תומ"ס 2

הגדרה: אם $a_1,\dots a_n\in\mathbb{Z}$ נגדיר $(a_1,a_2,\dots a_n)=\{a_1x_1+\dots+a_nx_n \mid x_i\in\mathbb{Z}\}$

יהי $A=(a_1,..a_n)$, אם $x,y\in A$ אז $x+y\in A, x-y\in A$, $ra\in A$ $r\in\mathbb{Z}$.

טענה 3: אם $a,b\in\mathbb{Z}$ אז קיים $d\in\mathbb{Z}$ כך ש- $(d)=(a,b)$

הוכחה: אם $a=b=0$ כותבים $d=0$.

אם $a\neq 0$ או $b\neq 0$ אז קיים מספר חיובי $x\in(a,b)$

יהי $d\in\mathbb{Z}$ המספר החיובי $d\in(a,b)$ הקטן ביותר. $d\in(a,b)$, $d>0$, d קטן ביותר.

מכיוון ש- $d\in(a,b)$ לכן $(d)\subset(a,b)$. נראה ש- $(a,b)\subset(d)$

יהי $c\in(a,b)$. לפי טענה 2, קיימים q,r כך ש- $c=qd+r$ $0\le r<d$.

הודות ל- $c,d\in(a,b)$ אנו רואים ש- $r=c-qd\in(a,b)$.

אבל $0\le r<d$ ו-d מינימלי חיובי, לכן $r=0$.

לכן $c=qd$ כלומר $c\in(d)$. קיבלנו ש- $(a,b)\subset(d)$, $(d)\subset(a,b)$

$\Rightarrow (d)=(a,b)$ ■

הגדרה: יהיו $a,b\in\mathbb{Z}$. מספר שלם $d\in\mathbb{Z}$ נקרא מחלק משותף מרבי של a ו-b אם $d|a$, $d|b$, וכל מחלק משותף c של a ו-b מתקיים $c|d$.

דוגמא: 3- הוא ממ"מ של 9,6, וכן גם 3+.

אם c מחלק משותף מרבי אחר של a,b אז $d|c$ וגם $c|d$, לכן $c=\pm d$. $\Leftarrow$ ממ"מ, אם קיים, יחיד עד כדי סימן.

טענה: יהיו $a,b\in\mathbb{Z}$. אם $(a,b)=(d)$ אז d הוא ממ"מ של $\{a,b\}$.

הוכחה: הודות ל- $a\in(d)$ ו- $b\in(d)$, d הוא מחלק משותף של a ו-b.

אם c מחלק משותף של a ו-b כלשהו, כלומר $c|a$, $c|b$ אזי $c|(ax+by)$

לכל $x,y\in\mathbb{Z}$. לכן $c|d$ לכן d הוא ממ"מ של a,b.

$\Leftarrow$ הוכחנו שממ"מ של a,b קיים ודרך d הוא הקומבינציה לינארית של a,b.

יהיו $a,b\in\mathbb{Z}$. אם d_1,d_2 ש- d_1,d_2 שני ממ"מים של a,b אז $d_2=\pm d_1$

אז מוחרים בממ"מ החיובי וכותבים $\gcd(a,b)=d$.

הגדרה: אומרים ש- a,b **זרים** (relatively prime / coprime

אם כל המחלקים המשותפים הם ± 1 או בשקול $\gcd(a,b)=1$.

דוגמה: 6 ו- 7 זרים.

טענה: נניח $a|bc$ ו- $\gcd(a,b)=1$. אזי $a|c$.

הוכחה: היות ו- $\gcd(a,b)=1$ קיימים $r,s\in\mathbb{Z}$ כך ש- $ra+sb=1$.

לכן $rac+sbc=c$. אבל $a|rac$ וגם $a|sbc$ מהנתון. לכן $a|c$ כנדרש ■

⚠ זה לא נכון אם $\gcd(a,b)\neq 1$ למשל $24=3\cdot 8$, $6|3\cdot 8$ אבל $6\nmid 8$.

מסקנה 1: אם p ראשוני ו- $p|bc$ אזי או ש $p|b$ או ש- $p|c$.

הוכחה: כל המחלקים של p הם $\pm p$, ± 1.

אז או $\gcd(p,b)=1$ או $\gcd(p,b)=p$ $\Leftarrow$ אם $\gcd(p,b)=p$ אזי $p|b$ וסיימנו.

אחרת, ו-$\gcd(p,b)=1$ אז לפי הטענה ~~gcd~~ $p|c$ ודי סיימנו ■

ניסוח אחר: אם p ראשוני, $p\nmid b$ $\wedge$ $p\nmid c$ $\Leftarrow$ $p\nmid bc$.

⚠ זה לא נכון עבור אי-פריקים א-פריקים ב $\mathbb{Z}[\sqrt{-5}]$.

2 הוא אי פריק ב- $\mathbb{Z}[\sqrt{-5}]$ $2|6=(1+\sqrt{-5})(1-\sqrt{-5})$ אבל ברור ש $2\nmid(1\pm\sqrt{-5})$.

מסקנה 2: יהי p ראשוני, $a,b\in\mathbb{Z}$. אז $\boxed{\mathrm{ord}_p ab=\mathrm{ord}_p a+\mathrm{ord}_p b}$

הוכחה: יהי $\alpha=\mathrm{ord}_p a$, $\beta=\mathrm{ord}_p b$. אז $a=p^\alpha c_{p\nmid c}$, $b=p^\beta d_{p\nmid d}$.

לפי מסקנה 1, $p\nmid cd$. מקבלים ש- $ab=p^{\alpha+\beta}cd$, $p\nmid cd$.

אז $p^{\alpha+\beta}|ab$ ו- $p^{\alpha+\beta+1}\nmid ab$ (הוכחה) אם $p^{\alpha+\beta+1}|ab$ אז

$p^{\alpha+\beta+1}u=ab$, $u\in\mathbb{Z}$, $p^{\alpha+\beta+1}\cdot u=p^{\alpha+\beta}cd$ / $pu=cd$ $\Rightarrow$ $p|cd$ וזו סתירה).

$\Leftarrow$ $\alpha+\beta=\mathrm{ord}_p ab$. לפי הגדרה. ■

⚠ אם $p|c$ אז $p^{\alpha+1}|p^\alpha c=a$.

הוכחת המשפט על פירוק יחיד לראשוניים:

כותבים: $n=(-1)^{\varepsilon(n)}\prod_{p\in P}p^{a(p)}$

עבור ראשוני q כותבים את הסדר של n ב- q ומשתמשים במסקנה 2.

$\mathrm{ord}_q n=\varepsilon(n)\,\mathrm{ord}_p(-1)+\sum_{p\in P}a(p)\,\mathrm{ord}_q p$

המשך תרגול 2

⚠ $ord_q(ab)=ord_q(a)+ord_q(b)$, $ord_q(a^k)=k\cdot ord_q(a)$

המשך ההוכחה:

אם $ord_q(p)=\begin{cases}0 & p\neq q\\ 1 & p=q\end{cases}$, $ord_q(-1)=0$.

מקבלים ש- $ord_q(n)=a(q)\cdot 1=a(q)$

← $ord_q(n)$ לא תלוי בפירוק לכן הוא יחיד.

מסקנה: אם $a=(-1)^{\varepsilon}\prod_{p\in P}p^{\alpha(p)}$, $b=(-1)^{\delta}\prod_p p^{\beta(p)}$

אז $gcd(a,b)=\prod_p p^{\gamma(p)}$ כאשר $\gamma(p)=min(\alpha(p),\beta(p))$

הוכחה: נגדיר $c=\prod_p p^{\gamma(p)}$ אז ברור ש- $c|a$, $c|b$.

בכיוון ההפוך יהי $d|a$, $d|b$, $d\neq 0$. אז $d=\prod_p p^{\xi(p)}$

$d|a$ לכן $\xi(p)\le\alpha(p)$, $d|b$ לכן $\xi(p)\le\beta(p)$ לכן $\xi(p)\le\gamma(p)$ לכן $d|c$ ■

סעיף: משפט אוקלידס ואלגוריתם אוקלידס

משפט אוקלידס: יש אינסוף מספרים ראשוניים.

הוכחה: יהי p ראשוני. נתבונן את כל הראשוניים הקטנים או שווים ל-p.

$\underset{2}{p_1}\cdot\underset{3}{p_2}\cdot...\cdot p_n(=p)$. נגדיר $N=p_1\cdot p_2\cdot...\cdot p_n+1$

אז $N>1$. לכל $1\le i\le n$ מתקיים: $p_i\nmid N$.

$N>1$ לכן קיים מס' ראשוני p' כך ש- $p'|N$. אבל לכל $1\le i\le n$: $p'\neq p_i$.

לכן $p'>p$ ■

אלגוריתם אוקלידס ← איך נחשב GCD בזמן פולינומיאלי.

יהי $a,b\in\mathbb{Z}$, $a\neq 0$, $b\neq 0$. איך נחשב $gcd(a,b)$?

למה: יהיו q,r כך ש- $a=bq+r$, $0\le r<b$. אזי $gcd(a,b)=gcd(b,r)$.

הוכחה: אם $d|a$, $d|b$, אז $d|r$ לכן $gcd(a,b)|r$.

לכן $gcd(a,b)|gcd(b,r)$.

בצד שני אם $d|b$, $d|r$ אז $d|a$ ← $gcd(b,r)|a$ ← $gcd(b,r)|gcd(a,b)$

לכן $gcd(b,r)=gcd(a,b)$ (שניהם חיוביים) ■

האלגוריתם

a, b. $a = q_1 b + r_1$ $\quad 0 \le r_1 < b$

אם $r_1 \neq 0$ כותבים $b = q_2 r_1 + r_2$, $0 \le r_2 < r_1$

ושוב, אם $r_2 \neq 0$ כותבים $r_1 = q_3 r_2 + r_3$ $\quad 0 \le r_3 < r_2$

$b > r_1 > r_2 > \dots r_k$ יש סוף! $r_k = 0$ $\quad r_{k-2} = r_{k-1} q_k + r_k$ $\quad 0 < r_{k-1} < r_{k-2}$

$$r_{k-1} = r_k \cdot q_{k+1} + 0$$

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