Взаимно прости числа

Дефиниция
Числата $a \in \mathbb{Z}$ и $b \in \mathbb{Z}$ наричаме **взаимно прости** т.с.т.когато те нямат общи делители по-големи от 1($\iff (a,b) = 1$).

Твърдения:
1. Ако $a \mid b_1 b_2$ и $(a, b_1) = 1 \implies a \mid b_2$
2. Ако $a_1 \mid b$ и $a_2 \mid b$ и $(a_1, a_2) = 1 \implies a_1 a_2 \mid b$

Доказателство:
1. $(a, b_1) = 1 = ua + vb_1$ (от тъждеството на Безу)
Умножаваме двете страни на равенството с b_2 и получаваме, че $b_2 = uab_2 + vb_1 b_2$ (1)
Знаем, че $a|a \Rightarrow a|uab_2$ (2)
Дадено е, че $a|b_1 b_2 \Rightarrow a|vb_1 b_2$ (3)
От (1), (2), и (3) $\implies a|b_2$. $\square$

2. $a_1|b \Rightarrow b = a_1 t_1,\ t_1 \in \mathbb{Z}$
$a_2|b \Rightarrow a_2|a_1 t_1$, но $(a_1, a_2) = 1 \implies a_2|t_1$ (от твърдение 1))
$\implies t_1 = a_2 x \Rightarrow b = a_1 a_2 x \implies a_1 a_2|b$. $\square$

Прости числа

Дефиниция
Естествените числа, които имат точно два естествени делителя(1 и себе си), наричаме **прости числа**.

1 не е просто![1]

Свойства на простите числа

Нека p е просто число.
Тогава:

- $(p,a) = \begin{cases} 1, & p \nmid a \\ p, & p \mid a \end{cases}$
- $p \mid a_1 a_2 \implies p \mid a_1$ или $p \mid a_2$ (не е изключващо или)

Забележка: Горните две свойства остават без доказателство!

1. $x \in \mathbb{Z},\ x \neq \pm 1 \implies x$ се дели на поне едно просто число.
2. Има безброй много прости числа.

Доказателство:
1. Да разгледаме най-малкия положителен делител p на x, по голям от 1. Има 2 случая:

1. $p = x$, в такъв случай, очевидно x няма други делители освен $\pm 1, \pm x$ следователно x е просто и $x|x$, с което твърдението е доказано.
2. $p < x$. Да допуснем, че p не е просто. Тогава съществува положително число q, такова че $q|p \& q > 1 \& q < p$. Очевидно $q|p|x$, противоречие с факта, че p е най-малкият положителен делител $\neq 1$. Следователно p е просто и $p|x$ $\square$.

2. Допускаме, че има краен брой прости числа $p_1, p_2, \cdots, p_k$.
Разглеждаме числото $P = p_1 p_2 \cdots p_k + 1$.
Ако P се дели на някое просто число p_i(което трябва да бъде измежду числата $p_1, p_2, \cdots p_k$), то тогава и числото 1 ще трябва да се дели на p_i, което е противоречие.
Тогава P очевидно има само два делителя - 1 и себе си(защото не се дели на никое просто число) и следователно е просто. Това е противоречие с допускането, твърдението е доказано. $\square$

Основна теорема на аритметиката

Нека $n > 1,\ n \in \mathbb{N}$. Тогава съществува представяне на n като произведение на прости множители, т.е.
$n = p_1 p_2 \cdots p_k,\ \ p_i$-прости, и то е единствено с точност до реда на множителите.
Наричаме представянето *Канонично разлагане/Каноничен вид на N*.

Доказателство:
$|\exists|$ *Съществуване*:
Провеждаме индукция по n:

1. $n = 2$. 2 е просто и следователно това е подходящо представяне.
2. Нека е доказано за всички числа по-малки или равни на n.
3. За $n+1$:
    1. Ако $n+1$ е просто - готово
    2. $n+1$ не е просто, и от горното твърдение за прости числа - съществува число p_0 - просто, такова че $p_0 \mid n+1$. Освен това $p_0 \neq n+1$ (защото n + 1 не е просто), следователно $n+1 = p_0 . b$. Прилагаме индукционната хипотеза за b и получаваме, че b се представя като $p_1 p_2 \cdots p_t$ където p_i са прости числа. Така получихме, че $n+1 = p_0 . b = p_0 p_1 p_2 \cdots p_t$

$|!|$ *Единственост*:
Нека $a = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_s$ са две различни представяния на a.
$p_1 | p_1 p_2 \cdots p_t \implies p_1 | q_1 q_2 \cdots q_s$
Следователно съществува поне едно q_i (например q_1), такова че $p_1 | q_1$.
И тъй като p_1 и q_1 са прости $\implies p_1 = q_1$.

Разделяме двете страни на равенството на p_1 и получаваме, че
$p_2 p_3 \cdots p_t = q_2 q_3 \cdots q_s$.

С прилагане на същото разсъждение краен брой пъти ще получим, че $t = s$ и $p_i = q_i,\ i = 1, 2, \cdots, t$ (разбира се, с преномерация). $\square$

Следствие: $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$,където $p_i \neq p_j$ за $i \neq j, \quad k_i \in \mathbb{N}$.

Твърдения:
Нека $a, b \in \mathbb{N}$ и $a, b > 1$.
От следствието от основната теорема на аритметиката имаме, че:
$a = l_1^{x_1} l_2^{x_2} \cdots l_m^{x_m}$
$b = l_1^{y_1} l_2^{y_2} \cdots l_m^{y_m}$, където l_i са прости числа, а $x_i, y_i \in \mathbb{N} \cup \{0\}$, за $\forall i = 1 \cdots m$.

Тогава:
1) НОД$(a, b) = l_1^{z_1} l_2^{z_2} \cdots l_m^{z_m}$, където $z_i = min(x_i, y_i)$.
2) НОК$(a, b) = l_1^{u_1} l_2^{u_2} \cdots l_m^{u_m}$, където $u_i = max(x_i, y_i)$.

Дефиниция (Най-малко общно кратно или НОК)
Нека $a, b \in \mathbb{N}$. *Най-малкото общо кратно* на **a** и **b**, наричаме **минималното** естествено число **c**, за което *a*|*c* и *b*|*c*.
Отбелязваме НОК(a,b) = c. Или още [a,b] = c, lcm(a,b) = c (least common multiple).

Пример за НОК
За числата 12 и 18 получаваме, че [12, 18] = 36, тъй като 12|36 и 18|36
а за всяко друго естествено число **s**, по-малко от 36 следва, че $12 \nmid s$ или $18 \nmid s$.

Друг лесен начин за намиране на НОК(a,b) е чрез формулата $[a,b] = \frac{ab}{(a,b)}$.

Числови сравнения

Дефиниция
Нека $n \in \mathbb{N},\ n \neq \pm 1, 0$ и нека $a, b \in \mathbb{Z}$.
Казваме, че a е сравнимо с b по модул n, ако n дели разликата на a и b.
Записваме:
$a \equiv b (mod\ n)$

Еквивалентни дефиниции:

$$\begin{aligned} a \equiv b \pmod{n} &\iff n | (a-b) \\ &\iff a = b + sn \\ &\iff a = q_1 n + r, \quad b = q_2 n + r \end{aligned} \tag{1}$$

(т.е. a и b дават един и същи остатък при деление с n).[2]

Свойства на числовите сравнения

1. $a \equiv a \pmod{n}$ (**рефлексивност**)
2. $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ (**симетричност**)
3. $a \equiv b \pmod{n}, \quad b \equiv c \pmod{n} \implies a \equiv c \pmod{c}$ (**транзитивност**)
   offtopic: от изброените до тук свойства можем да твърдим, че релацията $\equiv$ е *релация на еквивалентност* (ако ви питат, да знаете ;))
4. $a_1 \equiv b_1 \pmod{n}, \quad a_2 \equiv b_2 \pmod{n} \implies$
   1. $ka_1 \equiv kb_1 \pmod{n}, \quad k \in \mathbb{Z}$
   2. $k + a_1 \equiv k + b_1 \pmod{n}, \quad k \in \mathbb{Z}$
   3. $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
   4. $a_1 - k \equiv b_1 - k \pmod{n}, \quad k \in \mathbb{Z}$
   5. $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$
   6. $a_1 a_2 \equiv b_1 b_2 \pmod{n}$
   7. $a_1^t \equiv b_1^t \pmod{n}, \quad t \in N + \{0\}$
   8. $f(a_1) \equiv f(b_1) \pmod{n}$, където f е полином:
      $f(x) = c_0 x^k + c_1 x^{k-1} + \cdots + c_k, \quad c_i \in \mathbb{Z},\ k \in N + \{0\}$
5. $a \equiv b \pmod{n}$, следователно $(a,n) = (b,n)$

Забележка: 5^{то} свойство **не е** давано на лекции (или поне човека, който е писал първи статията не го е написал), обаче то очевидно се ползва в доказателството на мултипликативността на φ в края на главата (където не е доказано), затова реших да го отделя като свойство на сравненията.
Забележка: Всъщност е доказано в тема "1" при алгоритъм на Евклид
$(a,n) = (b,n)$, ако $a = qb + n$

Доказателства:
Всяко едно от тези двойства се доказва почти непосредствено, следвайки дадените дефиниции и свойствата на делимостта.
Освен това някои са просто обобщение на други.

Ето и няколко примерни доказателства:

За свойство 1:
$n|0$ (свойство на делимостта)
$0 = a - a$ (от втори или трети клас)
$\Longrightarrow n|(a-a) \Rightarrow a \equiv a \pmod{n}$. $\square$

За свойство 4.4:
Дадено е, че:
$a_1 \equiv b_1 \pmod{n} \Longrightarrow n|(a_1 - b_1)$
$a_2 \equiv b_2 \pmod{n} \Longrightarrow n|(a_2 - b_2)$

Образуваме си разликата
$a_1 a_2 - b_1 b_2 = a_1 a_2 - a_1 b_2 + a_1 b_2 - b_1 b_2 = a_1 (\underbrace{a_2 - b_2}_{n|}) + b_2 (\underbrace{a_1 - b_1}_{n|})$

$\Longrightarrow n|(a_1 a_2 - b_1 b_2) \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{n}$. $\square$

За свойство 5:
Нека $(a,n) = d_1$ и $(b,n) = d_2$. От сравнението имаме, че $n \mid a - b$, и понеже $d_1 \mid n \& d_1 \mid a$ получаваме $d_1 \mid b$, следователно $d_1 \mid (b,n) = d_2$. Сега прилагаме същото разсъждение но за d_2: понеже $d_2 \mid n \mid a - b \& d_2 \mid b$ имаме $d_2 \mid a$, следователно $d_2 \mid (a,n) = d_1$. Така окончателно получихме $d_1 = d_2$, т.е $(a,n) = (b,n)$

От свойствата на числовите сравнения ясно се вижда, че две (и повече) сравнения може да ги правим всичко друго, освен да ги делим подобаващо.
Разбира се, и такова животно има, но с известни уточнения.
За нетърпеливите, ето и очакваното \cdots

Твърдение:
Нека $n \in \mathbb{N}, \quad n \neq \pm 1, 0$
Ако $ta \equiv tb \pmod{n}$, тогава $a \equiv b \pmod{\frac{n}{(n,t)}}$.

Доказателство (ала Зори ;)):
Нека $(n,t) = d$ и $n = n_1 d$, а $t = t_1 d$
Тогава $(n_1, t_1) = 1$ (*) //иначе d нямаше да е най-големият общ делител на n и t.

$ta \equiv tb \pmod{n} \Longrightarrow n|t(a-b)$. Заместваме и получаваме, че
$n_1 d | t_1 d (a-b) \Rightarrow n_1 | t_1 (a-b)$ (#)

От (*) и (#) следва, че $n_1 | (a-b)$, т.е. $a \equiv b \pmod{n_1}$

Но $n_1 = \frac{n}{d} = \frac{n}{(n,t)}$ и следователно $a \equiv b \pmod{\frac{n}{(n,t)}}$. $\square$

Функция на Ойлер

Дефиниция
Нека $n \in \mathbb{N}$ и $n > 1$.

$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$

С $\varphi(n)$ отбелязваме броя на естествените числа, ненадминаващи n и взаимно прости с n.

Примери:
$\varphi(2) = 1$, понеже 1 е единственото естествено число, ненадминаващо 2 и взаимно просто с 2.
$\varphi(3) = 2$, понеже 1 и 2 са единствените естествени числа, ненадминаващи 3 и взаимно прости с 3.
$\varphi(4) = 2$, (1 и 3)
$\varphi(5) = 4$, (1,2,3 и 4).

Свойства на функцията на Ойлер

1) Ако p е просто, то $\varphi(p) = p - 1$.
2) Ако n е степен на просто число просто, то $\varphi(n) = \varphi(p^k) = p^k - p^{k-1}$.

Доказателство:
1) Тъй като p е просто число, то p е взаимно просто със всички естествени числа, ненадминаващи p, които са $p - 1$ на брой.
Т.е. $\varphi(p) = p - 1$. $\square$

2)Тъй като p е просто число, то числата, които не надминават p^k, и **не** са взаимно прости с p^k, са само тези, които са кратни на p; т.е. числата
$p,\ 2p,\ 3p,\ \cdots,\ p.p,\ (p+1)p,\ \cdots,\ (p^{k-1}-1)p,\ p^{k-1}p$, които са точно p^{k-1} на брой.

Всички естествени числа, ненадминаващи p^k, са $1, 2, \cdots, p^k$, демек p^k на брой.

Така, за броят на естествените числата, които не надминават p^k и са взаимно прости с p^k, получаваме $p^k - p^{k-1}$.
Т.е. $\varphi(p^k) = p^k - p^{k-1}$. $\square$

Теорема

Нека n е естествено число и $n = ab,\ (a,b) = 1$.
Тогава $\varphi(n) = \varphi(a)\varphi(b)$. Тоест, $\varphi(n)$ е *мултипликативна функция*.

Доказателство:
Построяваме си матрицата

$$A_{b,a} = \begin{pmatrix} 1 & 2 & \cdots & a \\ a+1 & a+2 & \cdots & 2a \\ \vdots & \vdots & \ddots & \vdots \\ (b-1)a+1 & (b-1)a+2 & \cdots & ba \end{pmatrix} \tag{2}$$

Първо ще докажем, че елементите във x-тия стълб дават остатък x при деление с a:
Да разгледаме x-тия стълб:

$$X = \begin{pmatrix} x \\ a+x \\ \vdots \\ (b-1)a+x \end{pmatrix} \tag{3}$$

Общия вид на елементите му е $X_i = ai + x$[3], където $i = \overline{0, b-1}$. Не е трудно да се види, че $a \mid X_i - x = ai + x - x = ai$, т.е имаме, че $X_i \equiv x \pmod{a}$, за всяко $i = \overline{0, b-1}$.

Ще докажем, че числата във произволен стълб образуват пълна система остатъци при деление на b[4]:
Да допуснем, че има два елемента от един и същи стълб, които дават еднакви остатъци при деление на b. Нека това са X_i и X_j, т.е нека $X_i \equiv X_j \pmod{b}$. $b \mid X_i - X_j = (ia + x) - (ja + x) = (i-j)a$. Сега използваме, че $(a, b) = 1$, заедно с първото свойство за взаимно прости числа и получаваме $b \mid i - j$. Е да обаче $i - j < |b|$ (защото и двете са неотрицателни, по-малки от b), т.е $i - j = 0 \iff i = j$.
С това показахме, че два произволни елемента на произволен стълб дават различни остатъци. Остава да преборим редовете (да - точно b на брой са) и да заключим, че щом всеки два елемента от всеки стълб дават различни остатъци (общо b на брой остатъка) и самите елементи са b - значи всеки остатък се получава точно по веднъж.

Сега остава да приложим 5[то] свойсто на сравненията (това неофициалното) за да заключим, че:

- ако $(x, a) = 1$, то в x-тия стълб всички числа са взаимно прости с a
- ако $(y, a) > 1$, то в y-тия стълб всички числа НЕ са взаимно прости с a

От горните две получаваме, че всички числа (и само те) взаимно прости с a се намират във стълбовете с индекси, взаимно прости с a.

- във всеки стълб броя на взаимно простите с b числа е точно колкото са взаимно простите с b числа от 0 до $b-1$ - т.е точно $\varphi(b)$.

Сега сглобяваме картинката и получаваме, че ако търсим числата взаимно прости с $n = a.b$, то всъщност търсим числата, взаимно простите едновременно с a и b. Във всичките $\varphi(a)$ стълба от числа взаимно прости с a точно $\varphi(b)$ числа от всеки стълб са взаимно прости с b. Следователно търсения брой е $\varphi(a).\varphi(b)$ $\square$

Следствие:
Нека $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, където $k_i \in \mathbb{N}$, p_i - прости числа и $p_i \neq p_j$ за $i \neq j$ (Канонично разлагане на N).
Тогава:
$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_s^{k_s})$.

И тъй като p_i са прости числа, получаваме еквивалентните предствяния:

$$\begin{aligned}
\varphi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_s^{k_s} - p_s^{k_s-1}) \\
&= p_1^{k_1-1} p_2^{k_2-1} \cdots p_s^{k_s-1} (p_1 - 1)(p_2 - 1) \cdots (p_s - 1) \\
&= \underbrace{p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}}_{n} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s}) \\
&= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s})
\end{aligned} \tag{4}$$

Би трябвало да е очевидно, но все пак - горният израз винаги се разписва до цяло число.

Пример:

$$\begin{aligned}
360 &= 2^3 3^2 5 \\
\varphi(360) &= 360(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) \\
&= 360 \ \frac{1}{2} \ \frac{2}{3} \ \frac{4}{5} \\
&= 96
\end{aligned} \tag{5}$$

Доста по-добре е отколкото да почнеш да броиш самите числа, ненадминаващи 360 и взаимно прости с 360.

Footnotes

1. Струва ми се, че това е нещо, за което доц. Великова би скъсала някой (например мен)
2. Някой ако може и иска, да подравни; аз се изнервих вече ;) (edit) - за теб -

винаги ;)
3. с X_i бележим i-тия елемент (броено от нула) в стълба
4. това означава че остатъците които дават при деление на b са всички числа от 0 до $b-1$ точно по веднъж

page revision: 19, last edited: 22 Jun 2011, 00:17 (746 days ago)