \mathbb{Z}[\zeta] \cap \mathbb{Q} = \mathbb{Z}$ ולכן $x \equiv y \pmod p$ מתלכד עם המשמעות הישנה.
$(x+y)^p \equiv x^p + y^p \pmod p$ (נובע מהעובדה ש־$p \mid \binom{p}{i}$ ל־$i = 1, \ldots, p-1$). כעת,
$G^p \equiv \sum_{a=1}^{q-1}(\frac{a}{q})\zeta^{ap} \pmod p$.
תהי $\bar{p}$ שארית מודולו q כך ש־$p\bar{p} \equiv 1 \pmod q$. אז

$$G^p = \sum_{a=1}^{q-1}(\tfrac{a\bar{p}}{q})\zeta^a = (\tfrac{\bar{p}}{q})G = (\tfrac{p}{q})^{-1}G = (\tfrac{p}{q})G$$

ולכן $G^p \equiv (\frac{p}{q})G \pmod p$. מצד שני,

$$\begin{aligned} G^p &= G(G^2)^{\frac{p-1}{2}} \\ &= G((-1)^{\frac{q-1}{2}}q)^{\frac{p-1}{2}} \\ &= (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}q^{\frac{p-1}{2}}G \\ &\equiv (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}(\tfrac{q}{p})G \pmod p \end{aligned}$$

קיבלנו $G(\frac{p}{q}) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{q}{p})G$. נשים לב כי $G\bar{G} = q$ ונכפול ב־$\bar{G}$:
$(\frac{p}{q})q \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{q}{p})q \pmod p$.
$(q,p) = 1$, לכן $(\frac{p}{q}) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{q}{p}) \pmod p$. שני האגפים הם ± 1, לכן הם גם שווים.

כעת נחשב את $(\frac{2}{p})$: נשתמש בחוג $\mathbb{Z}[i]$. $(1+i)^p \equiv 1 + i^p \pmod p$, ומצד שני, גם נקבל $(1+i)^p = (1+i)[(1+i)^2]^{\frac{p-1}{2}} = (1+i)(2i)^{\frac{p-1}{2}} \equiv (1+i)i^{\frac{p-1}{2}}(\frac{2}{p}) \pmod p$. אם כן,

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

[12] במתמטיקה קוראים לכל סכום מהצורה $\sum_{a\in\mathbb{F}_q^*}\chi(a)\psi(a)$ כאשר $\psi(a+b) = \psi(a)\psi(b)$ (קרקטר חיבורי) ו־$\chi(ab) = \chi(a)\chi(b)$ (קרקטר כפלי) **סכום גאוס**, אבל זה לא סכום גאוס המקורי.

[13] הערה לידעי ח״ן: $\mathbb{Q}(\zeta) \subsetneq \mathbb{Q}(\sqrt{(-1)^{\frac{q-1}{2}}q})$, שדה מדרגה 2 בתוך שדה מדרגה $q-1$.

עוד הוכחה ל־$\mathbb{Z}[\zeta]\cap\mathbb{Q}=\mathbb{Z}$, בלי שימוש באייזנשטיין:

$$\mathbb{Z}\cdot 1+\mathbb{Z}\cdot\zeta+\ldots+\mathbb{Z}\cdot\zeta^{q-2}=\mathbb{Z}[\zeta]\subseteq\mathbb{Q}[\zeta]=\mathbb{Q}\cdot 1+\mathbb{Q}\zeta+\ldots+\mathbb{Q}\zeta^{q-2}$$

גם אם אלה לא בסיס, זה מרחב וקטורי ממימד סופי מעל $\mathbb{Q}$. יהי $\alpha_1,\ldots,\alpha_d$ בסיס. בלי הגבלת הכלליות, $\alpha_1=1$. יהי N טבעי המשמש מכנה משותף לכל המכנים המופיעים בפיתוחים של $1,\zeta,\ldots,\zeta^{q-2}$ כצירופים לינאריים של $\alpha_1,\ldots,\alpha_d$. אז $\mathbb{Z}[\zeta]\subseteq\frac{1}{N}(\mathbb{Z}\alpha_1\oplus\mathbb{Z}\alpha_2\oplus\ldots\oplus\mathbb{Z}\alpha_d)$. בפרט, $\mathbb{Z}[\zeta]\cap\mathbb{Q}\subseteq\frac{1}{N}\mathbb{Z}$ (שהרי $\alpha_1=1$). אבל $\mathbb{Z}[\zeta]\cap\mathbb{Q}$ סגור לכפל, והתת־חוג היחידי של $\frac{1}{N}\mathbb{Z}$ הינו $\mathbb{Z}$.

29.6.2008 התעניינו במבנה החבורה $G=(\mathbb{Z}/p^n\mathbb{Z})^*$; היה לנו משפט שאמר שאם p אי־זוגי, אזי G חבורה ציקלית מסדר $(p-1)p^{n-1}$. ל־$p=2$, $(\mathbb{Z}/2^n\mathbb{Z})^*\cong C_2\times C_{2^{n-2}}$. (לא נוכיח ל־$p=2$; דומה להוכחה ל־$p$ אי־זוגי.)

עובדה מחבורות: בחבורה ציקלית כפלית מסדר n, אם n אי־זוגי, כל איבר הוא ריבוע, ואם n זוגי, בדיוק מחצית מאיברי החבורה הם ריבועים.

טענה 39: נניח $m=2^ep_1^{e_1}\cdot\ldots\cdot p_l^{e_l}$ כש־p_i ראשוניים אי־זוגיים שונים, ויהי $a\in\mathbb{Z}$, $(a,m)=1$. אזי למשוואה $x^2\equiv a\pmod m$ יש פתרון אם"ם מתקיים (א) לכל $i=1,\ldots,l$, a ריבוע מודולו p_i (כלומר, יש פתרון ל־$x^2\equiv a\pmod{p_i}$), ו־(ב) אם $e=2$ אזי $a\equiv 1\pmod 4$, ואם $e\geq 3$ אזי $a\equiv 1\pmod 8$.

תזכורת: p ראשוני, $(a,p)=1$ אז a ריבוע מודולו p אם"ם $a^{\frac{p-1}{2}}=1$.

יהי p ראשוני אי־זוגי. נתבונן ברשימת המספרים

$$Y=\{-\frac{p-1}{2},-\frac{p-1}{2}+1,\ldots,-2,-1,1,2,3,\ldots,\frac{p-1}{2}\}$$

אלו נציגי כל מחלקות הקונגרואנציה מודולו p הזרות ל־p.

למה 40 (גאוס): יהי $a\in\mathbb{Z}$ כך ש־$(a,p)=1$. נתבונן בשאריות החלוקה ב־p בתוך Y של הקבוצה הבאה: $X=\{1\cdot a,2\cdot a,\ldots,\frac{p-1}{2}a\}$. נסמן ב־$\mu$ את מספר השאריות השליליות בקבוצה זו. אזי $(\frac{a}{p})=(-1)^\mu$.

הוכחה. נסמן ב־$m_1,m_2,\ldots,m_{\frac{p-1}{2}}$ את שאריות החלוקה של X מתוך הקבוצה Y.

דוגמה. ל־$p=11$, $a=3$, $X=\{3,6,9,12,15\}$ ושאריות X ב־Y הן $\{3,-5,-2,1,4\}$.

נציין שאם $i\neq j$ אזי $m_i\neq m_j$, כי $(a,p)=1$ ולכן הכפלה ב־a זו תמורה על המחלקות מודולו p. יתר על כן, גם לא אפשרי $m_i=|m_j|$, כי אם $m_i=-m_j$, $ia\equiv -ja\pmod p$, $(i+j)a\equiv 0\pmod p$ ומאחר ש־$(a,p)=1$, נובע ש־$i+j\equiv 0\pmod p$, אך זה לא ייתכן כי $1\leq i,j\leq\frac{p-1}{2}$.

נסמן $n_i=|m_i|$. $n_1,n_2,\ldots,n_{\frac{p-1}{2}}$ כולם שונים ובין 1 ל־$\frac{p-1}{2}$, ולכן זו בדיוק הקבוצה $1,2,\ldots,\frac{p-1}{2}$ בסדר אחר.

אז $m_1m_2\cdot\ldots\cdot m_{\frac{p-1}{2}}=(-1)^\mu n_1n_2\cdot\ldots\cdot n_{\frac{p-1}{2}}=(-1)^\mu 1\cdot 2\cdot\ldots\cdot\frac{p-1}{2}$.

$m_i = i \cdot a \pmod p$ ולכן $(\frac{p-1}{2})! \equiv \prod m_i \equiv (-1)^{\mu}(\frac{p-1}{2})!$. אז $a^{\frac{p-1}{2}} \cdot \prod_{i=1}^{\frac{p-1}{2}} i = \prod_{i=1}^{\frac{p-1}{2}} (ia) \overset{p}{\equiv}$
$(\frac{p-1}{2})! = (-1)^{\mu}(\frac{p-1}{2})!\, a^{\frac{p-1}{2}}$ ולכן[14] $a^{\frac{p-1}{2}} = (-1)^{\mu}$, ותמיד $(\frac{a}{p}) = a^{\frac{p-1}{2}}$.

טענה 41: 2 הוא שארית ריבועית מודולו p ראשוני (אי־זוגי) אם"ם $p \equiv \pm 1 \pmod 8$.

הוכחה. μ הוא בעצם מספר האיברים בסדרה $2 \cdot 1, 2 \cdot 2, \ldots, 2 \cdot i, \ldots, 2 \cdot \frac{p-1}{2}$ שגדולים מ־$\frac{p}{2}$.
יהי m השלם המקיים $2m \leq \frac{p-1}{2}$ ו־$2(m+1) > \frac{p}{2}$. אז ברור ש־$\mu = \frac{p-1}{2} - m$.
אם $p = 8k+1$, $\frac{p-1}{2} = 4k$ ואז $m = 2k$ ו־$\mu = 4k - 2k = 2k$ זוגי.
אם $p = 8k-1$, $\frac{p-1}{2} = \frac{8k-2}{2} = 4k-1$, $m = 2k-1$ ואז $\mu = (4k-1)-(2k-1) = 2k$ זוגי.
אם $p = 8k+3$, $\frac{p-1}{2} = \frac{8k+2}{2} = 4k+1$, $m = 2k$ ואז $\mu = 4k+1-2k = 2k+1$.
אם $p = 8k+5$, $\frac{p-1}{2} = \frac{8k+4}{2} = 4k+2$, $m = 2k+1$ ואז $\mu = 4k+2-(2k+1) = 2k+1$ אי־זוגי.

משפט 42 (ההדדיות הריבועית): p ו־q ראשוניים אי־זוגיים; $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

למה 1.42: יהיו p ראשוני אי־זוגי ו־a שלם אי־זוגי כך ש־$a \nmid p$. נסמן $\nu = \sum_{m=1}^{\frac{p-1}{2}} \lfloor \frac{ma}{p} \rfloor$.
אזי $(\frac{a}{p}) = (-1)^{\nu}$.

הוכחה. צריך להראות ש־$\nu \equiv \mu \pmod 2$ בסימונים הקודמים.
$ma = \lfloor \frac{ma}{p} \rfloor \cdot p + r$ ו־$1 \leq r < p$ השארית של חלוקת ma ב־p.
$\sum_{m=1}^{\frac{p-1}{2}} ma = \sum_{m=1}^{\frac{p-1}{2}} \lfloor \frac{ma}{p} \rfloor p + \sum_{j=1}^{\mu} b_j + \sum_{j=1}^{t} l_j$ ($t + \mu = \frac{p-1}{2}$).
$l_1, l_2, \ldots, l_t, p-b_1, p-b_2, \ldots, p-b_\mu$ נמצאים בין 1 ל־$\frac{p-1}{2}$, וכמו בהוכחה הקודמת, מהווים סידור אחר של הקבוצה $\{1, 2, \ldots, \frac{p-1}{2}\}$.

$$\begin{aligned} a(\tfrac{\frac{p-1}{2} \cdot \frac{p-1}{2}+1}{2}) &= \textstyle\sum_{m=1}^{\frac{p-1}{2}} \lfloor \frac{ma}{p} \rfloor + \sum_{j=1}^{\mu} b_j + \sum_{j=1}^{t} l_j \\ &= p \cdot \nu + (1 + 2 + \ldots + \tfrac{p-1}{2}) - \mu p + 2\textstyle\sum_{j=1}^{\mu} b_j \\ &= p(\nu - \mu) + \frac{\frac{p-1}{2} \cdot (\frac{p-1}{2}+1)}{2} + 2\textstyle\sum_{j=1}^{\mu} b_j \end{aligned}$$

מכאן, $(a-1)\frac{\frac{p-1}{2} \cdot \frac{p-1}{2}+1}{2} = p(\nu - \mu) + 2\sum b_i$. $a-1$ זוגי ו־$\frac{\frac{p-1}{2} \cdot \frac{p-1}{2}+1}{2}$ שלם, לכן נקבל $p(\nu - \mu) \equiv 0 \pmod 2$ ומכאן $\nu - \mu \equiv 0 \pmod 2$.

הוכחה (עכשיו אלמנטרית לגמרי). על־פי הלמה, מספיק להראות כי

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

נסתכל במלבן $\{(x,y) \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\} = Z$. מספר הנקודות בו הוא $\frac{p-1}{2} \cdot \frac{q-1}{2}$.
תהא A התת־קבוצה של Z של הזוגות (x,y) עם $yp < xq$ ותהא B התת־קבוצה של Z של הזוגות $yp > xq$. (לא ייתכן $yp = xq$.)

[14] מותר לצמצם כי $(\frac{p-1}{2}!)$ זר ל־p.

בהינתן x, כדי לקבל $(x,y) \in A$ צריך $yp < xq$, כלומר $y < \frac{xq}{p}$, כלומר $1 \le y \le \lfloor \frac{xq}{p} \rfloor$.
אז $|A| = \sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{xq}{p} \rfloor$. באופן זהה, $|B| = \sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{yp}{q} \rfloor$.

6.7.2008 **דוגמה.** רוצים לחשב את $(\frac{561}{659})$. יודעים ש־$561 = 3 \cdot 11 \cdot 17$, ונשים לב גם כי $659 \equiv 3 \pmod 4$ ומכאן $\frac{659-1}{2}$ אי־זוגי. אז

$$\begin{aligned}
(\tfrac{561}{659}) &= (\tfrac{3}{659}) \cdot (\tfrac{11}{659}) \cdot (\tfrac{17}{659}) \\
&= (\tfrac{659}{3})(-1)^{\frac{659-1}{2} \cdot \frac{3-1}{2}} (\tfrac{659}{11})(-1)^{\frac{659-1}{2} \cdot \frac{11-1}{2}} (\tfrac{659}{17})(-1)^{\frac{659-1}{2} \cdot \frac{17-1}{2}} \\
&= (\tfrac{2}{3})(-1)(\tfrac{-1}{11})(-1)(\tfrac{13}{17}) \\
&= (-1)(-1)(-1)(-1)(\tfrac{17}{13})(-1)^{\frac{17-1}{2} \cdot \frac{13-1}{2}} \\
&= (-1)^4(\tfrac{4}{13}) \cdot 1 = 1
\end{aligned}$$

כלומר, 561 שארית ריבועית מודולו 659.

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

טענה 43: p ראשוני אי־זוגי. $(\frac{3}{p}) = 1$ אם"ם $p \equiv \pm 1 \pmod{12}$.

הוכחה. $(\frac{p}{3})(-1)^{\frac{p-1}{2}} = (\frac{p}{3})(-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} = (\frac{3}{p})$. מתי $(\frac{3}{p}) = 1 = (\frac{p}{3})(-1)^{\frac{p-1}{2}}$? זה קורה אם"ם (א) $(\frac{p}{3}) = 1$ וגם $\frac{p-1}{2}$ זוגי, או (ב) $(\frac{p}{3}) = -1$ וגם $\frac{p-1}{2}$ אי־זוגי.

מקרה (א) אומר ש־$p \equiv 1 \pmod 3$ וגם $p \equiv 1 \pmod 4$. או, באופן שקול, $p \equiv 1 \pmod{12}$ (על־פי משפט השאריות הסיני).

מקרה (ב) אומר ש־$p \equiv 2 \pmod 3$ וגם $p \equiv 3 \pmod 4$. או, באופן שקול, $p \equiv -1 \pmod{12}$ (לפי הסיני).

טענה 44: $(\frac{5}{p}) = 1$ אם"ם $p \equiv 1, 3, 7, 9 \pmod{20}$.

טענה 45: יהי $0 \ne a \in \mathbb{Z}$. אזי a שארית ריבועית לאינסוף ראשוניים.

סמל יעקובי **הגדרה.** בהינתן a ו־b כך ש־b שלם חיובי אי־זוגי ו־a שלם כלשהו, נכתוב $b = p_1 \cdot \ldots \cdot p_l$ מכפלת ראשוניים (לאו דווקא שונים) ונגדיר $(\frac{a}{p_l}) \cdot \ldots \cdot (\frac{a}{p_2}) \cdot (\frac{a}{p_1}) = (\frac{a}{b})$ – **סמל יעקובי**.

תכונות סמל יעקובי:

1. $(\frac{a_1}{b}) = (\frac{a_2}{b})$ אם $a_1 \equiv a_2 \pmod b$;
2. $(\frac{a_1 a_2}{b}) = (\frac{a_1}{b})(\frac{a_2}{b})$;
3. $(\frac{a}{b_1 b_2}) = (\frac{a}{b_1})(\frac{a}{b_2})$.

אזהרה חמורה: אם $(\frac{a}{b}) = -1$, אזי a אינו שארית ריבועית מודולו b (אין פתרון למשוואה $x^2 \equiv a \pmod b$). עם זאת, ייתכן $(\frac{a}{b}) = 1$ ובכל זאת a לא שארית ריבועית מודולו b. למשל, $(\frac{2}{15}) = 1 = (-1)(-1) = (\frac{2}{5})(\frac{2}{3})$, אך 2 אינו שארית ריבועית מודולו 15.

משפט 46: אם a ו־b שלמים חיוביים ואי־זוגיים, אזי $(\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$. (נשתמש בכך ש־$\frac{s-1}{2} + \frac{r-1}{2} \equiv \frac{rs-1}{2} \pmod 2$ ל־r ו־s אי־זוגיים.)

דוגמה. בלי לפרק לגורמים: $(\frac{561}{659}) = (\frac{659}{561})(-1)^{\frac{561-1}{2}\cdot\frac{659-1}{2}} = (\frac{98}{561}) = (\frac{2\cdot 49}{561}) = (\frac{2}{561})\cdot(\frac{49}{561})$

הוכחה. צריך למצוא אינסוף ראשוניים q כך ש־$(\frac{a}{q}) = 1$. נכתוב $a = 2^e p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_l^{e_l}$. אז $(\frac{a}{q}) = (\frac{2}{q})^e(\frac{p_1}{q})^{e_1}\cdot\ldots\cdot(\frac{p_l}{q})^{e_l}$. מתוך זה ברור שאפשר להניח ש־a הוא מהצורה $a = 2^e l_1\cdot\ldots l_s$, כאשר $e = 0, 1$ ו־$l_1, \ldots, l_s$ ראשוניים.

צריך, אם כן, למצוא אינסוף q־ים כך ש־$(\frac{2}{q})^e(\frac{l_1}{q})\cdot\ldots\cdot(\frac{l_s}{q}) = 1$. נניח ש־$q \equiv 1 \pmod 8$. $(\frac{q}{l_i}) = (\frac{l_1}{q}) = (-1)^{\frac{q-1}{2}\cdot\frac{l_i-1}{2}}\cdot(\frac{q}{l_i})$. מאחר ש־$q \equiv 1 \pmod 8$, $\frac{q-1}{2}$ זוגי ולכן נדרוש גם ש־$q \equiv 1 \pmod{l_i}$ לכל $i = 1, \ldots, s$. בסך הכול, $q \equiv 1 \pmod{8\cdot l_1\cdot\ldots\cdot l_s}$. על־פי משפט דיריכלה, יש אינסוף q־ים שיקיימו זאת.

1.9 מבחני ראשוניות

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. $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65,537$. אלה ראשוניים, אך זו שאלה פתוחה האם יש אינסוף (או סתם עוד) ראשוניי פרמה.

משפט 47 (קריטריון הראשוניות של Pépin): F_n ראשוני אם"ם $3^{\frac{F_n-1}{2}} = -1 \pmod{F_n}$.

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

$(\frac{F_n}{3}) = (\frac{3}{F_n})(-1)^{\frac{F_n-1}{2}\cdot\frac{3-1}{2}} = (\frac{F_n}{3})$ ו־$3^{\frac{F_n-1}{2}} = -1$. אז[15] $F_n \equiv 2^{2^n} + 1 \equiv 2 \pmod 3$.

כעת נניח $3^{\frac{F_n-1}{2}} = -1 \pmod{F_n}$. יהי p מחלק ראשוני של F_n. $3^{\frac{F_n-1}{2}} \equiv -1 \pmod p$. נעלה בריבוע ונקבל $3^{F_n-1} = 1 \pmod p$. נעיר כי $F_n - 1 = 2^{2^n}$.

אזי $3^{2^{2^n}} = 1 \pmod p$ אם כאשר m הסדר של 3 בחבורה $(\mathbb{Z}/p\mathbb{Z})^*$. $m \mid 2^{2^n}$ לכן $m = 2^r$ לאיזשהו $1 \leq r \leq 2^n$. נסמן $s = 2^n - r$. אם $s > 0$,

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

לכן $s = 0$, לכן $r = 2^n$.

כלומר, הסדר של 3 מודולו p הוא 2^{2^n}. זה חייב להיות קטן מ־ או שווה ל־$p - 1$, וקיבלנו $2^{2^n} \leq p - 1$. אז $p \geq 2^{2^n} + 1 = F_n$. $p \mid F_n$, לכן $p = F_n$.

יהי n כללי. מתי n ראשוני? ברור שיש דרך לעשות זאת – לבדוק התחלקות בראשוניים עד $\sqrt{n}$ **(הנפה של אריסטופנס)**, אך שיטה זו איננה יעילה.

תנאי הכרחי: אם n ראשוני, אזי לכל $(a, n) = 1$, $a^{n-1} \equiv 1 \pmod n$.

[15] $2^{2k} \equiv 1 \pmod 3$.

אבל יש מספרים n־ים לא ראשוניים כך שזה בכל אופן קורה: $n = 561 = 3 \cdot 11 \cdot 17$. ל־$n$ זה, $a^{n-1} \equiv 1 \pmod{n}$ לכל a. (מספיק להוכיח לכל $p = 3, 11, 17$ ש־$a^{560} \equiv 1 \pmod{p}$, לפי הסיני).

כאן $n = p_1p_2p_3$ ו־$p_i - 1 | n-1$. לכן $a^{n-1} = a^{(p_i-1)r_i} \pmod{p_i} = 1^{r_i} \pmod{p_i} = 1 \pmod{p_i}$.

13.7.2008 כזכור, אם p ראשוני, אזי לכל $1 \le a < p-1$, $a^{p-1} \equiv 1 \pmod{p}$. יהי n כלשהו ונתבונן ב־$\{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{n-1} \equiv 1 \pmod{n}\}$. זו חבורה חלקית של $(\mathbb{Z}/n\mathbb{Z})^*$, ולכן או כולם מקיימים זאת או לפחות מחציתם אינם מקיימים זאת.

מספר קרמייקל **הגדרה.** מספר חיובי אי־זוגי n נקרא **מספר Carmichael** אם לכל $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^{n-1} \equiv 1 \pmod{n}$.

דוגמה. מספר קרמייקל הקטן ביותר הוא $561 = 3 \cdot 11 \cdot 17$. ואכן, $2 \mid 560$, $10 \mid 560$, $16 \mid 560$.

טענה 48: אם n מספר קרמייקל, אזי לכל p ראשוני, $p^2 \nmid n$ (הוא square-free – חסר ריבועים).

הוכחה. נניח $p^2 \mid n$ ראשוני אי־זוגי. אזי יש מספר g טבעי שיוצר את החבורה $(\mathbb{Z}/p^2\mathbb{Z})^*$, כלומר יש איבר g מסדר $p(p-1)$ ב־$|(\mathbb{Z}/p^2\mathbb{Z})^*| = p(p-1)$. n מספר קרמייקל, לכן $g^{n-1} \equiv 1 \pmod{n}$, ובפרט $g^{n-1} \equiv 1 \pmod{p^2}$. לכן $o(g) = p(p-1) \mid n-1$. כלומר $p \mid n$ ו־$p \mid n-1$, לכן $p \mid 1$, בסתירה.

טענה 49: $n \in \mathbb{N}$ אי־זוגי הוא מספר קרמייקל אם"ם לכל $p \mid n$ מתקיים $p-1 \mid n-1$.

הוכחה. לפי הטענה הקודמת, $n = p_1 \cdots p_k$ מכפלת ראשוניים שונים. צריך להראות כי לכל $i = 1, \ldots, t$, $p_i - 1 \mid n-1$; ואכן, יהי $g \in \mathbb{N}$ איבר פרימיטיבי מודולו n (איבר שיוצר את $(\mathbb{Z}/p\mathbb{Z})^*$); אז $g^{p-1} \equiv 1 \pmod{p}$ ו־$o(g) = p-1$. מתקיים ש־$g^{n-1} \equiv 1 \pmod{n}$ ולכן גם $g^{n-1} \equiv 1 \pmod{p}$. לכן $n-1 \mid p-1$, כנדרש.

להיפך, נניח ש־n מכפלה של ראשוניים שונים ולכל $p \mid n$ מתקיים $p-1 \mid n-1$. צריך להראות ש־n קרמייקל. יהי $1 \le a \le n$ כך ש־$(a, n) = 1$. $n = p_1 \cdots p_l$ וצריך להראות $a^{n-1} \equiv 1 \pmod{n}$. אנו יודעים שלכל $i = 1, \ldots, t$ מתקיים $a^{n-1} \equiv a^{(p_i-1)s_i} \equiv 1^{s_i} \equiv 1 \pmod{p_i}$, $n - 1 = (p_i - 1)s_i$, $s_i \in \mathbb{N}$. $b = a^{n-1}$ הוא פתרון למערכת המשוואות $x \equiv 1 \pmod{p_i}$ ל־$1 \le i \le t$, ולכן $b \equiv 1 \pmod{p_1 \cdots p_t} \equiv 1 \pmod{n}$.

משפט 50: $n \in \mathbb{N}$ חיובי אי־זוגי הוא ראשוני אם"ם לכל $(a, n) = 1$, $a^{\frac{n-1}{2}} = \left(\frac{2}{a}\right) \pmod{n}$.

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 $a^{n-1} = (a^{\frac{n-1}{2}})^2 \equiv \left(\frac{a}{n}\right)^2 \equiv 1 \pmod{n}$ ולכן $n = p_1 \cdots p_t$ מכפלת ראשוניים שונים זה מזה, $p_i - 1 \mid n-1$. ניקח $p = p_1$, $l(p-1) = n-1$.

נניח $t > 1$. נניח ש־l אי־זוגי. נבחר $b_1 \pmod p$ כך ש־$(\frac{b_1}{p}) = -1$ ונבחר $b_2 \pmod{\frac{n}{p}}$ כך ש־$(\frac{b_2}{\frac{n}{p}}) = -1$.[16] אחרי שבחרנו b_1 ו־b_2 כנ"ל, נבחר לפי המשפט הסיני $1 \le b \le n$ כך ש־$b \equiv b_1 \pmod{p_1}, b \equiv b_2 \pmod{\frac{n}{p_1}}$ ונחשב:

$$\begin{aligned}(\tfrac{b}{n}) &= (\tfrac{b}{p\cdot\frac{n}{p}}) \\ &= (\tfrac{b}{p})(\tfrac{b}{\frac{n}{p}}) \\ &= (\tfrac{b_1}{p})(\tfrac{b_2}{\frac{n}{p}}) \\ &= (-1)(-1) = 1\end{aligned}$$

אבל $b^{\frac{n-1}{2}} = b^{\frac{p-1}{2}\cdot l} \equiv (\frac{b}{p})^l \pmod p \equiv (\frac{b_1}{p})^l = (-1)^l = -1 \pmod p$. כלומר, $b^{\frac{n-1}{2}} \equiv -1 \pmod p, b^{\frac{n-1}{2}} \not\equiv (\frac{b}{n}) \pmod n \equiv 1 \pmod p$ ולכן ודאי $(\frac{b}{n}) \equiv 1 \pmod n$.

עכשיו נניח ש־l זוגי. נבחר b_1 כך ש־$(\frac{b_1}{p}) = -1$ ו־b_2 כך ש־$(\frac{b_2}{\frac{n}{p}}) = 1$ (זה ניתן להיעשות).
נבחר b כך ש־$b \equiv b_1 \pmod p, b \equiv b_2 \pmod{\frac{n}{p}}$.
נחשב: $b^{\frac{n-1}{2}} = b^{\frac{p-1}{2}l} \equiv (\frac{b}{p})^l = 1 \pmod p$
ולכן $(\frac{b}{n}) = (\frac{b}{p\cdot\frac{n}{p}}) = (\frac{b}{p})(\frac{b}{\frac{n}{p}}) = (\frac{b_1}{p})(\frac{b_2}{\frac{n}{p}}) = -1 = (-1)1$
אז $b^{\frac{n-1}{2}} \not\equiv (\frac{b}{2}) \pmod p$, ולכן גם $b^{\frac{n-1}{2}} \not\equiv (\frac{b}{n}) \pmod n$ כי $p \mid n$, בסתירה.

1.9.1 אלגוריתם Solovay-Strassen

יהי n שלם חיובי אי־זוגי גדול. כדי לבדוק האם הוא ראשוני:

הגרל b מקרי וחשב $b^{\frac{n-1}{2}}$ ו־$(\frac{b}{n})$ (מספר פעולות החישוב בכל מקרה הוא $O(\log^3 n)$ – תרגיל. חישוב סמל יעקובי קל יחסית בזכות חוק ההדדיות הריבועית: $(\frac{n}{b}) = (\frac{b}{n})(-1)^{\frac{n-1}{2}\cdot\frac{b-1}{2}}$, וכמו באלגוריתם אוקלידס, כמות הצעדים לוגריתמית).

אם $b^{\frac{n-1}{2}} \neq (\frac{b}{n}) \pmod n$, הכרז על n כפריק. אם שווים, העלה מונה ב־1. אם המונה קטן מ־100, חזור לצעד א'. אם המונה $= 100$, הכרז על n כראשוני בהסתברות $\ge 1 - \frac{1}{2^{100}} \approx 1$.

הצדקה: $H = \{b \in (\mathbb{Z}/n\mathbb{Z})^* \mid b^{\frac{n-1}{2}} = (\frac{b}{n}) \pmod n\}$ מהווה חבורה חלקית של $(\mathbb{Z}/n\mathbb{Z})^*$, ולכן אם n לא ראשוני, על־פי המשפט, לפחות חצי מהמספרים בין 1 ל־n לא מקיימים את המשוואה, כי זה ודאי כך לאלו שאינם זרים ל־n.

טריק לחיסכון חישובי: צריך לחשב $f(x) = \sum_{i=0}^n a_i x^i$ כאשר $a_i \in F, x \in F$. אז נכתוב $f(x) = \ldots x(x((a_n x + a_{n-1})x + a_{n-2}) + a_{n-3})\ldots$. למה זה שימושי לנו? אם רוצים לחשב $a^m \pmod n$, נרשום $m = \sum_{i=0}^r b_i 2^i$ כאשר $b_i = 0, 1$. אז $a^m = a^{\sum_{i=0}^r b_i 2^i} = \prod_{i=1}^r (a^{2^i})^{b_i}$, ויש כאן פחות פעולות. אפשר גם לייעל עוד.

20.7.2008 **משפט 51:** $n \in \mathbb{N}$ אי־זוגי; אזי n ראשוני אם"ם לכל $1 \le a \le n$ עם $(a, n) = 1$ מתקיים $(*)$

[16] תמיד יש כזה, כי $\frac{n}{p} = p_2 \cdots p_t$; נבחר מספר c_2 שאינו שארית ריבועית מודולו p_2 ולכל $i = 3, \ldots, t$ נבחר c_i שהוא כן שארית ריבועית מודולו p_i, ואז נפתור את המערכת $x \equiv c_i \pmod{p_i}$, $i = 2, \ldots, t$. הפתרון b_2 יקיים $(\frac{b_2}{\frac{n}{p}}) = (\frac{b_2}{p_2 p_3 \cdots p_t}) = (\frac{b}{p_2})(\frac{b}{p_3})\cdots(\frac{b}{p_t}) = (\frac{c_2}{p_2})\cdots(\frac{c_t}{p_t}) = -1$.

$1 \leq a \leq n$ מקיימים $a^{\frac{n-1}{2}} \pmod n = (\frac{a}{n})$. יתר על כן, אם n לא ראשוני, אזי לפחות חצי מהאיברים $a^{\frac{n-1}{2}} \not\equiv (\frac{a}{n}) \pmod n$.

1.9.2 אלגוריתם Miller-Rabin

נניח n מספר אי־זוגי חיובי גדול ו־$b \in (\mathbb{Z}/n\mathbb{Z})^*$ המקיים $b^{n-1} \equiv 1 \pmod n$. הרעיון הוא להתחיל ולהסתכל בשרשים ריבועיים $b^{\frac{n-1}{2}}, b^{\frac{n-1}{4}}, \ldots, b^{\frac{n-1}{2^k}}$ עד $b^{\frac{n-1}{2^t}}$ אי־זוגי. אם n ראשוני, אזי אם $b^{\frac{n-1}{2^{s-1}}} = 1 \pmod n$ ו־$b^{\frac{n-1}{2^s}} \neq 1 \pmod n$, אזי בהכרח $b^{\frac{n-1}{2^s}} = -1 \pmod n$, כי בשדה יש ל־1 רק שני שרשים, ± 1. (לעומת זאת, אם n מכפלת ראשוניים, $b^{\frac{n-1}{2^s}}$ יכול להיות כל מיני דברים.)

בסימונים הקודמים, נאמר ש־b עד חזק לראשוניות n אם בסדרה $b^{\frac{n-1}{2^s}} \pmod n$ מופיע -1.

אלגוריתם רבין־מילר מתבסס על כך שאם n אינו ראשוני, אזי פחות מ־25% מהאיברים בין 1 ל־n הם עדים חזקים.

מבין כל ה־n־ים עד $2.5 \cdot 10^{10}$, רק מספר אחד $n = 3215031751$ עבר את מבחן רבין־מילר עבור $b = 2, 3, 5, 7$ על אף שאינו ראשוני.

לפני כמה שנים, פתאום קבוצה של הודים – אחד מהנדס חשמל והשאר תלמידי תואר ראשון – מצאו אלגוריתם דטרמיניסטי פולינומיאלי, עם הוכחה, לבדיקת ראשוניות.[17]

1.10 שדות סופיים

אם F שדה סופי, אזי $1 = 0 + 1 + 1 + \ldots + 1$ פעם ראשונה לאחר p צעדים, p ראשוני, $p = \operatorname{char} F$. מכאן נובע ש־$F$ מכיל את $\mathbb{F}_p = \{0, 1, 2 = 1 + 1, \ldots, p - 1\}$. F הוא מרחב וקטורי מעל $\mathbb{F}_p$ ולכן $|F| = p^n$ לאיזשהו n.

משפט 52: לכל p ראשוני ולכל $n \in \mathbb{N}$ קיים שדה מסדר p^n. שדה זה יחיד עד כדי איזומורפיזם.

הוכחה (בערך). ב־$\mathbb{F}_p[x]$, לכל n יש פולינום (מתוקן) ראשוני (אי פריק) ממעלה n. ניקח $f(x)$ פולינום כזה. נסתכל ב־$F = \mathbb{F}_p[x]/(f(x))$. מאחר ש־$f(x)$ אי־פריק, $(f(x))$ מקסימלי ולכן F שדה. קל לראות ש־$|F| = p^n$.

דוגמה. נבנה שדה מסדר p^2. יהי $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ כך ש־$(\frac{a}{p}) = -1$. כלומר, a לא ריבוע. נסתכל בפולינום $f(x) = x^2 - a$ הוא פולינום אי־פריק. $F = \mathbb{F}_p[x]/(f(x))$, או באופן קונקרטי, $F = \{x + y\sqrt{a} \mid x, y \in \mathbb{F}_p\}$. זה שדה מסדר p^2, עם הפעולות הרגילות.

אם φ אוטומורפיזם של F, $\varphi : F \to F$, אזי $\varphi(b) = b$ לכל $b \in \mathbb{F}_p$, ובפרט $\varphi(a) = a$, ואז $\varphi(\sqrt{a}) = \pm\sqrt{a}$. אם $\varphi(\sqrt{a}) = \sqrt{a}$ אזי $\varphi \equiv id$, כי עבור $x, y \in \mathbb{F}_p$, מתקיים $\varphi(x + y\sqrt{a}) = \varphi(x) + \varphi(y)\varphi(\sqrt{a}) = x + y\sqrt{a}$. לכן יש רק אוטומורפיזם אחד ויחיד שאיננו טריוויאלי. (בדוק ש־$\varphi(\sqrt{a}) = -\sqrt{a}$ אכן מגדיר אוטומורפיזם של F.)

[17] ניתן לקרוא את המאמר כאן: http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf.

גם ההעתקה $Fr : F \to F$ המוגדרת על־ידי $Fr(h) = h^p$ ל־$h \in F$ היא אוטומורפיזם, כי (א) ודאי שומרת על כפל: $Fr(h_1h_2) = (h_1h_2)^p = h_1^p h_2^p$; (ב) גם שומרת על חיבור: $(h_1+h_2)^p = h_1^p+\binom{p}{1}h_1^{p-1}h_2+\ldots+\binom{p}{p-1}h_1h_2^{p-1}+h_2^p$, אך $p \mid \binom{p}{i}$ לכל $1 \le i \le p-1$ ולכן $= h_1^p + h_2^p$. לכן F_p הומומורפיזם. הוא אוטומורפיזם כי הוא חד־חד ערכי.

$0 \mapsto 0$, אז $Fr : F^* \to F^*$. $|F^*| = p^2 - 1$, ולכן $(p, p^2-1) = 1$ ולכן העלאה בחזקת p זו העתקה חד־חד ערכית, ולכן Fr אוטומורפיזם שאינו טריוויאלי: אם היה טריוויאלי, זה היה אומר שלכל $h \in F$, $h^p = h$, כלומר לפלולינום $x^p - x$ יש p^2 שרשים, וזה בלתי אפשרי. לכן $Fr = \varphi$ שלמעלה.

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

יהי $b \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ כך ש־$(\frac{b}{p}) = 1$, כלומר יש לו שורש ריבועי. נרצה למצוא אותו. נגריל t מקרי ב־$\mathbb{F}_p$ עד שנקבל כזה כך ש־$\alpha = t^2 - b$ אינו ריבוע. נסמן $\beta = \sqrt{\alpha}$ ונסתכל בשדה $F = \{x + y\beta \mid x, y \in \mathbb{F}_p\}$. זה שדה מסדר p^2. נתבונן ב־$\gamma = (\beta + t)^{\frac{p+1}{2}}$.

טענה 53: (א) $\gamma \in \mathbb{F}_p$; (ב) $\gamma^2 = b$.

הוכחה. נציין ש־(ב) $\Longleftarrow$ (א), כי התחלנו ב־b שיש לו שורש ב־$\mathbb{F}_p$, לכן יש לו בדיוק שני שרשים ב־F, ושניהם ב־$\mathbb{F}_p$.

נוכיח את (ב).

$$\begin{aligned}
\gamma^2 &= ((\beta+t)^{\frac{p+1}{2}})^2 \\
&= (\beta+t)^{p+1} \\
&= (\beta+t)^p(\beta+t)^1 \\
&= Fr(\beta+t)(t+\beta) \\
&= \varphi(t+\beta)(t+\beta) \\
&= (t-\beta)(t+\beta) \\
&= t^2-\beta^2 \\
&= t^2-\alpha \\
&= t^2-(t^2-b) \\
&= b
\end{aligned}$$

2 קריפטוגרפיה: הצפנה ציבורית

2.1 שיטת RSA

סיפור. ניקח דוגמה בלי מתמטיקה. לי יש מילון עברית־סינית (סינית זו שפה שאף אחד לא יודע). בעצם, יותר מזה: אני ממציא שפה שלא קיימת בעולם ובונה לה מילון. חצי ראשון של המילון זה תרגום מעברית לסינית, והחצי השני זה תרגום מסינית לעברית.

עכשיו, אנחנו רוצים לדבר. אז אני אלמד אותך איך לדבר אליי, ואתה תלמד אותי איך לדבר אליך. אין שום סיבה שבעולם שזה יהיה אותו דבר. כמובן, זה מיועד לתקשורת בין מחשבים; אז אני שולח אליך את החצי־מילון שמתרגם מעברית לסינית, אבל את החצי השני שמתרגם מסינית לעברית אני שומר אצלי.

עכשיו, כל האויבים, הטובים והרעים, שומעים את כל התקשורת בינינו. אז גם להם יש את המילון שמתרגם מעברית לסינית. אתה רוצה לשלוח לי הודעה בעברית, שלא יבינו אותה; אז אתה לוקח את חצי המילון, מתרגם את ההודעה לסינית ושולח אליי. אני, שיש לי חצי המילון שמתרגם מסינית לעברית, יכול להבין את המסר שלך, אבל כל האחרים, למרות שגם להם יש המילון כמו שלך, שמתרגם מעברית לסינית, אין להם המילון ההפוך, ולכן הם לא יכולים להבין מה אמרתי. יתר על כן, גם אתה, אם תסתכל על ההודעה ששלחת, לא תבין כלום.

ההנחה היא שלבנות מילון הפוך זו בעיה קשה. אנחנו מחפשים פונקציה שלוקח המון זמן להפוך אותה: המשחק הוא, למעשה, משחק על הזמן. כשדיפי והלמן פירסמו את המאמר שלהם, עדי שמיר ממכון ויצמן, שבאותם ימים היה פוסט־דוקטורנט צעיר ב־MIT דיבר עם ריבסט ועם אדלמן, והם התחילו להשתעשע בנסיונות לחפש פונקציה כזאת. אחרי כל מיני ניסיונות וחזרות, הם המציאו את הפונקציה המתוארת להלן.

אזהרה. עד היום אין הוכחה שזו אכן פונקציה טובה.

נבחר p ו־q ראשוניים גדולים. (יש לנו אלגוריתמים מצוינים לעשות זאת.) נתבונן ב־$n = p \cdot q$. נסתכל ב־$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(p)\varphi(q) = (p-1)(q-1)$. נבחר $1 \le e \le \varphi(n)$, $(e, \varphi(n)) = 1$ מקרי ונפרסם בציבור את (n, e).

מי שרוצה לשלוח אלינו הודעה $1 \le x < n$, ישלח במקום זה את $x^e \pmod n$. אנו, שיש בידינו את $\varphi(n)$, יודעים למצוא $1 \le f \le \varphi(n)$ כך ש־$e \cdot f \equiv 1 \pmod{\varphi(n)}$.[18]

$(x^e)^f = x^{1+r\varphi(n)} = x \cdot x^{r\varphi(n)} = x \cdot 1^r = x$, ולכן תהליך הפיענוח: $ef = 1 + r\varphi(n)$

יש פה הנחה סמויה ש־x זר מ־n, אבל **דחילק**, אין סיכוי שזה יקרה: n מכפלת שני ראשוניים, וכמה מספרים בני מאתיים ספרות שמתחלקים ב־p או ב־q כבר יש? חוץ מזה, n ידוע והשולח יכול לבדוק.

אנו מסתמכים כאן על "אקסיומה" מפוקפקת: אין אלגוריתם יעיל לפירוק n למרכיביו p ו־q.

הערה: ידיעת $\varphi(n)$ נותנת פירוק של n (כאשר $n = pq$), כי

[18] תזכורת: אם $(a, m) = 1$, על־ידי אלגוריתם אוקלידס נמצא את $a^{-1} \pmod m$: הראינו איך למצוא x, y כך ש־$ax + my = 1$, ואז $x = a^{-1} \pmod m$.

$$\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1$$

לכן ידיעת $n = pq$ ו־$\varphi(n)$ נותנת ידיעת $p+q$ ואז נפתור את המערכת $pq = n$, $p+q = x$ (כאשר שוב, x ידוע).

27.7.2008 אם מישהו יודע למצוא m כך ש־$a^m \equiv 1 \pmod n$ לכל $a \in (\mathbb{Z}/n\mathbb{Z})^*$, אז הוא יודע לפרק את n, כי: (א) m חייב להיות זוגי (מתחלק ב־$p-1$ וב־$q-1$); (ב) נבדוק אם גם ל־$\frac{m}{2}$ יש התכונה $a^{\frac{m}{2}} \equiv 1 \pmod n$. - יש בדיקה הסתברותית מהירה לכך (כי אוסף ה־a־ים שמקיימים תכונה זו הוא חבורה חלקית). לכן נמשיך עד שנגיע ל־m כזה שמקיים את התכונה אבל $\frac{m}{2}$ לא מקיים. למה $\frac{m}{2}$ לא מקיים? זה אומר שלא לכל a, $a^{\frac{m}{2}} \equiv 1 \pmod p$ או שלא לכל a מתקיים $a^{\frac{m}{2}} \equiv 1 \pmod q$. זה אומר ש־$p-1 \nmid \frac{m}{2}$ או $q-1 \nmid \frac{m}{2}$.

במקרה הראשון, $q-1 \mid \frac{m}{2}$ ואז לכל a, $a^{\frac{m}{2}} \equiv 1 \pmod q$ ולמחצית לפחות $a^{\frac{m}{2}} \not\equiv 1 \pmod p$. אז בהסתברות של לפחות 50% a מקרי יקיים $a^{\frac{m}{2}} - 1$ מתחלק ב־q ולא ב־p, כלומר $(a^{\frac{m}{2}} - 1, n) = q$ ולכן נמצא בקלות q ובכך פירוק ל־n.

המקרה השני סימטרי.

אם שני המקרים קורים, $p-1 \nmid \frac{m}{2}$ ו־$q-1 \nmid \frac{m}{2}$, אזי יש חלוקה ל־25% לכל 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 סיכוי של $\frac{1}{2}$ שיהיה לו גורם משותף עם n.

2.2 שיטת רבין

p, q ראשוניים, $n = pq$. במקום לשדר x ($1 \le x \le n$), נשדר $m \equiv x^2 \pmod n$.

אנו, שיודעים את p ו־q, נחשב r_p כך ש־$r_p^2 \equiv m \pmod p$ ו־r_q כך ש־$r_q^2 \equiv m \pmod q$. (כזכור, יש אלגוריתם מהיר להוצאת שורש מודולו ראשוני.)

אם נדאג לבחור את p ו־q להיות $p \equiv q \equiv 3 \pmod 4$, אזי יש אלגוריתם מאוד מהיר להוצאת שורש ל־m: $(m^{\frac{p+1}{4}})^2 = m^{\frac{p+1}{2}} \equiv m^{\frac{p-1}{2}+\frac{2}{2}} \equiv m^{\frac{p-1}{2}} m \equiv (\frac{m}{p}) m \equiv 1 \cdot m \equiv m - m^{\frac{p+1}{4}} \pmod p$ (סימן לז'נדר שווה 1, שהרי m שארית ריבועית מודולו p).

מתוך r_p ו־r_q, על־ידי משפט השאריות הסיני, מקבלים a יחיד כך ש־$a \equiv r_p \pmod p$, $a \equiv r_q \pmod q$.

הערה: קל למצוא y ו־z כך ש־$yp + zq = 1$, כלומר $yp \equiv 1 \pmod q$, $zq \equiv 1 \pmod p$. נתבונן ב־$a = r_q yp + r_p zq$. זאת אומרת, קל למצוא $a \equiv r_p \pmod p$ ו־$a \equiv r_q \pmod q$. פתרון למשפט השאריות הסיני, ולכן לאחר שמצאנו r_p ו־r_q, קל למצוא את a: $a^2 \equiv r_p^2 \equiv m \pmod p$; $a^2 \equiv r_q^2 \equiv m \pmod q$.

הבעיה: r_p ו־r_q אינם נקבעים באופן יחיד: לכל אחד מהם יש שתי אפשרויות, ולפיכך יש ארבעה פיענוחים אפשריים. אפשר לפתור את זה על־ידי קביעת תבנית מסוימת היכנשהו, אבל זה קצת מחליש את הצופן.

טענה 54: $n = pq$. אם יש אלגוריתם יעיל שבהינתן $n \ge m \ge 1$ שהוא שארית ריבועית נותן את אחד משורשיו הריבועיים (כזכור, יש בדיוק ארבעה כאלה) מודולו n, אזי ניתן לפרק את n.

הוכחה. נגריל באופן מקרי y־ים, $1 \leq y \leq n$, ונכניס לקופסה. נכניס לקופסה את $y^2 \pmod n$. הקופסה תחזיר לי שורש של y^2. ב־50% מהמקרים, היא תחזיר לי את $\pm y \pmod n$, ואז אין שום תועלת בכך. אבל ב־50% מהמקרים, נקבל שורש $z \neq \pm y$. במקרה כזה, $0 \equiv y^2 - z^2 = (y-z)(y+z) \pmod n$. $y-z \not\equiv 0 \pmod n$ ו־$y+z \not\equiv 0 \pmod n$. זה אומר ש־$p \mid y-z$ ו־$q \mid y+z$ או להיפך. בכל מקרה, $y - z$ לא זר ל־n, ואז נחשב $(y - z, n)$ ונפרק את n.

הנה כי כן, פיצוח האלגוריתם שקול לאפשרות לפרק כל מספר לגורמיו, אך מאמינים שזו בעיה קשה.

2.3 חתימה דיגיטלית / zero-knowledge proofs

$n = pq$ ידוע לכול. פורסם x^2. מטרתי לשכנע שאני יודע את x בלי לחשוף מהו.

נגריל y ונשלח את y^2. אתם זכאים, אחרי שקיבלתם את y^2, לדרוש ממני לפרסם את y או את $xy(n)$ (אבל רק אחד מהם).[19] אחרי מספר חזרות מספיק, תיאלצו להאמין לי.

בשיטה זו, לא מסגירים אינפורמציה על x.

2.4 הפצת מפתחות / לוגריתם דיסקרטי

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

A מגריל מספר מקרי $1 \leq a \leq p-1$ ו־B מגריל מספר מקרי $1 \leq b \leq p-1$. (כל האריתמטיקה מתבצעת מודולו p.)

A שולח ל־B את g^a. B שולח ל־A את g^b. A לוקח את g^b ומעלה בחזקת a ומקבל את $(g^b)^a = g^{ba}$. B לוקח את g^a ומעלה בחזקת b, ומקבל $(g^a)b = g^{ab}$. עכשיו, ל־A ול־B יש סוד משותף: $g^{ab} = g^{ba}$. האחרים אינם יודעים אותו. זה יכול לשמש כמפתח לשימוש בהצפנה סטנדרטית.

האויב יודע את g, g^a ו־g^b. עליו להוציא לוגריתם בבסיס g: זו בעיה (שמאמינים שהיא) קשה.

[19] על־ידי העלאה בריבוע ניתן לוודא זאת, כי x^2 ו־y^2 ידועים.

3 המספרים ה־p־אדיים

p קבוע ראשוני. נתבונן בסדרות $\{a_i\}_{i=0}^{\infty} = (a_0, a_1, \ldots, a_n, \ldots)$ כך ש־$a_n \equiv a_{n-1} \pmod{p^n}$.
נאמר ששתי סדרות כאלה $\{a_i\}$ ו־$\{b_i\}$ שקולות אם לכל n, $a_n \equiv b_n \pmod{p^{n+1}}$.

הגדרה. מספר שלם p־אדי זו מחלקת שקילות של סדרות כאלו.

כל מספר p־אדי מיוצג על־ידי סדרה $\{a_i\} = (a_0, a_1, \ldots)$ כך ש־$0 \le a_n < p^{n+1}$.
הגדרת חיבור וכפל: $\{a_i\}+\{b_i\} = \{a_i+b_i\}$, $\{a_i\}\cdot\{b_i\} = \{a_ib_i\}$. תרגיל: הוכח שמוגדר היטב.

טענה 55: זה חוג, כאשר $0 = (0, 0, \ldots)$, $1 = (1, 1, \ldots)$.

נקרא לחוג זה $\hat{\mathbb{Z}}_p$ חוג השלמים ה־p־אדיים.
יש שיכון של $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}_p$ על־ידי $n \mapsto (n, n, \ldots)$. זה הומומורפיזם חד־חד ערכי.
איך נראים מספרים כאלו? בה"כ, $0 \le a_0 < p$. $0 \le a_1 < p^2$, ו־$a_1 \equiv a_0 \pmod{p}$, ולכן $a_1 = a_0 + b_1p$, $0 \le b_1 < p$. $a_2 \equiv a_1 \pmod{p^2}$, $0 \le a_2 < p^3$. לכן $a_2 = a_1 + b_2p^2$, $0 \le b_2 < p$. אז $a_2 = a_0 + b_1p + b_2p^2$.
נמשיך. אם נקרא ל־$b_0 = a_0$, $a_n = b_0 + b_1p + b_2p^2 + b_3p^3 + \ldots + b_np^n$, $0 \le b_i < p$.
ניתן לזהות את השלם ה־p־אדי $\alpha = \{a_i\}$ עם הטור הפורמלי $\sum_{i=0}^{\infty} b_ip^i$.
$\mathbb{N} \ni n \mapsto (n \pmod{p}, n \pmod{p^2}, \ldots) = (a_0, a_1, \ldots)$ $(n, n, \ldots)$. בכתיבה כטור, זה בדיוק $n = \sum_{i=0}^{r} b_ip^i$ ($r \sim \log_p n$).

טענה 56: $\hat{\mathbb{Z}}_p \ni \alpha = \{a_i\} = \sum_{i=0}^{\infty} b_ip^i$ הפיך בחוג $\hat{\mathbb{Z}}_p$ אם"ם $a_0 (= b_0) \not\equiv 0 \pmod{p}$.

הערה: החיבור במונחי טורים הוא חיבור עם carry: אם $b_i + b_i' \ge p$, $\sum b_ip^i + \sum b_i'p^i$: מוסיפים 1 לשלב הבא. כפל הוא הכפל הפורמלי של שני טורים ב־p, ושוב עם carry. זה מבדיל את $\hat{\mathbb{Z}}_p$ מ־$\mathbb{F}_p[[x]] = \{\sum b_ix^i \mid b_i \in \mathbb{F}_p\}$, שבו אין carry.

הוכחה. אם $\alpha = (a_0, a_1, \ldots)$ הפיך, פירושו שקיים $\gamma = (c_0, c_1, \ldots)$, $0 \le c_i \le p^{i+1}$ כך ש־$a_ic_i \equiv 1 \pmod{p^{i+1}}$.
בפרט, אם α הפיך, אזי $a_0c_0 \equiv 1 \pmod{p}$ ולכן $a_0 \not\equiv 0 \pmod{p}$.
בכיוון השני, נניח ש־$a_0 \not\equiv 0 \pmod{p}$. אזי מאחר שעל־פי ההגדרה $a_i \equiv a_0 \pmod{p}$ לכל i, הרי $a_i \not\equiv 0 \pmod{p}$ לכל i ולכן הפיך בחוג $\mathbb{Z}/p^{i+1}\mathbb{Z}$ ולכן יש c_i כך ש־$a_ic_i \equiv 1 \pmod{p^{i+1}}$. תרגיל: $(c_0, c_1, \ldots)$ אכן שלם p־אדי.

הפיתוח של השליליים איננו סופי: הטור שמתאים ל־1 הוא $(1, 1, 1, \ldots)$; הטור שמתאים ל־-1 – אם מחברים, מקבלים משהו שקול ל־0. אז $(p-1, p^2-1, p^3-1, \ldots)$. זה טור ששקול ל־0. במונחי b, נקבל $\alpha = (p-1) + (p-1)p + (p-1)p^2 + \ldots$.
$\sum_{i=0}^{n}(p-1)p^i = \sum_{i=0}^{\infty}(p-1)p^i = (p-1)\cdot\frac{p^{n+1}-1}{p-1} \equiv p^{n+1} - 1 \equiv -1 : -1 \pmod{p^{n+1}}$.

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

מסקנה 57: כל איבר α ב־$\hat{\mathbb{Z}}_p$ ניתן לכתיבה כ־$p^m\varepsilon$ כאשר ε הפיך ב־$\hat{\mathbb{Z}}_p$.

הוכחה. $\alpha = \sum_{i=m}^{\infty} b_i p^i$, m הראשון כך ש־$b_m \neq 0$, $0 \leq b_i < p-1$.
$\alpha = p^m(\sum_{i=0}^{\infty} b_{m+1}p^i)$, ו־$\sum_{i=0}\infty b_{m+1}p^i$ הפיך כי $b_m \neq 0 \pmod p$.

טענה 58: ב־$\hat{\mathbb{Z}}_p$ אין מחלקי אפס, כלומר הוא תחום שלמות.

מסקנה 59: יש לו שדה שברים, שיסומן $\mathbb{Q}_p$ – שדה המספרים ה־p־אדיים.

טענה 60: $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}_p$ ולכן $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

$\alpha = p^m\varepsilon$, $\beta = p^n\varepsilon'$, $\frac{\alpha}{\beta} = \frac{p^m\varepsilon}{p^n\varepsilon'} = p^{m-n}(\varepsilon\varepsilon'^{-1})$.

מסקנה 61: כל איבר של $\mathbb{Q}_p$ ניתן להצגה כ־$\sum_{i=\nu}^{\infty} b_i p^i$, $\nu \in \mathbb{Z}$. כלומר, $\mathbb{Q}_p$ = טורי לורנט פורמליים ב־p.

עבור $\gamma = \sum_{i=\nu}^{\infty} b_i p^i$, $\nu \in \mathbb{Z}$, $b_v \neq 0$, $0 \leq b_i < p$. $|\gamma| = \frac{1}{p^\nu}$. נגדיר מטריקה על $\mathbb{Q}_p$:
$d(\alpha,\beta) = |\alpha - \beta|$.

טענה 62: זו מטריקה, כלומר מתקיים **(1)** $\alpha = \beta \iff d(\alpha,\beta) = 0$; **(2)** $d(\alpha,\beta) = d(\beta,\alpha)$;
(3) $d(\alpha,\gamma) \leq d(\alpha,\beta) + d(\beta,\gamma)$. (הוכח!)

$p^i \to 0$, כי $d(p^i,0) = |p^i - 0| = |p^i| = \frac{1}{p^i} \to 0$. תרגיל: $n! \to 0$.

טענה 63: **(א)** $\mathbb{Q}_p$ שדה שלם, דהיינו כל סדרת קושי מתכנסת. **(ב)** $\mathbb{Q}_p$ מכיל את $\mathbb{Q}$ כתת־שדה צפוף.

הוכחה. **(ב)** נראה קודם ש־$\mathbb{N}$ צפופים ב־$\hat{\mathbb{Z}}_p$: $\beta = \sum_{i=0}^{\infty} b_i p^i$ ונקרב אותו על־ידי המספרים הטבעיים $\beta_n = \sum_{i=0}^{n} b_i p^i$. $\beta - \beta_n = \sum_{i=n+1}^{\infty} b_i p^i$, ולכן $\beta - \beta_n \to 0$.
אם $\beta \ni \mathbb{Q}_p$ כללי, לאו דווקא שלם, אזי $\beta = \sum_{i=\nu}^{\infty} b_i p^i$, $\beta_n = \sum_{i=\nu}^{n} b_i p^i$. ∎

משפט 64 (Ostrovski): אם F שדה שלם המכיל את $\mathbb{Q}$ כתת־שדה צפוף, אזי $F \cong \mathbb{R}$ או $F \cong \mathbb{Q}_p$ לאיזשהו p.

טענה 65: $\alpha_i \in \mathbb{Q}_p$. הטור $\sum_{i=1}^{\infty} \alpha_i$ מתכנס אמ"ם $\alpha_i \to 0$.

4 תרגילים

4.1 12.6.2008

1. חשב: (א) $5^{10^6} \pmod{144}$; (ב) $(21432, 6666)$; (ג) $(6188, 4709)$; (ד) $2^{90} \pmod{91}$.
2. פתור: (א) $7x = 23 \pmod{101}$; (ב) $12x + 21y = 27$; (ג) $22x = 11 \pmod{121}$.
3. הוכח שלכל n, $30 \mid n^5 - n$, ולכל n אי־זוגי כך ש־$3 \nmid n$ מתקיים $6 \mid n^2 - 1$.
4. הוכח שאם $p = a^n - 1$ ראשוני, אזי $a = 2$ ו־n ראשוני (כלומר, p ראשוני של מרסן). רמז: $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + y^{n-1})$.
5. הוכח שאם $p = a^n + 1$ ראשוני אזי a זוגי ו־n חזקה של 2 (ראשוני של פרמה). רמז: ל־n אי־זוגי, $x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 + \ldots + y^{n-1})$.
6. נסמן ב־$\nu(n)$ את מספר המחלקים החיוביים של n. הוכח (א) שאם $n = p_1^{d_1} \cdot \ldots \cdot p_l^{d_l}$, p_i ראשוניים שונים, אזי $\nu(n) = \prod_{i=1}^{l}(d_i + 1)$; (ב) ν פונקציה של תורת המספרים.
7. מצא את כל הפתרונות השלמים וחיוביים למשוואה $19x + 20y = 1909$.
8. יהי $f(x) = \sum_{i=1}^{n} a_i x^i$ פולינום ב־$\mathbb{Z}[x]$. הוכח שאם קיימים $d, k \in \mathbb{Z}$ כך ש־$d \mid f(k+j)$ לכל $j = 0, \ldots, d-1$, אזי $d \mid f(n)$ לכל $n \in \mathbb{Z}$. הראה על־ידי דוגמה שיש $f(x)$ כזה גם עם $(a_0, \ldots, a_n) = 1$ (כלומר, מקדמי $f(x)$ זרים).
9. הוכח שאם $(a, b) = d$ אזי $\frac{\varphi(ab)}{d} = \frac{\varphi(a)\varphi(b)}{\varphi(d)}$.
10. הוכח שעבור $n > 1$, סכום השלמים החיוביים הקטנים מ־n וזרים לו שווה ל־$\frac{n\varphi(n)}{2}$.
11. הוכח שאם $d \mid n$ אזי $\varphi(d) \mid \varphi(n)$.
12. פתור את המערכת $x \equiv 1 \ (2)$, $x \equiv 1 \ (5)$, $x \equiv 3 \ (4)$, $x \equiv 4 \ (5)$.
13. הוכח שמספר שלם חיובי מתחלק ב־3 אם"ם סכום ספרותיו מתחלק ב־3 ומתחלק ב־9 אם"ם סכום ספרותיו מתחלק ב־9.
14. הוכח שאם $m = p^\alpha$ לאיזשהו $p > 2$ ראשוני אז $m = 2p^\alpha$ או הפתרונות היחידים למשוואה $x^2 \equiv 1 \pmod{m}$ הם ± 1, מודולו m. הוכח גם שאם m לא מהצורה הנ"ל אזי יש יותר משני פתרונות.
15. (א) הוכח שלכל $k \in \mathbb{Z}$ יש רק מספר סופי של $n \in \mathbb{N}$ כך ש־$\varphi(n) \leq k$; (ב) מצא סדרה של $n_i \in \mathbb{N}$ עם $\lim \frac{\varphi(n_i)}{n_i} = 1$ וסדרה עם $\lim \frac{\varphi(n_i)}{n_i} = 0$.
16. יהי F שדה סופי. הוכח שיש ב־$F[x]$ אינסוף פולינומים אי־פריקים (ראשוניים). מצא גם הערכות כמותיות טובות ככל האפשר.

6.7.2008 4.2

1. הוכח שיש אינסוף ראשוניים מהצורה $4k+1$. רמז: זכור ש־$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. אם $p_1, \ldots, p_l$ ראשוניים עם $p_i \equiv 1 \pmod 4$ התבונן ב־$N = (2p_1 \cdot \ldots \cdot p_l)^2 + 1$ ונתח מיהם הראשוניים p המחלקים אותו.

2. הוכח שיש אינסוף ראשוניים מהצורה $8k+7$. רמז: זכור ש־$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$. התבונן ב־$N = (4p_1 \cdot \ldots \cdot p_l)^2 - 2$. יהי p ראשוני אי־זוגי המחלק אותו. הוכח שלא ייתכן שכולם מהצורה $p \equiv 1 \pmod 8$.

3. יהי $a \in \mathbb{Z}$ שלם שאינו ריבוע של שלם אחר. הוכח שלאינסוף ראשוניים p, $(\frac{a}{p}) = -1$.

4. יהיו $r_1, \ldots, r_{\frac{p-1}{2}}$ השאריות הריבועיות מודולו p (ראשוני אי־זוגי). הוכח שמכפלתם שווה ל־1 (מודולו p) אם $p \equiv 3 \pmod 4$ ול־-1 (מודולו p) אם $p \equiv 1 \pmod 4$.

5. תאר את כל הראשוניים p כך ש־7 שארית ריבועית מודולו p.

6. תאר את כל הראשוניים p כך ש־15 שארית ריבועית מודולו p.

7. חשב (תוך שימוש בסמל יעקובי) את $(\frac{113}{997})$, $(\frac{215}{761})$, $(\frac{514}{1093})$, $(\frac{401}{757})$.

8. נניח p ראשוני ו־$p \equiv 1 \pmod 4$. הוכח שיש שלמים s ו־t כך ש־$pt = 1 + s^2$. הסק מכאן ש־p אינו ראשוני בחוג $\mathbb{Z}[i]$. (זכור שזהו חוג אוקלידי עם פריקות יחידה.)

9. (המשך 8) הסק גם שאם $p \equiv 1 \pmod 4$ אזי p ניתן לכתיבה כ־$p = a^2 + b^2$ כאשר a ו־b שלמים. רמז: רשום $p = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[i]$ ולא הפיכים שם, על־פי 8.

   הוכח שאם $p \equiv 3 \pmod 4$ אזי אינו ניתן לכתיבה כ־$p = a^2 + b^2$.

10. השתמש בתרגיל 4 מקובץ התרגילים הקודם כדי להוכיח ש־3 איננו שארית ריבועית מודולו p אם p הוא ראשוני של מרסן.

11. $a \in \mathbb{Z}$ נקרא פרימיטיבי מודולו p (ראשוני אי־זוגי) אם a יוצר את החבורה $(\mathbb{Z}/p\mathbb{Z})^*$. הוכח שאיבר פרימיטיבי אינו יכול להיות שארית ריבועית. האם כל איבר שאינו שארית ריבועית הוא פרימיטיבי?

12. (א) הוכח שאם p ראשוני של פרמה אזי $a \in \mathbb{Z}$ פרימיטיבי מודולו p אם"ם a איננו שארית ריבועית. (ב) הוכח שתכונה זו מאפיינת את הראשוניים של פרמה.

3.8.2008 4.3

1. (א) הוכח שהמשוואה $a_1x_1 + \ldots + a_nx_n = b$ כאשר $a_1, \ldots, a_n, b \in \mathbb{Z}$ פתירה מעל השלמים אם"ם היא פתירה מודולו m לכל $0 < m \in \mathbb{Z}$. (ב) הוכח את התוצאה האנלוגית עבור מערכת משוואות לינאריות.

2. השתמש בסמל לז'נדר על־מנת להראות שלמשוואה $(x^2-13)(x^2-17)(x^2-221) \equiv 0 \pmod m$ יש פתרון מודולו m לכל m שלם, אבל אין לה פתרון מעל השלמים.

3. יהי $p \neq 2$ ראשוני. נתבונן בתבנית הריבועית $f(x,y) = ax^2+bxy+cy^2$. הדיסקרימיננטה שלה מוגדרת להיות $d = ac - b^2$. הוכח שלמשוואה $f(x,y) \equiv 0 \pmod p$ יש פתרון שונה מ־0 אם"ם $d \equiv 0 \ (p)$ או $(\frac{-d}{p}) = 1$.

   הדרכה: יש פתרון אם"ם קיים וקטור $0 \neq v \in \mathbb{F}_p^2$ כך ש־$v^T Av = 0$, כאשר $A = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$.

   הוכח ש־A שקולה לתבנית ריבועית: זאת אומרת, קיימת מטריצה הפיכה C שמקיימת $C^T AC = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right) = A'$ ושקילות משנה את הדיסקרימיננטה בהכפלתה בשארית ריבועית. לכן התבנית שקולה לתבנית $f'(x,y) = \alpha x^2 + \beta y^2$ ומספיק להראות שלזו יש פתרון שונה מ־0 עם $d' = \alpha\beta$ ומספיק להוכיח שלזאת יש פתרון. אם $\alpha\beta = 0$, קל; אם $\alpha\beta \neq 0$, זה שקול לפתרון $d = (\frac{\beta y}{x})^2 \pmod p$.

4. הוכח שבשדה המספרים ה־p־אדיים, הסדרה $x_n = 1 + p + \ldots + p^{n-1}$ מתכנסת ל־$\frac{1}{1-p}$.

5. הוכח שלמשוואה $f(x) \equiv 0 \pmod{p^n}$ יש פתרון לכל n (p ראשוני קבוע) אם"ם יש לה פתרון בחוג המספרים ה־p־אדיים השלמים.

6. רשום את המספר $\frac{2}{3}$ בחוג $\hat{\mathbb{Z}}_5$ של המספרים השלמים ב־5־אדיים (כטור חזקות $\sum_{i=0}^{\infty} a_i 5^i$, $0 \leq a_i < 5$).

7. הוכח שבחוג $\hat{\mathbb{Z}}_p$ אין איבר $x \neq 1$ המקיים $x^p = 1$.

8. הוכח שבמספרים ה־p־אדיים הטור $\sum_{i=1}^{\infty} \alpha_i$ מתכנס אם"ם $\lim_{i\to\infty} \alpha_i = 0$.

9. אם $p \neq 2$ ו־$d \in \hat{\mathbb{Z}}_p$ כך ש־$d \equiv 1 \pmod p$ אזי ל־d יש שורש ב־$\hat{\mathbb{Z}}_p$. יתר על כן, אם $d = \sum_{n=0}^{\infty} a_n p^n$ אזי ל־d יש שורש ריבועי ב־$\hat{\mathbb{Z}}_p$ אם"ם $(\frac{a_0}{p}) = 1$.