Делимост на цели числа. Най-голям общ делител, тъждество на Безу. Прости числа, основна теорема на аритметиката.

Теорема 1. *За произволни цели числа $a, b \in \mathbb{Z}$, $b \neq 0$ съществува единствено частно $q \in \mathbb{Z}$ и остатък $r \in \mathbb{Z}$ при деление на a с b, така че $a = bq + r$ и $0 \leq r < |b|$.*

Доказателство. Представяме реалната права $\mathbb{R} = \cup_{z \in \mathbb{Z}}[z|b|, z|b|+|b|)$ като непресичащо се обединение на полу-отворени интервали $[z|b|, z|b| + |b|)$. Цялото число a попада в точно един интервал $[z|b|, z|b|+|b|)$. Ако $b > 0$, полагаме $q = z$. В случая $b < 0$ избираме $q = -z$, така че $z|b| = bq$. Тогава $bq \leq a < bq + |b|$, откъдето $r := a - bq$ изпълнява неравенствата $0 \leq r < |b|$.

□

Определение 2. *Цялото число $a \in \mathbb{Z} \setminus \{0\}$ дели цялото число $b \in \mathbb{Z}$, ако съществува $c \in \mathbb{Z}$, така че $b = ac$.*

Лема 3. *Нека $a, b \in \mathbb{Z} \setminus \{0\}$ са ненулеви цели числа.*
(i) Ако a дели b и b дели $c \in \mathbb{Z}$, то a дели c.
(ii) Ако a дели b и b дели a, то $b = \pm a$.

(i) По определение, ако a дели b, то съществува $a_1 \in \mathbb{Z}$, така че $b = aa_1$. Аналогично, от това че b дели c следва $c = bb_1$ за някое $b_1 \in \mathbb{Z}$. В резултат, $c = (aa_1)b_1 = a(a_1b_1)$ с $a_1b_1 \in \mathbb{Z}$, което означава, че a дели c.

(ii) Ако a дели b, то съществува $q_1 \in \mathbb{Z}$ с $aq_1 = b$. От друга страна, b дели a, така че съществува $q_2 \in \mathbb{Z}$ с $bq_2 = a$. Сега от $a = (aq_1)q_2 = a(q_1q_2)$ с $a \in \mathbb{Z} \setminus \{0\}$ следва $q_1q_2 = 1$. Затова $q_1 = q_2 = \pm 1$ и $b = \pm a$.

Определение 4. *Нека $a_1, \ldots, a_n \in \mathbb{Z}$ са неедновременно нулеви цели числа. Най-голям общ делител $d = \mathrm{GCD}(a_1, \ldots, a_n)$ на $a_1, \ldots, a_n$ е такова цяло число $d \in \mathbb{Z}$, че:*
(i) d дели $a_1, \ldots, a_n$;
(ii) ако $d_1 \in \mathbb{Z}$ е общ делител на $a_1, \ldots, a_n$, то d_1 дели d.

Ако съществува, най-големият общ делител $d = \mathrm{GCD}(a_1, \ldots, a_n)$ е определен с точност до знак. По-точно, ако $d \in \mathbb{Z}$ и $d' \in \mathbb{Z}$ са най-големи общи делители на $a_1, \ldots, a_n$, то d дели d', защото d е общ делител на $a_1, \ldots, a_n$, а d' е най-голям общ делител на $a_1, \ldots, a_n$. Обратно, d' дели d защото d' е общ делител на $a_1, \ldots, a_n$, а d е най-голям общ делител на $a_1, \ldots, a_n$. От d дели d' и d' дели d получаваме $d' = \pm d$.

Определение 5. *Неедновременно нулевите цели числа $a_1, \ldots, a_n \in \mathbb{Z}$ са взаимно прости, ако най-големият им общ делител е $\mathrm{GCD}(a_1, \ldots, a_n) = \pm 1$.*

Лема 6. *Нека $a_1, \ldots, a_n \in \mathbb{Z}$ са произволни неедновременно нулеви цели числа с най-голям общ делител $d = \mathrm{GCD}(a_1, \ldots, a_n)$. Тогава целите числа $\frac{a_1}{d}, \ldots, \frac{a_n}{d}$ са взаимно прости.*

Доказателство. Достатъчно е да докажем, че единствените цели общи делители c на $\frac{a_1}{d}, \ldots, \frac{a_n}{d}$ са $c = \pm 1$, за да получим, че най-големият общ делител $\mathrm{GCD}\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right) = \pm 1$. Наистина, ако c дели $\frac{a_i}{d}$, то съществуват $b_i \in \mathbb{Z}$ с $cb_i = \frac{a_i}{d}$ за всички $1 \leq i \leq n$. Тогава $cdb_i = a_i$ и cd е общ делител на $a_1, \ldots, a_n$. Следователно cd дели най-големия общ делител d на $a_1, \ldots, a_n$ и съществува $q \in \mathbb{Z}$ с $cdq = d$. Почленното деление на $d \in \mathbb{Z} \setminus \{0\}$ дава $cq = 1$. Това е изпълнено само за $c = q = \pm 1$.

□

Определение 7. *Ненулевите цели числа $a_1, \ldots, a_n \in \mathbb{Z}$ имат най-малко о бщо кратно $m = \mathrm{LCM}(a_1, \ldots, a_n) \in \mathbb{Z}$, ако:*

(i) $a_1, \ldots, a_n$ делят m и

(ii) всяко общо кратно μ на $a_1, \ldots, a_n$ се дели на m.

Ако съществува, най-малкото общо кратно $m = \mathrm{LCM}(a_1, \ldots, a_n)$ на $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ е определено с точност до знак. По-точно. ако m и m' са най-малки общи кратни на $a_1, \ldots, a_n$, то m дели m', защото m' е общо кратно, а m е най-малко общо кратно на $a_1, \ldots, a_n$. Обратно, m' дели m, защото m е общо кратно на $a_1, \ldots, a_n$, а m' е най-малко общо кратно на $a_1, \ldots, a_n$. От m дели m' и m' дели m следва $m' = \pm m$.

Твърдение 8. *(i) Нека $a_1, \ldots, a_n \in \mathbb{Z}$ са неедновременно нулеви цели числа. Тогава най-големият общ делител*

$$\mathrm{GCD}(a_1, \ldots, a_{n-1}, a_n) = \pm \mathrm{GCD}(\mathrm{GCD}(a_1, \ldots, a_{n-1}), a_n)$$

(ii) Нека $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ са ненулеви цели числа. Тогава най-малкото общо кратно

$$\mathrm{LCM}(a_1, \ldots, a_{n-1}, a_n) = \pm \mathrm{LCM}(\mathrm{LCM}(a_1, \ldots, a_{n-1}), a_n).$$

Доказателство. (i) Да означим

$$d := \mathrm{GCD}(a_1, \ldots, a_n), \quad d_1 := \mathrm{GCD}(a_1, \ldots, a_{n-1}), \quad \delta := \mathrm{GCD}(d_1, a_n).$$

Тогава d дели δ, защото d е общ делител на d_1 и a_n. По-точно, d дели d_1, защото d дели $a_1, \ldots, a_{n-1}$, а $d_1 = \mathrm{GCD}(a_1, \ldots, a_{n-1})$ е най-голям общ делител на $a_1, \ldots, a_{n-1}$. Обратно, δ дели d, защото δ е общ делител на $a_1, \ldots, a_{n-1}, a_n$. Тук използваме, че δ дели d_1 и d_1 дели $a_1, \ldots, a_{n-1}$, откъдето δ дели $a_1, \ldots, a_{n-1}$. От d дели δ и δ дели d получаваме, че $\delta = \pm d$.

(ii) Да означим,

$$m := \mathrm{LCM}(a_1, \ldots, a_n), \quad m_1 = \mathrm{LCM}(a_1, \ldots, a_{n-1}), \quad \mu := \mathrm{LCM}(m_1, a_n).$$

Тогава m дели μ, защото μ е общо кратно на $a_1, \ldots, a_n$. По-точно, μ е кратно на a_n и m_1, а m_1 е общо кратно на $a_1, \ldots, a_{n-1}$, откъдето μ е общо кратно на $a_1, \ldots, a_{n-1}$. От друга страна, μ дели m, защото m е общо кратно на на m_1 и a_n. Тук използваме, че m е общо кратно на $a_1, \ldots, a_{n-1}$, така че най-малкото общо крато m_1 на $a_1, \ldots, a_{n-1}$ дели m. От m дели μ и μ дели m следва $\mu = \pm m$.

□

Твърдение 9. *За произволни ненулеви цели числа $a, b \in \mathbb{Z} \setminus \{0\}$ е в сила*

$$\mathrm{GCD}(a, b)\mathrm{LCM}(a, b) = \pm ab.$$

Доказателство. Означаваме

$$d := \mathrm{GCD}(a,b), \quad m := \mathrm{LCM}(a,b),$$

и забелязваме, че $\frac{ab}{m}$ дели d. По-точно, най-малкото общо кратно m на a и b дели общото кратно ab и $\frac{ab}{m} \in \mathbb{Z}$. Числото $\frac{ab}{m}$ е общ делител на a и b, съгласно

$$a = \left(\frac{ab}{m}\right)\left(\frac{m}{b}\right) \quad \text{и} \quad b = \left(\frac{ab}{m}\right)\left(\frac{m}{a}\right) \quad \text{с} \quad \frac{m}{b}, \frac{m}{a} \in \mathbb{Z}.$$

Следователно $\frac{ab}{m}$ дели d и съществува $q_1 \in \mathbb{Z}$ с

$$\frac{ab}{m} q_1 = d.$$

От друга страна, m дели $\frac{ab}{d}$. Тук $\frac{ab}{d} = \left(\frac{a}{d}\right) b \in \mathbb{Z}$, защото d дели a. Цялото число

$$\frac{ab}{d} = a\left(\frac{b}{d}\right) = b\left(\frac{a}{d}\right) \quad \text{с} \quad \frac{b}{d}, \frac{a}{d} \in \mathbb{Z}$$

е общо кратно на a и b, откъдето m дели $\frac{ab}{d}$ и

$$\frac{ab}{d} = mq_2 \quad \text{за някое} \quad q_2 \in \mathbb{Z}.$$

В резултат,

$$\frac{m}{q_1} = \frac{ab}{d} = mq_2,$$

откъдето $m = mq_1q_2$ и$q_1q_2 = 1$ след почленно деление с $m \in \mathbb{Z} \setminus \{0\}$. Следователно $q_1 = q_2 = \pm 1$ и $md = \pm ab$.

□

Съгласно Твърдение 8 и Твърдение 9, намирането на на най-голям общ делител ии на най-малко общо кратно на няколно числа се свежда до намиране на най-голям общ делител $\mathrm{GCD}(a,b)$ на неедновременно нулеви цели числа $a, b \in \mathbb{Z}$. Това се извършва по следния алгоритъм на Евклид:

Нека $a, b \in \mathbb{Z}$, $b \neq 0$. Делим последователно a на b с частно и остатък:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|,$$

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2},$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1},$$

$$r_{n-1} = r_nq_{n+1}.$$

Редицата от остатъци $\{r_i\}_{i \geq 1} \in \mathbb{Z}$ е строго намаляваща и след краен брой стъпки достига до 0. Нека r_n е последният ненулев остатък.

Ако $a = bq_1 + r_1$, то твърдим че $\mathrm{GCD}(a,b) = \pm\mathrm{GCD}(b,r_1)$. В резултат, $\mathrm{GCD}(a,b) = \pm\mathrm{GCD}(b,r_1) = \pm\mathrm{GCD}(r_1,r_2) = \pm\mathrm{GCD}(r_2,r_3) = \ldots = \pm rmGCD(r_{n-1},r_n) = \pm r_n$ и последният ненулев остатък r_n се оказва най-голям общ делител на a и b. За да докажем

$\mathrm{GCD}(a,b) = \mathrm{GCD}(b,r_1)$ да отбележим, че ако $d := \mathrm{GCD}(a,b)$ дели a и b, то d дели $r_1 = a - bq_1$, така че d дели $\delta := \mathrm{GCD}(b,r_1)$. Обратно, δ дели b и r_1, откъдето δ дели $a = bq_1 + r_1$, а оттам и d. От d дели δ и δ дели d следва $d = \pm\delta$.

Тъждеството на Безу за a и b гласи, че съществуват $u, v \in \mathbb{Z}$, за които

$$au + bv = \mathrm{GCD}(a,b).$$

Разглеждайки равенствата отдолу нагоре, $r_n \in r_{n-1}\mathbb{Z} + r_{n-2}\mathbb{Z}$ се представя като сума на кратни на r_{n-1} и r_{n-2}. Понататък, замествайки $r_{n-1} \in r_{n-2}\mathbb{Z} + r_{n-3}\mathbb{Z}$ в представянето на r_n получаваме $r_n \in r_{n-2}\mathbb{Z} + r_{n-3}\mathbb{Z}$. Продължавайки по същия начин извеждаме представяне $r_n \in r_2\mathbb{Z} + r_1\mathbb{Z}$. Въоснова на $r_2 \in r_1\mathbb{Z} + b\mathbb{Z}$ стигаме до извода, че $r_n \in r_1\mathbb{Z} + b\mathbb{Z}$. Накрая, от $r_1 \in a\mathbb{Z} + b\mathbb{Z}$ следва наличието на представяне $r_n \in a\mathbb{Z} + b\mathbb{Z}$, т.е. съществуването на $u, v \in \mathbb{Z}$ с $\mathrm{GCD}(a,b) = r_n = au + bv$. С това доказахме следното

Твърдение 10. (Тъждество на Безу:) *За произволни неедновременно нулеви $a, b \in \mathbb{Z}$ съществуват цели числа $u, v \in \mathbb{Z}$, така че най-големият общ делител*

$$\mathrm{GCD}(a,b) = au + bv.$$

Следствие 11. (Следствия от Тъждеството на Безу:)
(i) ако $a \in \mathbb{Z} \setminus \{0\}$ дели b_1b_2 за $b_1, b_2 \in \mathbb{Z}$ и $\mathrm{GCD}(a,b_1) = \pm 1$, то a дели b_2;
(ii) ако $a_1 \in \mathbb{Z} \setminus \{0\}$ и $a_2 \in \mathbb{Z} \setminus \{0\}$ делят $b \in \mathbb{Z}$ и $\mathrm{GCD}(a_1,a_2) = \pm 1$, то a_1a_2 дели b.

Доказателство. (i) Тъждеството на Безу за взаимно простите цели числа a и b_1 гласи, че $au + b_1v = 1$ за някакви цели числа $u, v \in \mathbb{Z}$. Почленното умножение на това равенство с b_2 дава $ab_2u + b_1b_2v = b_2$. От това, че a дели ab_2u и b_1b_2v получаваме, че a дели $b_2 = ab_2u + b_1b_2v$.

(ii) Съгласно Твърдение 9, от $\mathrm{GCD}(a_1,a_2) = \pm 1$ следва, че най-малкото общо кратно $LCM(a_1,a_2) = \pm a_1a_2$. По предположение, b е общо кратно на a_1 и a_2, така че най-малкото общо кратно a_1a_2 на тези цели числа дели b.

□

Определение 12. *Естествено число $p > 1$ е просто, ако единствените му естествени делители са 1 и p.*

Лема 13. *Ако просто число $p \in \mathbb{N}$ дели произведение $a_1 \dots a_n$ на цели числа $a_1, \dots, a_n \in \mathbb{Z}$, то p дели поне един от множителите a_i.*

Доказателство. Ако p дели произведение $a_1 \dots a_n$ на цели числа $a_1, \dots, a_n$ и p не дели a_1, то $\mathrm{GCD}(p,a_1) = \pm 1$ и p дели $a_2 \dots a_n$ съгласно Следствие 11 (i). С индукция по броя на множителите получаваме, че p дели a_i за някое $2 \le i \le n$.

□

Теорема 14. *Всяко естествено число $n > 1$ има единствено с точност до реда на множителите разлагане $n = p_1 \dots p_k$ в произведение на прости множители p_i.*

Доказателство. Съществуването на разлагане на n се доказва с индукция по $n \in \mathbb{N}$, $n > 1$. Да забележим, че $n = 2$ е просто число, а оттам и свое разлагане. В общия случай, ако n е просто число, то n е свое разлагане. Ако n е съставно, то n се разлага в произведение $n = n_1n_2$ на естествени числа $1 < n_1, n_2 < n$. По индукционно предположение, съществуват разлагания $n_1 = p_1 \dots p_s$ и $n_2 = p_{s+1} \dots p_k$ в прости множители, така че $n = p_1 \dots p_sp_{s+1} \dots p_k$ е разлагане на n в прости множители.

Нека $p_1 \dots p_k = n = q_1 \dots q_l$ са две разлагания на n в прости множители p_i, q_j. Без ограничение на общността можем да считаме, че $k \le l$. Простото число p_k дели

произведението $q_1 \dots q_l$, така че p_k дели q_i за някое $1 \leq i \leq l$. След преномерация можем да считаме, че p_k дели q_l. Понеже q_l е просто число и единствените естествени делители на q_l са 1 и q_l, оттук следва $q_l = p_k$ поради $p_k > 1$. След почленно деление на $p_k \neq 0$ получаваме $p_1 \dots p_{k-1} = q_1 \dots q_{l-1}$ с $k-1 \leq l-1$. С индукция по k оттук следва $k-1 = l-1$ и $p_i = q_i$ за всички $1 \leq i \leq k-1$ след подходяща преномерация на $q_1, \dots, q_{k-1}$.

□

Задача 15. *Нека $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ са ненулеви цели числа, а $\{p_1, \dots, p_s\}$ е обединението на простите множители на $a_1, \dots, a_n$, така че*

$$a_i = \pm \prod_{j=1}^{s} p_j^{k_{ij}} \quad \text{за някои} \quad k_{ij} \in \mathbb{Z}^{\geq 0}.$$

Тогава най-големият общ делител на $a_1, \dots, a_n$ е

$$\mathrm{GCD}(a_1, \dots, a_n) = \pm \prod_{j=1}^{s} p_j^{\min(k_{1j}, k_{2j}, \dots, k_{nj})},$$

а най-малкото общо кратно на $a_1, \dots, a_n$ е

$$\mathrm{LCM}(a_1, \dots, a_n) = \pm \prod_{j=1}^{s} p_j^{\max(k_{1j}, k_{2j}, \dots, k_{nj})}.$$

Доказателство. Да забележим, че

$$d := \prod_{j=1}^{s} p_j^{\min(k_{1j} k_{2j}, \dots, k_{nj})}$$

дели a_i за всяко $1 \leq i \leq n$, защото

$$\frac{a_i}{d} = \pm \prod_{j=1}^{s} p_j^{k_{ij} - \min(k_{1j}, \dots, k_{nj})} \in \mathbb{Z},$$

съгласно $k_{ij} \geq \min(k_{1j}, \dots, k_{nj})$. Следователно d е общ делител на $a_1, \dots, a_n$. Ако $d_1 \in \mathbb{Z}$ е общ делител на $a_1, \dots, a_n$, то

$$d_1 = \pm \prod_{j=1}^{s} p_j^{l_j} \quad \text{за} \quad l_j \in \mathbb{Z}^{\geq 0} \quad \text{и}$$

$$\frac{a_i}{d_1} = \pm \prod_{j=1}^{s} p_j^{k_{ij} - l_j} \in \mathbb{Z}$$

изисква $k_{ij} \geq l_j$ за всички $1 \leq i \leq n$ и всички $1 \leq j \leq s$. Оттук получаваме, че $\min(k_{1j}, \dots, k_{nj}) \geq l_j$ и

$$\frac{d}{d_1} = \pm \prod_{j=1}^{s} p_j^{\min(k_{1j}, \dots, k_{nj}) - l_j} \in \mathbb{Z}.$$

Това доказва, че $\mathrm{GCD}(a_1, \dots, a_n) = \pm d$.

Нека

$$m := \prod_{j=1}^{s} p_j^{\max(k_{1j}, \dots, k_{nj})}.$$

Тогава

$$\frac{m}{a_i} = \pm \prod_{j=1}^{s} p_j^{\max(k_{1j},\ldots,k_{nj})-k_{ij}} \in \mathbb{Z}$$

за всички $1 \leq i \leq n$, съгласно $\max(k_{1j},\ldots,k_{nj}) \geq k_{ij}$ и m е общо кратно на $a_1,\ldots,a_n$. Произволно общо кратно на $a_1,\ldots,a_n$ е от вида

$$m_1 = \pm \prod_{j=1}^{s} p_j^{r_j} \prod_{j=s+1}^{t} p_j^{r_j} \quad \text{с} \quad \frac{m_1}{a_i} = \pm \prod_{j=1}^{s} p_j^{r_j-k_{ij}} \prod_{j=s+1}^{t} p_j^{r_j} \in \mathbb{Z}$$

така че $r_j \geq k_{ij}$ за всички $1 \leq i \leq n$ и всички $1 \leq j \leq s$. Оттук, $r_j \geq \max(k_{1j},\ldots,k_{nj})$ и

$$\frac{m_1}{m} = \pm \prod_{j=1}^{s} p_j^{r_j-\max(k_{1j},\ldots,k_{nj})} \prod_{j=s+1}^{t} p_j^{r_j} \in \mathbb{Z}.$$

Това доказва, че m дели m_1 и $\mathrm{LCM}(a_1,\ldots,a_n) = \pm m$.

□

Определение 16. *Разбиване на множество S е представяне $S = \cup_{\alpha\in A} S_\alpha$ като обединение на две по две непресичащи се подмножества $S_\alpha \cap S_\beta = \emptyset$.*

Например, представянето $\mathbb{Z} = 2\mathbb{Z} \cup (2\mathbb{Z}+1)$ на целите числа като обединение на четни и нечетни е разбиване на $\mathbb{Z}$.

Определение 17. *Всяко подмножество R на $S \times S$ се нарича бинарна релация в S. Записваме $a \sim b$ за $a, b \in R$.*

Определение 18. *Казваме, че $R \subseteq S \times S$ е релация на еквивалентност, ако:*
(i) $a \sim a$ за всяко $a \in S$;
(ii) от $a \sim b$ следва $b \sim a$ за всички $a, b \in S$;
(iii) от $a \sim b$ и $b \sim c$ следва $a \sim c$ за $a, b, c \in S$.

Твърдение 19. *Разбиванията на множество S са във взаимно еднозначно съответствие с релациите на еквивалентност в S.*

Доказателство. Ако $S = \cup_{\alpha\in A} S_\alpha$ е разбиване на S, полагаме $a \sim b$, ако $a, b \in S_\alpha$ принадлежат на едно и също подмножество от разбиването. Тогава $a \sim a$ и от $a \sim b$ следва $b \sim a$. Ако $a \sim b$ и $b \sim c$, то съществуват $\alpha, \beta \in A$ с $a, b \in S_\alpha$ и $b, c \in S_\beta$. Съгласно $S_\alpha \cap S_\beta = \emptyset$ за $S_\alpha \neq S_\beta$, стигаме до извода, че $S_\alpha = S_\beta$ и $a, b, c \in S_\alpha$. Оттук, $a \sim c$ и $\sim$ е релация на еквивалентност.

Нека $\sim$ е релация на еквивалентност в S. За всяко $a \in S$ разглеждаме класа на еквивалентност $C_a := \{x \in S \,|\, x \sim a\}$ на a. Тогава $S = \cup_{a\in S} C_a$ и ако $C_a \cap C_b \neq \emptyset$ за някои $a, b \in S$, то $C_a = C_b$. По-точно, ако съществува $c \in C_a \cap C_b$, то $c \sim a$ и $c \sim b$, откъдето $a \sim b$. Сега за всяко $x \in C_a$ е в сила $x \sim a$. Комбинирайки с $a \sim b$, получаваме $x \sim b$. В резултат, $x \in C_b$ и $C_a \subseteq C_b$. Аналогично, ако $y \in C_b$, то $y \sim b$. Съгласно $b \sim a$ получаваме $y \sim a$. Оттук, $y \in C_a$ и $C_b \subseteq C_a$. Това доказва $C_a = C_b$ за $C_a \cap C_b \neq \emptyset$ и установява, че $S = \cup_{a\in S} C_a$ е разбиване на S.

Ако $S = \cup_{\alpha\in A} S_\alpha$ е разбиване на S, то за всяко $a \in S_\alpha$ класът на еквивалентност

$$C_a = \{x \in S \,|\, x \sim a\} = \{x \in S \,|\, x \in S_\alpha\} = S_\alpha$$

съвпада с S_α и разбиванията $S = \cup_{\alpha\in A} S_\alpha = \cup_{a\in S} C_a$ съвпадат.

Ако $\sim$ е релация на еквивалентност в S, то разбиването $S = \cup_{a\in S} C_a$ отговаря на релацията на еквивалентност $R' \subseteq S \times S$, за която $(a, b) \in R'$ точно когато $b \in C_a$.

Съгласно $C_a = \{x \in S \,|\, x \sim a\}$, R' съвпада с първоначалната релация на еквивалентност и съответствието между разбиванията на S и релациите на еквивалентност в S е биективно.

□

Твърдение 20. *Релациите на еквивалентност в множество S са във взаимно еднозначно съответствие със сюрективните изображения $f : S \to T$ на S.*

Доказателство. Съгласно Твърдение 19, достатъчно е да проверим, че съществува взаимно еднозначно съответствие между разбиванията $S = \cup_{\alpha \in A} S_\alpha$ на S и сюрективните изображения на множества $f : S \to T$.

Ако $S = \cup_{\alpha \in A} S_\alpha$ е разбиване на S и $T := \{S_\alpha \,|\, \alpha \in A\}$, то $f : S \to T$, $f(a) = S_\alpha$ за $a \in S_\alpha$ е сюрективно изображение. Обратно, всяко сюрективно изображение $f : S \to T$ задава разбиване $S = \cup_{t \in T} f^{-1}(t)$, защото за $t_1 \neq t_2$ от T е в сила $f^{-1}(t_1) \cap f^{-1}(t_2) = \emptyset$. По-точно, допускането за съществуване на $a \in f^{-1}(t_1) \cap f^{-1}(t_2)$ води до $t_1 = f(a) = t_2$, което е противоречие.

Ако разбиването $S = \cup_{\alpha \in A} S_\alpha$ отговаря на сюрективното изображение $f : S \to T = \{S_\alpha \,|\, \alpha \in A\}$, $f(a) = S_\alpha$ за $a \in S_\alpha$, то слоевете $f^{-1}(S_\alpha) = \{a \in S \,|\, a \in S_\alpha\} = S_\alpha$ на f съвпадат с подмножествата S_α на S.

Ако сюрективното изображение $f : S \to T$ задава разбиване $S = \cup_{t \in T} f^{-1}(t)$ то сюрективното изображение $f_1 : S \to T_1 = \{f^{-1}(t) \,|\, t \in T\}$ отговаря на разбиването $S = \cup_{t \in T} f^{-1}(t)$. Тук $f^{-1}(t)$ се разглежда като точка на T_1 и като подмножество на S.

Това доказва биективността на съответствието между разбиванията на S и сюрективните изображения на множества $f : S \to T$, а оттам и биективността на съответствието между релациите на еквивалентност в S и сюрективните изображения на множества $f : S \to T$.

□

Определение 21. *Целите числа $a, b \in \mathbb{Z}$ са сравними по модул $n \in \mathbb{N}$, $n > 1$, ако n дели $a - b$. Записваме $a \equiv b (\mathrm{mod}\, n)$.*

Нека $a = nq_1 + r_1$ и $b = nq_2 + r_2$ са деленията на n с частни $q_1, q_2 \in \mathbb{Z}$ и остатъци $r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1, r_2 \leq n - 1$. Тогава

$$a - b = n(q_1 - q_2) + (r_1 - r_2) \quad \text{с} \quad -(n-1) \leq r_1 - r_2 \leq n - 1$$

се дели на n тогава и само тогава, когато $r_1 - r_2 = 0$. С други думи, $a \equiv b (\mathrm{mod}\, n)$ точно когато a и b имат един и същи остатък при деление на n.

Сравнимостта по модул $n \in \mathbb{N}$, $n > 1$ е релация на еквивалентност, защото n дели $a - a = 0$ за всяко $a \in \mathbb{Z}$. Ако n дели $a - b$, то n дели $b - a$. Ако $a - b$ и $b - c$ са кратни на n, то n дели $(a - b) + (b - c) = a - c$.

За всяко цяло число $0 \leq r \leq n - 1$, класът на еквивалентност

$$C_r = \{x \in \mathbb{Z} \,|\, x \equiv r (\mathrm{mod}\, n)\}$$

се състои от всички цели числа x с остатък r при деление на n. Разбиването на $\mathbb{Z}$, отговарящо на сравнимостта по модул n е $\mathbb{Z} = \cup_{r=0}^{n-1} C_r$. Ако $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ е множеството на остатъците при деление на n, то сравнимостта по модул n съответства на сюрективното изображение на множества $f : \mathbb{Z} \to \mathbb{Z}_n$, съпоставящо на цяло число a остатъка $f(a) = \overline{a}$ на a при деление на n.