תורת המספרים

מאיה פרבר ברודסקי

סיכומי ההרצאות של פרופ' דורון פודר, סמסטר ב' תשפ"א, אוניברסיטת תל אביב.

תוכן עניינים

1 אריתמטיקה בסיסית של השלמים

1.1 חלוקה עם שארית

הגדרה 1.1 ערך שלם עבור $x \in \mathbb{R}$, נסמן $\lfloor x \rfloor = \min \{n \in \mathbb{Z} \mid n \leq x\}$ את הערך השלם של x.

טענה 1.2 חלוקה עם שארית יהיו $a, b \in \mathbb{Z}$ עם $a > 0$. אזי קיימים ויחידים $q, r \in \mathbb{Z}$ כך ש־$b = qa + r$ ו־$0 \leq r < a$. במקרה זה, r נקראת השארית בחלוקת b ב־a.

הוכחה: נגדיר $q = \left\lfloor \frac{b}{a} \right\rfloor$ וכן $r = b - qa$. כמובן מתקיים $b = qa + r$, נותר להוכיח $0 \leq r < a$ ויחידות.

מתקיים $\frac{b}{a} - 1 < \left\lfloor \frac{b}{a} \right\rfloor \leq \frac{b}{a}$ מאי השוויון $>$ נובע $\frac{b}{a} - 1 < q$ ולכן $b - a < qa$ כלומר $r = b - qa < a$. מאי השוויון $\leq$ נובע $q \leq \frac{b}{a}$ ולכן $qa \leq b$ כלומר $r = b - qa \geq 0$. בסך הכל, $0 \leq r < a$.

עבור יחידות, נניח $b = q'a + r'$ עם $0 \leq r' < a$ אז $r - r' = (b - qa) - (b - q'a) = (q' - q)\, a$, כלומר $r - r'$ כפולה של a אבל מתוך $0 \leq r, r' < a$ מקבלים $-a < r - r' < a$ ולכן בהכרח $(q' - q)\, a = r - r' = 0$, כלומר $r = r'$ וכן $q' - q = 0$ (כי $a > 0$) ולכן $q = q'$, וקיבלנו יחידות. ■

1.2 מחלקים ו־gcd

הגדרה 1.3 מחלק עבור $a, b \in \mathbb{Z}$ נסמן $a \mid b$ אם a מחלק את b, כלומר אם קיים $c \in \mathbb{Z}$ כך ש$ac = b$.

טענה 1.4 תכונות בסיסיות

1. $1 \mid n$ לכל $n \in \mathbb{Z}$ ־ כי $n = 1 \cdot n$.
2. $n \mid 0$ לכל n ־ כי $0 = 0 \cdot n$.
3. $0 \nmid n$ אלא אם $n = 0$ ־ כי $0 \cdot m = 0$ לכל m.
4. אם $b \neq 0$ וגם $a \mid b$ אז $|a| \leq |b|$ ־ קיים c כך ש$ac = b$, ואז $|a|\,|c| = |b|$, $b \neq 0$ לכן $c \neq 0$ כלומר $|c| \geq 1$, ולכן $|a| \leq |b|$.
5. אם $n \mid a$ וגם $n \mid b$ אז $n \mid xa + yb$ לכל $x, y \in \mathbb{Z}$ ־ קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש$\alpha n = a, \beta n = b$ ולכן $xa + yb = x\alpha n + y\beta n = (x\alpha + y\beta)\, n$ ולכן $n \mid xa + yb$.
6. אם $b \mid a$ וגם $a \mid b$ אז $a = b$ או $a = -b$ ־ אם $b = 0$ הטענה ברורה, אחרת מתקיים $a = mb, b = na$ ולכן $b = na = n \cdot mb$ ולכן $b\,(1 - nm) = 0$, $b \neq 0$ ולכן $nm = 1$, בפרט $|n|\,|m| = 1$ אבל $|m|, |n| \geq 1$ ולכן $|n| = |m| = 1$, אם $n = m = 1$ אז $a = b$ ואם $n = m = -1$ אז $a = -b$.

הגדרה 1.5 מחלק משותף, gcd יהיו $a, b \in \mathbb{Z}$ כך ש$(a, b) \neq (0, 0)$. מחלק משותף של a, b הוא שלם $d \in \mathbb{Z}$ המקיים $d \mid a, d \mid b$. מחלק משותף מקסימלי, או gcd, הוא $D \in \mathbb{Z}$ שהוא מחלק משותף של a, b ומקסימלי ביחס לסדר החלוקה, כלומר אם $d \in \mathbb{Z}$ מחלק משותף של a, b אז $d \mid D$. מסמנים $D = \gcd(a, b) = (a, b)$.

טענה 1.6 יחידות הgcd הוא יחיד עד כדי כפל בהפיך, כלומר ± 1.

הוכחה: אם D_1, D_2 שניהם gcd אז $D_1 \mid D_2, D_2 \mid D_1$ ולכן $D_1 = D_2$ או $D_1 = -D_2$. ■

משפט 1.7 קיום לכל $a, b \in \mathbb{Z}$ לא שניהם 0 יש gcd.

הוכחה: נתבונן בקבוצה $I = \{xa + yb \mid x, y \in \mathbb{Z}\}$. נשים לב כי I סגורה לחיבור ולכפל בסקלר שלם, כלומר אם $i_1, i_2 \in I$ אז $i_1 + i_2 \in I$, וכן אם $i \in I, m \in \mathbb{Z}$ אז $mi \in I$.

אכן, אם $i_1 = x_1 a + y_1 b, i_2 = x_2 a + y_2 b$ אז $i_1 + i_2 = (x_1 + x_2)\, a + (y_1 + y_2)\, b \in I$ מסגירות השלמים לחיבור, ואם $i = xa + yb, m \in \mathbb{Z}$ אז $mi = mxa + mby \in I$ מסגירות השלמים לכפל.

בI יש מספרים חיוביים, יהי $D \in I$ החיובי המינימלי בI. נטען שכל $i \in I$ הוא כפולה של d. יהי $i \in I$ ונחלק אותו עם שארית בD, $i = qD + r$ כאשר $0 \le r < D$. מתקיים $D \in I, q \in \mathbb{Z}$ לכן מהתכונות שהראינו $qD \in I$ ומכאן גם $r = i - qD \in I$. קיבלנו $r \in I$ וכן $0 \le r < D$ ולכן $r = 0$, כי D הוא החיובי המינימלי בI. אז $i = qD$, כלומר i כפולה של D.

כעת נראה $D = \gcd(a, b)$. הוא מחלק משותף כי $a, b \in I$ ולכן כפי שהראינו שניהם כפולה של D. הוא מקסימלי כי אם $d \mid a, b$ אז $d \mid xa + yb$ לכל $x, y \in \mathbb{Z}$ ולכן d מחלק כל איבר בI ובפרט את D, כלומר $d \mid D$. ■

מסקנה 1.8 הלמה של בזו לכל $a, b \in \mathbb{Z}$ לא שניהם 0 יש $x, y \in \mathbb{Z}$ כך ש$\gcd(a, b) = xa + yb$.

הוכחה: נובע ישירות מההוכחה, בחרנו $D = \gcd(a, b) \in I = \{xa + yb \mid x, y \in \mathbb{Z}\}$. ■

הערה 1.9 חוגים קומטטיביים כלליים $\mathbb{Z}$ היא דוגמה לחוג קומטטיבי עם יחידה, מבנה אלגברי שמקיים את כל אקסיומות השדה פרט לקיום הופכי כפלי. דוגמאות נוספות הן $\mathbb{F}[x]$ חוג הפולינומים מעל שדה $\mathbb{F}$, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ חוג השלמים של גאוס.

בתוך חוג קומוטטיבי A, תת קבוצה $I \subseteq A$ נקראת אידיאל אם היא מקיימת את התכונות של הקבוצה I לעיל, כלומר אם $i_1, i_2 \in I$ אז $i_1 \pm i_2 \in I$, ואם $i \in I, a \in A$ אז $ai \in I$.

אלגוריתם 1.10 אוקלידס לחישוב gcd בהינתן $a, b \in \mathbb{Z}$ לא שניהם 0, נחלק עם שארית שוב ושוב:

$$\begin{aligned}
a &= q_1 b + r_1 & 0 &< r_1 < b \\
b &= q_2 r_1 + r_2 & 0 &< r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &< r_3 < r_2 \\
&\vdots \\
r_{k-2} &= q_k r_{k-1} + r_k & 0 &< r_k < r_{k-1} \\
r_{k-1} &= q_{k+1} r_k + 0
\end{aligned}$$

עוצרים כאשר מקבלים שארית אפס, ואז ה־gcd הוא r_k.

טענה 1.11 נכונות האלגוריתם האלגוריתם תמיד עוצר, אחרי לכל היותר $c \cdot \log(\min\{a, b\})$ צעדים עבור $c > 0$ קבוע. הוא מחזיר את התוצאה הנכונה, כלומר $r_k = \gcd(a, b)$, והוא מספק גם דרך למצוא את מקדמי בזו.

הוכחה: מתקיים $b > r_1 > r_2 > \cdots$ זו סדרה יורדת של שלמים חיוביים ולכן חייבים להגיע לאפס, כלומר האלגוריתם חייב לעצור. את הסיבוכיות לא הוכחנו בכיתה.

על מנת להראות נכונות נראה שאם $a = qb + r$ אז $\gcd(a, b) = \gcd(b, r)$. אכן, לשני הזוגות אותם מחלקים משותפים כי אם $d \mid a, b$ אז $d \mid b, d \mid a - qb = r$. להיפך, אם $d \mid b, d \mid r$ אז $d \mid b, d \mid qb + r = a$. כעת, נשתמש בכך עבור ה$r_i$ים ונקבל

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$$

כדי למצוא את מקדמי בזו מהאלגוריתם, נכתוב בצורה איטרטיבית את השאריות כקומבינציות לינאריות

$$\begin{aligned}
r_1 &= a - q_1 b \\
r_2 &= b - q_2 r_1 = b - q_2 (a - q_1 b) = -q_2 a + (1 + q_2 q_1) b \\
&\vdots \\
r_k = \gcd(a, b) &= \ldots
\end{aligned}$$

■

הגדרה 1.12 $a, b \in \mathbb{Z}$ נקראים זרים אם $\gcd(a, b) = \pm 1$.

1.3 משוואות דיופנטיות לינאריות

הגדרה 1.13 משוואה דיופנטית זו משוואה עם נעלמים שמחפשים עבורה פתרונות בשלמים.

פתרון משוואה דיופנטית לינארית במשתנה אחד יהיו $a,b\in\mathbb{Z}$, יש פתרון ל$ax=b$ אם ורק אם $a\mid b$, ואז יש פתרון יחיד $\frac{b}{a}$, אלא אם $a=b=0$ ואז יש אינסוף פתרונות.

פתרון משוואה דיופנטית לינארית בשני משתנים יהיו $a,b,c\in\mathbb{Z}$, יש פתרון ל$ax+by=c$ אם ורק אם $\gcd\left(a,b\right)\mid c$, זאת כי ראינו $I=\left\{ax+by\mid x,y\in\mathbb{Z}\right\}$ ובI ה$\gcd$ הוא המינימלי, וכל איבר אחר בI הוא כפולה שלו. נניח כי אכן $\gcd\left(a,b\right)\mid c$, אז אם $\left(x_0,y_0\right)$ פתרון פרטי (ניתן למצוא לדוגמה מהלמה של בזו) אז קבוצת הפתרונות היא

$$\left\{\left(x_0-\frac{b}{\gcd\left(a,b\right)}k,y_0+\frac{a}{\gcd\left(a,b\right)}k\right)\mid k\in\mathbb{Z}\right\}$$

הוכחה: נניח $ax_1+by_1=c,ax_2+by_2=c$ אז $a\left(x_1-x_2\right)+b\left(y_1-y_2\right)=0$ ולכן $a\Delta x=-b\Delta y$ ואז $\Delta x=-\frac{b}{a}\Delta y$. נרשום $a=a'\cdot\gcd\left(a,b\right),b=b'\cdot\gcd\left(a,b\right)$ אז $\Delta x=\frac{b'}{a'}\Delta y$ וכן a',b' זרים, זה צריך להיות מספר שלם וזה קורה אם ורק אם $a'\mid\Delta y$, כלומר $\Delta y=ka'=k\frac{a}{\gcd(a,b)}$ לאיזשהו $k\in\mathbb{Z}$, ואז $\Delta x=-\frac{b'}{a'}k\frac{a}{\gcd(a,b)}=-\frac{b}{\gcd(a,b)}k$. ■

2 ראשוניים והמשפט היסודי של האריתמטיקה

הגדרה 2.1 ראשוני $p\in\mathbb{N}$ עם $p\geq 2$ נקרא ראשוני אם המחלקים שלו הם רק $\pm1,\pm p$.

למה 2.2 אוקלידס יהיו $a,b\in\mathbb{Z}$, p ראשוני. אם $p\mid ab$ אז $p\mid a$ או $p\mid b$.

הוכחה: נניח $p\mid ab$ וכן $p\nmid a$, אז $\gcd(a,p)=1$ ולפי הלמה של בזו ניתן לרשום $1=xa+yp$ עבור $x,y\in\mathbb{Z}$, ואז $b=b\cdot 1=b(xa+yp)=bxa+byp$. מתקיים $p\mid ab$ ולכן $p\mid bxa$, כמו כן $p\mid byp$ ולכן $p\mid bxa+byp=b$. ■

הערה 2.3 באופן כללי, בחוג קומטטיבי עם יחידה איבר x נקרא ראשוני אם הוא מקיים את התכונה של הלמה, ואיבר x נקרא אי פריק אם הוא מתחלק רק בעצמו או בהפיכים בחוג. איבר ראשוני הוא תמיד אי פריק, אבל ההפך לא תמיד נכון (בשלמים כן, זו בדיוק הלמה של אוקלידס).

משפט 2.4 היסודי של האריתמטיקה כל $n\in\mathbb{N}$ נתון באופן יחיד (עד כדי שינוי סדר) כמכפלה של ראשוניים.

הוכחה: קיום: באינדוקציה על n, $n=2$ ברור ועבור הצעד נניח שהטענה נכונה לכל $2\leq m\leq n-1$, אז עבור n, אם n ראשוני סיימנו, ואחרת בהכרח יש $k\in\mathbb{N}$ כך ש$k\mid n$ וכן $k\neq 1,n$, כלומר $2\leq k\leq n-1$ וכן $2\leq\frac{n}{k}\leq n-1$ ולכן ניתן לכתוב את $k,\frac{n}{k}$ כמכפלה של ראשוניים, וn יהיה מכפלת המכפלות הללו.

יחידות: לכל $n\geq 2$ נסמן ב$k(n)$ את אורך המכפלה הקצרה ביותר של ראשוניים ששווה לn. נראה באינדוקציה על $k(n)$, עבור $k(n)=1$ n ראשוני ולכן אם $n=p_1\cdots p_k$ אז בפרט $p_1\mid n$ אבל n ראשוני ולכן $p_1=n$, ואז $p_2\cdots p_k=1$ כלומר זו שוב מכפלה של ראשוני אחד, n. עבור הצעד, נניח שהטענה נכונה לכל m עם $k(m)<k(n)$ ונניח $n=p_1p_2\cdots p_{k(n)}=q_1q_2\cdots q_r$ אז בפרט $q_r\mid p_1\cdots p_{k(n)}$ ולפי הפעלה חוזרת של הלמה של אוקלידס $q_r\mid p_i$ לאיזה $1\leq i\leq k(n)$, בה"כ $q_r\mid p_{k(n)}$, שניהם ראשוניים ולכן שווים. קיבלנו $\frac{n}{q_r}=p_1p_2\cdots p_{k(n)-1}=q_1q_2\cdots q_{r-1}$ ולפי הנחת האינדוקציה אלו אותם ראשוניים עד כדי שינוי סדר, ולכן גם $p_1,\ldots,p_{k(n)}$ ו$q_1,\ldots,q_{r-1}$ הם אותם ראשוניים עד כדי שינוי סדר. ■

הערה 2.5 גרסה של המשפט נכונה בכל חוג בו אי פריק שקול לראשוני.

מסקנה 2.6 אם נכתוב $n=p_1^{r_1}\cdots p_k^{r_k}$ עם $p_1<p_2<\cdots<p_k$ וכן $r_i\in\mathbb{N}$ אז המחלקים של n הם $\pm p_1^{s_1}\cdots p_k^{s_k}$ כאשר $0\leq s_i\leq r_i$, ובפרט מספר המחלקים הוא $2(r_1+1)\cdots(r_k+1)$.
אם $a=\pm p_1^{r_1}\cdots p_k^{r_k}, b=\pm p_1^{s_1}\cdots p_k^{s^k}$ כאשר $s_i,r_i\in\mathbb{N}\cup\{0\}$ אז $\gcd(a,b)=\pm p_1^{\min\{r_1,s_1\}}\cdots p_k^{\min\{r_k,s_k\}}$.

הגדרה 2.7 הlcm בהינתן $a,b\in\mathbb{Z}$ לא שניהם 0, הlcm הוא $L\in\mathbb{Z}$ שמקיים $a,b\mid L$ וכן אם $a,b\mid\ell$ אז $L\mid\ell$.

טענה 2.8 אם $a=\pm\prod_{i=1}^{k}p_i^{r_i}, b=\pm\prod_{i=1}^{k}p_i^{s_i}$ אז $\operatorname{lcm}(a,b)=\pm\prod_{i=1}^{k}p_i^{\max\{r_i,s_i\}}$ וכן $\operatorname{lcm}(a,b)\gcd(a,b)=\pm ab$.

משפט 2.9 אוקלידס יש אינסוף מספרים ראשוניים.

הוכחה: נניח בשלילה שיש מספר סופי $p_1,\ldots,p_n$ של ראשוניים, נסמן $N=p_1p_2\cdots p_n+1$ אז לכל i נניח בשלילה $p_i\mid N$ אז מכך ש$p_i\mid p_1\cdots p_n$ נובע $p_i\mid N-p_1\cdots p_n=1$, בסתירה לכך ש$p_i$ ראשוני. כלומר אף אחד מבין הראשוניים לא מחלק את N, ובפרט לא ניתן לרשום את N כמכפלה של ראשוניים, בסתירה למשפט היסודי של האריתמטיקה. אז יש אינסוף ראשוניים. ■

משפט 2.10 דיריכלה (ללא הוכחה) לכל $a,d\in\mathbb{N}$ זרים יש אינסוף ראשוניים בסדרה $a+d,a+2d,a+3d,\ldots$.

דוגמה 2.11 בקבוצה $\{4k+3\mid k\in\mathbb{N}\}$ נוכל להוכיח שיש, נניח בשלילה שיש מספר סופי $q_1,\ldots,q_r$. אם המכפלה נותנת שארית 1 בחלוקה ב4 נסמן $N=q_1\cdots q_n+2$, אם שארית 3 נסמן $N=q_1\cdots q_n+4$. בכל מקרה שארית החלוקה של N ב4 היא 3 ולכן בפירוק לראשוניים של N יש ראשוני מהצורה $4k+3$ (אחרת כולם עם שארית 1 ולכן גם N), נניח q_i. אז $q_i\mid N-q_1\cdots q_n$ כלומר $q_i\mid 2$ או $q_i\mid 4$, וזו סתירה.

השערת התאומים הראשוניים יש אינסוף ערכים של $n\in\mathbb{N}$ כך ש$n,n+2$ שניהם ראשוניים (השערה פתוחה).

2.1 משפט המספרים הראשוניים

נסמן $p_1 < p_2 < \cdots$ את הראשוניים, ונגדיר $\pi(x) = \#\{p \le x \mid p \text{ is prime}\}$.
מתקיים $\pi(p_n) = n$, ולכן אם נבין טוב את $\pi(x)$ נוכל להבין גם מהו סדר הגודל של p_n.

טענה 2.12 חסם ראשון $p_n < 2^{2^n}$, ולכן לכל $x \ge 2$ מתקיים $\pi(x) \ge \log_2 \log_2 x - 1$.

הוכחה: לכל n נגדיר $q_n = p_1 \cdots p_n + 1$ אז כל גורם ראשוני של q_n הוא p_k עם $n < k$, ובפרט $p_{n+1} \le p_k \le q_n$.
באינדוקציה, עבור $n = 1$ מתקיים $p_1 = 2 < 2^{2^1} = 4$, נניח עבור n אז

$$p_{n+1} \le p_1 \cdots p_n + 1 < 2^{2^1} \cdots 2^{2^n} + 1 = 2^{2^{n+1}-2} + 1 < 2^{2^{n+1}}$$

■

משפט 2.13 המספרים הראשוניים (ללא הוכחה) $\pi(x) \sim \frac{x}{\log x}$, כלומר $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$.

הערה 2.14 משפט זה שקול ל$p_n \sim n \log n$, כי $\pi(n \log n) \sim \frac{n \log n}{\log(n \log n)} = \frac{n \log n}{\log n + \log \log n} \sim \frac{n \log n}{\log n} = n$.
במילים אחרות, לכל $0 < a < 1 < b$ יש $x_0 > 0$ כך שלכל $x \ge x_0$ מתקיים $a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}$.

משפט 2.15 צ'בישב קיימים $0 < a < 1 < b$ כך שלכל $x \ge 2$ מתקיים $a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}$.

הוכחה: חסם עליון

למה א': לכל $x \in \mathbb{R}$ מתקיים $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0,1\}$.

הוכחה: $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$ ולכן $2\lfloor x \rfloor \le 2x < 2\lfloor x \rfloor + 2$, ומכאן $2\lfloor x \rfloor \le \lfloor 2x \rfloor \le 2\lfloor x \rfloor + 1$, נחסיר $2\lfloor x \rfloor$ ונקבל $0 \le \lfloor 2x \rfloor - 2\lfloor x \rfloor \le 1$.

כעת נראה $\pi(x) - \pi\left(\frac{x}{2}\right) < \beta\frac{x}{\log x}$ עבור $1 < \beta$ כלשהו.

יהי n טבעי, אז $\pi(2n) - \pi(n) = \#\{n < p \le 2n \mid p \text{ is prime}\}$. מתקיים $\prod_{n<p\le 2n} p \mid \binom{2n}{n} = \frac{(2n)!}{n!n!}$ כי כל הראשוניים מופיעים רק במונה. בפרט $n^{\pi(2n)-\pi(n)} < \prod_{n<p\le 2n} p < \binom{2n}{n}$, נוציא $\log$ ונקבל

$$(\pi(2n) - \pi(n)) \log n < \log \binom{2n}{n} < \log\left(2^{2n}\right) = 2n \cdot \log 2$$

ולכן $\pi(2n) - \pi(n) < 2\log 2\frac{n}{\log n} = \beta_1 \frac{n}{\log n}$, עדיין צריך להוכיח את הטענה עבור $x \in \mathbb{R}$ כללי.
נניח $x \ge 8$, אז

$$\pi(x) - \pi\left(\frac{x}{2}\right) = \pi(\lfloor x \rfloor) - \pi\left(\left\lfloor \frac{x}{2} \right\rfloor\right) \overset{\text{Lemma (a)}}{\le} 1 + \pi\left(2 \cdot \left\lfloor \frac{x}{2} \right\rfloor\right) - \pi\left(\left\lfloor \frac{x}{2} \right\rfloor\right) < 1 + \beta_1 \frac{\left\lfloor \frac{x}{2} \right\rfloor}{\log \left\lfloor \frac{x}{2} \right\rfloor} \le 1 + \beta_1 \frac{\frac{x}{2}}{\log\left(\frac{x}{2} - 1\right)}$$
$$= 1 + \frac{\beta_1}{2} \cdot \frac{x}{\log\left(\frac{x}{2} - 1\right)} \overset{x\ge 8 \implies \frac{x}{2}-1 \ge \sqrt{x}}{\le} 1 + \frac{\beta_1}{2}\frac{x}{\log\sqrt{x}} = 1 + \beta_1\frac{x}{\log x} < (1+\beta_1)\frac{x}{\log x}$$

עבור $2 \le x < 8$ נמצא $\beta_2 > 0$ כך ש$\pi(x) - \pi\left(\frac{x}{2}\right) \le \beta_2\frac{x}{\log x}$, קיים כי $\pi(x) - \pi\left(\frac{x}{2}\right) \in \{1,2\}$ ואילו $\frac{x}{\log x}$ חסומה מלמטה על ידי איזה $m > 0$. נגדיר $\beta = \max\{\beta_2, 1+\beta_1\}$ וקיבלנו לכל $x \ge 2$ את $\pi(x) - \pi\left(\frac{x}{2}\right) < \beta\frac{x}{\log x}$.
לסיום ההוכחה, מתקיים לכל $x \ge 2$

$$\pi(x)\log x - \pi\left(\frac{x}{2}\right)\log\left(\frac{x}{2}\right) = \pi(x)\log x - \pi\left(\frac{x}{2}\right)(\log x - \log 2) = \left(\pi(x) - \pi\left(\frac{x}{2}\right)\right)\log x + \pi\left(\frac{x}{2}\right)\log 2$$
$$< \beta\frac{x}{\log x} \cdot \log x + \frac{x}{2}\log 2 = \left(\beta + \frac{\log 2}{2}\right)x = \beta_3 x$$

כעת, ניקח m כך ש$\frac{x}{2^{m+1}} < 2 \le \frac{x}{2^m}$ אז

$$\pi(x)\log x = \left(\sum_{i=0}^{m} \pi\left(\frac{x}{2^i}\right)\log\left(\frac{x}{2^i}\right) - \pi\left(\frac{x}{2^{i+1}}\right)\log\left(\frac{x}{2^{i+1}}\right)\right) < \sum_{i=0}^{m} \beta_3\frac{x}{2^i} =< 2\beta_3 x = bx$$

ולכן $\pi\left(x\right)<b\frac{x}{\log x}$ לכל $x\geq2$, כדרוש.

חסם תחתון:

למה ב': עבור n טבעי וp ראשוני, נסמן בr_{p} את החזקה הגבוהה ביותר של p שהיא קטנה מn, כלומר $p^{r_{p}}\leq n<p^{r_{p}+1}$ אז החזקה הגבוהה ביותר של p שמחלקת את $n!$ היא $p^{\sum_{k=1}^{r_{p}}\left\lfloor \frac{n}{p^{k}}\right\rfloor }$.

הוכחה: $\left\lfloor \frac{n}{p^{k}}\right\rfloor$ הוא מספר המספרים בין $1,\ldots,n$ שמתחלקים בp^{k}, ולכן סופר תרומה אחת של כל מספר כזה לחזקה הכוללת של p. כך, המספר $1\leq r\leq n$, אם $p^{j}\mid r$ אבל $p^{j+1}\nmid r$ אז סופרים את r בדיוק j פעמים, ב$\left\lfloor \frac{n}{p}\right\rfloor ,\left\lfloor \frac{n}{p^{2}}\right\rfloor ,\ldots,\left\lfloor \frac{n}{p^{j}}\right\rfloor$.

כעת נראה $\binom{2n}{n}\mid\prod_{p\leq2n}p^{r_{p}}$ כאשר r_{p} מתאים ל$2n$, $p^{r_{p}}\leq2n<p^{r_{p}+1}$.

החזקה הגבוהה ביותר של p שמחלקת את $\left(2n\right)!$ היא $\sum_{k=1}^{r_{p}}\left\lfloor \frac{2n}{p^{k}}\right\rfloor$, ואת $n!$ היא $\sum_{k=1}^{r_{p}}\left\lfloor \frac{n}{p^{k}}\right\rfloor$, ולכן חזקת p שמופיעה ב$\binom{2n}{n}$ היא

$$\sum_{k=1}^{r_{p}}\left\lfloor \frac{2n}{p^{k}}\right\rfloor -2\left\lfloor \frac{n}{p^{k}}\right\rfloor \overset{\text{Lemma (a)}}{\leq}\sum_{k=1}^{r_{p}}1=r_{p}$$

ולכן אכן $\binom{2n}{n}\mid\prod_{p\leq2n}p^{r_{p}}$, ובפרט

$$\binom{2n}{n}\leq\prod_{p\leq2n}p^{r_{p}}\overset{p^{r_{p}}\leq2n}{\leq}\left(2n\right)^{\pi\left(2n\right)}\overset{\log}{\Longrightarrow}n\log2=\log\left(2^{n}\right)\leq\log\binom{2n}{n}\leq\pi\left(2n\right)\log2n$$

קיבלנו $\pi\left(2n\right)\geq\frac{\log2}{2}\cdot\frac{2n}{\log2n}=a_{1}\frac{2n}{\log2n}$, הוכחנו את הרצוי לכל הזוגיים וצריך להוכיח ל$2\leq x\in\mathbb{R}$ כללי.

נניח $x\geq4$, אז

$$\pi\left(x\right)\geq\pi\left(2\cdot\left\lfloor \frac{x}{2}\right\rfloor \right)\geq a_{1}\frac{2\left\lfloor \frac{x}{2}\right\rfloor }{\log\left(2\left\lfloor \frac{x}{2}\right\rfloor \right)}\overset{\text{Lemma (a)}}{\geq}a_{1}\frac{\left\lfloor x\right\rfloor -1}{\log\left(2\cdot\frac{x}{2}\right)}\geq a_{1}\frac{x-2}{\log x}\overset{x\geq4\implies x-2\geq\frac{1}{2}x}{\geq}\frac{a_{1}}{2}\frac{x}{\log x}$$

עבור $x\in\left[2,4\right]$ יש a_{2} כך ש$\pi\left(x\right)\geq a_{2}\frac{x}{\log x}$, ניקח $a=\min\left\{ a_{2},\frac{a_{1}}{2}\right\}$ ואז לכל $x\geq2$ מתקיים $a\frac{x}{\log x}\leq\pi\left(x\right)$. ■

מסקנה 2.16 קיימים $\alpha,\beta>0$ כך שלכל $n\geq2$ טבעי מתקיים $\alpha n\log n<p_{n}<\beta n\log n$.

הוכחה: ראינו שקיימים $0<a<1<b$ כך ש$a\frac{x}{\log x}<\pi\left(x\right)<b\frac{x}{\log x}$. אז בפרט

$$n=\pi\left(p_{n}\right)<b\frac{p_{n}}{\log p_{n}}\implies p_{n}>\frac{1}{b}n\log p_{n}>\frac{1}{b}n\log n=\alpha n\log n$$

בכיוון השני, נשים לב כי לכל $n\geq\frac{2}{a}$ מתקיים $p_{n}\leq n^{4}$ שכן $\frac{r^{2}}{2}=\frac{r}{2}r<\frac{1}{a}r<\frac{p_{n}}{\log p_{n}}<\frac{\sqrt{p_{n}}}{2}$, וכעת לכל $n\geq\frac{2}{a}$

$$n=\pi\left(p_{n}\right)>a\frac{p_{n}}{\log p_{n}}\implies p_{n}<\frac{1}{a}n\log p_{n}\leq\frac{1}{a}n\log n^{4}=\frac{4}{a}n\log n$$

עבור $2\leq n\leq\frac{2}{a}$ יש מספר סופי של rים וניקח β_{1} כך שלכל אחד מהם מתקיים אי השוויון הרצוי, ואז עבור $\beta=\max\left\{ \frac{4}{a},\beta_{1}\right\}$ זה מתקיים. ■

טענה 2.17 $\sum_{n=1}^{\infty}\frac{1}{p_{n}}$ מתבדר.

הוכחה: לפי המסקנה מצ'בישב לכל $n\geq2$ מתקיים $\frac{1}{\beta n\log n}<\frac{1}{p_{n}}<\frac{1}{\alpha n\log n}$, ולכן

$$\sum_{n=1}^{\infty}\frac{1}{p_{n}}\text{ diverges}\iff\sum_{n=2}^{\infty}\frac{1}{n\log n}\text{ diverges}\iff\int_{2}^{\infty}\frac{1}{x\log x}dx\text{ diverges}$$

נחשב

$$\int_{2}^{\infty}\frac{1}{x\log x}dx=\left[\begin{array}{c}
t=\log x\\
\frac{dt}{dx}=\frac{1}{x}
\end{array}\right]=\int_{\log2}^{\infty}\frac{1}{t}dt=\left[\log t\right]_{\log2}^{\infty}=\left[\log\log x\right]_{2}^{\infty}=\infty$$

כלומר אכן מתבדר. ■

משפט 2.18 השערת ברטרנד לכל $n>1$ טבעי יש לפחות ראשוני אחד $n<p<2n$.

הוכחה: נוכיח בהסתמך על משפט המספרים הראשוניים, עבור $n>N_0$ מספיק גדול.
נבחר $0<a<1<b$ כלשהם כך ש$2a-b>0$, אז יש N_0 כך שלכל $n>N_0$ מתקיים $a\frac{n}{\log n}<\pi\left(n\right)<b\frac{n}{\log n}$, ואז

$$\pi\left(2n\right)-\pi\left(n\right)>a\frac{2n}{\log 2n}-b\frac{n}{\log n}=\frac{2an\log n-bn\log 2n}{\log n\cdot\log 2n}=n\cdot\frac{\left(2a-b\right)\log n-b\log 2}{\log n\cdot\log 2n}$$

בחרנו $2a-b>0$ אז עבור n גדול מספיק $\left(2a-b\right)\log n-b\log 2>0$ ואז $\pi\left(2n\right)-\pi\left(n\right)>0$ ובפרט יש ראשוני ביניהם. ■

השערת רימן

הגדרה 2.19 פונקציית Li מוגדרת $\mathrm{Li}\left(x\right)=\int_2^x\frac{1}{\log t}dt$.

טענה 2.20 $\mathrm{Li}\left(x\right)\sim\frac{x}{\log x}$, כלומר $\frac{\mathrm{Li}(x)}{x/\log x}\xrightarrow{x\to\infty}1$ (תרגיל). ממשפט המספרים הראשוניים נובע $\mathrm{Li}\left(x\right)\sim\pi\left(x\right)$.

הגדרה 2.21 פונקציית זטא של רימן לכל s ממשי, מגדירים $\zeta\left(s\right)=\sum_{n=1}^{\infty}\frac{1}{n^s}$, זה מתכנס לכל $s>1$.

הערה 2.22 לכל $s>1$ מתקיים $\zeta\left(s\right)=\prod_{p\text{ is prime}}\frac{1}{1-\frac{1}{p^s}}$, וכן ניתן להעריך את $\zeta\left(s\right)$ גם עבור מרוכבים עם $\Re z>1$. יותר מזה, רימן גילה שיש המשכה אנליטית לζ, כלומר פונקציה אנליטית שמוגדרת על כל $\mathbb{C}\setminus\{1\}$ שמזדהה עם ζ בתחום ההגדרה שלה.

השערת רימן (גרסה 1) לכל $\beta>\frac{1}{2}$ קיים x_0 כך שלכל $x\geq x_0$ מתקיים $\left|\pi\left(x\right)-\mathrm{Li}\left(x\right)\right|\leq x^\beta$. כלומר, $\left|\pi\left(x\right)-\mathrm{Li}\left(x\right)\right|$ חסום בערך על ידי $\sqrt{x}$ (אבל לא ממש על ידיו, ידוע שהטענה לא נכונה עבור $\beta=\frac{1}{2}$).

השערת רימן (גרסה 2) כל האפסים הלא טריויאליים (לא $-2n$ כאשר $n\in\mathbb{N}$) של פונקציית זטא של רימן הם על הציר הקריטי $\Re z=\frac{1}{2}$.

3 קונגרואנציות

הגדרה 3.1 קונגרואנציה יהי n טבעי, נאמר כי $a,b\in\mathbb{Z}$ שווים מודולו n ונסמן $a\equiv b \mod n$ אם $n\mid a-b$.
נעיר כי זה יחס שקילות מודולו n, ובמילים אחרות טוען כי a,b נותנים אותה שארית חלוקה ב-n.

טענה 3.2 נניח $a_1\equiv a_2 \mod n$ וכן $b_1\equiv b_2 \mod n$ אז $a_1+b_1\equiv a_2+b_2 \mod n$ וכן $a_1b_1\equiv a_2b_2 \mod n$.
כלומר, ניתן להגדיר חיבור וכפל על מחלקות השקילות מודולו n, שנסמן $\bar{a}$ או $a+n\mathbb{Z}$.

הוכחה: עבור חיבור, מתקיים $n\mid a_1-a_2, n\mid b_1-b_2$ ולכן $n\mid(a_1-a_2)+(b_1-b_2)=(a_1+b_1)-(a_2-b_2)$ כלומר $a_1+b_1\equiv a_2+b_2 \mod n$. עבור כפל, מתקיים $n\mid a_1-a_2, n\mid b_1-b_2$ ולכן

$$a_1b_1-a_2b_2=a_1b_1-a_1b_2+a_1b_2-a_2b_2=a_1(b_1-b_2)+b_2(a_1-a_2)$$

ו-n מחלק אותו, כי זה צירוף לינארי. ■

מסקנה 3.3 יהי $f(x)\in\mathbb{Z}[x]$ פולינום עם מקדמים שלמים אז $a_1\equiv a_2 \mod n \implies f(a_1)\equiv f(a_2) \mod n$.

3.1 חוג השלמים מודולו n

הגדרה 3.4 נסמן $\mathbb{Z}_n={}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ את קבוצת מחלקות השקילות מודולו n. זה אכן חוג קומטטיבי עם יחידה.

טענה 3.5 יהי $a\in\mathbb{Z}$ ו-$n\geq 2$ טבעי. האיבר $\bar{a}$ הפיך ב-$\mathbb{Z}_n$ אם ורק אם $\gcd(a,n)=1$.

הוכחה: $\bar{a}$ הפיך $\iff$ קיים $b\in\mathbb{Z}$ כך ש-$ab\equiv 1 \mod n$ $\iff$ קיים $b\in\mathbb{Z}$ כך ש-$n\mid ab-1$ $\iff$ קיימים $b,k\in\mathbb{Z}$ כך ש-$kn=ab-1$ $\iff$ קיימים $b,k\in\mathbb{Z}$ כך ש-$ab-kn=1$ $\iff$ לפי הלמה של בזו, $\gcd(a,n)=1$. ■

מסקנה 3.6 $\mathbb{Z}_n$ שדה $\iff$ n ראשוני.

הוכחה: אם n ראשוני אז $\gcd(a,n)=1$ לכל $1\leq a\leq p-1$, ולכן כל $\bar{a}\neq\bar{0}$ ב-$\mathbb{Z}_p$ הוא הפיך, ו-$\mathbb{Z}_p$ מקיים את כל אקסיומות השדה. אם n אינו ראשוני אז יש לו מחלק לא טריויאלי d, ואז $\gcd(d,n)=d$ ול-$\bar{d}$ אין הופכי. ■

אלגוריתם 3.7 חישוב הופכי מודולו n כדי למצוא את ההופכי של a מודולו n נשתמש באלגוריתם אוקלידס כדי למצוא $x,y\in\mathbb{Z}$ כך ש-$ax+ny=\gcd(a,n)$, אם $\gcd(a,n)\neq 1$ אין הופכי, ואם הוא 1 אז ההופכי הוא x.

הגדרה 3.8 חבורת ההפיכים נסמן $\mathbb{Z}_n^*$ קבוצת ההפיכים ב-$\mathbb{Z}_n$, זו חבורה אבלית ביחס לכפל.

הגדרה 3.9 פונקציית אוילר $\varphi(n)=|\mathbb{Z}_n^*|=\#\{1\leq a\leq n\mid\gcd(a,n)=1\}$. מתקיים $\varphi(p)=p-1$.

משפט 3.10 משפט השאריות הסיני אם $m,n\in\mathbb{N}$ זרים אז לכל $a,b\in\mathbb{Z}$ יש פתרון יחיד מודולו mn של המערכת $\begin{cases}x\equiv a \mod m\\ x\equiv b \mod n\end{cases}$.

הוכחה: **קיום:** נמצא $\hat{n},\hat{m}\in\mathbb{Z}$ כך ש-$n\hat{n}\equiv 1 \mod m, m\hat{m}\equiv 1 \mod n$ (קיימים כי n,m זרים ולכן כל אחד מהם הפיך מודולו השני), ונגדיר $x=an\hat{n}+bm\hat{m}$ אז $x\equiv an\hat{n}\equiv a \mod m, x\equiv bm\hat{m}\equiv b \mod n$ הוא פתרון.
יחידות: משיקולי ספירה, יש בדיוק mn מחלקות מודולו mn ויש פתרון לכל אחת מ-mn המערכות האפשריות (בחירה של a,b), ולכן הפתרון הוא יחיד. ■

אלגוריתם 3.11 פתרון מערכת מהצורה $\begin{cases}x\equiv a_1 \mod n_1\\ \vdots\\ x\equiv a_k \mod n_k\end{cases}$ **כאשר** $n_1,\ldots,n_k$ **זרים בזוגות**

לכל i נמצא $\hat{n}_i$ הופכי ל-$\prod_{j\neq i}n_j$ מודולו n_i באמצעות אלגוריתם אוקלידס (קיים, כי $n_1,\ldots,n_k$ זרים בזוגות ולכן n_i זר ל-$\prod_{j\neq i}n_j$), אזי הפתרון היחיד הוא $x\equiv\sum_{i=1}^{k}a_i\left(\prod_{j\neq i}n_j\right)\hat{n}_i \mod n_1\cdots n_k$.

מסקנה 3.12 ההעתקה $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ המוגדרת $x \to (x \mod m, x \mod n)$ היא חח"ע ועל, ומצטמצמת להעתקה חח"ע ועל $\mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. באופן יותר חזק, היא איזו' של חוגים, כלומר גם משמרת חיבור וכפל.

הוכחה: נראה את החלק השני, לגבי צמצום להפיכים.

$\subseteq$ יהי $x \in \mathbb{Z}_{mn}^*$ אז יש $y \in \mathbb{Z}$ כך ש$xy \equiv 1 \mod mn$, ולכן $mn \mid xy-1$ כלומר גם $m,n \mid xy-1$ ולכן $xy \equiv 1 \mod m, xy \equiv 1 \mod n$. כלומר x הפיך מודולו m ולכן $x \mod m \in \mathbb{Z}_m^*$, וכנ"ל עבור n. לכן $f(x) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

$\supseteq$ יהי $x \in \mathbb{Z}_{mn}$ כך ש$f(x) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ כלומר x הפיך מודולו m ומודולו n, אז יש y_1, y_2 כך ש$xy_1 \equiv 1 \mod m, xy_2 \equiv 1 \mod n$. לפי משפט השאריות הסיני יש פתרון יחיד מודולו mn למערכת $x \equiv y_1 \mod m, x \equiv y_2 \mod n$, נסמן אותו ב$x_0$ אז $xx_0 \equiv 1 \mod m, xx_0 \equiv 1 \mod n$ ומכך שm,n זרים נובע $xx_0 \equiv 1 \mod mn$, כלומר $x = x_0^{-1}$ הפיך מודולו mn.

אז התמונה של f על $\mathbb{Z}_{mn}^*$ היא בדיוק $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$, והיא גם חח"ע ועל כי היא חח"ע ועל בכל התחום. ∎

מסקנה 3.13 φ **כפלית** כלומר אם $m,n \in \mathbb{N}$ זרים אז $\varphi(mn) = \varphi(m)\varphi(n)$.

הוכחה: הפונקציה f מהמסקנה היא חח"ע ועל בצמצום, ולכן

$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m)\varphi(n)$$

∎

משפט 3.14 נוסחה עבור φ לכל $n \in \mathbb{N}$, $\varphi(n) = n \cdot \prod_{p|n}\left(1-\frac{1}{p}\right)$.

הוכחה: ראשית נוכיח עבור המקרה הפרטי $n = p^k$. אכן, מתקיים $p \nmid a \iff \gcd(a, p^k) = 1$, ולכן כל המספרים מ1 עד p^k זרים לו, מלבד p^{k-1} המספרים שמתחלקים בp. כלומר $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$ כדרוש. כעת, עבור $n \in \mathbb{N}$ כללי נרשום מהמשפט היסודי של האריתמטיקה $n = \prod_{i=1}^k p_i^{t_i}$, אז $p_i^{t_i}$ זרים ולכן מכפליות הפונקציה φ שהראינו

$$\varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{t_i}\right) = \prod_{i=1}^k \varphi\left(p_i^{t_i}\right) = \prod_{i=1}^k p_i^{t_i}\left(1-\frac{1}{p_i}\right) = \prod_{i=1}^k p_i^{t_i} \cdot \prod_{p|n}\left(1-\frac{1}{p}\right) = n \cdot \prod_{p|n}\left(1-\frac{1}{p}\right)$$

∎

מסקנה 3.15 לכל n טבעי $n = \sum_{d|n}\varphi(d)$.

הוכחה: נרשום $n = \prod_{i=1}^k p_i^{t_i}$, אזי המחלקים שלו הם בדיוק כל המספרים מהצורה $\prod_{i=1}^k p_i^{s_i}$ כאשר $0 \le s_i \le t_i$. אז

$$\sum_{d|n}\varphi(d) = \sum_{\substack{0 \le s_1 \le t_1 \\ \vdots \\ 0 \le s_k \le t_k}} \varphi\left(\prod_{i=1}^k p_i^{s_i}\right) = \sum_{\substack{0 \le s_1 \le t_1 \\ \vdots \\ 0 \le s_k \le t_k}} \left(\prod_{i=1}^k \varphi\left(p_i^{s_i}\right)\right) = \prod_{i=1}^k\left(\sum_{0 \le s_i \le t_i}\varphi\left(p_i^{s_i}\right)\right)$$
$$= \prod_{i=1}^k\left(1 + \sum_{1 \le s_i \le t_i}\left(p_i^{s_i} - p_i^{s_i-1}\right)\right) \overset{\text{telescopic sum}}{=} \prod_{i=1}^k p_i^{t_i} = n$$

∎

אלגוריתם 3.16 פתרון קונגרואנציה מהצורה $ax \equiv c \mod n$

ראינו שלמשוואה הדיופנטית הלינארית בשני נעלמים $ax + by = c$ יש פתרון $\iff$ $\gcd(a,b) \mid c$, ואם (x_0, y_0) פתרון פרטי אז קבוצת הפתרונות נתונה על ידי

$$\left\{\left(x_0 - k\frac{b}{\gcd(a,b)}, y_0 + k\frac{a}{\gcd(a,b)}\right) \mid k \in \mathbb{Z}\right\}$$

כעת נשים לב כי למשוואה $ax \equiv c \mod n$ יש פתרון $\iff$ למשוואה $ax + ny = c$ יש פתרון, כלומר $\iff$ $\gcd(a,n) \mid c$, ובמקרה זה יש $\gcd(a,n)$ פתרונות ב$\mathbb{Z}_n^*$ והם $\left\{x_0 + k\frac{n}{\gcd(a,n)} \mid k \in \{0,1,\ldots,n-1\}\right\}$.

4 חבורת ההפיכים ושורשים פרימיטיביים

4.1 החבורה הכפלית $\mathbb{Z}_n^*$

הגדרה 4.1 סדר בחבורת ההפיכים יהי $n \geq 2$, $a \in \mathbb{Z}_n^*$. הסדר של a הוא $\operatorname{ord}_n(a) = \min\left\{k \in \mathbb{N} \mid a^k \equiv 1 \mod n\right\}$.

טענה 4.2 אם $\operatorname{ord}_n(a) = k$, אז $a^m \equiv 1 \mod n \iff k \mid m$.

הוכחה: $\Longleftarrow$ נניח $a^m \equiv 1 \mod n$, נחלק את m בk עם שארית $m = qk + r$ כאשר $0 \leq r < k$. מתקיים

$$1 \equiv a^m \equiv a^{qk+r} \equiv \left(a^k\right)^q a^r \equiv a^r \mod n$$

ולכן אם $0 < r < k$ אז זו סתירה לכך ש$\operatorname{ord}_n(a) = k$, ומכאן בהכרח $r = 0$ כלומר $k \mid qk = m$.

$\Longrightarrow$ נניח $k \mid m$, נרשום $m = qk$ אז $a^m \equiv a^{qk} \equiv \left(a^k\right)^q \equiv 1^q \equiv 1 \mod n$. ■

משפט 4.3 פרמה־אוילר $\operatorname{ord}_n(a) \mid \varphi(n)$.

הוכחה: יהיו $x_1, \ldots, x_{\varphi(n)}$ איברי החבורה $\mathbb{Z}_n^*$, אזי גם $ax_1, \ldots, ax_{\varphi(n)}$ הם בדיוק כל איברי החבורה, אולי בסדר שונה. מכאן

$$\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} ax_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i \mod n$$

אך $\prod_{i=1}^{\varphi(n)} x_i$ הפיך לכן ניתן לכפול בהופכי שלו, ואז נקבל $a^{\varphi(n)} \equiv 1 \mod n$, ומהטענה $\operatorname{ord}_n(a) \mid \varphi(n)$. ■

מסקנה 4.4 המשפט הקטן של פרמה אם $a \in \mathbb{Z}$ מקיים $\gcd(a, p) = 1$ אז $a^{p-1} \equiv 1 \mod p$. או, לכל $a \in \mathbb{Z}$ מתקיים $a^p \equiv a \mod p$.

משפט 4.5 וילסון אם p ראשוני אז $\prod_{i=1}^{\varphi(p)} x_i \equiv -1 \mod p$, כלומר $(p-1)! \equiv -1 \mod p$.

הוכחה: אם $a \in \mathbb{Z}_p^*$ וכן $a^{-1} \neq a$ אז a, a^{-1} מתבטלים במכפלה. האיברים היחידים שלא מתבטלים הם אלה עם $a^{-1} = a$ כלומר $a^2 = 1$, ומכך שp ראשוני $\mathbb{Z}_p$ שדה ולכן זה רק $a \equiv \pm 1 \mod p$. כלומר המכפלה היא $1 \cdot (-1) = -1$, כדרוש. ■

משפט 4.6 אורך המחזור של $\frac{1}{N}$ בכתיב עשרוני אם $\gcd(N, 10) = 1$, אז אורך המחזור של $\frac{1}{N}$ הוא $\operatorname{ord}_N(10)$.

הוכחה: נבצע חילוק ארוך:

$$\begin{aligned}
10 &= a_1 N + r_1 \\
10r_1 &= a_2 N + r_2 \\
10r_2 &= a_3 N + r_3 \\
&\vdots
\end{aligned}$$

זה בדיוק התהליך שמבצעים בחילוק ארוך של $\frac{1}{N}$, והספרה הi אחרי הנקודה בכתיב העשרוני היא a_i.

מתקיים $r_1 \equiv 10 \mod N$ ובכל שלב $r_{i+1} \equiv 10r_i \mod N$, ולכן $r_i \equiv 10^i \mod N$. אורך המחזור הוא בדיוק הi הקטן ביותר כך ש$r_i \equiv 1 \mod N$ (כי אז מקבלים בשורה $10r_i = a_{i+1}N + r_{i+1}$ בדיוק את אותה חלוקה כמו בשורה הראשונה, ולכן $a_{i+1} = a_1$), שזה בדיוק $\operatorname{ord}_N(10)$ כדרוש. ■

4.2 שורש פרימיטיבי וקריטריון אוילר

הגדרה 4.7 שורש פרימיטיבי מודולו N הוא איבר $a\in\mathbb{Z}_N^*$ כך ש$\varphi(N)=\mathrm{ord}_N(a)$.

טענה 4.8 a הוא שורש פרימיטיבי מודולו N $\iff$ a יוצר את $\mathbb{Z}_N^*$.

הוכחה: a ש"פ $\iff$ $|\langle a\rangle|=\mathrm{ord}_N(a)=\varphi(N)=|\mathbb{Z}_N^*|$ $\iff$ $\langle a\rangle=\mathbb{Z}_N^*$. ■

הערה 4.9 אם יש שורש פרימיטיבי אז יש $\varphi(\varphi(n))$ כאלה, כי נניח a שורש פרימיטיבי אז כל איברי החבורה הם $1,a,a^2,\ldots,a^{\varphi(n)-1}$, ומתקיים $\mathrm{ord}_n(a^i)=\frac{\mathrm{ord}_n(a)}{\gcd(i,\mathrm{ord}_n(a))}$ כלומר שווה ל$\varphi(n)$ $\mathrm{ord}_n(a)=\varphi(n)$ אם ורק אם i זר ל$\mathrm{ord}_n(a)=\varphi(n)$, ויש בדיוק $\varphi(\varphi(n))$ iים כאלה, מהגדרה.

משפט 4.10 תנאי לקיום ש"פ יש שורש פרימיטיבי מודולו n $\iff$ $n=2,4,p^k,2p^k$ כאשר p אי זוגי, k שלם.

הוכחה: נוכיח רק את המקרה $n=p$, זה נקרא **משפט גאוס**.

לכל $d\mid p-1$, נסמן $\psi(d)=\#\left\{x\in\mathbb{Z}_p^*\mid \mathrm{ord}_n(x)=d\right\}$. אז $\sum_{d|p-1}\psi(d)=p-1$, כי לכל $x\in\mathbb{Z}_p^*$ מתקיים $\mathrm{ord}_n(x)\mid\varphi(p)=p-1$ ולכן זה בדיוק סכום על כל האיברים מסדר כלשהו, ולכל איבר יש סדר. כמו כן ראינו בעבר $\sum_{d|n}\varphi(d)=n$ לכל n, ובפרט עבור $p-1$. כלומר שוויון זה מתקיים עבור φ,ψ.

למה: אם $\psi(d)>0$ אז $\psi(d)=\varphi(d)$.

הוכחה: נניח $\psi(d)>0$, אז יש $x\in\mathbb{Z}_p$ עם $\mathrm{ord}_n(x)=d$. יש בדיוק d איברים שונים ב$\mathbb{Z}_p^*$ שהם חזקות של x, וכולם שורשים של הפולינום x^d-1. $\mathbb{Z}_p$ הוא שדה, ולכן לפולינום זה יש לכל היותר d שורשים, כלומר חזקות x הן בדיוק כל השורשים.

כמו כן, מתקיים $\mathrm{ord}_n(x^i)=\frac{\mathrm{ord}_n(x)}{\gcd(i,\mathrm{ord}_n(x))}=\frac{d}{\gcd(i,d)}$ ולכן יש בדיוק $\varphi(d)$ חזקות של d מסדר d, אלה עם מעריך זר לd. מכאן יש בדיוק $\varphi(d)$ איברים ב$\mathbb{Z}_p^*$ מסדר d בסך הכל, כי איברים שאינם חזקות של x לא יכולים להיות שורש של הפולינום x^d-1, ובפרט לא יכולים להיות מסדר d. כלומר, $\psi(d)=\varphi(d)$. ■

כעת, בהינתן הלמה, לכל $d\mid p-1$ מתקיים $\psi(d)\in\{0,\varphi(d)\}$, אך $\sum_{d|p-1}\varphi(d)=p-1=\sum_{d|p-1}\psi(d)$ ולכן בהכרח $\psi(d)=\varphi(d)$ לכל d, בפרט $\psi(p-1)=\varphi(p-1)$ ולכן יש $\varphi(p-1)=\varphi(\varphi(p))$ איברים ב$\mathbb{Z}_p^*$ מסדר $p-1=\varphi(p)$, כלומר $\varphi(\varphi(p))$ שורשים פרימיטיביים, ובפרט לא אפס. ■

משפט 4.11 קריטריון אוילר נניח כי ב$\mathbb{Z}_n^*$ יש שורש פרימיטיבי, ויהי $a\in\mathbb{Z}_N^*$. אזי יש פתרון למשוואה $x^m\equiv a \mod n$ $\iff$ $a^{\frac{\varphi(n)}{\gcd(m,\varphi(n))}}\equiv 1 \mod n$, ואם יש פתרון אז יש בדיוק $\gcd(m,\varphi(n))$ פתרונות.

הוכחה: נניח g ש"פ מודולו n ונסמן $d=\gcd(\varphi(n),m)$.

$\Leftarrow$ נניח $x^m\equiv a \mod n$, אז

$$a^{\frac{\varphi(n)}{d}}\equiv(x^m)^{\frac{\varphi(n)}{d}}\equiv\left(x^{\varphi(n)}\right)^{\frac{m}{d}}\equiv 1^{\frac{m}{d}}\equiv 1 \mod n$$

$\Longrightarrow$ נניח $a^{\frac{\varphi(n)}{d}}\equiv 1 \mod n$ ונרשום $a\equiv g^r \mod n$ (אפשר כי g ש"פ), אז $g^{\frac{r\cdot\varphi(n)}{d}}\equiv(g^r)^{\frac{\varphi(n)}{d}}\equiv 1 \mod n$, ולכן $\varphi(n)\mid\frac{r\cdot\varphi(n)}{d}$, כלומר $\frac{r}{d}$ שלם ולכן $\gcd(m,\varphi(n))=d\mid r$. אזי יש פתרון למשוואה הדיופנטית $mt+\varphi(n)s=r$, ולכן יש פתרון לקונגרואנציה $mt\equiv r \mod \varphi(n)$. נגדיר $x\equiv g^t \mod n$, אז

$$x^m\equiv\left(g^t\right)^m\equiv g^{mt}\equiv g^r\equiv a \mod n$$

למעשה יש $\gcd(m,\varphi(n))$ פתרונות לקונגרואנציה הנ"ל, ולכן גם למשוואה $x^m\equiv a \mod n$. ■

דוגמה 4.12 -1 הוא ריבוע מודולו $p>2$ $\iff$ $1\equiv(-1)^{\frac{\varphi(p)}{\gcd(2,\varphi(p))}}\equiv(-1)^{\frac{p-1}{2}} \mod p$ $\iff$ $p\equiv 1 \mod 4$.

5 שאריות ריבועיות

5.1 סימן לז'נדר וחוק ההדדיות הריבועית

הגדרה 5.1 שארית ריבועית $a \in \mathbb{Z}$ היא שארית ריבועית מודולו p אם קיים $x \in \mathbb{Z}$ כך ש$x^2 \equiv a \mod p$.

טענה 5.2 יהי $p > 2$ ראשוני, אז בדיוק חצי מאיברי $\mathbb{Z}_p^*$ הם שאריות ריבועיות.

הוכחה: אם $a \in \mathbb{Z}_p^*$ שארית ריבועית מודולו p אז יש $x \in \mathbb{Z}_p^*$ כך ש$x^2 \equiv a \mod p$, ומכאן גם $(-x)^2 \equiv a \mod p$. p אי זוגי לכן $x \not\equiv -x \mod p$, כלומר $x, -x$ שני שורשים שונים לפולינום $x^2 - a$ ב$\mathbb{Z}_p$. p ראשוני לכן $\mathbb{Z}_p$ שדה לכן לפולינום זה יש לכל היותר 2 שורשים, ומכאן $x, -x$ השורשים היחידים שלו.

כלומר לכל פולינום $x^2 - a$ עם $a \in \mathbb{Z}_p^*$ יש שני שורשים או אפס, וכל איבר ב$\mathbb{Z}_p^*$ הוא שורש של בדיוק פולינום אחד כנ"ל, ולכן משיקולי ספירה בדיוק לחצי מהפולינומים הנ"ל יש שורשים, כלומר בדיוק חצי מאיברי $\mathbb{Z}_p^*$ הם שאריות ריבועיות. ■

הגדרה 5.3 סימן לז'נדר עבור $p > 2$ ראשוני ו$a \in \mathbb{Z}$ (בדרך כלל נניח $p \nmid a$ כלומר a זר לp), נגדיר

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a, a \text{ is a quadratic residue mod } p \\ -1 & p \nmid a, a \text{ is a quadratic nonresidue mod } p \\ 0 & p \mid a \end{cases}$$

טענה 5.4 מסקנה מקריטריון אוילר יהי a זר לp, אז $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

הוכחה: אם $a^{\frac{p-1}{2}} \equiv 1 \mod p$ אז מקריטריון אוילר (ניתן להשתמש בו, כי ממשפט גאוס ב$\mathbb{Z}_p^*$ יש שורש פרימיטיבי) יש פתרון ל$x^2 \equiv a \mod p$ כלומר a שארית ריבועית מודולו p, ולכן מהגדרה גם $\left(\frac{a}{p}\right) \equiv 1 \mod p$.

אחרת, בכל מקרה ממשפט פרמה הקטן $\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \mod p$ ולכן $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$, ולכן בהכרח $a^{\frac{p-1}{2}} \equiv -1 \mod p$. במקרה זה מקריטריון אוילר a אינה שארית ריבועית, ואכן $\left(\frac{a}{p}\right) \equiv -1 \equiv a^{\frac{p-1}{2}} \mod p$. ■

טענה 5.5 תכונות של סימן לז'נדר

1. אם $a \equiv b \mod p$ אז $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. אם $p \nmid a$ אז $\left(\frac{a^2}{p}\right) = 1$.
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

הוכחה: 1 ו2 קל להוכיח, נראה את 3. אם $p \mid a$ או $p \mid b$ אז שני האגפים הם אפס. אחרת, נניח a, b שניהם זרים לp אז ממהמסקנה מקריטריון אוילר

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

■

משפט 5.6 חוק ההדדיות הריבועית יהיו $p \neq q$ ראשוניים אי זוגיים. אזי

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\ -\left(\frac{q}{p}\right) & p, q \equiv 3 \mod 4 \end{cases}$$

נספח 1: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$. נספח 2: $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$.

הוכחה: נתבונן באיברי $\mathbb{Z}_{pq}^*$, הם מתחלקים לזוגות של איברים שונים $\{x,-x\}$.
נבחר באופן שרירותי נציג אחד מכל זוג, ונכפול את הנציגים מודולו pq ־ המכפלה P מוגדרת ביחידות עד כדי סימן. נעביר את P דרך האיזומורפיזם $f\colon \mathbb{Z}_{pq}^*\to\mathbb{Z}_p^*\times\mathbb{Z}_q^*$ הנתונה ממשפט השאריות הסיני, ונקבל (a,b). בבחירה אחרת של הנציגים, אם מקבלים את המכפלה $-P$, הפונקציה תחזיר $(-a,-b)$. נחשב:

חישוב 1: נבחר את הנציג הקטן ביותר בכל זוג (כמספרים בין 1 לpq), כלומר את הנציגים מבין $1,2,\ldots,\frac{pq-1}{2}$.
כלומר, ניקח את כל המספרים הללו ונוריד את הכפולות של p,q:

$$\frac{[1\cdots(p-1)]\cdot[(p+1)\cdots(2p-1)]\cdots\left[\left(\left(\frac{q-1}{2}-1\right)p+1\right)\cdots\left(\frac{q-1}{2}p-1\right)\right]\cdots\left[\left(\frac{q-1}{2}p+1\right)\cdots\left(\frac{q-1}{2}p+\frac{p-1}{2}\right)\right]}{q\cdot 2q\cdots\left(\frac{p-1}{2}q\right)}$$

נעביר את P הזו דרך f (כדי לחשב מודולו q מבצעים תהליך סימטרי, מורידים כפולות q ואז מחלקים בp)

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

$$P\equiv\frac{(q-1)!^{\frac{p-1}{2}}}{\left(\frac{p}{q}\right)}\mod q$$

כלומר, קיבלנו $f(P)=\left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right),(q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right)$.

חישוב 2: קודם בחרנו נציגים מבין $\{x,-x\}$ לפני ההפעלה של f, עכשיו נבחור נציגים מבין $\{(a,b),(-a,-b)\}$, אחרי ההפעלה של f. נבחר את הנציגים $\{1,2,\ldots,p-1\}\times\left\{1,2,\ldots,\frac{q-1}{2}\right\}$, הפונקציה f שומרת על כפל לכן $f(P)$ זה בדיוק המכפלה של כל הנציגים שבחרנו, כלומר הקואורדינטות הן

$$(1\cdot 2\cdots(p-1))^{\frac{q-1}{2}}\equiv(p-1)!^{\frac{q-1}{2}}\mod p$$

$$\left(1\cdot 2\cdots\frac{q-1}{2}\right)^{p-1}\equiv\prod_{j=1}^{\frac{q-1}{2}}j^{p-1}\equiv\prod_{j=1}^{\frac{q-1}{2}}j^{\frac{p-1}{2}}\cdot(-j)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\prod_{j=1}^{q-1}j^{\frac{p-1}{2}}$$
$$\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot(q-1)!^{\frac{p-1}{2}}\mod q$$

ולכן $f(P)=\left((p-1)!^{\frac{q-1}{2}},(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot(q-1)!^{\frac{p-1}{2}}\right)$.

שני החישובים מובילים לאותה תוצאה עד כדי סימן, ולכן אם $\left(\frac{q}{p}\right)=1$ אז הסימן זהה ולכן

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

ואם $\left(\frac{q}{p}\right)=-1$ אז הסימן הפוך ולכן $\left(\frac{p}{q}\right)=-(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.
בכל מקרה קיבלנו את חוק ההדדיות הריבועית.

כעת נעבור לנספחים ־ נספח 1 נובע ישירות מקריטריון אוילר, נותר להוכיח את נספח 2. אכן, מתקיים

$$\left(\frac{2}{p}\right)\equiv 2^{\frac{p-1}{2}}\equiv\frac{2\cdot4\cdot6\cdots(p-1)}{1\cdot2\cdot3\cdots\left(\frac{p-1}{2}\right)}=\frac{1\cdot(-1)\cdot2\cdot(-1)^2\cdot3\cdot(-1)^3\cdots\frac{p-1}{2}\cdot(-1)^{\frac{p-1}{2}}}{1\cdot2\cdot3\cdots\left(\frac{p-1}{2}\right)}$$
$$\equiv(-1)^{\sum_{i=1}^{\frac{p-1}{2}}i}\equiv(-1)^{\frac{\frac{p-1}{2}\left(1+\frac{p-1}{2}\right)}{2}}\equiv(-1)^{\frac{2(p-1)+p^2-2p+1}{8}}\equiv(-1)^{\frac{p^2-1}{8}}\mod p$$

■

משפט 5.7 שימוש בחוק ההדדיות יש אינסוף ראשוניים שהם 1 מודולו 4.

הוכחה: הוכחנו בעבר שיש אינסוף עם 3 מודולו 4, נראה עבור 1.
נניח בשלילה שיש מספר סופי כאלה, $q_1,\ldots,q_r\equiv 1 \mod 4$. נסמן $Q=\left(2\prod_{i=1}^{r}q_i\right)^2+1$, אז $Q\equiv 1 \mod 4$. ניקח $p\mid Q$ ראשוני כלשהו, הוא בהכרח אי זוגי כי Q אי זוגי. נניח בשלילה $p\equiv 1 \mod 4$ כלומר $p=q_i$ עבור i כלשהו, אז $q_i\mid Q$, אבל אז $q_i\mid Q-\left(2\prod_{i=1}^{r}q_i\right)^2=1$ בסתירה לכך ש־q_i ראשוני. אז בהכרח $p\equiv 3 \mod 4$, ולכן לפי נספח 1 נובע $\left(\frac{-1}{p}\right)=-1$ כלומר 1־ אינה שארית ריבועית מודולו p. אבל $p\mid Q=\left(2\prod_{i=1}^{r}q_i\right)^2+1$ לכן $\left(2\prod_{i=1}^{r}q_i\right)^2\equiv -1 \mod p$, כלומר 1־ כן שארית ריבועית מודולו p, וקיבלנו סתירה. ■

משפט 5.8 המספרים הראשוניים לסדרות חשבוניות

$$\lim_{x\to\infty}\frac{\#\left\{p\le x \mid p\equiv a \mod N\right\}}{\pi(x)}=\frac{1}{\varphi(N)}$$

5.2 סימן יעקובי

הגדרה 5.9 סימן יעקובי עבור $p_1\cdots p_r=m\in\mathbb{N}$ אי זוגי, לכל $a\in\mathbb{Z}$ נגדיר $\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)$, כאשר באגף שמאל זה סימן יעקובי ובאגף ימין מכפלת סימני לז'נדר.

הערה 5.10 אם $\left(\frac{a}{m}\right)=-1$ אז a לא שארית ריבועית מודולו לפחות אחד מה־p_i־ים ולכן אינה שארית ריבועית מודולו m. אבל הכיוון השני לא נכון, כלומר אם $\left(\frac{a}{m}\right)=1$ אז a לא בהכרח שארית ריבועית מודולו m.

טענה 5.11 תכונות

1. אם $a\equiv b \mod m$ אז $\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right)$.
2. אם b זר ל־m אז $\left(\frac{b^2}{m}\right)=1$.
3. $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.
4. הדדיות ריבועית: אם m,n אי זוגיים אז $\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}$, וגם הנספחים מתקיימים.

הוכחה: נוכיח את חוק ההדדיות הריבועית המוכלל.
למה: אם m אי זוגי, $m=k_1\cdots k_\ell$, אז $\frac{m-1}{2}\equiv\frac{k_1-1}{2}+\frac{k_2-1}{2}+\cdots+\frac{k_\ell-1}{2} \mod 2$.
הוכחה: נסמן $A_1=\#\left\{k_i\equiv 1 \mod 4\right\},A_3=\#\left\{k_i\equiv 3 \mod 4\right\}$.
אם $k_i\equiv 1 \mod 4$ אז $\frac{k_i-1}{2}\equiv 0 \mod 2$, ואם $k_i\equiv 3 \mod 4$ אז $\frac{k_i-1}{2}\equiv 1 \mod 2$, ולכן

$$\frac{m-1}{2}\equiv 0 \mod 2 \iff m\equiv 1 \mod 4 \iff A_3 \text{ is even} \iff \frac{k_1-1}{2}+\frac{k_2-1}{2}+\cdots+\frac{k_\ell-1}{2}\equiv 0 \mod 2$$

כעת, נרשום $m=p_1\cdots p_k,n=q_1\cdots q_\ell$ אז

$$\begin{aligned}\left(\frac{m}{n}\right)&=\prod_{i=1}^{k}\left(\frac{p_i}{n}\right)=\prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{p_i}{q_j}\right)=\prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right)(-1)^{\frac{q_j-1}{2}\frac{p_i-1}{2}}=\left(\frac{n}{m}\right)\prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{q_j-1}{2}\frac{p_i-1}{2}}\\&=\left(\frac{n}{m}\right)(-1)^{\sum_{i=1}^{k}\sum_{j=1}^{\ell}\frac{q_j-1}{2}\frac{p_i-1}{2}}=\left(\frac{n}{m}\right)(-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{\ell}\frac{q_j-1}{2}\right)}\overset{\text{Lemma}}{=}\left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\frac{n-1}{2}}\end{aligned}$$

■

6 הצפנה ומבחני ראשוניות

6.1 הצפנת RSA

תהליך יצירת המפתח הפרטי והפומבי:

1. איילת בוחרת שני ראשוניים גדולים p,q. נסמן $N=pq$.
2. איילת מחשבת את $\varphi(N)=\varphi(p)\varphi(q)=(p-1)(q-1)$.
3. איילת מוצאת מספר e זר ל-$\varphi(N)$.
4. איילת מפרסמת את המפתח הפומבי (N,e), ושומרת את המפתח הפרטי $\varphi(N)$.

תהליך הצפנת הודעה:

1. בועז משיג את המפתח הפומבי של איילת אליה הוא רוצה לשלוח את ההודעה, (N,e).
2. בועז מקודד את ההודעה למספר $1\le P<N$.
3. בועז מחשב את $C\equiv P^e \mod N$, ושולח לאיילת.

תהליך פענוח הודעה:

1. איילת מקבלת הודעה C מבועז.
2. איילת מחשבת את ההופכי d של e מודולו $\varphi(N)$.
3. איילת מחשבת את $P\equiv C^d \mod N$, זו ההודעה המקורית.

טענה 6.1 נכונות הפענוח עובד, כלומר תחת ההגדרות הנ"ל אם $C\equiv P^e \mod N$ אז $P\equiv C^d \mod N$.

הוכחה: נניח $C\equiv P^e \mod N$ ההודעה המוצפנת, מכך ש-e,d הופכיים מודולו $\varphi(N)$ נובע $ed\equiv 1 \mod \varphi(N)$, כלומר $ed=1+k\varphi(N)$ עבור $k\in\mathbb{Z}$ כלשהו.
אם P זר ל-N: מתקיים

$$C^d\equiv(P^e)^d\equiv P^{ed}\equiv P^{1+k\varphi(N)}\equiv P\cdot\left(P^{\varphi(N)}\right)^k\equiv P\cdot 1^k\equiv P \mod N$$

אם P אינו זר ל-N: הסיכוי לכך הוא זניח ($\frac{1}{p}+\frac{1}{q}$, לכן לוקחים p,q גדולים מאוד), אבל הטענה עדיין נכונה. אכן, נניח בה"כ $P\mid q$, אז

$$C^d\equiv(P^e)^d\equiv(0^e)^d\equiv 0\equiv P \mod q$$
$$C^d\equiv(P^e)^d\equiv P^{ed}\equiv P^{1+k\varphi(N)}\equiv P\cdot\left(P^{\varphi(p)}\right)^{\varphi(q)k}\equiv P \mod p$$

כלומר $C^d-P\mid q,p$, ולכן מכך ש-q,p ראשוניים שונים ובפרט זרים $C^d-P\mid qp$ כלומר $C^d\equiv P \mod pq$ כלומר מודולו N, כדרוש. ■

6.2 מבחני ראשוניות

נסיון ראשון - מבחן ראשוניות לפי המשפט הקטן של פרמה

בהינתן N, אם נמצא $a \in \mathbb{Z}$ זר ל-N כך ש-$a^{N-1} \not\equiv 1 \mod N$, אז N פריק. a כזה נקרא עד פרמה עבור N.
אבל יש בעיה - לא לכל N פריק יש עד פרמה. לכן האלגוריתם לא יעבוד.

הגדרה 6.2 מספר קרמייקל N פריק כך שלכל $a \in \mathbb{Z}$ זר ל-N, $a^{N-1} \equiv 1 \mod N$. לדוגמה, 561.

משפט 6.3 (ללא הוכחה) N הוא קרמייקל $\iff$ $N = p_1 p_2 \cdots p_\ell$ כאשר $\ell \geq 2$, p_i ראשוניים שונים, וכן $p_i - 1 \mid N - 1$ לכל i.

נסיון שני - מבחן Solovay-Strassen לפי קריטריון אוילר

בהינתן N אי זוגי, אם נמצא $a \in \mathbb{Z}$ זר ל-N כך ש-$a^{\frac{N-1}{2}} \not\equiv \left(\frac{a}{N}\right) \mod N$. a כזה נקרא עד אוילר-יעקובי של N.

הערה 6.4 כל עד פרמה הוא עד אוילר-יעקובי, כי אם הוא לא עד אוילר-יעקובי אז $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N$ ולכן $a^{N-1} \equiv \left(\frac{a}{N}\right)^2 \equiv (\pm 1)^2 \equiv 1 \mod N$ כלומר הוא לא עד פרמה.

משפט 6.5 נכונות לכל N פריק אי זוגי יש עד אוילר-יעקובי (לא צריך לדעת להוכיח).

טענה 6.6 נסמן ב-L_N את קבוצת השקרנים עבור N, כלומר את קבוצת האיברים $a \in \mathbb{Z}_N^*$ שאינם עדי אוילר-יעקובי עבור N. אזי L_n היא תת חבורה של $\mathbb{Z}_N^*$.

הוכחה: לא הקלדתי, לא קשה. ■

מסקנה 6.7 $|L_N| \leq \frac{1}{2} |\mathbb{Z}_N^*|$.

הוכחה: מקרה פרטי של לגראנז', לוקחים $g \in G \setminus H$ ומסתכלים על H, gH, הן זרות ומגודל שווה. ■

7 הלמה של הנזל

מוטיבציה - איך ניתן לקבוע אם a הוא ריבוע מודולו N? נפרק את N לראשוניים שונים $N=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, אז לפי משפט השאריות הסיני a ריבוע מודולו n $\iff$ a ריבוע מודולו $p_i^{\alpha_i}$ לכל i. לכן המקרה המעניין הוא לבדוק אם a ריבוע מודולו p^α.

גישה 1: אם $p\neq 2$, ניתן להשתמש בקריטריון אוילר (כי יש ש"פ מודולו p^α), ולפיו a ריבוע מודולו p^α $\iff$ $a^{\frac{1}{2}\varphi(p^\alpha)}\equiv a^{\frac{\varphi(p^\alpha)}{\gcd(2,\varphi(p^\alpha))}}\equiv 1$.

גישה 2: אם a ריבוע מודולו p^α, אז הוא ריבוע מודולו p.

אם $\alpha=2$ ויש פתרון מודולו p^2 הנתון $a\equiv y^2 \mod p^2$, אז y הוא גם פתרון מודולו p. כלומר, אם נכתוב $y=bp+y_1$ כאשר $0\leq y\leq p^2-1$ וכן $0\leq b,y_1\leq p-1$, אז $a\equiv y^2\equiv (bp+y_1)^2\equiv y_1^2 \mod p$ כלומר y_1 הוא פתרון מודולו p.

נניח שמצאנו את y_1 כך ש$y_1^2\equiv a \mod p$, נמצא את y על ידי כך שנרשום $y=bp+y_1$ וננסה לפתור את המשוואה

$$\begin{aligned} a\equiv y^2\equiv (bp+y_1)^2 &\equiv 2bpy_1+y_1^2 \mod p^2\\ \implies 0 &\equiv 2bpy_1+\underbrace{(y_1^2-a)}_{\equiv 0 \mod p} \mod p^2\\ \implies 0 &\equiv 2by_1+\frac{y_1^2-a}{p} \mod p\\ \implies b &\equiv \frac{a-y_1^2}{p}\cdot (2y_1)^{-1} \mod p \end{aligned}$$

כאשר המעבר האחרון מתקיים אם $y_1\not\equiv 0 \mod p$ וכן $p\neq 2$, אם זה לא מתקיים הלמה של הנזל לא עוזרת.

מסקנה 7.1 יהי $p\neq 2$ ראשוני. אם $\left(\frac{a}{p}\right)=1$ אז a הוא ריבוע גם מודולו p^2, ולמעשה מודולו p^α לכל α.

מכאן נובע **מקרה פרטי של הלמה של הנזל:** יהי $p\neq 2$ ראשוני, a זר לp, $\alpha\geq 2$, ונניח שיש פתרון למשוואה $x^2\equiv a \mod p$. אז לכל פתרון $y_1^2\equiv a \mod p$ יש פתרון יחיד $y_\alpha^2\equiv a \mod p^\alpha$ המקיים $y_\alpha\equiv y_1 \mod p$, והוא נקרא הרמה של y_1.

דוגמה 7.2 נפתור את $x^2\equiv 14 \mod 125$. נפתור את $y_1^2\equiv 4 \mod 5$, הפתרונות הם $2,3$, נבחר $y_1=2$.

נמצא הרמה מודולו 25: נרשום $y_2=5b+2$, אז המשוואה היא $14\equiv y_2^2\equiv 20b+4 \mod 25$ ולכן $2\equiv 4b \mod 5$, הפתרון הוא $b\equiv 3 \mod 5$, ולכן $y_2\equiv 17 \mod 25$.

נמצא הרמה מודולו 125: נרשום $y_3=25b+17$, אז המשוואה היא $14\equiv y_3^2\equiv 850b+289\equiv -25b+39 \mod 125$ ולכן $25b\equiv 25 \mod 125$, כלומר $b\equiv 1 \mod 5$, ולכן $y_3\equiv 42 \mod 125$.

משפט 7.3 הלמה של הנזל יהי $f(x)\in\mathbb{Z}[x]$ פולינום עם מקדמים שלמים, $p\neq 2$ ראשוני, $\alpha\geq 2$ (ללא הוכחה). אזי לכל פתרון לא סינגולרי y_1 של $f(x)\equiv 0 \mod p$ (כלומר $f(y_1)\equiv 0 \mod p$ אבל $f'(y_1)\not\equiv 0 \mod p$) יש הרמה יחידה $y_k\in\mathbb{Z}_{p^k}$ כך ש$y_k\equiv y_1 \mod p$ וכן $f(y_k)\equiv 0 \mod p$.

הערה 7.4 במקרה $p=2$, יש שיטה אחרת: כדי לפתור את $x^2\equiv a \mod 2^k$ מוצאים פתרון x_0 ל$x^2\equiv a \mod 2^{k-1}$ ואז לוקחים $x=x_0+2^{k-1}s$ ומציבים. יש פתרון אחד עבור $k=1$, שניים עבור $k=2$, ו4 ל$k\geq 3$.

8 שברים משולבים וקירובים דיופנטיים

טענה 8.1 כתיב עשרוני של ממשיים כל ממשי ניתן לכתיבה כמספר עשרוני (אולי אינסופי).

יש ייצוג סופי $\Longleftrightarrow$ המספר הוא רציונלי מהצורה $\frac{p}{2^n \cdot 5^k}$ $\Longleftrightarrow$ הייצוג אינו יחיד (לדוגמה $1 = 0.9999$).

יש ייצוג מחזורי (החל ממקום מסוים) $\Longleftrightarrow$ המספר הוא רציונלי.

8.1 שברים משולבים

הגדרה 8.2 שבר משולב של מספר ממשי יהי $\theta \in \mathbb{R}$, נגדיר $a_0 = \lfloor \theta \rfloor$. אם $a_0 \neq \theta$ (כלומר $\theta \notin \mathbb{Z}$), מתקיים $0 < \theta - a_0 < 1$. נסמן $\theta_1 = \frac{1}{\theta - a_0} > 1$, אז מתקיים $\theta = a_0 + \frac{1}{\theta_1}$, נמשיך רקורסיבית על $\theta_1, \theta_2, \ldots$ עד אינסוף, או עד שנקבל θ_i שלם.

הביטוי המתקבל $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$ נקרא השבר המשולב של θ. מסמנים

$$[a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

טענה 8.3 יצוג שברי של שבר משולב יהיו $a_0 \in \mathbb{R}, a_1, \ldots, a_n \in \mathbb{R} \setminus \{0\}$, נגדיר

$$\begin{aligned}
p_0 &= a_0 \\
p_1 &= a_1 a_0 + 1 \\
\forall k \geq 2. p_k &= a_k p_{k-1} + p_{k-2} \\
q_0 &= 1 \\
q_1 &= a_1 \\
\forall k \geq 2. q_k &= a_k q_{k-1} + q_{k-2}
\end{aligned}$$

אזי $[a_0, a_1, \ldots, a_k] = \frac{p_k}{q_k}$.

הוכחה: באינדוקציה על k. עבור הבסיס,

$$\begin{aligned}
[a_0] &= a_0 = \frac{a_0}{1} = \frac{p_0}{q_0} \\
[a_0, a_1] &= a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}
\end{aligned}$$

נניח עבור k, אז

$$[a_0, a_1, \ldots, a_{k-1}, a_k, a_{k+1}] = \left[a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right] \overset{\text{ind. hyp.}}{=} \frac{p'_k}{q'_k}$$

עבור p'_k, q'_k המספרים שמתאימים ל-$a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}$. לכל $0 \leq i < k$ מתקיים $p_i = p'_i, q_i = q'_i$, ולכן

$$\frac{p'_k}{q'_k} = \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} = \frac{a_{k+1}\left(a_k p_{k-1} + p_{k-2}\right) + p_{k-1}}{a_{k+1}\left(a_k q_{k-1} + q_{k-2}\right) + q_{k-1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

■

למה 8.4 לכל $k \in \mathbb{N}$ מתקיים $\det \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$.

הוכחה: עבור $k=1$, $\det\begin{pmatrix}p_1 & p_0\\ q_1 & q_0\end{pmatrix}=\det\begin{pmatrix}a_1a_0+1 & a_0\\ a_1 & 1\end{pmatrix}=(a_1a_0+1)-a_1a_0=1=(-1)^{1-1}$.
באינדוקציה, נניח עבור $k-1$ אז מתכונות דטרמיננטה (לינאריות לפי עמודות, ...)

$$\det\begin{pmatrix}p_k & p_{k-1}\\ q_k & q_{k-1}\end{pmatrix}=\det\begin{pmatrix}a_kp_{k-1}+p_{k-2} & p_{k-1}\\ a_kq_{k-1}+q_{k-2} & q_{k-1}\end{pmatrix}=a_k\underbrace{\det\begin{pmatrix}p_{k-1} & p_{k-1}\\ q_{k-1} & q_{k-1}\end{pmatrix}}_{=0}+\det\begin{pmatrix}p_{k-2} & p_{k-1}\\ q_{k-2} & q_{k-1}\end{pmatrix}$$

$$=-\det\begin{pmatrix}p_{k-1} & p_{k-2}\\ q_{k-1} & q_{k-2}\end{pmatrix}=-(-1)^{(k-1)-1}=(-1)^{k-1}$$

■

מסקנה 8.5 אם $a_0,\dots,a_k\in\mathbb{Z}$ אז p_k,q_k זרים.

הוכחה: אם $d\mid p_k,q_k$ אז $d\mid p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}$ ולכן $d=\pm1$. ■

משפט 8.6 יהי $\theta\in\mathbb{R}$. אזי השבר המשולב של θ סופי $\iff$ θ רציונלי, ואם θ אי רציונלי אז

$$\lim_{n\to\infty}\frac{p_n}{q_n}=\lim_{n\to\infty}[a_0,a_1,\dots,a_n]=\theta$$

הוכחה: אם השבר סופי אז $\theta=[a_0,a_1,\dots,a_n]\in\mathbb{Q}$ (חיבור, מנה של רציונליים), ואם θ רציונלי אז תהליך בניית השבר המשולב, שמתבסס על אלגוריתם אוקלידס עבור a,b כאשר $\theta=\frac{a}{b}$, חייב לעצור.
כעת נניח כי θ אי רציונלי. בסימונים מהגדרת שבר משולב

$$\theta=[a_0,a_1,\dots,a_k,\theta_{k+1}]=\frac{\theta_{k+1}p_k+p_{k-1}}{\theta_{k+1}q_k+q_{k-1}}$$

ולכן

$$\left|\theta-\frac{p_k}{q_k}\right|=\left|\frac{\theta_{k+1}p_k+p_{k-1}}{\theta_{k+1}q_k+q_{k-1}}-\frac{p_k}{q_k}\right|=\left|\frac{\theta_{k+1}p_kq_k+p_{k-1}q_k-\theta_{k+1}q_kp_k-p_kq_{k-1}}{q_k\left(\theta_{k+1}q_k+q_{k-1}\right)}\right|$$
$$\overset{\text{lemma}}{=}\left|\frac{-(-1)^{k-1}}{q_k\left(\theta_{k+1}q_k+q_{k-1}\right)}\right|=\frac{1}{q_k\left(\theta_{k+1}q_k+q_{k-1}\right)}\overset{\theta_{k+1}>1,q_i\geq1}{<}\frac{1}{q_k^2}\xrightarrow{k\to\infty}0$$

הגבול נובע מכך ש-$q_k=a_kq_{k-1}+q_{k-2}$ וכן $a_k\geq1$, ולכן q_k זו סדרת טבעיים עולה ממש ולכן $q_k\to\infty$. ■

טענה 8.7 יהיו $p\in\mathbb{Z},q\in\mathbb{N},x\in\mathbb{R}$, אז

$$\left\lfloor\frac{p+x}{q}\right\rfloor=\left\lfloor\frac{p+\lfloor x\rfloor}{q}\right\rfloor$$

משפט 8.8 לגראנז' $\alpha\in\mathbb{R}$ הינו בעל ייצוג מחזורי בשברים משולבים, כלומר $\alpha=[a_0,\dots,a_{k-1},\overline{a_k,\dots,a_{k+m-1}}]$, אם ורק אם α שורש של משוואה ריבועית $ax^2+bx+c=0$ כאשר $a\neq0$ וכן $\Delta=b^2-4ac>0$ לא ריבוע שלם (לא להוכחה).

8.2 קירובים דיופנטיים

מסקנה 8.9 (מהמשפט שלפני לגראנז') לכל $\theta\in\mathbb{R}$ אי רציונלי יש אינסוף קירובים דיופנטיים שמקיימים $\left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{q_n^2}$. מסקנה זו משפרת את החסם הטריויאלי, שיש קירוב עם $\left|\theta-\frac{p}{q}\right|\leq\frac{1}{2q}$.
כמו כן היא ייחודית לאי רציונליים, כי עבור $\frac{a}{b}\in\mathbb{Q}$, אם $q>b$ אז $\left|\frac{a}{b}-\frac{p}{q}\right|=\left|\frac{aq-bp}{bq}\right|\geq\frac{1}{bq}>\frac{1}{q^2}$, ויש מספר סופי של אפשרויות עם $q\leq b$ (כי בהינתן $q,\frac{a}{b}$, המספר p נקבע ביחידות).

משפט 8.10 הרישות $\frac{p_n}{q_n}$ של הפיתוח של $\theta\in\mathbb{R}$ לשברים משולבים נותנות את הקירוב הטוב ביותר במובן הבא:

1. **המובן החלש:** לכל $a,b\in\mathbb{Z}$ כך ש $1\le b<q_n$ מתקיים $\left|\theta-\frac{p_n}{q_n}\right|<\left|\theta-\frac{a}{b}\right|$. כלומר, לא ניתן להגיע לקירוב טוב יותר מבלי להגדיל את המכנה.

2. **המובן החזק:** לכל $a,b\in\mathbb{Z}$ כך ש$1\le b<q_{n+1}$ מתקיים $|q_n\theta-p_n|\le|b\theta-a|$. תכונה זו היא למעשה קריטריון הכרחי ומספיק לקירובים $\frac{p_n}{q_n}$ של θ. אכן, בהינתן p_n,q_n, ניתן להגדיר את p_{n+1},q_{n+1} להיות זוג השלמים עם q_{n+1} מינימלי כך ש־$|q_n\theta-p_n|>|q_{n+1}\theta-p_{n+1}|$.

הגדרה 8.11 מספר אלגברי $\alpha\in\mathbb{R}$ נקרא אלגברי אם הוא שורש של פולינום $f\in\mathbb{Z}[x]$ (באופן שקול, שור של $f\in\mathbb{Q}[x]$). אם α אלגברי, המעלה של α זו המעלה המינימלית של פולינום כזה ש־α שורש שלו. בנוסף, אם α אינו אלגברי הוא נקרא טרנסצנדנטי.

משפט 8.12 ליוביל לכל $\alpha\in\mathbb{R}$ אלגברי ממעלה d יש מספר $c=c(\alpha)>0$ כך שלכל רציונלי $\alpha\neq\frac{p}{q}$ מתקיים $\left|\alpha-\frac{p}{q}\right|\ge\frac{c}{q^d}$.

הוכחה: נפריד למקרים $d=1,d\ge2$.

אם $d=1$, α רציונלי. נניח $\alpha=\frac{a}{b}$ ונגדיר $c(\alpha)=\frac{1}{b}$, אז לכל $\alpha\neq\frac{p}{q}$ מתקיים

$$\left|\alpha-\frac{p}{q}\right|=\left|\frac{a}{b}-\frac{p}{q}\right|=\frac{|aq-bp|}{bq}\ge\frac{1}{bq}=\frac{c}{q}$$

אם $d\ge2$, יהי $f=\sum_{i=0}^{d}a_ix^i\in\mathbb{Z}[x]$ כך ש$f(\alpha)=0$. לf אין שורשים רציונליים, כי אם $f\left(\frac{p}{q}\right)=0$ אז $f(x)=\left(x-\frac{p}{q}\right)g(x)$ ואז $g(\alpha)=0$ ו־g פולינום רציונלי ולכן מעלת α היא לכל היותר $d-1$, סתירה.
הנגזרת $f'(x)$ חסומה בקטע $[\alpha-1,\alpha+1]$ ע"י $M>0$ (כי היא רציפה וזה קטע קומפקטי). ניקח את המקדם $c(\alpha)=\min\left\{1,\frac{1}{M}\right\}$, ונראה שלכל $\frac{p}{q}\in\mathbb{Q}$ מתקיים $\left|\alpha-\frac{p}{q}\right|\ge\frac{c}{q^d}$. אם $\left|\alpha-\frac{p}{q}\right|\ge1$ אז $\left|\alpha-\frac{p}{q}\right|\ge c\ge\frac{c}{q^d}$, ואם $\left|\alpha-\frac{p}{q}\right|<1$ אז לפי משפט לגראנז' יש x_0 בין α ל$\frac{p}{q}$ שמקיים $f'(x_0)=\frac{f\left(\frac{p}{q}\right)-f(\alpha)}{\frac{p}{q}-\alpha}$. מתקיים $f(\alpha)=0$ וכן

$$0\neq\left|f\left(\frac{p}{q}\right)\right|=\left|\sum_{i=0}^{d}a_i\frac{p^i}{q^i}\right|=\frac{1}{q^d}\left|\sum_{i=0}^{d}a_iq^{d-i}p^i\right|\ge\frac{1}{q^d}$$

ולכן

$$\left|\frac{p}{q}-\alpha\right|=\frac{\left|f\left(\frac{p}{q}\right)\right|}{|f'(x_0)|}\ge\frac{\frac{1}{q^d}}{M}\ge\frac{c}{q^d}$$

כדרוש. ■

מסקנה 8.13 מספר שניתן לקרב לכל $d\in\mathbb{N}$ על ידי $\frac{p}{q}$ כך ש־$\left|\frac{p}{q}-\theta\right|<\frac{1}{q^d}$ הוא טרנסצנדנטי. מספרים אלו נקראים **מספרי ליוביל**, ויש טרנסצנדנטיים שאינם מספרי ליוביל (לדוגמה π,e). לדוגמה,

$$\theta=\sum_{n=1}^{\infty}\frac{1}{10^{n!}}=0.11000100\ldots$$

הוא ליוביל ובפרט טרנסצנדנטי.

9 סכומי ריבועים

9.1 חוג השלמים של גאוס

הגדרה 9.1 המספרים של גאוס $\mathbb{Q}(i)=\{r+is \mid r,s\in\mathbb{Q}\}\subseteq\mathbb{C}$.

טענה 9.2 $\mathbb{Q}(i)$ הוא תת־שדה של $\mathbb{C}$, כלומר הוא מכיל את $0,1$, וסגור לחיבור, חיסור, כפל, והופכי כפלי.

הוכחה: $0,1\in\mathbb{Q}(i)$ ברור, נניח $r,r',s,s'\in\mathbb{Q}$ אז $(r+is)+(r'+is')=(r+r')+i(s+s')$ והסגירות נובעת מסגירות רציונליים לחיבור. כפל תרגיל, ועבור הופכי נניח $0\neq r+is\in\mathbb{Q}(i)$ אז

$$\frac{1}{r+is}=\frac{r-is}{(r+is)(r-is)}=\frac{r-is}{r^2+s^2}=\frac{r}{r^2+s^2}+i\cdot\frac{-s}{r^2+s^2}\in\mathbb{Q}(i)$$

שוב, מכך שהרציונליים הם שדה. ∎

הערה 9.3 $\mathbb{Q}(i)$ הוא גם מרחב וקטורי מעל $\mathbb{Q}$ ממימד 2, וזו דוגמה להרחבת שדות ריבועית של $\mathbb{Q}$.

הגדרה 9.4 הצמדה ונורמה לכל $z=x+iy\in\mathbb{C}$, הצמוד הוא $\bar{z}=x-iy$ ומתקיים $\overline{zw}=\bar{z}\bar{w}$. כמו כן נגדיר נורמה $N\colon\mathbb{C}\to\mathbb{R}_{\geq0}$ על ידי $N(z)=z\cdot\bar{z}=|z|^2$, היא מקיימת $N(z)=0\iff z=0$ וכן $N(zw)=N(z)N(w)$.
השלמים של גאוס $\mathbb{Z}[i]=\{m+ni \mid m,n\in\mathbb{Z}\}\subseteq\mathbb{Q}(i)$.

טענה 9.5 $\mathbb{Z}[i]$ הוא תת־חוג של $\mathbb{Q}(i)$ (או של $\mathbb{C}$), כלומר הוא מכיל את $0,1$, וסגור לחיבור, חיסור, וכפל. אבל, הוא אינו תת־שדה (לא סגור להופכי).

הערה 9.6 נסתכל על הנורמה $N\to\mathbb{Z}[i]\to\mathbb{Z}_{\geq0}$, התמונה שלה היא בדיוק כל סכומי הריבועים.

טענה 9.7 ההפיכים ב־$\mathbb{Z}[i]$ הם $\pm1,\pm i$, כלומר האיברים עם $N(\alpha)=1$.

הוכחה: אם $\alpha\beta=1$ אז $N(\alpha)N(\beta)=N(\alpha\beta)=1$ וכן $N(\alpha),N(\beta)\in\mathbb{Z}_{\geq0}$ לכן שניהם 1. ∎

טענה 9.8 $\mathbb{Z}[i]$ הוא חוג אוקלידי, כלומר קיים בו אלגוריתם חלוקה בשארית ביחס לנורמה. משמע, לכל $\alpha,\beta\in\mathbb{Z}[i]$ עם $\beta\neq0$ יש $q,r\in\mathbb{Z}[i]$ כך ש־$\alpha=q\beta+r$ ובנוסף $N(r)<N(\beta)$.

הוכחה: מתקיים $|r|^2=N(r)<N(\beta)=|\beta|^2$ אם ורק אם $|r|<|\beta|$, אם ורק אם $\left|\frac{r}{\beta}\right|<1$. נרשום $\frac{\alpha}{\beta}=r+is\in\mathbb{Q}(i)$, נבחר $\frac{\alpha}{\beta}$ נמצא באיזשהו ריבוע עם קודקודים ב־$\mathbb{Z}[i]$, נבחר את הקרוב ביותר (נעגל את שתי הקואורדינטות) ונקבל $q\in\mathbb{Z}[i]$ כך ש־$\left|\frac{r}{\beta}\right|=\left|\frac{\alpha}{\beta}-q\right|\leq\frac{\sqrt{2}}{2}<1$, כדרוש. ∎

מסקנה 9.9 תכונות של החוג בחוג $\mathbb{Z}[i]$ יש $\gcd$ (יחיד עד כדי כפל בהפיך), מקדמי בזו, אי פריק שקול לראשוני, ויחידות פירוק לראשוניים כפול הפיך עד כדי כפל בהפיך ושינוי סדר הראשוניים.

9.2 משפט פרמה־גאוס

משפט 9.10 אם p ראשוני וכן $p\equiv3 \mod 4$ אז p אי פריק ב־$\mathbb{Z}[i]$.

הוכחה: נניח בשלילה שיש α,β לא הפיכים כך ש־$\alpha\beta=p$, אז $N(\alpha)N(\beta)=N(p)=p^2$ וכן $N(\alpha),N(\beta)>1$ ולכן $N(\alpha)=N(\beta)=p$. לכן p סכום ריבועים (תמונת N היא בדיוק כל סכומי הריבועים), אבל זו סתירה לכך ש־$p\equiv3 \mod 4$ (מהכיוון $\Leftarrow$ במשפט הבא, שלא מסתמך על תוצאה זו). ∎

משפט 9.11 פרמה־גאוס מספר ראשוני p הוא סכום שני ריבועים $\iff$ $p\not\equiv3 \mod 4$.

הוכחה: $\Longleftarrow$ למעשה כיוון זה נכון עבור $n \in \mathbb{N}$ כללי, לא בהכרח ראשוני. אכן, השאריות הריבועיות מודולו 4 הן $0,1$, ולכן סכום של שני ריבועים מודולו 4 הוא אחד מבין $0+0=0, 0+1=1, 1+1=2$, כלומר אם n סכום שני ריבועים אז $n \not\equiv 3 \mod 4$.

$\Longrightarrow$ נניח $p \equiv 1 \mod 4$ ראשוני. רוצים להראות שp סכום ריבועים, באופן שקול פריק כאיבר של $\mathbb{Z}[i]$ (זה שקול כי אם $p = x^2 + y^2$ סכום ריבועים אז $p = (x+iy)(x-iy)$ פריק, ובכיוון השני אם הוא פריק אז מהמשפט $p \equiv 3 \mod 4$ בסתירה להנחה). כעת, נניח בשלילה p אי פריק ב$\mathbb{Z}[i]$ אז הוא גם ראשוני. נזכר כי $\left(\frac{-1}{p}\right) = 1$ כי $p \equiv 1 \mod 4$, ולכן יש $x \in \mathbb{Z}$ כך ש$x^2 \equiv -1 \mod p$, כלומר $p \mid x^2 + 1 = (x+i)(x-i)$ ולכן $p \mid x \pm i$ (אחד מהם), כלומר קיים $m + ni$ כך ש$pm + pni = p(m+ni) = x \pm i$, אז $pn = \pm 1$ סתירה. ■

מסקנה 9.12 (תרגיל) n טבעי הוא סכום שני ריבועים $\Longleftrightarrow$ בפירוק לראשוניים $n = \prod_{i=1}^{r} p_i^{e_i}$ החזקה של כל p_i שמקיים $p_i \equiv 3 \mod 4$ היא זוגית.

טענה 9.13 אי פריקים ב$\mathbb{Z}[i]$ האיברים האי־פריקים היחידים ב$\mathbb{Z}[i]$ הם $1-i$ ראשוניים עם $p \equiv 3 \mod 4$ או $x \pm iy$ כך שיש ראשוני $p \equiv 1 \mod 4$ כך ש$p = (x+iy)(x-iy)$.

הוכחה: אם $\alpha \in \mathbb{Z}[i]$ אי פריק אז $\alpha \mid \alpha \cdot \overline{\alpha} = p_1^{e_1} \cdots p_r^{e_r}$, בפירוק ב$\mathbb{Z}[i]$ מופיעים רק איברים מהפירוק שכתבנו, ומיחידות הפירוק α חבר של אחד האי פריקים בפירוק זה. ■

דוגמה 9.14 נפרק לאי פריקים את $8 - i \in \mathbb{Z}[i]$. מתקיים $N(8-i) = 65 = 5 \cdot 13$, נפרק:

$$5 = (2+i)(2-i)$$
$$13 = (2+3i)(2-3i)$$

בדיוק אחד מבין $2+i, 2-i$ בפירוק של $8-i$, במקרה הזה זה $2+i$ (מחלקים ובודקים אם יוצא שלם גאוס). בדיוק אחד מבין $2+3i, 2-3i$ בפירוק של $8-i$, במקרה הזה $2+3i$. נחשב $(2+i)(2+3i) = 1 + 8i$, ואם מכפילים ב$-i$ (הפיך) מקבלים בדיוק את הדרוש.

10 הרחבות ריבועיות

הגדרה 10.1 הרחבה ריבועית (לא לגמרי חלק מהקורס) תת שדה של $\mathbb{C}$ (שמכיל את $\mathbb{Q}$, אבל זה נכון לכל תת שדה) וכמרחב וקטורי מעל $\mathbb{Q}$ הוא דו־מימדי. לדוגמה, ראינו את $\mathbb{Q}(i)$.

טענה 10.2 (תרגיל) השדות הללו הם בדיוק מהצורה $\mathbb{Q}\left(\sqrt{d}\right) = \left\{r + s\sqrt{d} \mid r, s \in \mathbb{Q}\right\}$ עבור $d \in \mathbb{Z}$ שאינו ריבוע.

10.1 הרחבות ריבועיות דמיוניות וממשיות

הרחבות ריבועיות דמיוניות

הרחבה ריבועית כאשר $d < 0$, לדוגמה עבור $d = -1$ מקבלים את $\mathbb{Q}(i)$.

הגדרה 10.3 צמוד הצמוד המרוכב $\overline{x + y\sqrt{d}} = x - y\sqrt{d}$.
נורמה $N(z) = z\bar{z} = x^2 - dy^2 = |z|^2$.

טענה 10.4 ההפיכים ב$\mathbb{Z}\left[\sqrt{d}\right]$ הם כל האיברים עם $N(z) = 1$.

הערה 10.5 כדי למצוא את ההפיכים צריך לפתור את $x^2 - dy^2 = 1$, אם $d = -1$ אז $\alpha = \pm 1, \pm i$ ואם $d \le -2$ אז $y = 0$ (כי $-d \ge 2$) ולכן $\alpha = \pm 1$.

הרחבות ריבועיות ממשיות

הרחבה ריבועית כאשר $d > 0$, לדוגמה עבור $d = 2$ מקבלים את $\mathbb{Q}\left(\sqrt{2}\right)$.

הגדרה 10.6 צמוד הצמוד האלגברי של α מוגדר $\tilde{\alpha} = r - s\sqrt{d}$.
נורמה (כעת עשויה להיות שלילית, אבל היא עדיין כפלית) $N(\alpha) = \alpha\tilde{\alpha} = r^2 - ds^2$.

טענה 10.7 $\tilde{\alpha\beta} = \tilde{\alpha}\tilde{\beta}, \alpha \tilde{+} \beta = \tilde{\alpha} + \tilde{\beta}, N(\alpha\beta) = N(\alpha)N(\beta)$. **ההפיכים** ב$\mathbb{Z}\left[\sqrt{d}\right]$ הם כל האיברים עם $N(z) = \pm 1$, באופן שקול הפתרונות של המשוואה $x^2 - dy^2 = \pm 1$, שנקראת משוואת פל.

הערה 10.8 לכל $0 \neq \alpha \in \mathbb{Q}\left(\sqrt{d}\right)$ מתקיים $N(\alpha) \neq 0$, אחרת $x^2 - dy^2 = 0$ ולכן $\sqrt{d} = \frac{x}{y}$ אבל $\sqrt{d}$ אינו רציונלי.

10.2 משוואת פל

הערה 10.9 פתרונות משוואת פל מתאימים לאיברים ההפיכים ב$\mathbb{Z}\left[\sqrt{d}\right]$, ולכן יש להם מבנה של חבורה, כאשר הכפל הוא

$$(x, y) \cdot (a, b) = (ax + byd, ay + bx)$$

קבוצת הפתרונות סגורה לכפל, יש בה איבר יחידה $(1, 0)$ והופכי לכל איבר.

מסקנה 10.10 אם יש פתרון לא טריויאלי, כלומר לא $(\pm 1, 0)$, אז יש אינסוף פתרונות.

הוכחה: אם $\pm 1 \neq x + y\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$ הפיך, בה"כ ניתן להניח $x \ge 0, y \ge 1$ ואז $x + y\sqrt{d} > 1$, ואז

$$\left(x + y\sqrt{d}\right)^n \xrightarrow{n \to \infty} \infty$$

וכל חזקה כזו מהווה פתרון, כי זו חבורה. ■

למה 10.11 (x, y) פתרון חיובי $\iff$ $x + y\sqrt{d} > 1$.

הוכחה: אם $x,y>0$ אז $x+y\sqrt{d}>1$, אז $x<0,y<0$ אז $x+y\sqrt{d}<-1$, ואם $x>0,y<0$ אז $\frac{1}{\alpha}=\frac{\tilde{\alpha}}{N(\alpha)}=\pm\tilde{\alpha}=\pm\left(x-y\sqrt{d}\right)$ ובביטוי הנ"ל $x,-y$ שווי סימן, ולכן $-1<\alpha<1$. ∎

משפט 10.12 לכל $d>0$ לא ריבוע יש פתרון לא טריויאלי למשוואת פל.

הוכחה: **למה:** קיים $k\in\mathbb{Z}$ כך שיש אינסוף פתרונות בשלמים ל$x^2-dy^2=k$.

הוכחה: $\sqrt{d}\notin\mathbb{Q}$, לכן יש לו אינסוף קירובים דיופנטיים $\left|\frac{x}{y}-\sqrt{d}\right|<\frac{1}{y^2}$. עבור קירוב כזה

$$\left|x^2-dy^2\right|=y^2\left|\left(\frac{x}{y}\right)^2-d\right|=y^2\left|\frac{x}{y}-\sqrt{d}\right|\cdot\left|\frac{x}{y}+\sqrt{d}\right|<\frac{x}{y}+\sqrt{d}\leq 1+2\sqrt{d}$$

לכן לכל $x,y>0$ שמקיימים $\left|\frac{x}{y}-\sqrt{d}\right|<\frac{1}{y^2}$ מתקיים $\mathbb{Z}\ni\left|x^2-dy^2\right|<1+2\sqrt{d}$, יש מספר סופי של אפשרויות לכן אינסוף מבין ה(x,y)ים מקבלים אותו ערך.

נחזור להוכחת המשפט. עבור k זה, יש אינסוף פתרונות לכן ניתן למצוא שני פתרונות שונים $\alpha_1=x_1+y_1\sqrt{d},\alpha_2=x_2+y_2\sqrt{d}$ ששקולים מודולו k, כלומר $x_1\equiv x_2 \mod k, y_1\equiv y_2 \mod k$. נניח בה"כ $\alpha_2>\alpha_1$ ונראה ש$\frac{\alpha_2}{\alpha_1}$ פתרון חיובי, שלם, לא טריויאלי ל$x^2-dy^2=1$.

פתרון: מכפליות הנורמה $N\left(\frac{\alpha_2}{\alpha_1}\right)=\frac{N(\alpha_2)}{N(\alpha_1)}=\frac{k}{k}=1$. **חיובי ולא טריויאלי:** $\frac{\alpha_2}{\alpha_1}>1$ כי $\alpha_2>\alpha_1$.

שלם: מתקיים $\frac{\alpha_2}{\alpha_1}=\frac{\alpha_2\tilde{\alpha_1}}{\alpha_1\tilde{\alpha_1}}=\frac{\alpha_2\tilde{\alpha_1}}{k}=\frac{(x_1x_2-y_1y_2d)+\sqrt{d}(x_1y_2-x_2y_1)}{k}$, והמונה מתחלק ב$k$ כי

$$(x_1x_2-y_1y_2d)+\sqrt{d}\,(x_1y_2-x_2y_1)\equiv(x_1x_1-y_1y_2d)+\sqrt{d}\,(x_1y_1-x_1y_1)\equiv k+0\equiv 0 \mod k$$

ולכן $\frac{\alpha_2}{\alpha_1}\in\mathbb{Z}\left[\sqrt{d}\right]$ כדרוש. ∎

מסקנה 10.13 יש פתרון (x,y) עם $x+y\sqrt{d}>0$.

כמו כן יש פתרון מינימלי מעל 1, $1<\varepsilon_d=x_1+y_1\sqrt{d}$.

הוכחה: הראשון כי יש פתרון חיובי, והשני כי אם $x+y\sqrt{d}$ פתרון חיובי אז יש מספר סופי של פתרונות בקטע $\left(1,x+y\sqrt{d}\right)$ ולכן יש ביניהם מינימלי. ∎

משפט 10.14 הפתרונות של משוואת פל הם $\{\pm\varepsilon_d^n \mid n\in\mathbb{Z}\}$.

הוכחה: לכל פתרון (x,y) מתאים פתרון חיובי על ידי שינוי סימן $\alpha=x+y\sqrt{d}$. כעת קיים $n\in\mathbb{Z}$ כך ש$\varepsilon_d^n\leq\alpha<\varepsilon_d^{n+1}$, ואז $1\leq\frac{\alpha}{\varepsilon_d^n}<\varepsilon_d$ ו$\frac{\alpha}{\varepsilon_d^n}$ פתרון כי הוא הפיך. ממינימליות ε_d נובע $\frac{\alpha}{\varepsilon_d^n}=1$ כלומר $\alpha=\varepsilon_d^n$, ולכן הפתרון המקורי הוא $\pm\varepsilon_d^n$. ∎