ТЕОРИЯ НА ЧИСЛАТА

ЮЗУ "Неофит Рилски", зимен семестър 2006/2007
доц. Петър Бойваленков

1. Делимост. Теорема за деление с частно и остатък.
2. Бройни системи.
3. Най-голям общ делител. Алгоритъм на Евклид.
4. Прости числа. Основна теорема на аритметиката.
5. Взаимно прости числа. Най-малко общо кратно. Връзка между най-голям общ делител и най-малко общо кратно.
6. Числови сравнения. Основни свойства.
7. Функция на Ойлер.
8. Теорема на Ойлер.
9. Теорема на Ферма.
10. Група на класовете остатъци, взаимно прости с модула.
11. Показател на число по даден модул.
12. Примитивни корени.
13. Сравнения с едно неизвестно. Системи сравнения.
14. Линейни сравнения с едно неизвестно.
15. Линейни системи сравнения с едно неизвестно. Китайска теорема за остатъците.
16. Сравнения по прост модул с едно неизвестно.
17. Сравнения по прост модул с няколко неизвестни. Теорема на Шевалие.
18. Теорема на Уилсън. Близнаци прости числа.
19. Квадратични остатъци. Критерий на Ойлер.
20. Символ на Льожандър. Закон за реципрочност.
21. Мултипликативни функции.
22. Функция-сума.
23. Сума от делителите на естествено число. Съвършени числа.
24. Функцията $[x]$. Приложения на $[x]$.
25. Метод на безкрайното спускане. Решения в цели числа на уравненията $x^2+y^2=z^2$ и $x^4+y^4=z^2$.
26. Диофантови уравнения.

1. Делимост. Теорема за деление с частно и остатък

Делимост – дефиниция и основни свойства

Нека $\mathbb{Z}$ е множеството от целите числа.

Дефиниция 1. Нека $a, b \in \mathbb{Z}$, $a \neq 0$. Ще казваме, че a *дели* b (записва се $a|b$), ако съществува число $k \in \mathbb{Z}$, за което $ak = b$. Ако $a|b$, то числото a се нарича *делител* на b.

Ако a не дели b (т.е. не съществува число k с описаните свойства), ще записваме $a \not| b$. Директно от Дефиниция 1 следват някои елементарни свойства на релацията делимост.

(1) $a|a$ за всяко $a \in \mathbb{Z}$, $a \neq 0$.

(2) Ако $a|b$ и $b \neq 0$, то $|a| \leq |b|$.

(3) Ако $a|b$ и $b|a$, то $a = \pm b$.

(4) Ако $a|b$ и $b|c$, то $a|c$.

(5) Ако $a|b$ и $a|c$, то $a|b \pm c$.

(6) Ако $a|b$ и c е произволно число, то $a|bc$.

(7) Ако $a|b_1$, $a|b_2$,..., $a|b_n$ и $c_1, c_2, \ldots, c_n$ са произволни цели числа, то $a|b_1c_1 + b_2c_2 + \cdots + b_nc_n$ (това свойство обобщава (5) и (6)).

(8) Ако $a|b$, то $a| - b$.

(9) Ако $a|b$ и $a|b + c$, то $a|c$.

Лема 1. Ако $a \neq 0$ е цяло число, то има краен брой делители.

Доказателство: Ако d е делител на a, то $1 \leq |d| \leq |a|$ съгласно свойство (2). Следователно за естественото число $|d|$, оттам и за d, има краен брой възможности.

Теорема за деление с частно и остатък

Теорема 1. За всеки две цели числа a и $b \neq 0$ съществуват еднозначно определени цели числа q (частно) и r (остатък), за които

$$a = bq + r, \quad 0 \leq r < |b|.$$

Доказателство: Съществуване: Ако $a = 0$, то частното $q = 0$ и остатъкът $r = 0$ удовлетворяват условията на теоремата. Нека $a > 0$ и $b > 0$. Съществува естествено число k, за което $kb > a$ и нека k е минималното с това свойство. Тогава $(k-1)b \leq a < kb$ и можем да положим $q = k - 1$ и $r = a - bq$. Лесно се проверява, че $a = bq + r$, и $0 \leq r < b$. Случаите $a > 0$, $b < 0$; $a < 0$, $b < 0$; $a < 0$, $b > 0$ се свеждат към горния.

Единственост: Да допуснем, че съществуват двойки (q_1, r_1) и (q_2, r_2) с исканите свойства, т.е.

$$a = bq_1 + r_1,\ 0 \leq r_1 < |b| \ \text{ и } \ a = bq_2 + r_2,\ 0 \leq r_2 < |b|.$$

Тогава $b(q_1 - q_2) = r_2 - r_1$, което означава, че b дели разликата $r_2 - r_1$. Следователно $|b| \leq |r_2 - r_1|$, което е невъзможно. С това теоремата е доказана.

В ситуацията от Теорема 1 казваме, че a дава остатък r при деление на b.

Следствие 1. Ако a, b и $c \neq 0$ са цели числа, то c дели разликата $a - b$ тогава и само тогава, когато a и b дават едни и същи остатъци при деление на c.

Доказателство: Нека $a = cq_1 + r_1$, $0 \leq r_1 < |c|$ и $b = cq_2 + r_2$, $0 \leq r_2 < |c|$.

Необходимост: Ако c дели $a - b$, то от равенството $a - b = c(q_1 - q_2) + r_1 - r_2$ следва, че c дели и разликата $r_1 - r_2$. Тъй като $|r_1 - r_2| < |c|$, единствената възможност за това е $r_1 - r_2 = 0$, т.е. $r_1 = r_2$.

Достатъчност: Ако $r_1 = r_2$, то $a - b = c(q_1 - q_2)$ и оттук следва, че c дели $a - b$.

Задачи

1. а) Да се докаже, че за произволни цели числа a и b числото:

а) $a^2 - b^2$ се дели на $a - b$ и на $a + b$, $a \pm b \neq 0$;

б) $a^k - b^k$ се дели на $a - b$ за всяко естествено число k, $a - b \neq 0$;

в) $a^k + b^k$ се дели на $a + b$ за всяко нечетно естествено число k, $a + b \neq 0$.

2. Да се докаже, че $n^4 + 4$ се дели на $n^2 + 2n + 2$ за всяко цяло число n.

3. Да се докаже, че $a^3 + b^3 + c^3 - 3abc$ се дели на $a + b + c$ за произволни цели числа a, b и c, $a + b + c \neq 0$.

4. Да се намерят всички естествени числа n, за които:

а) $n + 1$ дели $n^2 + 2$; б) $n - 3$ дели $n^3 - 3$;

в) числото $\dfrac{22n + 12}{7n + 10}$ е цяло.

а) *Решение.* От представянето $n^2 + 2 = (n - 1)(n + 1) + 3$ следва, че ако $n + 1$ дели $n^2 + 2$, то $n + 1$ дели 3. Тогава $n + 1 = 3$, откъдето $n = 2$.

5. Да се докаже, че за всяко естествено число n числото:

а) $n^3 + 5n$ се дели на 6; б) $n^5 - n$ се дели на 30;

в) $n^5 - 5n^3 + 4n$ се дели на 120.

6. Да се докаже, че за всяко нечетно естествено число n числото:

а) $n^3 + 3n^2 - n - 3$ се дели на 48. б) $n^{12} - n^8 - n^4 + 1$ се дели на 512.

7. Да се докаже, че за всяко естествено число n числото:

а) $5^{n+1} - 4n - 5$ се дели на 16;

б) $k^{n+1} - (k - 1)n - k$ се дели на $(k - 1)^2$, където k е естествено число;

в) $3^{2n+3} + 40n - 27$ се дели на 64; г) $10^n + 18n - 1$ се дели на 27;

д) $4^n + 15n - 1$ се дели на 9; е) $5^n + 2.3^n + 1$ се дели на 4;

ж) $2^{n+2}.3^n + 5n - 4$ се дели на 25; з) $2^{2^{n+1}} + 2^{2^n} + 1$ се дели на 21.

8.* Да се докаже, че ако целите числа a, b, c и d са такива, че $a - c$ дели $ab + cd$, то $a - c$ дели и $ad + bc$.

9. Да се докаже, че числото $x^2 + 3x + 5$ не се дели на 121 за никое цяло число x.

10. Да се докаже, че ако a, b, c и d са цели числа, за които числото $ax^3 + bx^2 + cx + d$ се дели на 5 за всяко цяло число x, то a, b, c и d се делят на 5.

11. Да се намерят частното и остатъкът от деленето на:

а) 120 на 15; б) 2005 на 95; в) 2048 на 23; г) 729 на 99; д) 12096 на 1024.

12. Ако a, b и $m \neq 0$ са цели числа, то m дели разликата $a - b$ тогава и само тогава, когато a и b дават един и същ остатък при деление на m.

13. Да се докаже, че квадратът на естествено число дава остатък:

а) 0 или 1 при деление на 4.

б) 0, 1 или 4 при деление на 8.

14. Да се докаже, че кубът на естествено число дава остатък 0, 1 или 8 при деление на 9.

15. Да се докаже, че сумата от квадратите на две последователни естествени числа дава остатък 1 при деление на 4.

16. Да се докаже, че никое число от вида $3k + 2$ не е точен квадрат.

17. Да се докаже, че ако 3 дели $x^2 + y^2$, където x и y са естествени числа, то 3 дели x и y.

18. Да се докаже, че ако естествените числа x, y и z са страни на правоъгълен триъгълник, то поне едно от тях се дели на:

а) 2; б) 3; в) 5.

19. Да се докаже, че сумата на квадратите на три (пет) последователни естествени числа никога не е точен квадрат.

20. Да се докаже, че измежду n последователни цели числа точно едно се дели на n.

21.* Нека a и b са естествени числа и q и r са съответно частното и остатъкът при делението на числото a^2+b^2 с числото $a+b$. Да се намерят всички двойки $(a;b)$, за които $q^2+r=1977$.

2. Бройни системи

Теоремата за деление с частно и остатък дава възможност за въвеждане на бройните системи и признаците за делимост.

Теорема 1. Нека a и $p \geq 2$ са естествени числа. Тогава съществува единствено представяне на a във вида

$$a = b_n p^n + b_{n-1}p^{n-1} + \cdots + b_1 p + b_0,$$

където $0 \leq b_i < p$ за всяко $i = 0, 1, \ldots, n$ и $b_n \neq 0$.

Доказателство: Единственост: Да допуснем за момент, че съществуват две представяния от искания вид, т.е.

$$a = b_n p^n + b_{n-1}p^{n-1} + \cdots + b_1 p + b_0 = c_k p^k + c_{k-1}p^{k-1} + \cdots + c_1 p + c_0,$$

където $0 \leq b_i < p$ за всяко $i = 0, 1, \ldots, n$, $b_n \neq 0$, $0 \leq c_i < p$ за всяко $i = 0, 1, \ldots, k$ и $c_k \neq 0$. Тогава p дели $b_0 - c_0$, откъдето следва, че $b_0 = c_0$. Получаваме

$$\frac{a-b_0}{p} = b_n p^{n-1} + b_{n-1}p^{n-2} + \cdots + b_2 p + b_1 = \frac{a-c_0}{p} = c_k p^{k-1} + c_{k-1}p^{k-2} + \cdots + c_2 p + c_1,$$

откъдето можем да продължим по същия начин. В частност, $k = n$ и $b_n = c_n$, $b_{n-1} = c_{n-1}$ и т.н.

Съществуване: Ще проведем индукция по a. При $a = 1$ имаме $n = 0$ и $b_0 = 1$ (същото разсъждение доказва твърдението за всяко $a < p$). Нека $a > 1$ и исканото представяне да съществува за всички естествени числа, по-малки от a. Съгласно Теорема 1 можем да запишем $a = pq + r$, където $0 \leq r < p$. Можем да считаме, че $q > 0$. Тъй като частното q е делител на $a - r$, заключаваме, че $q < |a - r| < a$ и следователно за q е в сила индукционното предположение.

Нека $q = b_k p^k + b_{k-1}p^{k-1} + \cdots + b_1 p + b_0$. Тогава

$$a = pq + r = b_k p^{k+1} + b_{k-1}p^k + \cdots + b_1 p^2 + b_0 p + r$$

има исканите свойства, с което индукционната стъпка е завършена.

Описаното в Теорема 1 представяне се нарича *представяне на a в p-ична бройна система* или *в система с основа p* (използва се и терминът *p-ичен запис на a*). В практиката се използва десетичната бройна система, а в информатиката често се работи с двоична бройна система.

В някои бройни системи е удобно да се формулират признаци за делимост.

Например в десетичната бройна система не е трудно да се докаже, че едно число се дели на 2 (съответно на 4 и 8), ако последната му цифра (съответно числото, образувано от последните му две и три цифри се дели на 4 и 8).

Да разгледаме по-подробно познатият ни от 5-ти клас признак за делимост на 9 (в десетична бройна система).

Ако $a = b_n 10^n + b_{n-1}10^{n-1} + \cdots + b_1 10 + b_0$, то можем да запишем

$$a = b_n(10^n - 1) + b_{n-1}(10^{n-1} - 1) + \cdots + b_1(10 - 1) + (b_n + b_{n-1} + \cdots + b_1 + b_0).$$

Лесно се доказва, че 9 дели $10^k - 1$ за всяко естествено k (по-общо, от тъждеството $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$ следва, че $a - b$ дели $a^k - b^k$ за всяко естествено k).

Следователно, ако 9 дели a, то 9 дели и $b_n+b_{n-1}+\cdots+b_1+b_0$, което е точно сумата от цифрите на a. Обратно, ако 9 дели сумата от цифрите $b_n+b_{n-1}+\cdots+b_1+b_0$, то 9 дели всички събираеми отдясно и значи дели и a.

Задачи

Във всички задачи става въпрос за десетичен запис.

1. (*Признаци за делимост*) Да се докаже, че едно естествено число се дели на:

а) 2 тогава и само тогава, когато последната му цифра се дели на 2;

б) 4 тогава и само тогава, когато числото, образувано от последните му две цифри се дели на 4;

в) 8 тогава и само тогава, когато числото, образувано от последните му три цифри се дели на 8;

г) 5 тогава и само тогава, когато последната му цифра е 0 или 5;

д) 3 тогава и само тогава, когато сборът от цифрите му се дели на 3.

е) 9 тогава и само тогава, когато сборът от цифрите му се дели на 9.

2. Да се докаже, че разликата на две естествени числа, които имат равни сборове на цифрите, се дели на 9.

3. Да се докаже, че естественото число $\overline{a_na_{n-1}a_{n-2}\ldots a_1a_0}$ се дели на 11 тогава и само тогава, когато $a_n-a_{n-1}+a_{n-2}-\cdots$ се дели на 11.

3. Най-голям общ делител. Алгоритъм на Евклид. Теорема на Безу

Най-голям общ делител

Нека $a_1,a_2,\ldots,a_n$ са цели числа, поне едно от които е различно[1] от 0. Всяко число d, което дели едновременно $a_1,a_2,\ldots,a_n$ се нарича техен общ делител. Например 1 е общ делител при произволен избор на $a_1,a_2,\ldots,a_n$. От друга страна, тъй като всяко от числата $a_1,a_2,\ldots,a_n$ има краен брой делители, общите делители също ще бъдат краен брой. В частност, един от тези делители е най-голям измежду всички общи делители.

Дефиниция 1. Най-големият измежду общите делители на $a_1,a_2,\ldots,a_n$ се нарича техен най-голям общ делител (съкратено НОД, на английски GCD – greatest common divisor). Ако d е НОД на $a_1,a_2,\ldots,a_n$, ще записваме

$$d=(a_1,a_2,\ldots,a_n).$$

НОД не е определен единствено в случая, когато $a_1=a_2=\cdots=a_n=0$. Затова винаги ще считаме, че поне едно от числата $a_1,a_2,\ldots,a_n$ е различно от 0.

Ясно е, че $(\pm a,\pm b)=(a,b)$ (т.е. знаците на числата a и b нямат значение за техния НОД). Освен това $(0,b)=|b|$. Следователно е достатъчно да знаем да намираме НОД на положителни числа.

Лема 1. Ако $d=(a,b)$, $a=a_1d$ и $b=b_1d$, то $(a_1,b_1)=1$.

Доказателство: Да допуснем, че $(a_1,b_1)=m>1$. Тогава от $a=a_1d=a_2md$ следва, че md дели a. Аналогично се вижда, че md дели b, т.е. $md>d$ е общ делител на a и b – противоречие.

Алгоритъм на Евклид за намиране на най-голям общ делител на две числа

Нека a и b са цели числа. Техният най-голям общ делител $d=(a,b)$ може да бъде намерен по следния алгоритъм, който е бил известен още на Евклид.

[1] Навсякъде в този въпрос ще предполагаме, че $|a_1|+|a_2|+\cdots+|a_n|>0$, т.е. поне едно от числата $a_1,a_2,\ldots,a_n$ е различно от 0.

Можем да считаме, че $a > 0$ и $b > 0$. Нека за определеност да приемем, че $a \geq b$. Съгласно теоремата за деление с частно и остатък последователно имаме:

$$\begin{aligned} a &= bq_1 + r_1, \quad \text{където } 0 \leq r_1 < b, \\ b &= r_1q_2 + r_2, \quad \text{където } 0 \leq r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \quad \text{където } 0 \leq r_3 < r_2, \\ &\vdots \\ r_{k-2} &= r_{k-1}q_k + r_k, \quad \text{където } 0 \leq r_k < r_{k-1}, \\ r_{k-1} &= r_kq_{k+1}, \quad \text{където } 0 = r_{k+1}. \end{aligned}$$

(в строго намаляващата редица от цели неотрицателни числа

$$b > r_1 > r_2 > r_3 > \cdots > r_{k-1} > r_k > r_{k+1} \cdots$$

непременно се появява 0 и приемаме, че $r_k > 0$ и $r_{k+1} = 0$). Описаната процедура се нарича алгоритъм на Евклид.

Теорема 1. Имаме $(a, b) = r_k$.

Доказателство: От последното равенство в алгоритъма на Евклид следва, че r_k дели r_{k-1}. Тогава от предпоследното заключаваме, че r_k дели r_{k-2}. Аналогично продължаваме и достигаме до извода, че r_k дели b (на предпоследната стъпка) и a на последната стъпка). Следователно r_k е общ делител на a и b. Остава да докажем, че той е най-големият общ делител.

Ако d е общ делител на a и b, то от първото равенство следва, че d дели r_1. Оттук и от второто равенство следва, че d дели r_2. Продължавайки аналогично, на последната стъпка получаваме, че d дели r_k. Следователно $|d| \leq |r_k|$, откъдето $d \leq r_k$.

Теорема 1 има многобройни следствия, които ще използваме по-нататък.

Следствие 1. Ако $c|a$ и $c|b$, то $c|(a, b)$.

Доказателство: Това всъщност е втората част от доказателството на Теорема 1.

Следствие 2. (Критерий за НОД) Естественото число d е НОД на $a \neq 0$ и $b \neq 0$ тогава и само тогава, когато са изпълнени условията:

(1) $d|a$ и $d|b$ (d е общ делител);

(2) ако $d_1|a$ и $d_1|b$, то $d_1|d$ (всеки друг общ делител дели d).

Доказателство: Ако $d = (a, b)$, то (1) следва по дефиниция, а (2) – от Следствие 1. Обратно, ако (1) и (2) са изпълнени, то d е общ делител поради (1), а от прилагането на (2) за $d_1 = (a, b)$ следва, че $d_1 = d$.

Следствие 3. (Теорема на Безу) Ако $a, b \in \mathbf{Z}$ и $d = (a, b)$, то съществуват $u, v \in \mathbf{Z}$, за които $au + bv = d$, като при това $(u, v) = 1$.

Доказателство: От алгоритъма на Евклид имаме

$$d = r_k = r_{k-2} - r_{k-1}q_k = r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1})q_k = (1 + q_{k-1}q_k)r_{k-2} - q_kr_{k-3}$$

и т.н., докато в крайна сметка получим $d = au + bv$. Ако $a = a_1d$ и $b = b_1d$, то $1 = a_1u + b_1v$ и $(a_1, b_1) = 1$ съгласно Лема 1. Ако m е общ делител на u и v, то m дели $a_1u + b_1v = 1$, т.е. $m = 1$. Следователно $(u, v) = 1$.

Следствие 4. Нека $a_1, a_2, \ldots, a_n$ са цели числа и $d_2 = (a_1, a_2)$, $d_3 = (d_2, a_3)$, $\ldots$, $d_n = (d_{n-1}, a_n)$. Тогава $(a_1, a_2, \ldots, a_n) = d_n$.

Доказателство: Тъй като d_n дели d_{n-1}, то дели и a_{n-1} и d_{n-2}. Продължаваме аналогично и получаваме, че d_n дели всяко от числата $a_1, a_2, \ldots, a_n$. Ако d е общ делител на $a_1, a_2, \ldots, a_n$, то d дели d_2, оттам d дели d_3 и т.н., докато заключим, че d дели d_n. Следователно $(a_1, a_2, \ldots, a_n) = d_n$, което и трябваше да докажем.

Следствие 5. (Тъждество на Безу – обобщение) Нека $a_1, a_2, \ldots, a_n$ са цели числа и $d = (a_1, a_2, \ldots, a_n)$. Тогава съществуват цели числа $u_1, u_2, \ldots, u_n$, за които

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = d.$$

Доказателство: При $n = 2$ това е Следствие 3. Нека твърдението е вярно за $n - 1 \geq 2$ числа. Тогава съществуват $v_1, v_2, \ldots, v_{n-1}$, за които

$$a_1v_1 + a_2v_2 + \cdots + a_{n-1}v_{n-1} = (a_1, a_2, \ldots, a_{n-1}) = d_{n-1}.$$

Съгласно Следствие 3 за

$$d = (a_1, a_2, \ldots, a_n) = (d_{n-1}, a_n)$$

съществуват числа u и v, за които $d = d_{n-1}u + a_nv$. Следователно

$$d = d_{n-1}u + a_nv = a_1v_1u + a_2v_2u + \cdots + a_{n-1}v_{n-1}u + a_nv,$$

с което индукционната стъпка е завършена ($u_1 = uv_1, u_2 = uv_2, \ldots, u_{n-1} = uv_{n-1}, u_n = v$).

Следствие 6. Ако $(a, b) = 1$ и a дели bc, то a дели c.

Доказателство: Съгласно тъждеството на Безу имаме числа u и v, за които $au + bv = 1$. Тогава $c = auc + bvc$ и тъй като дясната страна се дели на a, получаваме, че и c се дели на a.

Задачи

1. Да се намери:

а) $(120, 45)$; б) $(378, 291)$; в) $(81, 46)$; г) $(1204, 220)$; д) $(4610, 43)$;

е) $(72, 144, 182)$; ж) $(300, 225, 72, 1280)$; з) $[10, 32]$; и) $[72, 105]$;

й) $[6^6, 10^4]$; к) $[4, 15, 21]$; л) $[2, 3, 5, 154]$.

2. Да се докаже, че ако $d = (a, b)$ и u и v са произволни цели числа, то $d|ua + vb$.

3. Да се докаже, че $d = (a, b)$ е най-малкото естествено число, което се представя във вида $ua + vb$, където u и v са цели числа.

4. Да се докаже, че за всяко естествено число n:

а) $(n, n + 1) = 1$; б) $(2n + 1, 2n + 3) = 1$; в) $(10n + 9, n + 1) = 1$.

5. Да се докаже, че $(a, b) = (5a + 3b, 13a + 8b)$.

6. Да се докаже, че ако $d = (a, b)$, $a = a_1d$ и $b = b_1d$, то $(a_1, b_1) = 1$.

7. Да се докаже, че ако:

а) $a|bc$ и $(a, b) = 1$, то $a|c$.

б) $a|c$, $b|c$ и $(a, b) = 1$, то $ab|c$.

в) $(a, b) = (a, c) = 1$, то $(a, bc) = 1$.

8. Да се докаже, че всяко общо кратно на числата a и b има вида $\dfrac{tab}{(a, b)}$, където t е цяло число.

9. Да се докаже, че ако a и b са естествени числа, то $[a, b](a, b) = ab$.

10. а) Да се докаже, че ако $(a, b) = 1$, то $(11a + 2b, 18a + 5b) = 1$ или 19.

б) Да се докаже, че $(a^2 + 1, 2a + 3) = 1$ или 13.

в) Да се докаже, че ако $(a, b) = 1$, то $(a + b, a^2 + ab + b^2) = 1$ и $(a + b, a^2 - ab + b^2) = 1$ или 3.

11. Да се докаже, че ако p е просто число и k е естествено число, като $1 \leq k \leq p-1$, то p дели биномния коефициент $\binom{p}{k}$.

4. Прости числа. Основна теорема на аритметиката

Прости числа

Дефиниция 1. Естественото число $p > 1$ се нарича *просто*, ако всички негови делители са ± 1 и $\pm p$. Ако естественото число n не е просто, то се нарича *съставно*.

Първите десет прости числа са $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. Числото 4 не е просто, защото се дели на 2 (освен на ± 1 и ± 4). Първите десет съставни числа са $4, 6, 8, 9, 10, 12, 14, 15, 16, 18$.

Лема 1. Всяко естествено число $n > 1$ има поне един делител, който е просто число (прост делител).

Доказателство: Първите няколко естествени числа осигуряват база за индукция. Нека всички числа, по-малки от n имат прости делители. Ако n е просто, няма какво да доказваме. Ако n не е просто, нека $a \neq \pm 1, \pm n$ е негов делител (не непременно прост). Тогава естественото число $\frac{n}{a}$ е по-малко от n и по индукционно предположение има прост делител p. Тогава p дели и n, с което индукционната стъпка е завършена.

Лема 2. Всяко съставно естествено число n има поне един прост делител, който е по-малък или равен от $\sqrt{n}$.

Доказателство: Нека p е прост делител на n. Ако $p \leq \sqrt{n}$, няма какво да доказваме. Ако $p > \sqrt{n}$, то $\frac{n}{p} < \frac{n}{\sqrt{n}} = \sqrt{n}$. Тогава всеки прост делител на $\frac{n}{p}$ е делител на n и е по-малък от $\sqrt{n}$.

Лема 3. Съществуват безбройно много прости числа.

Доказателство: (Евклид) Да допуснем, че съществуват само краен брой прости числа и нека това са числата $p_1, p_2, \ldots, p_k$. Да разгледаме числото

$$P = p_1 p_2 \ldots p_k + 1.$$

Съгласно Лема 1 числото P има прост делител. От нашето допускане следва, че този прост делител е едно от числата $p_1, p_2, \ldots, p_k$. Нека например p_i дели P за някое $i \in \{1, 2, \ldots, k\}$. Тогава p_i дели раликата $P - p_1 p_2 \ldots p_k = 1$, т.е. $p_i = 1$ – противоречие.

Лема 4. Естественото число $p > 1$ е просто тогава и само тогава, когато за всеки две числа a и b, за които p дели произведението ab, следва, че p дели поне едно от числата a и b.

Доказателство: Да отбележим, че ако p е просто число и c е произволно цяло число, то $(c, p) = 1$ или p.

(Необходимост) Нека p е просто число и p дели ab за някои цели числа a и b. Ако $(p, a) = p$, то p дели a. Ако пък $(p, a) = 1$, то оттук и от факта, че p дели ab следва (вж. Следствие 6 от Въпрос 2), че p дели b.

(Достатъчност) Нека p удовлетворява условието и да допуснем, че p е съставно. Тогава съществуват делители a и b на p, за които $p = ab$, като $1 < a \leq b < p$. Но p дели поне едно от числата a и b, т.е. $p \leq a$ или $p \leq b$ – противоречие.

От Лема 4 лесно следва, че ако простото число p дели произведението $a_1 a_2 \ldots a_k$, то p дели поне едно от числата a_i.

Основна теорема на аритметиката

Въвеждането на понятието просто число и разглеждането на елементарните свойства на простите числа дава възможност за формулиране и доказване на следната важна теорема.

Теорема 1. (Основна теорема на аритметиката) Всяко естествено число $n > 1$ се представя като произведение на краен брой прости числа

$$n = q_1 q_2 \dots q_k,$$

като това представяне е единствено с точност до реда на множителите.

Доказателство: (Съществуване) Първите няколко естествени числа осигуряват база за индукция. Нека всички числа, по-малки от n притежават разлагане на краен брой прости делители. Ако n е просто, няма какво да доказваме (представянето е $n = n$). Ако n не е просто, нека q_1 е негов прост делител (такъв прост делител съществува съгласно Лема 1). Тогава естественото число $\frac{n}{q_1}$ е по-малко от n и по индукционно предположение притежава разлагане на прости делители $\frac{n}{q_1} = q_2 q_3 \dots q_k$. Следователно $n = q_1 q_2 \dots q_k$ е искането разлагане за n, с което индукционната стъпка е завършена.

(Единственост) Да допуснем, че

$$n = q_1 q_2 \dots q_k = r_1 r_2 \dots r_m$$

са две представяния на n. Простото число q_1 дели произведението $r_1 r_2 \dots r_m$, което означава, че $q_1 = r_i$ за някое i. Продължавайки по същия начин, достигаме до заключението, че $k = m$ и числата $q_1, q_2, \dots, q_k$ съвпадат в някакъв ред с числата $r_1, r_2, \dots, r_m$.

Следствие 1. (Канонично разлагане) Всяко естествено число $n > 1$ се представя по единствен начин с точност до реда на множителите във вида

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

(p_i са прости, $\alpha_i \geq 1$ са цели).

Доказателство: В разлагането от Теорема 1 групираме еднаквите степени.

Задачи

1. Просто ли е числото:

а) 127; б) 1001; в) $2^{2^3} + 1$.

2. Да се намери броят на простите числа:

а) по-малки от 100; б) по-големи от 100 и по-малки от 156.

3. Да се докаже, че квадратът на просто число $p \geq 5$ дава остатък 1 при деление на 24.

4. а) Да се докаже, че всяко естествено число $a > 1$ притежава поне един прост делител.

б) Да се докаже, че всяко съставно естествено число $a > 1$ притежава поне един прост делител p, за който $p \leq \sqrt{a}$.

в) Да се намерят простите делители на всяко от числата 512, 576, 1001 и 2003.

5. а) Да се докаже, че ако p е просто число и a е цяло число, то $p|a$ или $(a, p) = 1$.

б) Да се докаже, че ако простото число p дели произведението ab (a и b са цели числа), то p дели поне едно от числата a и b.

в) Да се докаже, че ако простото число p дели a^n (a и n са естествени числа), то p дели a.

6. Да се намерят всички естествени числа n, за които числата $n + 10$ и $n + 14$ са прости.

7. Да се намерят всички прости числа p, за които:

а) числото $2p^2 + 1$ е просто. б) числата $4p^2 + 1$ и $6p^2 + 1$ са прости.

8. Да се докаже, че ако числата p и $8p^2 + 1$ са прости, то и числото $8p^2 + 2p + 1$ е просто.

9. Да се намери каноничното разлагане на числото:

а) 60; б) 5005; в) 100^4; г) $7^4 - 1$.

10.* Да се намери най-малкото естествено число n, за което числото $n^2 - n + 11$ има точно 4 (не непременно различни) прости делителя.

11. а) Да се докаже, че ако a и b са взаимнопрости естествени числа, чието произведение е точен квадрат, то a и b са точни квадрати.

б) Да се докаже, че ако a и b са взаимнопрости естествени числа, за които $ab = x^k$, $k \geq 2$ и x са естествени числа, то $a = x_1^k$ и $b = x_2^k$, където x_1 и x_2 са цели числа, за които $x_1 x_2 = x$.

12. Да се докаже, че не съществува естествено число n, за което $n(n+1)$ е точна степен на естествено число.

13. Нека a, b и c са естествени числа, за които ab, bc и ca са точни квадрати. Да се докаже, че $a = ta_1^2$, $b = tb_1^2$ и $c = tc_1^2$ за някои естествени числа t, a_1, b_1 и c_1.

14. Нека x и y са естествени числа, за които $2x^2 + x = 3y^2 + y$. Да се докаже, че числата $x - y$, $2x + 2y + 1$ и $3x + 3y + 1$ са точни квадрати.

15.* Нека a и b са цели числа и k е естествено число. Да се докаже, че ако уравнението $a^k x - b^k y = a - b$ има за решение двойка (x, y) от последователни цели числа, то $|a - b|$ е точна k-та степен.

16. Нека $n \geq 5$ е естествено число. Да се докаже, че произведението на всички прости числа, по-малки от n, е по-голямо от n.

17. Да се намерят всички двойки естествени числа x и y, за които числата $x + y$, $x + 41$, $y + 41$ и $x + y + 41$ са точни квадрати.

18. Да се докаже, че ако естественото число $n > 1$ има каноничното разлагане $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, то броят на естествените делители на n е $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$.

19. Да се докаже, че естественото число $n > 1$ има нечетен брой естествени делители тогава и само тогава, когато n е точен квадрат.

20. Да се намерят всички естествени числа от вида $3^\alpha 5^\beta$, които имат точно 143 естествени делители.

21.** Да се намерят всички естествени числа n, за които от $n | a^2 b + 1$ следва, че $n | a^2 + b$ (a и b са естествени числа).

22.** Да се намери най-голямото естествено число n, за което съществува множество $\{a_1, a_2, \dots, a_n\}$ от естествени числа със следните свойства:

(1) числата a_i са съставни;

(2) всеки две от тези числа са взаимно прости;

(3) $1 < a_i \leq (3n + 1)^2$ за $i = 1, \dots, n$.

5. Взаимно прости числа. Най-малко общо кратно. Връзка между най-голям общ делител и най-малко общо кратно

Взаимно прости числа

Случаят на НОД, равен на 1, представлява специален интерес.

Дефиниция 1. Ако $(a, b) = 1$, ще казваме, че числата a и b са *взаимно прости*. По-общо, ако $(a_1, a_2, \dots, a_n) = 1$, $n \geq 2$, ще казваме, че числата $a_1, a_2, \dots, a_n$ са взаимно прости.

С помощта на понятието за взаимно прости числа тъждеството на Безу и Следствие 7 от Въпрос 3 се формулират по следния начин:

Ако a и b са взаимно прости, то съществуват цели числа u и v, за които

$$au + bv = 1.$$

Ако a е взаимно просто с b и дели произведението bc, то a дели c. Този факт ще бъде използван многократно.

Лема 1. Ако $(a, b) = 1$ и числата a и b поотделно делят c, то произведението ab също дели c.

Доказателство: Тъй като a дели c, имаме $c = ak$ за някое цяло число k. Тогава b дели ak и от Следствие 6 получаваме, че b дели k, т.е. $bm = k$ за някое цяло . Следователно $c = ak = abm$ се дели на ab.

Най-малко общо кратно

Ако $a \neq 0$ и $b \neq 0$ са цели числа, то естественото число c се нарича общо кратно на a и b, ако се дели и на двете (т.е. е кратно и на двете). Ясно е, че за фиксирани a и b съществуват безбройно много техни общи кратни ($|ab|$ е такова, а всички кратни на едно общо кратно също са общи кратни). Все пак – тъй като всяко множество от естествени числа има най-малък елемент, измежду общите кратни съществува най-малко такова и то се нарича най-малко общо кратно (НОК) на a и b. Ако m е НОК на a и b, ще записваме

$$m = [a, b].$$

Аналогично се дефинира и най-малко общо кратно на повече от две числа.

Връзка между НОД и НОК

Теорема 1. Ако a и b са естествени числа, то

$$[a, b] = \frac{ab}{(a, b)}.$$

Доказателство: Очевидно числото $m = \dfrac{ab}{(a, b)}$ е цяло. Ще покажем, че всяко общо кратно на a и b има вида $mt = t \cdot \dfrac{ab}{(a, b)}$, откъдето лесно следва твърдението.

Нека $d = (a, b)$, $a = a_1 d$, $b = b_1 d$ и c е общо кратно на a и b. Ако $c = ac_1$, то за цялото число $\dfrac{c}{b}$ имаме $\dfrac{c}{b} = \dfrac{ac_1}{b_1 d} = \dfrac{a_1 c_1}{b_1}$. Следователно b_1 дели $a_1 c_1$ и от Следствие 6 заключаваме, че b_1 дели c_1, т.е. $c_1 = tb_1$. Тогава

$$c = ac_1 = atb_1 = a\frac{b}{d}t = \frac{ab}{(a, b)}t.$$

Следствие 1. Ако a и b са взаимно прости, то $[a, b] = ab$.

С индукция по n може да се докаже, че:
(1) $[a_1, a_2, \ldots, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$.
(2) Ако $a_1, a_2, \ldots, a_n$ са две по две взаимно прости, то

$$[a_1, a_2, \ldots, a_n] = a_1 a_2 \cdots a_n.$$

(3) Ако всяко от числата $a_1, a_2, \ldots, a_n$ дели b, то $[a_1, a_2, \ldots, a_n]$ дели b.

Формули за НОД и НОК

Нека a и b са естествени числа и $p_1, p_2, \ldots, p_m$ са всички прости числа, които влизат в каноничните разлагания на a или b. Можем да запишем

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} \text{ и } b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_m^{\beta_m},$$

като тези представяния не са непременно каноничните (възможно е някои от степенните показатели да са равни на 0). Тогава за (a, b) и $[a, b]$ са в сила следните формули:

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_m^{\gamma_m},$$

където

$$\gamma_i = \min\{\alpha_i, \beta_i\},\ i = 1, 2, \ldots, m,$$

и

$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \ldots p_m^{\delta_m},$$

където

$$\delta_i = \max\{\alpha_i, \beta_i\},\ i = 1, 2, \ldots, m.$$

Оттук лесно следва ново доказателство на формулата

$$[a, b] = \frac{ab}{(a, b)}$$

(разгледайте поотделно показателя на всеки от множителите $p_1, p_2, \ldots, p_m$ от двете страни).

По-общо, всеки общ делител d на a и b има вида

$$d = p_1^{\mu_1} p_2^{\mu_2} \ldots p_m^{\mu_m},$$

където

$$\mu_i \leq \min\{\alpha_i, \beta_i\},\ i = 1, 2, \ldots, m,$$

а всяко общо кратно m на a и b има вида

$$m = p_1^{\nu_1} p_2^{\nu_2} \ldots p_m^{\nu_m},$$

където

$$\nu_i \geq \min\{\alpha_i, \beta_i\},\ i = 1, 2, \ldots, m.$$

Задачи

1. Нека m, n, a, $b > 1$ са естествени числа, като $(a, b) = 1$.

а) Да се докаже, че ако $a^m + b^m$ дели $a^n + b^n$, то m дели n.

б) Вярно ли е твърдението: "Ако m дели n, то $a^m + b^m$ дели $a^n + b^n$"?

2.* Да се докаже, че ако m, n и $a > 1$ са естествени числа, то $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

3.* Да се докаже, че ако m и $a > 1$ са естествени числа, то $\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (m, a - 1)$.

4.* Нека k и $n > 1$ са взаимнопрости естествени числа. За $i \in \{1, 2, \ldots, n - 1\}$ означаваме с r_i остатъка от делението на ik с n. Да се докаже, че $\frac{r_1}{1} + \frac{r_2}{2} + \cdots + \frac{r_{n-1}}{n - 1} \geq n - 1$.

5.** Нека $f(n) = n^2 - n + 1$, където $n > 1$ е естествено число. Да се докаже, че всеки две от числата $n, f(n), f(f(n)), \ldots$ са взаимно прости.

6. Числови сравнения. Основни свойства.

Числови сравнения

Дефиниция 1. Нека a, b и m са цели числа. Ще казваме, че a *е сравнимо с* b *по модул* m и ще записваме $a \equiv b (\mathrm{mod}\ m)$ тогава и само тогава, когато m дели разликата $a - b$.

От Следствие 1 от Въпрос 1 следва, че $a \equiv b (\mathrm{mod}\ m)$ тогава и само тогава, когато a и b дават един и същи остатък при деление на m. Когато a не е сравнимо с b по модул m, ще записваме $a \not\equiv b (\mathrm{mod}\ m)$.

Имаме например $6 \equiv 10 (\mathrm{mod}\ 2)$, $100 \equiv 0 (\mathrm{mod}\ 25)$, $996 \equiv -3 (\mathrm{mod}\ 9)$, $2^m \equiv 0 (\mathrm{mod}\ 4)$ за всяко цяло $m \geq 2$ и т.н., докато $4 \not\equiv 7 (\mathrm{mod}\ 2)$, $6 \not\equiv 10 (\mathrm{mod}\ 3)$ и т.н.

Основни свойства на числовите сравнения

Теорема 1. Релацията сравнимост притежава следните свойства:

(1) $a \equiv a (\mathrm{mod}\ m)$ (идентичност);

(2) ако $a \equiv b (\mathrm{mod}\ m)$, то $b \equiv a (\mathrm{mod}\ m)$ (симетричност);

(3) ако $a \equiv b (\mathrm{mod}\ m)$ и $b \equiv c (\mathrm{mod}\ m)$, то $a \equiv c (\mathrm{mod}\ m)$ (транзитивност);

(4) ако $a + b \equiv c (\mathrm{mod}\ m)$, то $a \equiv c - b (\mathrm{mod}\ m)$ (прехвърляне на събираемо от другата страна на сравнение);

(5) ако $a \equiv b (\mathrm{mod}\ m)$ и $c \equiv d (\mathrm{mod}\ m)$, то $a + c \equiv b + d (\mathrm{mod}\ m)$ (събиране на сравнения);

(6) ако $a_1 \equiv b_1 (\mathrm{mod}\ m)$, $a_2 \equiv b_2 (\mathrm{mod}\ m)$, $\ldots$, $a_k \equiv b_k (\mathrm{mod}\ m)$, то $a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k (\mathrm{mod}\ m)$ (умножаване на сравнения) и, в частност, ако $a \equiv b (\mathrm{mod}\ m)$, то $a^k \equiv b^k (\mathrm{mod}\ m)$ (степенуване на сравнения);

(7) ако $a \equiv b (\mathrm{mod}\ m)$ и $f(x)$ е полином с цели коефициенти, то $f(a) \equiv f(b) (\mathrm{mod}\ m)$ (обобщение на (5) и (6)).

Доказателство: (1) и (2) са очевидни.

(3) Тъй като m дели $a-b$ и $b-c$, то дели и тяхната сума $(a-b)+(b-c) = a-c$, т.е. $a \equiv c (\mathrm{mod}\ m)$.

(4) Следва от $(a + b) - c = a - (c - b)$.

(5) Тъй като m дели $a - b$ и $c - d$, то дели и тяхната сума $(a - b) + (c - d) = (a + c) - (b + d)$, т.е. $a + c \equiv b + d (\mathrm{mod}\ m)$. Това свойство лесно се обобщава за повече събираеми.

(6) От $a_i \equiv b_i (\mathrm{mod}\ m)$, $1 \leq i \leq k$, следва, че $a_i - b_i = mt_i$ за някои цели числа $t_1, t_2, \ldots, t_k$. Тогава

$$a_1 a_2 \ldots a_k = (b_1 + mt_1)(b + mt_2) \ldots (b + mt_k) = b_1 b_2 \ldots b_k + mt$$

за някое цяло число t. Това означава, че $a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k (\mathrm{mod}\ m)$. При $a_1 = a_2 = \cdots = a_k = a$ и $b_1 = b_2 = \cdots = b_k = b$ получаваме $a^k \equiv b^k (\mathrm{mod}\ m)$.

(7) Следва от многократно прилагане на (5) и (6).

Съкращаване на общ множител от двете страни на сравнение

Описаните в Теорема 1 свойства на сравненията са аналогични на съответните свойства на равенствата. Но при съкращаването на общ множител от двете страни има важна разлика.

Теорема 2. Ако $ak \equiv bk (\mathrm{mod}\ m)$, то $a \equiv b (\mathrm{mod}\ \frac{m}{(k,m)})$. В частност, при $(k, m) = 1$ имаме $a \equiv b (\mathrm{mod}\ m)$.

Доказателство: Нека $(k, m) = d$, $k = dk_1$ и $m = dm_1$. Тогава числото $m_1 = \frac{m}{d}$ дели разликата $a - b$, защото числото

$$\frac{ka - kb}{m} = \frac{k(a - b)}{m} = \frac{k_1(a - b)}{m_1}$$

е цяло и $(k_1, m_1) = 1$. Следователно $a \equiv b (\mathrm{mod}\ \frac{m}{(k,m)})$.

Теорема 3. Ако $a \equiv b (\mathrm{mod}\ m_1)$, $a \equiv b (\mathrm{mod}\ m_2)$, $\ldots$, $a \equiv b (\mathrm{mod}\ m_k)$, то $a \equiv b (\mathrm{mod}\ M)$, където

$$M = [m_1, m_2, \ldots, m_k].$$

Доказателство: Имаме $m_1 | a - b$, $m_2 | a - b$, $\ldots$, $m_k | a - b$, откъдето следва, че $M = [m_1, m_2, \ldots, m_k] | a - b$, т.е. $a \equiv b (\mathrm{mod}\ M)$.

Пълна система остатъци по даден модул

Дефиниция 2. Нека $a_1, a_2, \ldots, a_m$ и $m \geq 2$ са цели числа. Ще казваме, че $(a_1, a_2, \ldots, a_m)$ е пълна система остатъци по модул m, ако измежду остатъците, които дават съответно $a_1, a_2, \ldots, a_m$ при деление на m, се срещат всички възможни остатъци (т.е. числата $0, 1, \ldots, m - 1$).

Например самите остатъци $0, 1, \ldots, m-1$ образуват пълна система остатъци по модул m. В доказателството на Теорема 1 всеки стълб от числа, взаимно прости с n, образува пълна система остатъци по модул m.

Теорема 4. Нека $(a_1, a_2, \ldots, a_m)$ е пълна система остатъци по модул m и a е цяло число. Тогава:

а) $(a + a_1, a + a_2, \ldots, a + a_m)$ също е пълна система остатъци по модул m,

б) ако $(a, m) = 1$, то $(aa_1, aa_2, \ldots, aa_m)$ също е пълна система остатъци по модул m.

Доказателство: а) Да допуснем противното. Тогава $a + a_i \equiv a + a_j (\mathrm{mod}\ m)$ за някои i и j, $1 \leq i < j \leq m$, откъдето следва, че $a_i \equiv a_j (\mathrm{mod}\ m)$ – противоречие.

б) Да допуснем противното. Тогава $aa_i \equiv aa_j (\mathrm{mod}\ m)$ за някои i и j, $1 \leq i < j \leq m$, откъдето съгласно Теорема 2 следва, че $a_i \equiv a_j (\mathrm{mod}\ m)$ – противоречие.

Задачи

1. Да се докаже, че $a \equiv b (\mathrm{mod}\ m)$ тогава и само тогава, когато числата a и b дават един и същ остатък при деление на m.

2. Да се докаже, че ако $a \equiv b (\mathrm{mod}\ m)$, то $(a, m) = (b, m)$.

3. Да се докаже, че ако $ka \equiv kb (\mathrm{mod}\ m)$, то $a \equiv b (\mathrm{mod}\ \dfrac{m}{(k, m)})$.

Решение. Нека $(k, m) = d$, $k = dk_1$ и $m = dm_1$. Тогава $(k_1, m_1) = 1$ и числото $\dfrac{ka - kb}{m} = \dfrac{k_1(a - b)}{m_1}$ е цяло. Следователно m_1 дели $a - b$, т.е. $a \equiv b (\mathrm{mod}\ m_1)$.

4. Да се докаже, че:

а) $3^{2005} \equiv 3 (\mathrm{mod}\ 10)$; б) $7^{2006} \equiv 49 (\mathrm{mod}\ 100)$; в) $13^{682} \equiv 1 (\mathrm{mod}\ 7)$;
г) $2^{25} + 3^{26} \equiv 3 (\mathrm{mod}\ 11)$.

5. Да се намери последната цифра на числото:

а) $223^{12} - 44^{15}$; б) $9^{1003} - 7^{902} + 3^{801}$.

6. Да се намерят последните две цифри на числото:

а) 7^{129}; б) $29^{10} - 37^{10}$.

7. Да се намери остатъкът от делението на a на b, ако:

а) $a = 2^{128}$, $b = 31$; б) $a = (21^{108} - 113^6)^{22}$, $b = 11$.

в) $a = 73^8 + 72^7 + 71^6 + 70^5 + 69^4 + 68^3 + 67^2 + 66$, $b = 64$.

б) *Решение.* Търсеният остатък е единственото цяло число c, $0 \leq c \leq 10$, за което $(21^{108} - 113^6)^{22} \equiv c (\mathrm{mod}\ 11)$. Тъй като $21 \equiv -1 (\mathrm{mod}\ 11)$, получаваме $21^{108} \equiv (-1)^{108} \equiv 1 (\mathrm{mod}\ 11)$. Аналогично $113^6 \equiv 3^6 \equiv 3 (\mathrm{mod}\ 11)$ и следователно $(21^{108} - 113^6)^{22} \equiv (-2)^{22} \equiv 4.(2^5)^4 \equiv 4 (\mathrm{mod}\ 11)$.

8. Да се докаже, че $2^{2^5} + 1 \equiv 0 (\mathrm{mod}\ 641)$.

9. Да се докаже, че ако $a \equiv b (\mathrm{mod}\ m_1)$, $a \equiv b (\mathrm{mod}\ m_2)$ и $(m_1, m_2) = 1$, то $a \equiv b (\mathrm{mod}\ m_1 m_2)$.

10. Да се докаже, че $2^{15} - 1 \equiv 0 (\mathrm{mod}\ 11.31.61)$.

11. а) Да се докаже, че $5^{2^n} \equiv 1 (\mathrm{mod}\ 2^{n+2})$ за всяко естествено число n.

б) Да се докаже, че сравнението $5^{2^n} \equiv 1 (\mathrm{mod}\ 2^{n+3})$ не е изпълнено за никое естествено число n.

12. Да се докаже, че ако a и b са цели числа и p е просто число, то $(a + b)^p \equiv a^p + b^p (\mathrm{mod}\ p)$.

13. Да се докаже, че ако $a_1, a_2, \ldots, a_m$ са пълна система остатъци по модул m и $(k, m) = 1$, то числата $ka_1, ka_2, \ldots, ka_m$ също са пълна система остатъци по модул m.

14.* Ако p е просто, а n е естествено число, то $\binom{n}{p} \equiv \left[\dfrac{n}{p}\right] (\mathrm{mod}\ p)$.

Решение. Имаме $\binom{n}{p} = \dfrac{n(n-1)\ldots(n-p+1)}{p!}$. Множителите в числителя са p последователни естествени числа, измежду които точно едно се дели на p. Ако това число е a, то $\dfrac{n}{p} \geq \dfrac{a}{p} \geq$

$\frac{n-p+1}{p} > \frac{n}{p} - 1$, което означава, че $\left[\frac{n}{p}\right] = \frac{a}{p}$.

Числата $n, n-1, \ldots, n-p+1$ са пълна система остатъци по модул p и като махнем от тази система a, получаваме остатъците $1, 2, \ldots, p-1$. Следователно

$$n(n-1)\ldots(a+1)(a-1)\ldots(n-p+1) \equiv (p-1)!(\text{mod } p),$$

откъдето след умножаване на двете страни с $\frac{a}{p}$ получаваме

$$\frac{n(n-1)\ldots(n-p+1)}{p} \equiv \frac{a}{p}(p-1)!(\text{mod } p).$$

Тъй като $(p,(p-1)!) = 1$, можем да разделим двете страни на $(p-1)!$ и получаваме $\binom{n}{p} \equiv \frac{a}{p} \,(\text{mod } p)$, с което твърдението е доказано.

15.* Да се докаже, че съществуват безбройно много съставни числа от вида $(2^n+1)^2+4$.

7. Функция на Ойлер

Дефиниция 1. Нека $n > 1$ е естествено число. Да означим с $\varphi(n)$ броя на естествените числа, които са по-малки от n и са взаимно прости с n и нека $\varphi(1) = 1$. Функцията $\varphi(n) : \mathbf{N} \to \mathbf{N}$ се нарича *функция на Ойлер*.

Първите няколко стойности на функцията на Ойлер се намират директно. Имаме $\varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$ и т.н. Не е трудно да се съобрази, че ако p е просто число, то $\varphi(p) = p-1$ (всички естествени числа, по-малки от p, са взаимно прости с p).

Лема 1. Нека $(a,b) = 1$. Естественото число k е взаимно просто едновременно с a и b тогава и само тогава, когато $(k, ab) = 1$.

Доказателство: Нека $(k,a) = (k,b) = 1$ и да допуснем, че $(k,ab) > 1$. Тогава съществува просто число p, което дели k и ab. От последното обаче следва, че p дели поне едно от числата a и b, т.е. p дели (k,a) или (k,b) – противоречие.

Обратно, ако $(k,ab) = 1$, то от тъждеството на Безу $uk + vab = 1$ следва, че $(k,a) = (k,b) = 1$. Друго доказателство е аналогично на доказателството на необходимостта.

Лема 2. Нека a и m са цели числа и r е остатъкът при деление на a на m. Имаме $(a,m) = 1 \iff (m,r) = 1$.

Доказателство: Нека $a = mq + r$ съгласно теоремата за деление с частно и остатък. Ако $(a,m) = 1$ и допуснем, че $(m,r) = d > 1$, то d дели $mq + r = a$, което е невъзможно. Обратно, ако $(m,r) = 1$ и допуснем, че $(a,m) = d > 1$, то d дели $a - mq = r$ – противоречие.

Теорема 1. За всеки две взаимно прости естествени числа m и n е в сила равенството[2]

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Доказателство: Да запишем подред естествените числа $1, 2, \ldots, mn$ в правоъгълна таблица с m реда и n стълба:

$$\begin{array}{ccccccc} 1 & 2 & 3 & \ldots & n-1 & n \\ n+1 & n+2 & n+3 & \ldots & 2n-1 & 2n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \ldots & (m-1)n+n-1 & mn \end{array}$$

[2]Функции с това свойство се наричат мултипликативни.

Ще преброим по два начина числата в тази таблица, които са взаимно прости едновременно с m и n.

(Първи начин) Тъй като $(m,n) = 1$ съгласно Лема 1, едно число от таблицата е взаимно просто едновременно с m и n тогава и само тогава, когато е взаимно просто с произведението mn. Следователно разглеждания брой е $\varphi(mn)$.

(Втори начин) Ще преброим първо числата, които са взаимно прости с n и след това ще установим колко от тях са взаимно прости и с m.

В първия ред има точно $\varphi(n)$ числа, които са взаимно прости с n. Нещо повече, ако k е от първия ред и $(k,n) = 1$, то всички числа от стълба, определен от k, са взаимно прости с n (защото всяко число от този стълб има вида $qn + k$ и следователно всеки общ делител d на $qn + k$ и n дели разликата $(qn + k) - qn = k$). Получихме, че в таблицата има точно $\varphi(n)$ стълба, които се състоят от взаимно прости с n числа и това са всички взаимно прости с n числа в таблицата.

Числата от таблицата, които са взаимно прости едновременно с m и n, се намират в стълбовете ($\varphi(n)$ на брой), описани по-горе. Да разгледаме един такъв стълб

$$k, n + k, 2n + k, \ldots, (m-1)n + k.$$

Всеки две от тези числа дават различни остатъци при деление на m. Действително, ако допуснем, че $an+k$ и $bn+k$ дават един и същи остатък при деление на m, то m дели разликата $(an+k)-(bn+k) = (a-b)n$, откъдето m дели $a - b$, което е невъзможно.

Следователно $(k, n + k, 2n + k, \ldots, (m-1)n + k)$ е пълна система остатъци по модул m. Тогава (съгласно Лема 2) в този стълб има точно $\varphi(m)$ числа, които са взаимно прости с m (тези, чиито остатъци са взаимно прости с m).

От тези разсъждения следва, че числата от таблицата, които са взаимно прости едновременно с m и n, са $\varphi(m)\varphi(n)$ на брой (по $\varphi(m)$ от всеки от разглежданите $\varphi(n)$ стълба).

От направените две преброявания на едно и също число следва, че

$$\varphi(mn) = \varphi(m)\varphi(n),$$

с което теоремата е доказана.

Лема 3. Ако p е просто число и k е естествено число, то

$$\varphi(p^k) = p^{k-1}(p-1).$$

Доказателство: Числата, които са по-малки от p^k и не са взаимно прости с p^k, са точно тези, които се делят на p. Това са

$$p, 2p, 3p, \ldots, p^k - p = p(p^{k-1} - 1)$$

и техният брой е $p^{k-1} - 1$. Следователно

$$\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Теорема 2. Ако $n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ е каноничното разлагане на n, то

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \ldots p_s^{k_s-1}(p_1-1)(p_2-1)\ldots(p_s-1).$$

Доказателство: Следва от Теорема 1 и Лема 3.

След умножаване и разделяне на дясната страна на $p_1 p_2 \ldots p_s$ формулата от Теорема 2 се записва и във вида

$$\varphi(n) = n\frac{(p_1-1)(p_2-1)\ldots(p_s-1)}{p_1 p_2 \ldots p_s} = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right).$$

От формулата от Теорема 2 следва, че при $n > 2$ числото $\varphi(n)$ винаги е четно.

Задачи

Задача 1. Да се намери:
а) $\varphi(10)$; б) $\varphi(100)$; в) $\varphi(432)$; г) $\varphi(1001)$; д) $\varphi(2^n)$, $n \geq 2$.
Задача 2. а) Да се докаже, че $\varphi(2m) = \varphi(m)$ или $2\varphi(m)$.
б) Да се докаже, че $\varphi(m^k) = m^{k-1}\varphi(m)$
в) Да се намери естественото числа x, ако $\varphi(5^x) = 100$.
Задача 3. Да се намери $m = 3^\alpha 5^\beta 7^\gamma$, ако $\varphi(m) = 3600$.
Задача 4. Да се намери $m = p_1 p_2$, където p_1 и p_2 са прости числа, $p_1 - p_2 = 2$ и $\varphi(m) = 120$.

8. Теорема на Ойлер

Редуцирана система остатъци по даден модул

Въвеждането на функцията на Ойлер ни позволява да разгледаме и понятието редуцирана система остатъци, което е аналог на пълната система остатъци.

Дефиниция 1. Нека $a_1, a_2, \ldots, a_{\varphi(m)}$ и $m \geq 2$ са цели числа. Ще казваме, че $(a_1, a_2, \ldots, a_{\varphi(m)})$ е редуцирана система остатъци по модул m, ако измежду остатъците, които дават съответно $a_1, a_2, \ldots, a_{\varphi(m)}$ при деление на m, се срещат всички възможни остатъци, които са взаимнопрости с m.

Например системата от всички остатъци, които са взаимнопрости с модула, е редуцирана система остатъци. Когато m е просто число, редуцираната и пълната система остатъци съвпадат.

Теорема 1. Нека $(a_1, a_2, \ldots, a_{\varphi(m)})$ е редуцирана система остатъци по модул m и a е цяло число, като $(a, m) = 1$. Тогава $(aa_1, aa_2, \ldots, aa_{\varphi(m)})$ също е пълна система остатъци по модул m.

Доказателство: Да допуснем противното. Тогава $aa_i \equiv aa_j (\text{mod } m)$ за някои i и j, $1 \leq i < j \leq \varphi(m)$, откъдето съгласно Теорема 2 от Въпрос 7 следва, че $a_i \equiv a_j (\text{mod } m)$ – противоречие.

Теорема на Ойлер

Теорема 2. (Теорема на Ойлер) Ако a е цяло число и n е естествено число, като $(a, n) = 1$, то

$$a^{\varphi(n)} \equiv 1 (\text{mod } n).$$

Доказателство: Твърдението е вярно при $n = 1$. Нека $n > 1$ и $(a_1, a_2, \ldots, a_{\varphi(n)})$ е редуцирана система остатъци по модул n. Тогава от Теорема 1 следва, че $(aa_1, aa_2, \ldots, aa_{\varphi(n)})$ също е пълна система остатъци по модул m.

От горното следва, че са в сила сравненията

$$\begin{aligned} aa_1 &\equiv a_{i_1} (\text{mod n}) \\ aa_2 &\equiv a_{i_2} (\text{mod n}) \\ &\vdots \\ aa_{\varphi(n)} &\equiv a_{i_{\varphi(n)}} (\text{mod n}), \end{aligned}$$

където $(i_1, i_2, \ldots, i_{\varphi(n)})$ е пермутация на числата $(1, 2, \ldots, \varphi(n))$. Умножаваме почленно тези сравнения и съкращаваме (използвайки Теорема 2 от Въпрос 7) на произведението $a_1 a_2 \ldots a_{\varphi(n)}$. Получаваме $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, с което твърдението е доказано.

Задачи

Задача 1. (контролно за МОМ, Румъния) Нека $a > 1$ е естествено число. Да се докаже, че множеството $\{a^2 + a - 1, a^3 + a^2 - 1, \ldots, a^{n+1} + a^n - 1, \ldots\}$ съдържа безбройно много две по две взаимно прости числа.

Решение. Лесно се вижда, че всеки две съседни числа от разглежданото множество са взаимно прости (ако имат общ прост делител, той дели $a - 1$, оттам дели a – противоречие). Нека $a^{n_1+1} + a^{n_1} - 1, a^{n_2+1} + a^{n_2} - 1, \ldots, a^{n_k+1} + a^{n_k} - 1$ са k, $k \geq 2$ числа от дадените, всеки две от които са взаимно прости. Ще покажем, към тях може да се добави още едно от дадените, което е взаимно просто с всяко от тях.

Нека $N = \prod_{i=1}^{k}(a^{n_i+1} + a^{n_i} - 1)$. Тогава $(a, N) = 1$ и следователно $a^{\varphi(N)} \equiv 1 \pmod N$. Тогава $(N, a^{\varphi(N)+1} + a^{\varphi(N)} - 1) = 1$, защото в противен случай N и $a^{\varphi(N)+1}$ ще имат общ делител. Но това означава, че $a^{\varphi(N)+1} + a^{\varphi(N)} - 1$ е взаимно просто с всяко от числата $a^{n_1+1} + a^{n_1} - 1, a^{n_2+1} + a^{n_2} - 1, \ldots, a^{n_k+1} + a^{n_k} - 1$.

9. Теорема на Ферма

Ще докажем две помощни твърдения.

Лема 1. Ако p е просто число и k е естествено число, като $1 \leq k \leq p - 1$, то

$$\binom{p}{k} \equiv 0 (\mathrm{mod}\ p).$$

Доказателство: Следва от формулата $\binom{p}{k} = \dfrac{p(p-1)\ldots(p-k+1)}{k!}$ и $(p, k!) = 1$.

Лема 2. Ако p е просто число и $x_1, x_2, \ldots, x_n$ са цели числа, то

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p (\mathrm{mod}\ p).$$

Доказателство: При $n = 2$ имаме

$$\begin{aligned}(x_1 + x_2)^p &\equiv x_1^p + \binom{p}{1} x_1^{p-1} x_2 + \cdots + \binom{p}{1} x_1 x_2^{p-1} + x_2^p (\mathrm{mod}\ p) \equiv \\ &\equiv x_1^p + x_2^p (\mathrm{mod}\ p)\end{aligned}$$

поради Лема 1.

Нека $n > 2$ и твърдението е вярно за $n - 1$ числа. Тогава

$$\begin{aligned}(x_1 + x_2 + \cdots + x_n)^p &\equiv (x_1 + x_2 + \cdots + x_{n-1})^p + x_n^p (\mathrm{mod}\ p) \equiv \\ &\equiv x_1^p + x_2^p + \cdots + x_n^p (\mathrm{mod}\ p)\end{aligned}$$

с последователно прилагане на доказаното за $n = 2$ и индукционното предположение.

Теорема 1. (Теорема на Ферма) Ако a е цяло число и p е просто число, то

$$a^p \equiv a (\mathrm{mod}\ p).$$

Еквивалентно, ако a е цяло число и p е просто число, което не дели a, то

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

Доказателство: При $p = 2$ имаме

$$a^2 \equiv a (\mathrm{mod}\ 2) \iff a(a-1) \equiv 0 (\mathrm{mod}\ 2)$$

и последното очевидно е вярно (произведението на две последователни цели числа винаги е четно число).

Нека $p > 2$, т.е. p е нечетно просто число. Твърдението е тривиално за $a = 0$. Ако $a > 0$, прилагаме Лема 2 за $n = a$ и $x_1 = x_2 = \cdots = x_a = 1$ и получаваме

$$a^p = (1 + 1 + \cdots + 1)^p \equiv 1^p + 1^p + \cdots + 1^p = p \equiv 0 (\mathrm{mod}\ p)$$

(в сумите има по a събираеми).

При $a < 0$ имаме $(-a)^p \equiv -a (\mathrm{mod}\ p)$ защото $-a$ е положително. Тъй като p е нечетно, $(-a)^p = -a^p$, т.е.

$$-a^p \equiv -a (\mathrm{mod}\ p) \iff a^p \equiv a (\mathrm{mod}\ p).$$

При $(a, p) = 1$ можем да съкратим на a без да променяме модула – получаваме $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Обратно, ако последното сравнение е вярно, можем да го умножим с $a \equiv a (\mathrm{mod}\ p)$ и да получим $a^p \equiv a (\mathrm{mod}\ p)$.

Теоремата на Ферма показва, че условието $a^p \equiv a (\mathrm{mod}\ p)$ е необходимо, за да бъде числото p просто. Това условие обаче не е достатъчно, т.е. съществуват съставни числа n, за които $a^n \equiv a (\mathrm{mod}\ n)$. Едно такова число е $n = 341 = 11.31$.

Както ще видим по-нататък на лекции и упражнения, теоремата на Ферма има многобройни приложения. Тя обаче е частен случай от теоремата на Ойлер.

Задачи

Задача 1. Да се докаже, че ако $(a, 7) = 1$, то $7 | a^{12} - 1$.

Задача 2. Да се докаже, че ако $(a, 65) = (b, 65) = 1$, то $65 | a^{12} - b^{12}$.

Задача 3. Да се докаже, че $a^{13} \equiv a (\mathrm{mod}\ 2730)$.

Задача 4. Да се докаже, че $2^{11.31} \equiv 2 (\mathrm{mod}\ 11.31)$.

Задача 5. Да се намерят последните две чифри на числото:

а) 3^{4012}; б) 39^{247}.

Задача 6. Да се докаже, че ако $(a, m) = 1$, то сравнението $ax \equiv b (\mathrm{mod}\ m)$ има единствено решение $x = ba^{\varphi(m)-1}$.

Задача 7. Да се намери x, ако $x^{100} \equiv 2 (\mathrm{mod}\ 73)$ и $x^{101} \equiv 69 (\mathrm{mod}\ 73)$.

Задача 8. Нека p е просто число от вида $4k - 1$, което дели $x^2 + y^2$, където x и y са естествени числа. Да се докаже, че p дели x и y.

Задача 9. Да се докаже, че всички прости делители на $x^2 + 1$, където x е естествено число, са от вида $4k + 1$.

Задача 10. (МОМ2005) Нека $a_n = 2^n + 3^n + 6^n - 1$, $(n = 1, 2, \ldots)$. Да се намерят всички естествени числа, които са взаимно прости с всеки от членовете на редицата $a_1, a_2, \ldots$.

Задача 11. (Олимпиада в Унгария, 1995) Във върховете на квадрат са записани четири естествени числа. Разрешено е, за някое просто число p, числата в даден връх да се заменят с остатъка по модул p на произведението на числата от някои два други върха. Да се докаже, че за произволно p е възможно да достигнем до равни числа във всички върхове.

Задача 12. Да се докаже, че ако a и b са цели числа и $2a^3 - 3a^2b + 2b^3$ се дели на 5, то a и b се делят на 5.

Задача 13. Да се докаже, че ако $p > 3$ е просто число, то $3^p - 2^p - 1$ се дели на $42p$.

Задача 14. (БОМ 2004) Да се реши в прости числа уравнението $x^y - y^x = xy^2 - 19$.

Задача 15. (ПМТ Ямбол, 2004) Да се намерят всички нечетни прости числа p, за които числото $1^{p-1} + 2^{p-1} + \cdots + 2004^{p-1}$ се дели на p.

10. Група на класовете остатъци, взаимно прости с модула

Нека $m > 1$ е естествено число. Тъй като сравнимостта по модул m е релация на еквивалентност, всички цели числа се разделят в непресичащи се класове от остатъци по модул m. Всеки клас се описва равноправно от всеки свой представител. Затова ще записваме класовете с $\overline{a}$ – това е класът от цели числа, които при деление на m дават остатък, същия като остатъка, който дава a, т.е. $k \in \overline{a}$ означава, че k и a дават един и същи остатък при деление на m и, в частност, $a \in \overline{k}$.

Както знаем, точно $\varphi(m)$ от остатъците са взаимно прости с m. Следователно (вж. Лема 2 от Въпрос 5) точно $\varphi(m)$ от класовете остатъци по модул m се състоят от взаимно прости с m числа, а останалите класове (които засега няма да разглеждаме) се състоят от числа, които не са взаимно прости с m.

Дефиниция 1. Нека $\overline{r_1}, \overline{r_2}, \ldots, \overline{r_{\varphi(m)}}$ са класовете от числа, взаимно прости с m. Дефинираме умножение на класове по правилото

$$\overline{r_i}\ \overline{r_j} = \overline{r_i r_j}.$$

Теорема 1. Множеството $M = \{\overline{r_1}, \overline{r_2}, \ldots, \overline{r_{\varphi(m)}}\}$ е абелева група относно умножението на класове.

Доказателство: Произведението $\overline{r_i}\ \overline{r_j} = \overline{r_i r_j}$ е клас от остатъци, взаимно прости с m, защото от $(r_i, m) = (r_j, m) = 1$ следва $(r_i r_j, m) = 1$ (вж. Лема 1 от Въпрос 5). Следователно M е затворено относно умножението.

В сила е асоциативния закон

$$(\overline{r_i}\ \overline{r_j})\,\overline{r_k} = \overline{r_i r_j}\ \overline{r_k} = \overline{r_i r_j r_k} = \overline{r_i}\ \overline{r_j r_k} = \overline{r_i}(\overline{r_j}\ \overline{r_k})\,.$$

Единичен елемент е класът $\overline{1}$, а обратен на $\overline{r}$ е класът $\overline{r^{\varphi(m)-1}}$. Действително,

$$\overline{r}\,\overline{1} = \overline{r.1} = \overline{r}$$

за всяко r и

$$\overline{r}\,\overline{r^{\varphi(m)-1}} = \overline{r^{\varphi(m)}} = \overline{1}$$

съгласно Теоремата на Ойлер.

Следователно M е група. Нещо повече, тази група е абелева, защото

$$\overline{r_i}\ \overline{r_j} = \overline{r_i r_j} = \overline{r_j r_i} = \overline{r_j}\ \overline{r_i}$$

за произволни $r_i, r_j \in M$.

Да напомним, че от теоремата на Лагранж следва, че за крайна група G от ред n за всеки елемент $g \in G$ е в сила равенството $g^n = 1$. За групата M това означава, че $\overline{r}^{\varphi(m)} = \overline{1}$, което е всъщност Теоремата на Ойлер (т.е. Теоремата на Ойлер е следствие от Теоремата на Лагранж).

11. Показател на число по даден модул

Една от най-важните стъпки в изучаването на структурата на групата M от предишния въпрос е разглеждането на понятието показател.

Дефиниция 1. Нека $(a, m) = 1$, $m \geq 2$ е естествено число. Най-малкото естествено число (степенен показател) k, за което $a^k \equiv 1 (\mathrm{mod}\ m)$ се нарича *показател на a по модул m*. Ако k е показателят на a по модул m, ще казваме, че *a принадлежи на показател k по модул m* и ще записваме

$$a \in k \bmod m.$$

Например 2 е показател на 2 по модул 3 (Проверете!), 3 е показател на 2 по модул 7 (Проверете!), 6 е показател на 3 по модул 7 (Проверете!) и т.н. (съответно $2 \in 2 \bmod 2$, $2 \in 3 \bmod 7$ и $3 \in 6 \bmod 7$). Разгледайте други примери.

От Теоремата на Ойлер следва, че показателят винаги съществува (защото $\varphi(m)$ и всички негови кратни естествени числа са степенни показатели, за които съответната степен на a е сравнима с 1 по модул m). Тъй като всяко множество от естествени числа има най-малък елемент, Дефиниция 1 е коректна и показателят никога не е по-голям от $\varphi(m)$.

Теорема 1. (Основно свойство на показателя) Ако $(a, m) = 1$ и k е показателят на a по модул m, то

$$a^n \equiv 1(\text{mod } m) \iff k \text{ дели } n.$$

Доказателство: Ако $k|n$, т.е. $n = ks$ за някое цяло s, то

$$a^n = a^{ks} = \left(a^k\right)^s \equiv 1^s(\text{mod } m).$$

Обратно, ако n е такова, че $a^n \equiv 1(\text{mod } m)$, да разделим n на k с частно и остатък, $n = kq + r$, където $0 \leq r < k$. Ако $r = 0$, няма какво да доказваме и затова да допуснем, че $0 < r < k$. Тогава

$$a^n = a^{kq+r} = \left(a^k\right)^q a^r \equiv a^r(\text{mod } m),$$

т.е. $a^r \equiv 1(\text{mod } m)$, което противоречи на Дефиниция 1.

Следствие 1. Ако $(a, m) = 1$ и $a \in k \bmod m$, то k дели $\varphi(m)$.

Доказателство: Следва от Теоремата на Ойлер и Теорема 1.

Следствие 1 показва, че показателят трябва да се търси измежду делителите на $\varphi(m)$. Следователно можем да намираме показател на дадено число по даден модул по следния алгоритъм.

1. Дадени са взаимно прости естествени числа a и m и търсим показателя на a по модул m. Намираме $\varphi(m)$.

2. Намираме всички естествени делители на $\varphi(m)$.

3. Последователно (в нарастващ ред) проверяваме дали $a^d \equiv 1(\bmod m)$ за делителите от стъпка 2. Първият делител, за който това сравнение е изпълнено, е търсения показател.

В следващите два въпроса ще разгледаме специалния случай, когато показателят е точно равен на $\varphi(m)$. А сега ще продължим с изучаването на общите свойства на показателя.

Теорема 2. Ако $(a, m) = 1$ и $a \in k \bmod m$, то за произволно естествено число s имаме

$$a^s \in \frac{k}{(k, s)} \bmod m.$$

Доказателство: Нека $(k, s) = d$, $k = dk_1$ и $s = ds_1$, където $(k_1, s_1) = 1$. Трябва да докажем, че $a^s \in k_1 \bmod m$.

Нека $a^s \in t \bmod m$. Ще докажем, че $t = k_1$.

Тъй като $(a^s)^{k_1} = a^{s_1 dk_1} = a^{s_1 k} \equiv 1(\text{mod } m)$, то от Теорема 1 следва, че $t|k_1$, т.е. $t \leq k_1$. От друга страна, от $a^{st} \equiv 1(\text{mod } m)$ и отново от Теорема 1 следва, че k дели st. Тъй като $k = dk_1$ и $s = ds_1$, заключаваме, че k_1 дели $s_1 t$, откъдето $k_1|t$, т.е. $k_1 \leq t$. Следователно $k_1 = t$, с което твърдението е доказано.

Теорема 3. Ако $(a, m) = (b, m) = 1$, $a \in k \bmod m$, $b \in q \bmod m$ и $(k, q) = 1$, то $ab \in kq \bmod m$.

Доказателство: Нека $ab \in r \bmod m$. Трябва да докажем, че $r = kq$. От $(ab)^r \equiv 1(\text{mod } m)$ след повдигане на степен q получаваме $a^{qr} b^{qr} \equiv 1(\text{mod } m)$, откъдето $a^{qr} \equiv 1(\text{mod } m)$ (защото $b^{qr} = (b^q)^r \equiv 1^r = 1(\text{mod } m)$.

Тогава k дели qr и значи k дели r (защото $(k, q) = 1$ по условие). Аналогично се вижда, че q дели r. Тъй като $(k, q) = 1$, заключаваме, че kq дели r.

От друга страна, $(ab)^{kq} = (a^k)^q(b^q)^k \equiv 1^q 1^r = 1 (\mathrm{mod}\ m)$, т.е. r дели kq. Следователно $r = kq$, с което твърдението е доказано.

Задачи

Задача 1. Да се намери показателят на a по модул m за:

а) $a = 2$, $m = 11, 13, 17, 25, 37, 67, 89, 109, 169$;

б) $a = 3$, $m = 11, 19, 29, 37, 73, 109, 257$;

в) $a = 5$, $m = 7, 11, 23, 43, 73$;

г) $a = 7$, $m = 19, 31, 47$;

д) $a = 8$, $m = 11, 17, 29, 61, 83, 169$;

е) $a = 11$, $m = 23$.

Задача 2. Да се намерят всички естествени числа n, за които числото $\frac{3^{n+1}-2^{n+1}}{n+1}$ е цяло.

Решение: Ако p е най-малкият прост делител на $n+1$, то $p \geq 5$ (ясно е, че $n+1$ е взаимно просто с 6). Освен това $(n+1, p-1) = 1$.

Нека a е такова, че $2a \equiv 1 (\mathrm{mod}\ p)$. Тогава от $3^{n+1} \equiv 2^{n+1} (\mathrm{mod}\ p)$ следва $(3a)^{n+1} \equiv 1 (\mathrm{mod}\ p)$. Ако k е показателя на $3a$ по модул p, то k дели $p-1$ и $n+1$, което означава, че $k = 1$. Това вече лесно води до противоречие.

3. Да се реши в естествени числа уравнението $1 + 3^a = 2^b + 2^{2c-1}3^d$.

Решение: Ако $\min(b, 2c-1) \geq 3$, то $1 + 3^a$ се дели на 8, което е невъзможно. Следователно $\min(b, 2c-1) \leq 2$. От $2^b \equiv 1 \pmod 3$ се вижда, че b е четно. Да допуснем, че $b = 2$. Тогава $3^a = 3+2^{2c-1}3^d$, откъдето $d = 1$ и $3^{a-1} = 1+2^{2c-1}$. При $c \leq 2$ получаваме решенията $(a, b, c, d) = (2, 2, 1, 1)$ и $(3, 2, 2, 1)$. Ако $c \geq 3$, то $3^{a-1} \equiv 1 \pmod{16}$ и следователно $a-1$ се дели на 4, т.е. $a = 4a_1 + 1$. Но тогава $3^{a-1} = 3^{4a_1} = 81^{a_1} \equiv 1 \pmod 5$ и $2^c \equiv 0 \pmod 5$ – противоречие.

Нека сега $b \geq 4$ и $2c - 1 = 1$, т.е. $c = 1$ и $1 + 3^a = 2^b + 2.3^d$. Очевидно a е четно. Нека $a = 2a_1$ и $b = 2b_1$. Ако $d = 1$, получаваме уравнението $3^{2a_1} - 2^{2b_1} = (3^{a_1} - 2^{b_1})(3^{a_1} + 2^{b_1}) = 5$ с единствено решение $a_1 = b_1 = 1$, т.е. $b = 2$ – противоречие. Аналогично при $d = 2$ получаваме уравнението $3^{2a_1} - 2^{2b_1} = 17$ с единствено решение $a_1 = 2$, $b_1 = 3$, откъдето намираме решението $(a, b, c, d) = (4, 6, 1, 2)$. Ако $d \geq 3$, то $2^b \equiv 1 \pmod{27}$ и следователно b се дели на 18, $b = 18b_1$ и $2^b = (2^{18})^{b_1} \equiv 1 \pmod{73}$, откъдето $3^{a-d} \equiv 2 \pmod{73}$, което е невъзможно.

12. Примитивни корени

Примитивни корени по прост модул

Дефиниция 1. Ако $(a, m) = 1$ и $a \in \varphi(m) \bmod m$, ще наричаме a примитивен корен по модул m.

Тъй като $\varphi(m)$ е реда на групата M от Въпрос 8, всеки примитивен корен по модул m определя клас, който поражда M и обратно, всеки пораждащ елемент на M е клас от примитивни корени.

За примерите от Въпрос 11 виждаме, че 2 е примитивен корен по модул 3, 2 не е примитивен корен по модул 7 и 3 е примитивен корен по модул 7. За един по-сложен пример проверете, че 2 е примитивен корен по модул 53 (тъй като $\varphi(53) = 52 = 2^2.13$, трябва да се докаже, че $1, 2, 4, 13$ и 26 не са показатели на 2 по модул 53).

От друга страна, примитивни корени по модул 8 не съществуват. Действително, за всички "кандидати" 1, 3, 5 и 7 имаме $1^2 \equiv 3^2 \equiv 5^3 \equiv 7^2 \equiv 1 (\mathrm{mod}\ 8)$, докато $\varphi(8) = 4$. В този и следващия въпроси ще определим стойностите на m, за които съществуват примитивни корени по модул m.

Теорема 1. За всяко просто число p съществуват примитивни корени по модул p.

Доказателство: Нека $k_1, k_2, \ldots, k_m$ са всичките възможни (два по два) различни показатели на числата $1, 2, \ldots, p-1$ по модул p, като $\ell_j \in k_j \bmod p$. Полагаме $n = [k_1, k_2, \ldots, k_m]$ и нека $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$ е каноничното разлагане на n.

Да отбележим, че $b^n \equiv 1 (\mathrm{mod}\ p)$ за всяко $b \in \{1, 2, \ldots, p-1\}$ (защото всяко такова b има за показател едно от числата $k_1, k_2, \ldots, k_m$, а n е кратно на всички тези числа и можем да прилагаме Теорема 1 от предишния въпрос).

Всяко от числата $k_1, k_2, \ldots, k_m$ се дели на съответен множител $q_i^{\alpha_i}$, $1 \leq i \leq s$, съгласно свойствата на най-малкото общо кратно. Следователно за всяко $j = 1, 2, \ldots, m$ можем да запишем

$$k_j = a_{ij} q_i^{\alpha_i},$$

където a_{ij} са естествени числа (делители на съответното k_j).

Съгласно Теорема 1 от Въпрос 11, за всяко $j = 1, 2, \ldots, m$ показателят на числото $t_j = \ell_j^{a_{ij}}$, $j = 1, 2, \ldots, m$, е равен на $\dfrac{k_j}{a_{ij}} = q_j^{\alpha_j}$. Тогава от обобщението на Лема 3 от Въпрос 9 следва, че показателят на произведението $t_1 t_2 \ldots t_m$ е равен на $q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s} = n$.

Ще докажем, че $n = p - 1$, т.е. $t_1 t_2 \ldots t_m$ е примитивен корен по модул p. Да допуснем, че $n < p - 1$. Тогава $n + 1 \leq p - 1$ и следователно съществуват $n + 1$ различни цели числа $b_1, b_2, \ldots, b_n, b_{n+1}$ измежду $1, 2, \ldots, p - 1$ (можем да вземем например $b_1 = 1, b_2 = 2, \ldots, b_{n+1} = n + 1 \leq p - 1$).

Да разгледаме полинома

$$\begin{aligned} f(x) = x^n - 1 = &(x - b_1)(x - b_2) \ldots (x - b_n) + \alpha(x - b_1)(x - b_2) \ldots (x - b_{n-1}) \\ &+ \beta(x - b_1)(x - b_2) \ldots (x - b_{n-2}) + \cdots + \gamma(x - b_1) + \delta, \end{aligned}$$

където целите числа $\alpha, \beta, \ldots, \gamma, \delta$ се определят последователно едно от друго така, че горното равенство да е тъждество.

Полагайки последователно $x = b_1, b_2, \ldots, b_n$ получаваме, че всички коефициенти $\alpha, \beta, \ldots, \gamma, \delta$ се делят на p. Тогава

$$f(b_{n+1}) \equiv (b_{n+1} - b_1)(b_{n+1} - b_2) \ldots (b_{n+1} - b_n) \ (\mathrm{mod}\ p).$$

От друга страна, $f(b_{n+1}) = b_{n+1}^n - 1$ се дели на p съгласно забележката в началото на доказателството. Оттук заключаваме, че произведението $(b_{n+1} - b_1)(b_{n+1} - b_2) \ldots (b_{n+1} - b_n)$ се дели на p. Тъй като p е просто, то дели някой от множителите $b_{n+1} - b_i$, което е невъзможно, защото b_{n+1} и b_i са различни числа от множеството $\{1, 2, \ldots, p - 1\}$.

Теорема 2. Примитивни корени по модул 2^m съществуват тогава и само тогава, когато $m = 1$ или 2.

Доказателство: Ще докажем по индукция, че ако a е нечетно и $m > 2$, то $a^{2^{m-2}} \equiv 1 (\mathrm{mod}\ 2^m)$, което ще означава, че a не е примитивен корен по модул 2^m (да отбележим, че $\varphi(2^m) = 2^{m-1}$).

При $m = 3$ имаме $a^2 \equiv 1 (\mathrm{mod}\ 8)$, което е вярно. Нека $a^{2^{m-2}} \equiv 1 (\mathrm{mod}\ 2^m)$ за някое $m \geq 3$ и да разгледаме разликата

$$a^{2^{m-1}} - 1 = \left(a^{2^{m-2}}\right)^2 - 1 = \left(a^{2^{m-2}} - 1\right)\left(a^{2^{m-2}} + 1\right).$$

Числото $a^{2^{m-2}} + 1$ е четно, а по индукционно предположение $a^{2^{m-2}} - 1$ се дели на 2^m. Следователно тяхното произведение $a^{2^{m-1}} - 1$ се дели на 2^{m+1}, т.е. $a^{2^{m-1}} \equiv 1 (\mathrm{mod}\ 2^{m+1})$, с което теоремата е доказана.

Теорема 2. Ако p е нечетно просто число и m е естествено число, то:

а) съществуват примитивни корени по модул p^m;

б) съществуват примитивни корени по модул $2p^m$.

Теорема 3. Примитивни корени по модул n съществуват тогава и само тогава, когато $n = 2, 4, p^m$ или $2p^m$, където p е нечетно просто число.

Доказателство: Достатъчността (т.е. съществуването на примитивни корени в посочените случаи) следва от Теореми 1 и 2. Несъществуването на примитивни корени по модул 2^m при $m \geq 3$ беше доказано в Теорема 1. Остава да докажем, че ако n не е от вида 2^m ($m = 1, 2$), p^m и $2p^m$, то не съществуват примитивни корени по модул n.

Трябва да докажем, че ако $(a, n) = 1$, то a не е примитивен корен по модул n. От вида на n следва, че n може да се представи във вида $n = n_1 n_2$, където $n_1 > 2$, $n_2 > 2$ и $(n_1, n_2) = 1$. Тогава $(a, n_1) = (a, n_2) = 1$ и следователно $a^{\varphi(n_1)} \equiv 1 (\mathrm{mod}\ n_1)$ и $a^{\varphi(n_2)} \equiv 1 (\mathrm{mod}\ n_2)$ съгласно Теоремата на Ойлер.

Ако $k = [\varphi(n_1), \varphi(n_2)]$, то $a^k \equiv 1 (\mathrm{mod}\ n_1)$ и $a^k \equiv 1 (\mathrm{mod}\ n_2)$, откъдето $a^k \equiv 1 (\mathrm{mod}\ n)$. Остава да докажем, че $k < \varphi(n)$.

Числата $\varphi(n_1)$ и $\varphi(n_2)$ са четни и следователно не са взаимно прости. Тогава

$$k = [\varphi(n_1), \varphi(n_2)] < \varphi(n_1)\varphi(n_2) = \varphi(n_1 n_2) = \varphi(n)$$

(използвахме мултипликативността на функцията на Ойлер), с което доказателството е завършено.

Примитивни корени по съставен модул

В предишния въпрос отбелязахме, че примитивни корени по модул 8 не съществуват. Лесно се вижда, че 3 е примитивен корен по модул 4. Следователно при съставен модул са възможни и двете ситуации – да има и да няма примитивни корени (т.е. групата M може да е циклична или да не е циклична).

Да разгледаме първо случая на модул 2^m.

Теорема 1. Примитивни корени по модул 2^m съществуват тогава и само тогава, когато $m = 1$ или 2.

Доказателство: Ще докажем по индукция, че ако a е нечетно и $m > 2$, то $a^{2^{m-2}} \equiv 1 (\mathrm{mod}\ 2^m)$, което ще означава, че a не е примитивен корен по модул 2^m (да отбележим, че $\varphi(2^m) = 2^{m-1}$).

При $m = 3$ имаме $a^2 \equiv 1 (\mathrm{mod}\ 8)$, което е вярно. Нека $a^{2^{m-2}} \equiv 1 (\mathrm{mod}\ 2^m)$ за някое $m \geq 3$ и да разгледаме разликата

$$a^{2^{m-1}} - 1 = \left(a^{2^{m-2}}\right)^2 - 1 = \left(a^{2^{m-2}} - 1\right)\left(a^{2^{m-2}} + 1\right).$$

Числото $a^{2^{m-2}} + 1$ е четно, а по индукционно предположение $a^{2^{m-2}} - 1$ се дели на 2^m. Следователно тяхното произведение $a^{2^{m-1}} - 1$ се дели на 2^{m+1}, т.е. $a^{2^{m-1}} \equiv 1 (\mathrm{mod}\ 2^{m+1})$, с което теоремата е доказана.

Лема 1. Ако p е нечетно просто число и a е примитивен корен по модул p, то $a + p$ също е примитивен корен по модул p.

Доказателство: Очевидно – за всяко k имаме

$$a^k \equiv (a + p)^k (\mathrm{mod}\ p).$$

Лема 2. Ако p е нечетно просто число и a е примитивен корен по модул p, то поне едно от числата a^{p-1} и $(a + p)^{p-1}$ не е сравнимо с 1 по модул p^2.

Доказателство: Ако допуснем противното, получаваме, че p^2 дели разликата

$$(a + p)^{p-1} - a^{p-1} = (p - 1)pa^{p-2} + \binom{p-1}{2} p^2 a^{p-3} + \cdots + p^{p-1},$$

т.е. p дели $(p - 1)a^{p-2}$, което е невъзможно.

Теорема 2. Ако p е нечетно просто число и m е естествено число, то:

а) съществуват примитивни корени по модул p^m;

б) съществуват примитивни корени по модул $2p^m$.

Доказателство: а) От Леми 1 и 2 следва, че съществува примитивен корен a по модул p, за който $a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$. Действително, ако a не е такъв, то $a + p$ е такъв и при необходимост преименуваме $a + p$ на a.

Тогава $a^{p-1} = 1 + tp$, където t е цяло число и $(t, p) = 1$. Ще докажем, че a е примитивен корен по модул p^m за всяко $m \geq 1$.

Както в Теорема 1 по индукция се доказва, че

$$a^{p^i} = (1+tp)^{p^i} \equiv 1 + tp^{i+1} (\mathrm{mod}\ p^{i+2}),$$

където $(t,p) = 1$ (числото t е същото, както по-горе!) за всяко цяло $i = 0, 1, \ldots$. В частност, при $i = m-2$ получаваме

$$a^{p^{m-2}} \equiv 1 + tp^{m-1} \not\equiv 1 (\mathrm{mod}\ p^m).$$

Нека $a \in k \bmod p^m$. Трябва да докажем, че $k = \varphi(m) = (p-1)p^{m-1}$.

От свойствата на показателя (Теорема 1 от Въпрос 11) следва, че k дели $\varphi(p^m) = (p-1)p^{m-1}$. От друга страна, от $a \in p-1 \bmod p$ (понеже a е примитивен корен по модул p) и от $a^k \equiv 1 (\mathrm{mod}\ p)$ (последното следва от $a^k \equiv 1 (\mathrm{mod}\ p^m)$) заключаваме, че $p-1$ дели k. Следователно k има вида $(p-1)p^i$ за някое цяло $i \leq m-1$. Оттук и от $a^{p^{m-2}} \not\equiv 1 (\mathrm{mod}\ p^m)$ следва, че $k = (p-1)p^{m-1}$, с което теоремата е доказана в този случай.

б) Ако a е примитивен корен по модул p, то точно едно от числата a и $a + p^m$ е нечетно. Да означим това число с b. Тогава b е примитивен корен по модул p след евентуално многократно прилагане на Лема 1. Лесно се вижда, че $b \not\equiv 1 (\mathrm{mod}\ p^2)$. Тогава както в а) можем да докажем, че b е примитивен корен по модул p^m. Остава да видим, че $\varphi(2p^m) = \varphi(p^m)$.

Теорема 3. Примитивни корени по модул n съществуват тогава и само тогава, когато $n = 2, 4, p^m$ или $2p^m$, където p е нечетно просто число.

Доказателство: Достатъчността (т.е. съществуването на примитивни корени в посочените случаи) следва от Теореми 1 и 2. Несъществуването на примитивни корени по модул 2^m при $m \geq 3$ беше доказано в Теорема 1. Остава да докажем, че ако n не е от вида 2^m $(m = 1, 2)$, p^m и $2p^m$, то не съществуват примитивни корени по модул n.

Трябва да докажем, че ако $(a, n) = 1$, то a не е примитивен корен по модул n. От вида на n следва, че n може да се представи във вида $n = n_1 n_2$, където $n_1 > 2$, $n_2 > 2$ и $(n_1, n_2) = 1$. Тогава $(a, n_1) = (a, n_2) = 1$ и следователно $a^{\varphi(n_1)} \equiv 1 (\mathrm{mod}\ n_1)$ и $a^{\varphi(n_2)} \equiv 1 (\mathrm{mod}\ n_2)$ съгласно Теоремата на Ойлер.

Ако $k = [\varphi(n_1), \varphi(n_2)]$, то $a^k \equiv 1 (\mathrm{mod}\ n_1)$ и $a^k \equiv 1 (\mathrm{mod}\ n_2)$, откъдето $a^k \equiv 1 (\mathrm{mod}\ n)$. Остава да докажем, че $k < \varphi(n)$.

Числата $\varphi(n_1)$ и $\varphi(n_2)$ са четни и следователно не са взаимно прости. Тогава

$$k = [\varphi(n_1), \varphi(n_2)] < \varphi(n_1)\varphi(n_2) = \varphi(n_1 n_2) = \varphi(n)$$

(използвахме мултипликативността на функцията на Ойлер), с което доказателството е завършено.

Примитивни корени по съставен модул

В предишния въпрос отбелязахме, че примитивни корени по модул 8 не съществуват. Лесно се вижда, че 3 е примитивен корен по модул 4. Следователно при съставен модул са възможни и двете ситуации – да има и да няма примитивни корени (т.е. групата M може да е циклична или да не е циклична).

Да разгледаме първо случая на модул 2^m.

Теорема 1. Примитивни корени по модул 2^m съществуват тогава и само тогава, когато $m = 1$ или 2.

Доказателство: Ще докажем по индукция, че ако a е нечетно и $m > 2$, то $a^{2^{m-2}} \equiv 1 (\mathrm{mod}\ 2^m)$, което ще означава, че a не е примитивен корен по модул 2^m (да отбележим, че $\varphi(2^m) = 2^{m-1}$).

При $m = 3$ имаме $a^2 \equiv 1 (\mathrm{mod}\ 8)$, което е вярно. Нека $a^{2^{m-2}} \equiv 1 (\mathrm{mod}\ 2^m)$ за някое $m \geq 3$ и да разгледаме разликата

$$a^{2^{m-1}} - 1 = \left(a^{2^{m-2}}\right)^2 - 1 = \left(a^{2^{m-2}} - 1\right)\left(a^{2^{m-2}} + 1\right).$$

Числото $a^{2^{m-2}}+1$ е четно, а по индукционно предположение $a^{2^{m-2}}-1$ се дели на 2^m. Следователно тяхното произведение $a^{2^{m-1}}-1$ се дели на 2^{m+1}, т.е. $a^{2^{m-1}} \equiv 1 (\mathrm{mod}\ 2^{m+1})$, с което теоремата е доказана.

Лема 1. Ако p е нечетно просто число и a е примитивен корен по модул p, то $a+p$ също е примитивен корен по модул p.

Доказателство: Очевидно – за всяко k имаме

$$a^k \equiv (a+p)^k (\mathrm{mod}\ p).$$

Лема 2. Ако p е нечетно просто число и a е примитивен корен по модул p, то поне едно от числата a^{p-1} и $(a+p)^{p-1}$ не е сравнимо с 1 по модул p^2.

Доказателство: Ако допуснем противното, получаваме, че p^2 дели разликата

$$(a+p)^{p-1} - a^{p-1} = (p-1)pa^{p-2} + \binom{p-1}{2} p^2 a^{p-3} + \cdots + p^{p-1},$$

т.е. p дели $(p-1)a^{p-2}$, което е невъзможно.

Теорема 2. Ако p е нечетно просто число и m е естествено число, то:

а) съществуват примитивни корени по модул p^m;

б) съществуват примитивни корени по модул $2p^m$.

Доказателство: а) От Леми 1 и 2 следва, че съществува примитивен корен a по модул p, за който $a^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$. Действително, ако a не е такъв, то $a+p$ е такъв и при необходимост преименуваме $a+p$ на a.

Тогава $a^{p-1} = 1+tp$, където t е цяло число и $(t,p)=1$. Ще докажем, че a е примитивен корен по модул p^m за всяко $m \geq 1$.

Както в Теорема 1 (виж също Лема 1 от Въпрос 7) по индукция се доказва, че

$$a^{p^i} = (1+tp)^{p^i} \equiv 1 + tp^{i+1} (\mathrm{mod}\ p^{i+2}),$$

където $(t,p)=1$ (числото t е същото, както по-горе!) за всяко цяло $i = 0, 1, \ldots$. В частност, при $i = m-2$ получаваме

$$a^{p^{m-2}} \equiv 1 + tp^{m-1} \not\equiv 1 (\mathrm{mod}\ p^m).$$

Нека $a \in k \bmod p^m$. Трябва да докажем, че $k = \varphi(m) = (p-1)p^{m-1}$.

От свойствата на показателя (Теорема 1 от Въпрос 9) следва, че k дели $\varphi(p^m) = (p-1)p^{m-1}$. От друга страна, от $a \in p-1 \bmod p$ (понеже a е примитивен корен по модул p) и от $a^k \equiv 1 (\mathrm{mod}\ p)$ (последното следва от $a^k \equiv 1 (\mathrm{mod}\ p^m)$) заключаваме, че $p-1$ дели k. Следователно k има вида $(p-1)p^i$ за някое цяло $i \leq m-1$. Оттук и от $a^{p^{m-2}} \not\equiv 1 (\mathrm{mod}\ p^m)$ следва, че $k = (p-1)p^{m-1}$, с което теоремата е доказана в този случай.

б) Ако a е примитивен корен по модул p, то точно едно от числата a и $a+p^m$ е нечетно. Да означим това число с b. Тогава b е примитивен корен по модул p след евентуално многократно прилагане на Лема 1. Лесно се вижда, че $b \not\equiv 1 (\mathrm{mod}\ p^2)$. Тогава както в а) можем да докажем, че b е примитивен корен по модул p^m. Остава да видим, че $\varphi(2p^m) = \varphi(p^m)$.

Теорема 3. Примитивни корени по модул n съществуват тогава и само тогава, когато $n = 2, 4, p^m$ или $2p^m$, където p е нечетно просто число.

Доказателство: Достатъчността (т.е. съществуването на примитивни корени в посочените случаи) следва от Теореми 1 и 2. Несъществуването на примитивни корени по модул 2^m при $m \geq 3$

беше доказано в Теорема 1. Остава да докажем, че ако n не е от вида 2^m $(m = 1, 2)$, p^m и $2p^m$, то не съществуват примитивни корени по модул n.

Трябва да докажем, че ако $(a, n) = 1$, то a не е примитивен корен по модул n. От вида на n следва, че n може да се представи във вида $n = n_1 n_2$, където $n_1 > 2$, $n_2 > 2$ и $(n_1, n_2) = 1$. Тогава $(a, n_1) = (a, n_2) = 1$ и следователно $a^{\varphi(n_1)} \equiv 1 (\mathrm{mod}\ n_1)$ и $a^{\varphi(n_2)} \equiv 1 (\mathrm{mod}\ n_2)$ съгласно Теоремата на Ойлер.

Ако $k = [\varphi(n_1), \varphi(n_2)]$, то $a^k \equiv 1 (\mathrm{mod}\ n_1)$ и $a^k \equiv 1 (\mathrm{mod}\ n_2)$, откъдето $a^k \equiv 1 (\mathrm{mod}\ n)$. Остава да докажем, че $k < \varphi(n)$.

Числата $\varphi(n_1)$ и $\varphi(n_2)$ са четни и следователно не са взаимно прости. Тогава

$$k = [\varphi(n_1), \varphi(n_2)] < \varphi(n_1)\varphi(n_2) = \varphi(n_1 n_2) = \varphi(n)$$

(използвахме мултипликативността на функцията на Ойлер), с което доказателството е завършено.

13. Сравнения с едно неизвестно. Системи сравнения

Сравнения с едно неизвестно

Нека $f(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_{n-1} x + c_n$ е полином с цели коефициенти и $m \geq 2$ е естествено число. Тогава сравнението

$$f(x) \equiv 0 (\mathrm{mod}\ m),$$

се нарича *сравнение с едно неизвестно*. Решаването на сравнение с едно неизвестно се състои в намирането на всички цели стойности на x, за които $f(x)$ се дели на m (т.е. $f(x) \equiv 0 (\mathrm{mod}\ m)$. Степента на полинома $f(x)$ се нарича степен на сравнението.

Оказва се, че сравнение с едно неизвестно или има безброй много решения или няма решение.

Теорема 1. Ако числото a удовлетворява сравнението $f(x) \equiv 0 (\mathrm{mod}\ m)$, то всяко число от класа $\overline{a}$ от остатъци по модул m също удовлетворява това сравнение.

Доказателство: Нека $f(a) \equiv 0 (\mathrm{mod}\ m)$ и $b \in \overline{a}$, т.е. $a \equiv b (\mathrm{mod}\ m)$. От последното следва, че $f(a) \equiv f(b) (\mathrm{mod}\ m)$ съгласно едно от свойствата на сравненията. Тогава $f(b) \equiv 0 (\mathrm{mod}\ m)$, което означава, че b също е решение на сравнението.

От Теорема 1 следва, че дефиницията за решение на сравнение е коректна в следния вид – решение на $f(x) \equiv 0 (\mathrm{mod}\ m)$ е всеки клас от остатъци $\overline{a}$ по модул m, за който $f(a) \equiv 0 (\mathrm{mod}\ m)$. Тъй като броят на класовете остатъци е краен, решаването на сравнението може да се проведе чрез директна проверка на пълна система остатъци по модул m. Действително, можем да вземем пълна система $x_1, x_2, \ldots, x_m$ по модул m и да проверим кои от числата $f(x_1), f(x_2), \ldots, f(x_m)$ се делят на m.

Често се разглеждат сравнения от вида

$$f(x) \equiv g(x) (\mathrm{mod}\ m),$$

където $f(x)$ и $g(x)$ са полиноми с цели коефициенти.

Дефиниция 2. Сравненията

$$f_1(x) \equiv g_1(x) (\mathrm{mod}\ m) \quad \text{и} \quad f_2(x) \equiv g_2(x) (\mathrm{mod}\ m)$$

се наричат еквивалентни, ако всяко решение на едното е решение и на другото (т.е. множествата от решенията им съвпадат). В частност, всеки две сравнения, които нямат решение, са еквивалентни (както е при уравненията).

Свойствата на релацията еквивалентност на сравнения с едно неизвестно са описани в следващата теорема.

Теорема 2. (1) Ако към двете страни на сравнението

$$f(x) \equiv g(x) (\mathrm{mod}\ m)$$

прибавим един и същи полином $h(x)$ с цели коефициенти, полученото сравнение е еквивалентно на даденото, т.е.

$$f(x) \equiv g(x) (\mathrm{mod}\ m) \iff f(x) + h(x) \equiv g(x) + h(x) (\mathrm{mod}\ m).$$

(2) Ако умножим двете страни на сравнението

$$f(x) \equiv g(x) (\mathrm{mod}\ m)$$

с число, взаимно просто с m, полученото сравнение е еквивалентно на даденото, т.е. ако $(a, m) = 1$, то

$$f(x) \equiv g(x) (\mathrm{mod}\ m) \iff af(x) \equiv ag(x) (\mathrm{mod}\ m).$$

(3) Ако умножим двете страни и модула на сравнението

$$f(x) \equiv g(x) (\mathrm{mod}\ m)$$

с едно и също цяло число $k > 0$, полученото сравнение (по модул km) е еквивалентно на даденото, т.е.

$$f(x) \equiv g(x) (\mathrm{mod}\ m) \iff kf(x) \equiv kg(x) (\mathrm{mod}\ km).$$

Доказателство: И трите твърдения следват директно от дефиницията за еквивалентни сравнения и елементарните свойства на сравненията.

От Теорема 2 следва, че

$$f(x) \equiv g(x) (\mathrm{mod}\ m) \iff f(x) - g(x) \equiv 0 (\mathrm{mod}\ m)$$

(използвайте $h(x) = -g(x)$ в (1)). По тази причина ще разглеждаме само сравнения от вида $f(x) \equiv 0 (\mathrm{mod}\ m)$.

Да отбележим, че дефиницията за еквивалентност на сравнения не изисква равенство на степените на участващите полиноми. Това не е и задължително – например сравненията

$$2x + 1 \equiv 0 (\mathrm{mod}\ 3) \iff x^3 - 1 \equiv 0 (\mathrm{mod}\ 3)$$

(класът $\overline{1}$ е решение и на двете, а класовете $\overline{0}$ и $\overline{2}$ не са решения).

Системи сравнения

Аналогично на системите уравнения се разглеждат и системи сравнения. Ако $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ са полиноми с цели коефициенти, можем да търсим решение на системата

$$\left| \begin{array}{l} f_1(x) \equiv 0 (\mathrm{mod}\ m_1) \\ f_2(x) \equiv 0 (\mathrm{mod}\ m_2) \\ \qquad \vdots \\ f_s(x) \equiv 0 (\mathrm{mod}\ m_s) \end{array} \right. ,$$

като цели стойности на x, за които са удовлетворени едновременно всички от горните сравнения.

Нека

$$M = [m_1, m_2, \ldots, m_s]$$

и a е цяло число, за което $f_1(a) \equiv 0 (\mathrm{mod}\ m_1)$ $f_2(a) \equiv 0 (\mathrm{mod}\ m_2)$, ..., $f_s(a) \equiv 0 (\mathrm{mod}\ m_s)$. Ако $b \equiv a (\mathrm{mod}\ M)$ (т.е. b принадлежи на класа остатъци $\overline{a}$ по модул M), то $f_i(b) \equiv f_i(a) \equiv 0 (\mathrm{mod}\ )$.

Тогава $f_i(b) \equiv 0 (\mathrm{mod}\ m_i)$ за всяко $i = 1, 2, \ldots, s$, т.е. b също удовлетворява всички сравнения от системата. Следователно решенията на система от горния вид са класове от остатъци по модул M.

Задачи

1. Да се докаже, че ако сравнението $f(x) \equiv 0 (\mathrm{mod}\ m)$ има решение и $d|m$, то сравнението $f(x) \equiv 0 (\mathrm{mod}\ d)$ също има решение.

14. Линейни сравнения с едно неизвестно

Да разгледаме сравненията от вида

$$ax \equiv b (\mathrm{mod}\ m),$$

където a и b са дадени цели числа, а $m \geq 2$ е естествено число. Такива сравнения се наричат линейни.

Теорема 1. Ако числото $d = (a, m)$ не дели b, то линейното сравнение $ax \equiv b (\mathrm{mod}\ m)$ няма решение.

Доказателство: Да допуснем противното, т.е. че съществува цяло число x_0, за което е изпълнено сравнението $ax_0 \equiv b (\mathrm{mod}\ m)$. Тогава m дели $ax_0 - b$, откъдето следва, че d дели $ax_0 - b$, т.е. d дели b – противоречие.

От Теорема 1 следва, че е достатъчно да разглеждаме само сравненията $ax \equiv b (\mathrm{mod}\ m)$, за които най-големият общ делител d на a (коефициентът пред неизвестното) и m (модула) дели b (свободния член). Нещо повече, в тази ситуация можем да означим $a = a_1 d$, $m = m_1 d$ и $b = b_1 d$, като $(a_1, m_1) = 1$ и от $ax \equiv b (\mathrm{mod}\ m)$ следва $a_1 x \equiv b_1 (\mathrm{mod}\ m_1)$ и обратно. Следователно е достатъчно да разглеждаме линейни сравнения, за които $(a, m) = 1$.

Теорема 2. Ако $(a, m) = 1$, то линейното сравнение $ax \equiv b (\mathrm{mod}\ m)$ има единствено решение.

Доказателство: Нека x описва пълната система остатъци

$$0, 1, 2, \ldots, m - 1.$$

Тогава числата $(a.0 = 0, a.1 = a, 2a, \ldots, (m-1)a)$ също образуват пълна система остатъци. Следователно точно едно от числата ax е сравнимо с b по модул m и това е единственото решение, за което става дума.

Следващата теорема дава в явен вид единственото решение от Теорема 2.

Теорема 3. Ако $(a, m) = 1$, то единственото решение на линейното сравнение $ax \equiv b (\mathrm{mod}\ m)$ е класът $x \equiv ba^{\varphi(m)-1} (\mathrm{mod}\ m)$.

Доказателство: Непосредствено се проверява, че $x \equiv ba^{\varphi(m)-1} (\mathrm{mod}\ m)$ действително е решение. Това решение е единствено съгласно Теорема 2.

В следващата теорема е описан друг подход към решаването на линейни сравнения с едно неизвестно.

Теорема 4. Ако $(a, m) = 1$ и цялото число k е такова, че a дели $b + mk$, то единственото решение на линейното сравнение $ax \equiv b (\mathrm{mod}\ m)$ е класът $x \equiv \dfrac{b + mk}{a} (\mathrm{mod}\ m)$.

Доказателство: Непосредствено се проверява, че $x \equiv \dfrac{b + mk}{a} (\mathrm{mod}\ m)$ действително е решение, което е единствено съгласно Теорема 2.

Методът от Теорема 4 е приложим само за малки стойности на коефициента a, тъй като само тогава намирането на числото k става бързо. Действително, от $mk \equiv -b(\mathrm{mod}\ a)$ следва, че е необходимо решаване на сравнението $mx \equiv -b(\mathrm{mod}\ a)$ (например чрез проверка на пълна система остатъци по модул a).

Теорема 5. Ако $(a, m) = d$ и d дели b, то линейното сравнение

$$ax \equiv b(\mathrm{mod}\ m)$$

има точно d решения. Обединението на тези решения е клас по модул $\dfrac{m}{d}$.

Доказателство: Нека при означенията, въведени след Теорема 1 разгледаме сравнението $a_1 x \equiv b_1(\mathrm{mod}\ m_1)$ и нека класът $x \equiv k(\mathrm{mod}\ m_1)$ е неговото единствено решение. Числата от този клас образуват следните d класа по модул m:

$$x \equiv k(\mathrm{mod}\ m),\ x \equiv k + \frac{m}{d}(\mathrm{mod}\ m), \ldots, x \equiv k + \frac{(d-1)m}{d}(\mathrm{mod}\ m).$$

Тогава твърдението следва от $ax \equiv b(\mathrm{mod}\ m) \iff a_1 x \equiv b_1(\mathrm{mod}\ m_1)$.

Задачи

1. Да се решат сравненията:

а) $5x + 12 \equiv 0(\mathrm{mod}\ 3)$; б) $123x + 1 \equiv 0(\mathrm{mod}\ 4)$; в) $23x \equiv 19(\mathrm{mod}\ 5)$;

г) $x^2 \equiv 1(\mathrm{mod}\ 4)$; д) $x^2 + 3x + 1 \equiv 0(\mathrm{mod}\ 3)$; е) $x^5 - x + 35 \equiv 0(\mathrm{mod}\ 5)$.

а) *Решение* (директна проверка). Нека $x \equiv (\mathrm{mod}\ 3)$, където $a \in \{0, 1, 2\}$ е решение на сравнението. Тогава $5a + 12$ се дели на 3 и директната проверка показва, че $a = 0$ е единствената възможност.

2. Да се докаже, че ако p е нечетно просто число, то сравнението $2x \equiv 1(\mathrm{mod}\ p)$ има единствено решение.

3. а) Да се докаже, че ако $d = (a, m)$ не дели b, то сравнението $ax \equiv b(\mathrm{mod}\ m)$ няма решение.

б) Да се докаже, че ако $(a, m) = 1$, то сравнението $ax \equiv b(\mathrm{mod}\ m)$ има единствено решение.

4. Да се решат сравненията:

а) $65x \equiv 19(\mathrm{mod}\ 25)$; б) $23x \equiv 19(\mathrm{mod}\ 25)$.

15. Системи линейни сравнения с едно неизвестно. Китайска теорема за остатъците

Да разгледаме системата

$$\left| \begin{array}{l} x \equiv c_1(\mathrm{mod}\ m_1) \\ x \equiv c_2(\mathrm{mod}\ m_2) \end{array} \right. , \tag{1}$$

като означим $d = (m_1, m_2)$ и $M = [m_1, m_2]$.

Теорема 1. а) Ако d не дели разликата $c_1 - c_2$, то системата (1) няма решение.

б) Ако d дели разликата $c_1 - c_2$, то системата (1) има единствено решение, което е клас остатъци по модул M.

Доказателство: Нека x удовлетворява първото сравнение. Тогава $x = c_1 + m_1 t$ за някое цяло число t. Да се опитаме да подберем t така, че x да удовлетворява и второто сравнение, т.е. искаме да е изпълнено сравнението

$$c_1 + m_1 t \equiv c_2(\mathrm{mod}\ m_2) \iff m_1 t \equiv c_2 - c_1(\mathrm{mod}\ m_2).$$

а) Ако d не дели $c_2 - c_1$, то последното сравнение няма решение съгласно Теорема 1 от предишния въпрос. Следователно системата (1) също няма решение.

б) Ако d дели $c_2 - c_1$, то съгласно Теорема 5 от предишния въпрос сравнението $m_1 t \equiv c_2 - c_1 (\mathrm{mod}\ m_2)$ има решения, чието обединение е клас остатъци по модул $\dfrac{m_2}{d}$. Нека този клас е

$$\overline{\alpha} = \{\alpha + \frac{m_2 y}{d} | y = 0, \pm 1, \pm 2, \ldots\}.$$

Тогава решенията на системата имат вида

$$x = c_1 + m_1\Big(\alpha + \frac{m_2 y}{d}\Big) = c_1 + m_1\alpha + \frac{m_1 m_2 y}{d} = \beta + My,$$

което е точно клас остатъци по модул $M = [m_1, m_2] = \dfrac{m_1 m_2}{d}$.

Следствие 1. Ако $(m_1, m_2) = 1$, то системата (1) има единствено решение, което е клас остатъци по модул $M = m_1 m_2$.

Доказателство: Очевидно, тъй като $d = 1$ дели $c_1 - c_2$ и $[m_1, m_2] = m_1 m_2 = M$.

По-общо, да разгледаме системата

$$\left|\begin{array}{l} x \equiv c_1 (\mathrm{mod}\ m_1) \\ x \equiv c_2 (\mathrm{mod}\ m_2) \\ \qquad \vdots \\ x \equiv c_s (\mathrm{mod}\ m_s) \end{array}\right. . \tag{2}$$

Теорема 2. Системата (2) или няма решение, или има единствено решение, което е клас остатъци по модул $[m_1, m_2, \ldots, m_s]$.

Доказателство: Ще проведем индукция по броя на сравненията s. При $s = 2$ получаваме Теорема 1. Нека твърдението е вярно за система от $s \geq 2$ сравнения и да разгледаме система с $s+1$ сравнения

$$\left|\begin{array}{l} x \equiv c_1 (\mathrm{mod}\ m_1) \\ \qquad \vdots \\ x \equiv c_s (\mathrm{mod}\ m_s) \\ x \equiv c_{s+1} (\mathrm{mod}\ m_{s+1}) \end{array}\right. . \tag{3}$$

Да означим $M = [m_1, m_2, \ldots, m_s]$ и $M' = [m_1, m_2, \ldots, m_s, m_{s+1}]$. Знаем, че $M' = [M, m_{s+1}]$.

Ако системата от първите s сравнения на (3) няма решение, то и (3) няма решение. Да предположим, че системата от първите s сравнения на (3) има решение. Съгласно индукционното предположение това решение е клас от остатъци $\overline{\alpha}$ по модул M. Тогава системата (3) е еквивалентна на система от две сравнения

$$\left|\begin{array}{l} x \equiv \alpha (\mathrm{mod}\ M) \\ x \equiv c_{s+1} (\mathrm{mod}\ m_{s+1}) \end{array}\right. \tag{4}$$

От Теорема 1а) следва, че ако $\delta = [M, m_{s+1}]$ не дели $c_{s+1} - \alpha$, то системата (4) няма решение, откъдето и (3) няма решение. Ако пък δ дели $c_{s+1} - \alpha$, то съгласно Теорема 1б) системата (4) има единствено решение, което е клас остатъци по модул $M' = [M, m_{s+1}]$. С това доказателството е завършено.

Следствие 2. Ако числата $m_1, m_2, \ldots, m_s$ са взаимно прости две по две, то системата (2) има единствено решение, което е клас остатъци по модул $M = m_1 m_2 \ldots m_s$.

Доказателство: При $s = 2$ това е Следствие 1. По-нататък може да се проведе индукция както в Теорема 2.

Теорема 3. (Китайска теорема за остатъците) Нека $m_1, m_2, \ldots, m_s$ са взаимно прости две по две, $M = m_1 m_2 \ldots m_s$ и числата $y_1, y_2, \ldots, y_s$ са такива, че

$$\frac{M}{m_1} y_1 \equiv 1 (\text{mod } m_1), \frac{M}{m_2} y_2 \equiv 1 (\text{mod } m_2), \ldots, \frac{M}{m_s} y_s \equiv 1 (\text{mod } m_s)$$

Тогава единственото решение на системата (2) е класът

$$x \equiv x_0 (\text{mod } M),$$

където

$$x_0 = \frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + \cdots + \frac{M}{m_s} y_s c_s.$$

Доказателство: Съществуването и единствеността на решението следват от Следствие 2. Остава да докажем указания явен вид.

Ако $i \in \{1, 2, \ldots, s\}$ е фиксирано, то m_i дели $\frac{M}{m_j}$ за всяко $j \neq i$, т.е.

$$\frac{M}{m_j} y_j c_j \equiv 0 (\text{mod } m_i)$$

за $j \neq i$. Освен това $\frac{M}{m_i} y_i c_i \equiv c_i (\text{mod } m_i)$ и следователно $x_0 \equiv c_i (\text{mod } m_i)$. Последното сравнение е вярно за всяко $i = 1, 2, \ldots, s$, т.е. x_0 удовлетворява системата (2).

Задачи

Задача 1. Да се решат системите:

а) $\left| \begin{array}{ll} 2x & \equiv 3 \pmod 5 \\ 19x & \equiv 5 \pmod 7 \end{array} \right.$; б) $\left| \begin{array}{ll} 3x+1 & \equiv 0 \pmod{11} \\ 5x-7 & \equiv 0 \pmod{13} \end{array} \right.$;

в) $\left| \begin{array}{ll} x & \equiv 3 \pmod 5 \\ 10x & \equiv 3 \pmod 7 \\ 5x & \equiv -4 \pmod 9 \end{array} \right.$; г) $\left| \begin{array}{ll} 7x-2 & \equiv 0 \pmod 6 \\ 15x+27 & \equiv 0 \pmod{17} \\ 125x & \equiv 1 \pmod{127} \end{array} \right.$.

Задача 2. (тест Турция 2006) Нека x_1 е естествено число и $x_{n+1} = x_1^2 + x_2^2 + \cdots + x_n^2$ за всяко естествено $n \geq 1$. Да се намери минималната възможна стойност на x_1, ако е известно, че 2006 дели x_{2006}.

Решение. Да представим рекурентната връзка във вида

$$x_{n+1} = x_n + x_n^2 = x_1^2 (1 + x_2)(1 + x_3) \ldots (1 + x_n), \quad n \geq 3$$

Ясно е, че x_{2006} е четно и остава да изследваме делимостта на $1003 = 17.59$.

Да допуснем, че $17 | x_i + 1$ за някое i, $3 \leq i \geq 2005$. Тогава $x_{i-1}^2 + x_{i-1} + 1 \equiv 0 \pmod{17} \iff (2x_{i-1} + 1)^2 \equiv -3 \pmod{17} \iff (-3)^8 \equiv 1 \pmod{17}$ (Критерий на Ойлер), което е невярно. Следователно $17 | x_1^2 (x_2 + 1)$, откъдето $x_1 \equiv 0 \pmod{17}$ или $x_2 + 1 = x_1^2 + 1 \equiv 0 \pmod{17}$.

Аналогично се вижда, че $59 | x_1^2 (x_2 + 1)$, откъдето $x_1 \equiv 0 \pmod{59}$ или $x_2 + 1 = x_1^2 + 1 \equiv 0 \pmod{59}$. Последната възможност отпада, защото $x_1^2 + 1$ не може да има прости делители от вида $4k + 3$. Следователно x_1 се дели на 59.

Оттук нататък имаме две възможности за x_1, във всяка от които прилагаме Китайската теорема за остатъците:

1) $x_1 \equiv 0 \pmod{17}$ и $x_1 \equiv 0 \pmod{59}$. Тогава $x_1 = 17.59k \geq 17.59 = 1003$.

2) $x_1^2 + 1 \equiv 0 \pmod{17} \iff x_1 \equiv \pm 4 \pmod{17}$ и $x_1 \equiv 0 \pmod{59}$. Тъй като минималното естествено решение на сравненията $59k \equiv \pm 4 \pmod{17}$ е $k = 8$, получаваме $x_1 = 59(17m + 8) \geq 59.8 = 472$.

Следователно търсената минимална стойност е 472.

Задача 3. (Разширен списък МОМ 2005, контролни Русия, Германия, Франция 2006) Нека a и b са естествени числа, за които $a^n + n$ дели $b^n + n$ за всяко естествено число n. Да се докаже, че $a = b$.

Решение. Нека $p > \max\{a, b\}$ е просто число и n е степенен показател, за който $n \equiv 1 \pmod{p-1}$ и $a + n \equiv 0 \pmod{p}$. Такива n съществуват съгласно Китайската теорема за остатъците и можем да вземем например $n = (p-1)(a+1)+1$. Да отбележим, че $(a, p) = 1$ поради избора на p.

Тъй като

$$a^n + n = a(a^{p-1})^{a+1} + n \equiv a + n \equiv 0 \pmod{p},$$

имаме $p|a^n + n|b^n + n$, т.е. $a^n \equiv b^n \pmod{p}$, откъдето $(b, p) = 1$ и $a \equiv b \pmod{p}$. Последното обаче е невъзможно при $a \neq b$.

16. Сравнения по прост модул с едно неизвестно

Сравнения с едно неизвестно

Да разгледаме сравнения от вида

$$f(x) \equiv 0 (\mathrm{mod}\ p),$$

където p е просто число, а $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$ е полином с цели коефициенти, като $(c_0, p) = 1$.

Лема 1. Сравнението $c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n \equiv 0 (\mathrm{mod}\ m)$ е еквивалентно на сравнение от вида

$$x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n \equiv 0 (\mathrm{mod}\ m).$$

Доказателство: Достатъчно да умножим двете страни на даденото сравнение с число от класа, който е решение на сравнението $c_0y \equiv 1 (\mathrm{mod}\ p)$. Тъй като $(c_0, p) = 1$, такова решение има.

Лема 2. Ако $f(x)$ и $g(x)$ са полиноми с цели коефициенти, то

$$f(x) \equiv 0 (\mathrm{mod}\ p) \iff f(x) - (x^p - x)g(x) \equiv 0 (\mathrm{mod}\ p).$$

Доказателство: Достатъчно да отбележим, че $x^p - x \equiv 0 (\mathrm{mod}\ p)$ за всяко цяло x съгласно теоремата на Ферма.

Лема 3. Ако степента на $f(x)$ е по-голяма или равна на p и

$$f(x) = (x^p - x)g(x) + r(x),$$

където степента на $r(x)$ е по-малка от p, то

$$f(x) \equiv 0 (\mathrm{mod}\ p) \iff r(x) \equiv 0 (\mathrm{mod}\ p).$$

Доказателство: Следва от Лема 2.

Лема 4. Ако полиномите с цели коефициенти $f(x)$, $g(x)$, $h(x)$ и $r(x)$ са такива, че $f(x) = g(x)h(x) + r(x)$ и всички коефициенти на $r(x)$ се делят на p, то всяко число, което удовлетворява сравнението $f(x) \equiv 0 (\mathrm{mod}\ p)$, удовлетворява и поне едно от сравненията $g(x) \equiv 0 (\mathrm{mod}\ p)$ и $h(x) \equiv 0 (\mathrm{mod}\ p)$.

Доказателство: Ясно е, че $r(x) \equiv 0 (\mathrm{mod}\ p)$ за всяко x. Тогава от $f(x_0) \equiv 0 (\mathrm{mod}\ p)$ следва, че $g(x_0)h(x_0) \equiv 0 (\mathrm{mod}\ p)$, т.е. p дели произведението $g(x_0)h(x_0)$, т.е. p дели поне едно от числата $g(x_0)$

и $h(x_0)$. Обратно, ако x_0 е решение на някое от сравненията $g(x) \equiv 0 (\mathrm{mod}\ p)$ и $h(x) \equiv 0 (\mathrm{mod}\ p)$, то p дели $g(x_0)h(x_0)$, т.е.

$$f(x_0) = g(x_0)h(x_0) + r(x_0) \equiv 0 (\mathrm{mod}\ p).$$

Теорема 1. Сравнението

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n \equiv 0 (\mathrm{mod}\ p),$$

където $(c_0, p) = 1$, има не повече от n решения.

Доказателство: Ще проведем индукция по степента на сравнението n. При $n = 1$ твърдението е вярно съгласно Теорема 2 от Въпрос 15. Нека $n \geq 2$ и твърдението е вярно за сравнения от степен $n - 1$.

Ако $f(x) \equiv 0 (\mathrm{mod}\ p)$ няма решение, твърдението е вярно. Нека x_0 е цяло число, за което $f(x_0) \equiv 0 (\mathrm{mod}\ p)$ и да представим $f(x)$ във вида

$$f(x) = (x - x_0)g(x) + f(x_0)$$

(това представяне се нарича Теорема на Безу). Полиномът $g(x) = b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-2}x + b_{n-1}$ е от степен $n - 1$ и очевидно $c_0 = b_0$, т.е. $(b_0, p) = 1$.

Съгласно Лема 4 всяко решение на $f(x) \equiv 0 (\mathrm{mod}\ p)$ е решение на $g(x) \equiv 0 (\mathrm{mod}\ p)$ или на $x - x_0 \equiv 0 (\mathrm{mod}\ p)$. От индукционното предположение следва, че $g(x) \equiv 0 (\mathrm{mod}\ p)$ има най-много $n - 1$ решения, а линейното сравнение $x - x_0 \equiv 0 (\mathrm{mod}\ p)$ има единствено решение $x \equiv x_0 (\mathrm{mod}\ p)$. Следователно сравнението $f(x) \equiv 0 (\mathrm{mod}\ p)$ има не повече от $(n - 1) + 1 = n$ решения.

Да отбележим, че твърдението на Теорема 1 не е вярно за съставен модул. Например сравнението $x^2 - 3x + 2 \equiv 0 (\mathrm{mod}\ 6)$ е то втора степен и има четири решения $\overline{1}, \overline{2}, \overline{4}, \overline{5}$.

Следствие 1. Ако сравнението

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n \equiv 0 (\mathrm{mod}\ p)$$

има повече от n решения, то всички коефициенти се делят на p.

Доказателство: От Теорема 1 следва, че p дели c_0. Тогава сравнението е еквивалентно на

$$c_1x^{n-1} + \cdots + c_{n-1}x + c_n \equiv 0 (\mathrm{mod}\ p),$$

за което можем отново да приложим Теорема 1 и т.н.

Теорема 2. Нека $f(x) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$ е полином с цели коефициенти, $(c_n, p) = 1$ и $p - 1 \geq n$. Сравнението $f(x) \equiv 0 (\mathrm{mod}\ p)$ има точно n решения тогава и само тогава, когато всички коефициенти на остатъка при делението на $x^{p-1} - 1$ на $f(x)$ се делят на p.

Доказателство: Нека $x^{p-1} - 1 = f(x)g(x) + r(x)$, където степента на r е по-малка от n.

(Достатъчност) Нека всички коефициенти на $r(x)$ се делят на p и сравненията $f(x) \equiv 0 (\mathrm{mod}\ p)$ и $g(x) \equiv 0 (\mathrm{mod}\ p)$ имат съответно по s и t решения.

Сравнението $x^{p-1} - 1 \equiv 0 (\mathrm{mod}\ p)$ има $p - 1$ решения съгласно Теоремата на Ферма. Съгласно Лема 4, всяко от тези решения е решение на поне едно от сравненията $f(x) \equiv 0 (\mathrm{mod}\ p)$ и $g(x) \equiv 0 (\mathrm{mod}\ p)$. Следователно $s + t \geq p - 1$. От друга страна, сравнението $g(x) \equiv 0 (\mathrm{mod}\ p)$ е от степен $p - 1 - n$ и коефициентът пред най-високата степен е 1. Тогава от Теорема 1 следва, че $g(x) \equiv 0 (\mathrm{mod}\ p)$ има най-много $p - 1 - n$ решения, т.е. $t \leq p - 1 - n$. Следователно

$$s \geq p - 1 - t \geq p - 1 - (p - 1 - n) = n.$$

Но $s \leq n$ според Теорема 1 и окончателно получаваме $s = n$.

(Необходимост) Нека $f(x) \equiv 0(\mathrm{mod}\ p)$ има точно n решения. Ако x_0 е едно от тях, то от $f(x_0) \equiv 0(\mathrm{mod}\ p)$ и $(c_n, p) = 1$ следва, че $(x_0, p) = 1$. Тогава по Теоремата на Ферма имаме $x_0^{p-1} \equiv 1(\mathrm{mod}\ p)$ и оттук

$$r(x_0) \equiv x_0^{p-1} - 1 + f(x_0)g(x_0) \equiv 0(\mathrm{mod}\ p).$$

Следователно сравнението $r(x) \equiv 0(\mathrm{mod}\ p)$ има поне n решения (решенията на $f(x) \equiv 0(\mathrm{mod}\ p)$), което съгласно Следствие 1 означава, че всички коефициенти на $r(x)$ се делят на p.

Задачи

1. Да се решат сравненията:

а) $x^2 + x - 2 \equiv 0(\mathrm{mod}\ 6)$; б) $3x^2 - x - 1 \equiv 0(\mathrm{mod}\ 10)$.

2. Да се намерят всички цели стойности на x, за които квадратният тричлен $5x^2 + x + 4$ се дели на 10.

17. Сравнения по прост модул с няколко неизвестни. Теорема на Шевалие

Сравнения с няколко неизвестни

Да разгледаме сравнения от вида

$$f(x_1, x_2, \ldots, x_n) \equiv 0(\mathrm{mod}\ p), \tag{5}$$

където p е просто число, а $f(x_1, x_2, \ldots, x_n)$ е полином с цели коефициенти. Голяма част от свойствата на тези сравнения са аналози на съответните свойства на сравненията с едно неизвестно по прост модул. По тази причина няма да привеждаме подробни доказателства.

Теорема 1. Сравнението (1) е еквивалентно на сравнение, в което всички неизвестни участват в степен, ненадминаваща $p - 1$.

Доказателство: Достатъчно да докажем, че ако някое неизвестно x_i участва в лявата страна на (1) в степен, по-голяма от $p-1$, то (1) е еквивалентно на сравнение, в което x_i участва в степен, ненадминаваща $p - 1$. Това следва от факта, че (1) е еквивалентно на

$$f(x_1, x_2, \ldots, x_n) - (x_i^p - x_i)g(x_1, x_2, \ldots, x_n) \equiv 0(\mathrm{mod}\ p),$$

което се доказва по същия начин, както Лема 2 от предишния въпрос, след подходящ избор на полинома $g(x_1, x_2, \ldots, x_n)$.

Теорема 2. Ако в сравнението (1) всички неизвестни участват в степен, ненадминаваща $p - 1$ и (1) е изпълнено за всички стойности на променливите $x_1, x_2, \ldots, x_n$, то всички коефициенти на полинома $f(x_1, x_2, \ldots, x_n)$ се делят на p.

Доказателство: Ще проведем индукция по броя на неизвестните. При $n = 1$ получаваме Следствие 1 от предишния въпрос. Нека твърдението е вярно за $n-1$ променливи и да разгледаме (1) като сравнение с едно неизвестно x_n, представяйки лявата страна във вида

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= q_1(x_1, x_2, \ldots, x_{n-1})x_n^k + q_2(x_1, x_2, \ldots, x_{n-1})x_n^{k-1} + \\ &+ \cdots + q_k(x_1, x_2, \ldots, x_{n-1}). \end{aligned}$$

Тогава всички коефициенти $q_i(x_1, x_2, \ldots, x_{n-1})$, $i = 1, 2, \ldots, k$, се делят на p за всеки избор на променливите $x_1, x_2, \ldots, x_{n-1}$. Оттук и от индукционното предположение следва, че всички коефициенти на полиномите $q_i(x_1, x_2, \ldots, x_{n-1})$, $i = 1, 2, \ldots, k$, се делят на p. Остава да видим, че тези коефициенти са равни на коефициентите на $f(x_1, x_2, \ldots, x_n)$.

Теорема на Шевалие

Теорема 3. (Теорема на Шевалие) Нека в сравнението (1) полиномът $f(x_1, x_2, \ldots, x_n)$ има нулев свободен член. Ако степента на $f(x)$ е по-малка от n, то (1) има поне едно ненулево решение.

Доказателство: Да отбележим, че $f(0, 0, \ldots, 0) \equiv 0 (\text{mod } p)$ и да разгледаме сравнението

$$f(x_1, x_2, \ldots, x_n)^{p-1} \equiv 1 - (1 - x_1^{p-1})(1 - x_2^{p-1}) \ldots (1 - x_n^{p-1}) (\text{mod } p). \tag{6}$$

Степените отляво и отдясно на (2) са съответно $m(p-1)$ и $n(p-1)$, като втората е по-голяма. Освен това коефициентът пред старшия едночлен отдясно е $(-1)^{n+1}$, т.е. (2) не е тъждество. Следователно съществуват цели числа $a_1, a_2, \ldots, a_n$, които не удовлетворяват (2).

Лесно се вижда, че поне едно от числата a_i е различно от 0 (в противен случай получаваме $f(0, 0, \ldots, 0) \not\equiv 0 (\text{mod } p)$). За това a_i съгласно Теоремата на Ферма имаме $a_i^{p-1} \equiv 1 (\text{mod } p)$, откъдето следва, че лявата страна на (2) е сравнима с 1 по модул p за $(x_1, x_2, \ldots, x_n) = (a_1, a_2, \ldots, a_n)$.

Тогава

$$f(a_1, a_2, \ldots, a_n)^{p-1} \not\equiv 1 (\text{mod } p).$$

От Теоремата на Ферма обаче следва, че последното е възможно само при

$$f(a_1, a_2, \ldots, a_n) \equiv 0 (\text{mod } p),$$

т.е. $(a_1, a_2, \ldots, a_n)$ е ненулево решение на (1).

Да отбележим, че всъщност доказахме малко по-общо твърдение – ако $f(0, 0, \ldots, 0) \equiv 0 (\text{mod } p)$ и

$$f(x_1, x_2, \ldots, x_n)^{p-1} \equiv 1 - (1 - x_1^{p-1})(1 - x_2^{p-1}) \ldots (1 - x_n^{p-1}) (\text{mod } p)$$

не е тъждество, то (1) има поне едно ненулево решение.

18. Теорема на Уилсън. Близнаци прости числа

Теорема на Уилсън

Нека $p \geq 5$ е просто число и $k \in \{2, 3, \ldots, p-2\}$ е фиксирано. Както знаем, сравнението

$$kx \equiv 1 (\text{mod } p),$$

има единствено решение. От избора на k следва, че това решение не е $\overline{1}$, нито пък $\overline{p-1}$.

Следователно съществува единствено число $k' \in \{2, 3, \ldots, p-2\}$, за което $kk' \equiv 1 (\text{mod } p)$. Лесно се вижда, че $k \neq k'$ (в противен случай получаваме, че p дели $k^2 - 1 = (k-1)(k+1)$, което е невъзможно при $k \in \{2, 3, \ldots, p-2\}$).

Направеното разсъждение е в основата на доказателството на Теоремата на Уилсън.

Теорема 1. (Теорема на Уилсън) Естественото число p е просто тогава и само тогава, когато

$$(p-1)! + 1 \equiv 0 (\text{mod } p).$$

Доказателство: (Необходимост) Нека p е просто число. Трябва да докажем, че $(p-1)! + 1 \equiv 0 (\text{mod } p)$.

Твърдението е очевидно при $p = 2$ и $p = 3$. Нека $p \geq 5$. От горното разсъждение следва, че числата от множеството $\{2, 3, \ldots, p-2\}$ се разделят на $\dfrac{p-3}{2}$ непресичащи се двойки (k_1, k_1'), (k_2, k_2'), $\ldots$, $(k_{\frac{p-3}{2}}, k'_{\frac{p-3}{2}})$, за които

$$k_i k_i' \equiv 1 (\text{mod } p),$$

$i = 1, 2, \ldots, \dfrac{p-3}{2}$. Умножаваме всички тези сравнения и получаваме

$$(p-2)! \equiv 1 (\text{mod } p),$$

от което след умножаване на двете страни с $p-1$ получаваме исканото

$$(p-1)!+1 \equiv 0(\text{mod } p).$$

(Достатъчност) Нека за естественото число p е изпълнено сравнението $(p-1)!+1 \equiv 0(\text{mod } p)$. Очевидно $p > 1$. Да допуснем, че p не е просто. Тогава p има прост делител q, за който $1 < q < p$. Оттук следва, че $(p-1)!+1 \equiv 0(\text{mod } q)$, защото q дели p, и $(p-1)! \equiv 0(\text{mod } q)$, защото q е един от множителите в $(p-1)!$. От последните две сравнения обаче следва, че $1 \equiv 0(\text{mod } q)$, т.е. q дели 1 – противоречие.

Теорема 2. Нека p е нечетно просто число. Сравнението

$$x^2+1 \equiv 0(\text{mod } p)$$

има решение тогава и само тогава, когато $p \equiv 1(\text{mod } 4)$.

Доказателство: (Необходимост) Нека $x^2+1 \equiv 0(\text{mod } p)$ и да допуснем, че $p \equiv 3(\text{mod } 4)$. Тогава числото $\dfrac{p-1}{2}$ е нечетно и, повдигайки двете страни на сравнението $x^2 \equiv -1(\text{mod } p)$ на степен $\dfrac{p-1}{2}$, получаваме $x^{p-1} \equiv -1(\text{mod } p)$, което противоречи на Теоремата на Ферма.

(Достатъчност) Нека $p = 4k+1$. Тогава от Теоремата на Уилсън следва, че

$$0 \equiv (4k)!+1 = (2k)!(p-2k)(p-(2k-1))\ldots(p-1)+1 \equiv [(2k)!]^2+1(\text{mod } p),$$

т.е. числото $x = \left(\dfrac{p-1}{2}\right)!$ е решение на сравнението $x^2+1 \equiv 0(\text{mod } p)$.

Близнаци прости числа

Ако числата p и $p+2$ са едновременно прости, те се наричат близнаци. Теоремата на Уилсън дава критерий за проверка дали две последователни нечетни числа са близнаци прости числа.

Теорема 3. Естествените числа $p \geq 3$ и $p+2$ са едновременно прости тогава и само тогава, когато

$$4[(p-1)!+1]+p \equiv 0(\text{mod } p(p+2)).$$

Доказателство: (Необходимост) Нека p и $p+2$ са прости числа. Лесно се вижда, че сравнението от Теоремата на Уилсън за p е еквивалентно на

$$4[(p-1)!+1]+p \equiv 0(\text{mod } p)$$

(умножете по 4 и добавете p отляво).

От Теоремата на Уилсън за $p+2$ имаме $(p+1)!+1 \equiv 0(\text{mod } p+2)$, откъдето след умножение по 2 и с помощта на $p(p+1) \equiv 2(\text{mod } p+2)$ получаваме $4(p-1)!+2 \equiv 0(\text{mod } p+2)$. Последното е еквивалентно на $4[(p-1)!+1]+p \equiv 0(\text{mod } p+2)$ (добавете $p+2$ отляво).

Тъй като p и $p+2$ са взаимно прости, получаваме исканото

$$4[(p-1)!+1]+p \equiv 0(\text{mod } p(p+2)).$$

(Достатъчност) Нека $4[(p-1)!+1]+p \equiv 0(\text{mod } p(p+2))$. Тъй като $(p,4)=1$, по модул p получаваме $(p-1)!+1 \equiv 0(\text{mod } p)$, т.е. p е просто число съгласно Теоремата на Уилсън.

Както по-горе по модул $p+2$ получаваме $2(p+1)!+2 \equiv 0(\text{mod } p+2)$, което е еквивалентно на $(p+1)!+1 \equiv 0(\text{mod } p+2)$, т.е. $p+2$ е просто.

19. Квадратични остатъци. Критерий на Ойлер

Квадратични остатъци

Нека $p > 2$ е просто число и да разгледаме сравнението от втора степен

$$c_0x^2 + c_1x + c_2 \equiv 0(\text{mod } p), \tag{7}$$

където $(p, c_0) = 1$. Знаем, че такова сравнение има не повече от две решения. Отначало ще представим (1) в по-удобен вид.

Лема 1. Сравнението (1) е еквивалентно на сравнение от вида

$$(x + c)^2 \equiv a(\text{mod } p).$$

Доказателство: Тъй като $(c_0, p) = 1$, след умножаване на двете страни например с c_0^{p-2} получаваме еквивалентното сравнение

$$x^2 + b_1x + b_2 \equiv 0(\text{mod } p)$$

(това е всъщност Лема 1 за $n = 2$ от Въпрос 14).

По-нататък, ако числото b_1 е четно, с отделяне на точен квадрат получаваме еквивалентното сравнение

$$\left(x + \frac{b_1}{2}\right)^2 \equiv \frac{b_1^2}{4} - b_2(\text{mod } p),$$

а ако b е нечетно, то $b_1 + p$ е четно и тогава (1) е еквивалентно на

$$\left(x + \frac{b_1 + p}{2}\right)^2 \equiv \frac{(b_1 + p)^2}{4} - b_2(\text{mod } p).$$

В еквивалентното сравнение от Лема 2 можем да положим $x+c = y$. Следователно е достатъчно да разглеждаме само сравнения от вида

$$x^2 \equiv a(\text{mod } p).$$

Нещо повече, за последното сравнение е очевидно, че ако класът $\overline{x_0}$ е негово решение, то и класът $\overline{-x_0}$ е решение, като двата класа са различни, понеже $p > 2$. Следователно сравнението (1) или няма решение, или има точно две решения, като това зависи от p и a (защото няма от какво друго да зависи).

Дефиниция 1. Цялото число a се нарича *квадратичен остатък (неостатък) по модул* p, ако сравнението $x^2 \equiv a(\text{mod } p)$ има (няма) решение. Ако a е квадратичен остатък (неостатък) по модул p, то класът $\overline{a}$ се нарича *клас квадратични остатъци (неостатъци) по модул* p.

Например от Теорема 2 от предишния въпрос следва, че -1 е квадратичен остатък по модул p тогава и само тогава, когато $p \equiv 1(\text{mod } 4)$. Един подход за намиране на отговор на въпроса дали дадено число е квадратичен остатък по даден прост модул е предложен от Ойлер.

Критерий на Ойлер

Преди да разгледаме критерия на Ойлер, ще докажем едно помощно твърдение. Съгласно Теорема 2 от Въпрос 14 при решаването на сравнението $x^2 - a \equiv 0(\text{mod } p)$ трябва да разделим $x^{p-1} - 1$ на $x^2 - a$ с частно и остатък.

Лема 2. Остатъкът от делението на $x^{p-1} - 1$ на $x^2 - a$ е константата $a^{\frac{p-1}{2}} - 1$.

Доказателство: В делението с частно и остатък

$$y^{\frac{p-1}{2}} - 1 = (y - a)g(y) + r$$

имаме $r = a^{\frac{p-1}{2}} - 1$ съгласно Теоремата на Безу. Полагаме $y = x^2$ и получаваме

$$x^{p-1} - 1 = (x^2 - a)g(x^2) + a^{\frac{p-1}{2}} - 1,$$

т.е. търсеният остатък е константата $a^{\frac{p-1}{2}} - 1$.

Теорема 1. (Критерий на Ойлер) Нека $p > 2$ е просто число. Числото a, $(a, p) = 1$, е квадратичен остатък по модул p тогава и само тогава, когато

$$a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p).$$

Доказателство: Съгласно Теорема 2 от Въпрос 14 сравнението

$$x^2 \equiv a (\text{mod } p)$$

има точно две решения, когато всички коефициенти на остатъка при деление на $x^{p-1} - 1$ на $x^2 - a$ се делят на p. Сега твърдението следва от Лема 2.

Теорема 2. Ако $p > 2$ е просто число, то броят на квадратичните остатъци по модул p е равен на броя на квадратичните неостатъци по модул p (т.е. числата $1, 2, \ldots, p-1$ се разделят на две групи с по $\dfrac{p-1}{2}$ елемента – квадратични остатъци и неостатъци).

Доказателство: Достатъчно е да докажем, че различните квадратични остатъци измежду числата $1, 2, \ldots, p-1$ са точно $\dfrac{p-1}{2}$.

От критерия на Ойлер следва, че квадратичните остатъци са точно решенията на сравнението

$$x^{\frac{p-1}{2}} \equiv 1 (\text{mod } p).$$

Следователно техният брой е равен на броя на решенията на това сравнение. Но остатъкът от делението на $x^{p-1} - 1$ на $x^{\frac{p-1}{2}} - 1$ е равен на 0, защото

$$x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right).$$

Съгласно Теорема 2 от Въпрос 14, решенията на $x^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ са точно $\dfrac{p-1}{2}$, с което твърдението е доказано.

Теорема 3. Числата $1^2, 2^2, \ldots, \dfrac{(p-1)^2}{4}$ образуват пълна система от квадратични остатъци по модул p.

Доказателство: Очевидно $1^2, 2^2, \ldots, \dfrac{(p-1)^2}{4}$ са квадратични остатъци. Освен това техният брой е точно $\dfrac{p-1}{2}$ и остава да докажем, че те са представители на различни класове остатъци по модул p. Ако допуснем, че $a^2 - b^2$ се дели на p, то p дели поне едно от числата $a - b$ и $a + b$, което е невъзможно, когато a и b са различни числа измежду $1, 2, \ldots, \dfrac{p-1}{2}$.

20. Символ на Льожандър. Закон за реципрочност

Символ на Льожандър

Символът на Льожандър създава удобства при определяне дали дадено число е квадратичен остатък или неостатък.

Дефиниция 1. Нека $p > 2$ е просто число и $(a, p) = 1$. Числото

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ако } a \text{ е квадратичен остатък по модул } p \\ -1, & \text{ако } a \text{ е квадратичен неостатък по модул } p \end{cases}$$

се нарича *символ на Льожандър*.

Например имаме $\left(\frac{1}{p}\right) = 1$ за всяко p, $\left(\frac{-1}{p}\right) = 1$, когато $p \equiv 1 (\text{mod } 4)$ и $\left(\frac{-1}{p}\right) = -1$, когато $p \equiv 3 (\text{mod } 4)$. По-общо, от Дефиниция 2 получаваме следните елементарни свойства на символа на Льожандър.

Лема 1. а) Ако $a \equiv b (\text{mod } p)$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

б) $\left(\frac{a^2}{p}\right) = 1$.

в) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$ (това всъщност е друг запис на критерия на Ойлер).

г) $\left(\frac{a_1 a_2 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \dots \left(\frac{a_n}{p}\right)$.

д) Ако $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, то $\left(\frac{ab}{p}\right) = 1$ (т.е. произведението на два квадратични остатъка (неостатъка) винаги е квадратичен остатък).

Доказателство: а) и б) следват директно от дефиницията за символа на Льожандър.

в) Ако a е квадратичен остатък, твърдението е преформулировка на критерия на Ойлер. Ако a е квадратичен неостатък, трябва да докажем, че $a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$. Имаме

$$p | a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$$

и тъй като p е взаимно просто с първия множител съгласно кретирия на Ойлер, получаваме, че p дели $a^{\frac{p-1}{2}} + 1$, което е еквивалентно на исканото.

г) Следва от в).

д) Следва от г).

Символът на Льожандър се използва при формулировката на следното важно свойство, което ще приведем без доказателство.

Теорема 1. (Закон за реципрочност) Ако p и q са нечетни прости числа, то

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

21. Мултипликативни функции

Дефиниция 1. Всяка ненулева функция $f : \mathbf{N} \to \mathbf{R}$ се нарича аритметична. Ако една аритметична функция удовлетворява равенството

$$f(mn) = f(m)f(n)$$

за всички естествени взаимно прости m и n, тя се нарича *мултипликативна*.

Например функцията на Ойлер $\varphi(n)$ е мултипликативна.

Теорема 1. Ако $f(n)$ е мултипликативна функция, то $f(1) = 1$.

Доказателство: Нека a е естествено число, за което $f(a) \neq 0$. Тогава

$$f(a) = f(a.1) = f(a)f(1),$$

откъдето следва, че $f(1) = 1$.

Теорема 2. Ако $f_1, f_2, \ldots, f_k$ са мултипликативни функции, то тяхното произведение $f_1 f_2 \ldots f_k$ също е мултипликативна фунция.

Доказателство: По индукция или директно – ако $(m, n) = 1$, то

$$\begin{aligned}(f_1 f_2 \ldots f_k)(mn) &= f_1(mn)f_2(mn)\ldots f_k(mn) = f_1(m)f_1(n)\ldots f_k(m)f_k(n) = \\ &= (f_1 f_2 \ldots f_k)(m)(f_1 f_2 \ldots f_k)(n).\end{aligned}$$

Дефиниция 2. За всяко естествено n означаваме с $\tau(n)$ броят на различните естествени делители на n.

Функцията $\tau(n)$ е аритметична. Имаме например $\tau(2) = \tau(3) = \tau(5) = 2$ и изобщо $\tau(p) = 2$, ако p е просто, $\tau(4) = \tau(9) = 3$, $\tau(6) = \tau(8) = \tau(10) = 4$, $\tau(12) = 6$ и т.н.

Теорема 3. Ако $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ е каноничното разлагане на n, то

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1).$$

Доказателство: Всеки делител на n има канонично разлагане $p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, където $0 \leq \beta_i \leq \alpha_i$ за всяко $i = 1, 2, \ldots, k$. Всеки показател β_i може да се избере по $\alpha_i + 1$ начина. От правилото за умножение на възможностите следва, че броят на всички различни делители е $(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1)$, с което твърдението е доказано.

Следствие 1. Аритметичната функция $\tau(n)$ е мултипликативна.

Доказателство: Ако $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и $n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$ са взаимно прости, то измежду числата $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_s$ няма съвпадащи. Тогава каноничното разлагане на mn е $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$, откъдето съгласно Теорема 3 числата $\tau(mn)$ и $\tau(m)\tau(n)$ са равни на

$$(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1)(\beta_1 + 1)(\beta_2 + 1)\ldots(\beta_s + 1).$$

Нека $\nu(n)$ е броят на различните прости делители на естественото число n (като $\nu(1) = 0$ по дефиниция). Тогава лесно се вижда, че $\nu(mn) = \nu(m) + \nu(n)$ за взаимно прости m и n, откъдето например следва, че функцията $2^{\nu(n)}$ е мултипликативна.

22. Функция-сума

Дефиниция 1. Ако $f(n)$ е аритметична функция, то функцията

$$F(n) = \sum_{d|n} f(d)$$

се нарича *функция-сума* на $f(n)$.

Очевидно функцията-сума е аритметична функция.

Теорема 2. Функцията-сума $F(n)$ е мултипликативна тогава и само тогава, когато $f(n)$ е мултипликативна.

Доказателство: Нека $f(n)$ е мултипликативна. Вече отбелязахме, че $F(n)$ е аритметична функция. Имаме $F(1) = f(1) = 1$. Нека m и n са взаимно прости, $a_1, a_2, \ldots, a_k$ са всички различни делители на m и $b_1, b_2, \ldots, b_l$ са всички различни делители на n. Тогава всеки две от числата a_i и b_j, $1 \leq i \leq k$, $1 \leq j \leq l$, са взаимно прости и следователно всички различни делители на mn са произведенията $a_i b_j$ за $1 \leq i \leq k$ и $1 \leq j \leq l$. Имаме

$$\begin{aligned} F(m)F(n) &= \left[\sum_{i=1}^{k} f(a_i)\right]\left[\sum_{j=1}^{l} f(b_j)\right] = \\ &= \sum_{i,j} f(a_i)f(b_j) = \sum_{i,j} f(a_i b_j) = F(mn), \end{aligned}$$

т.е. $F(n)$ също е мултипликативна функция.

Нека функцията-сума $F(n)$ е мултипликативна. Тогава $1 = F(1) = f(1)$ и следователно $f(m.1) = f(m)f(1)$ за всяко m. Трябва да докажем, че за всяко естествено $n = n_1 n_2$, където $(n_1, n_2) = 1$, имаме $f(n) = f(n_1)f(n_2)$. Това е вярно при просто n, в частност при $n = 1, 2, 3$. Нека $n \geq 4$ и твърдението е вярно за всяко число, по-малко от n.

Ако d е делител на n, той може да се запише във вида $d_1 d_2$, където d_1 и d_2 са делители съответно на n_1 и n_2 (в частност, $(d_1, d_2) = 1$). Следователно

$$\begin{aligned} \sum_{d_1|n_1, d_2|n_2} f(d_1 d_2) &= \sum_{d|n} f(d) = F(n) = F(n_1 n_2) = F(n_1)F(n_2) = \\ &= \left[\sum_{d_1|n_1} f(d_1)\right]\left[\sum_{d_2|n_2} f(d_2)\right] = \sum_{d_1|n_1, d_2|n_2} f(d_1)f(d_2). \end{aligned}$$

В първата и последната от горните суми съгласно индукционното предположение имаме $f(d_1 d_2) = f(d_1)f(d_2)$ за всички събираеми, за които $d_1 d_2 < n$. След унищожаването на тези събираеми ще останат само $f(n_1 n_2)$ отляво и $f(n_1)f(n_2)$ отдясно, т.е. $f(n_1 n_2) = f(n_1)f(n_2)$, с което индукцията е завършена.

Теорема 2. Ако $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ е каноничното разлагане на n и $f(n)$ е мултипликативна функция, то за функцията-сума $F(n)$ е в сила равенството

$$F(n) = \prod_{i=1}^{k} \left[1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i})\right].$$

Доказателство: Тъй като $F(n)$ е мултипликативна функция съгласно Теорема 1, достатъчно е да докажем твърдението за $n = p^s$, където p е просто число. Но тъждеството

$$F(p^s) = 1 + f(p) + f(p^2) + \cdots + f(p^s)$$

следва директно от Дефиниция 1.

Следствие 1. За всяко естествено число n е в сила равенството

$$\sum_{d|n} \varphi(d) = n.$$

Доказателство: Съгласно Теорема 2 за функцията-сума (която е лявата страна на доказваното тъждество) на функцията на Ойлер $\varphi(n)$ имаме

$$\begin{aligned} F(n) &= \prod_{i=1}^{k} \left[1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i}\right] = \\ &= \prod_{i=1}^{k} \left[1 + (p_i - 1) + p_i(p_i - 1) + \cdots + p_i^{\alpha_i - 1}(p_i - 1)\right] = \prod_{i=1}^{k} p_i^{\alpha_i} = n, \end{aligned}$$

с което твърдението е доказано.

23. Сума от естествените делители на естествено число. Съвършени числа

Сума от естествените делители на естествено число

Дефиниция 1. За всяко естествено число n означаваме със $\sigma(n)$ сумата от всички различни естествени делители на n.

Например имаме $\sigma(2) = 3$, $\sigma(3) = 4$ (по-общо, $\sigma(p) = p+1$ за всяко просто p), $\sigma(4) = 7$, $\sigma(6) = 12$, $\sigma(28) = 56$ и т.н.

Теорема 1. Функцията $\sigma(n)$ е мултипликативна.

Доказателство: Нека m и n са взаимно прости естествени числа и $a_1 = 1, a_2, \ldots, a_k = m$ и $b_1 = 1, b_2, \ldots, b_l = n$ са всички естествени делители съответно на m и n. Тогава $a_i b_j$, $1 \leq i \leq k$, $1 \leq j \leq l$ са всички делители на mn. Имаме

$$\begin{aligned} \sigma(m)\sigma(n) &= (a_1 + a_2 + \cdots + a_k)(b_1 + b_2 + \cdots + b_l) = \\ &= \sum_{i,j} a_i b_j = \sigma(mn). \end{aligned}$$

Теорема 2. Ако $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ е каноничното разлагане на n, то

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Доказателство: От мултипликативността следва, че е достатъчно да докажем твърдението за $n = p^s$. Делителите на p^s са $1, p, p^2, \ldots, p^s$ и тяхната сума е

$$\sigma(p^s) = 1 + p + p^2 + \cdots + p^s = \frac{p^{s+1} - 1}{p - 1}.$$

Съвършени числа

Дефиниция 2. Естественото число n се нарича *съвършено*, ако $\sigma(n) = 2n$. С други думи, n е съвършено, ако е равно на сумата от делителите си, различни от n.

Например числата 6 и 28 са съвършени.

Теорема 3. Не съществуват съвършени числа от вида p^x, където p е просто число, а x е естествено число.

Доказателство: Ако допуснем, че p^x е съвършено за някое просто p, то съгласно Теорема 2 е изпълнено равенството

$$\sigma(p^x) = \frac{p^{x+1} - 1}{p - 1} = 2p^x \iff p^{x+1} - 1 = 2p^x(p - 1).$$

Последното равенство обаче е невъзможно, защото от него следва, че p дели 1.

Теорема 4. Не съществуват нечетни съвършени числа от вида $p^x q^y$, където p и q са прости числа, а x и y са естествени числа.

Доказателство: Да допуснем, че $n = p^x q^x$ е съвършено число (p и q са различни прости, x и y са естествени). Съгласно Теорема 2 имаме равенството

$$\frac{p^{x+1} - 1}{p - 1} \frac{q^{y+1} - 1}{q - 1} = 2p^x q^y.$$

Тъй като p не дели $\dfrac{p^{x+1}-1}{p-1}$, заключаваме, че p^x дели $\dfrac{q^{x+1}-1}{q-1}$. От друга страна, аналогично разсъждение показва, че $\dfrac{q^{x+1}-1}{q-1}$ дели $2p^x$. Следователно $\dfrac{q^{x+1}-1}{q-1}$ е равно на едно от числата p^x и $2p^x$. Аналогично получаваме, че $\dfrac{p^{x+1}-1}{p-1}$ е равно на едно от числата q^y и $2q^y$.

Да разгледаме например случая, в който са в сила равенствата

$$p^{x+1}-1 = q^y(p-1) \quad \text{и} \quad q^{y+1}-1 = 2p^x(q-1).$$

От тях по модул p получаваме съответно $q^y \equiv 1 (\mathrm{mod}\ p)$ и $q^{y+1} \equiv 1 (\mathrm{mod}\ p)$. Следователно $q \equiv 1 (\mathrm{mod}\ p)$ и, в частност, $q > p$.

Аналогично по модул q получаваме $p \equiv 2 (\mathrm{mod}\ q)$, откъдето поради $p < q$ следва, че $p = 2$. Последното противоречи на нечетността на $p^x q^y$, с което твърдението е доказано.

Теорема 5. Едно четно число n е съвършено тогава и само тогава, когато $n = 2^x(2^{x+1}-1)$, където x е такова естествено число, че $2^{x+1}-1$ е просто число.

Доказателство: Ако $n = 2^x(2^{x+1}-1)$, където $2^{x+1}-1$ е просто число, по формулата от Теорема 2 имаме

$$\sigma(n) = \sigma(2^x)\sigma(2^{x+1}-1) = (2^{x+1}-1)(2^{x+1}-1+1) = 2^{x+1}(2^{x+1}-1) = 2n,$$

т.е. n е четно съвършено число.

Нека n е четно съвършено число. Да представим n във вида $n = 2^x m$, където m е нечетно число. Тогава

$$2n = \sigma(n) = \sigma(2^x)\sigma(m) = (2^{x+1}-1)\sigma(m),$$

откъдето $2^{x+1}m = (2^{x+1}-1)\sigma(m)$. Следователно $2^{x+1}-1$ дели m. Нека $m = (2^{x+1}-1)k$, където k е нечетно число. След съкращаване на $2^{x+1}-1$ получаваме $\sigma(m) = 2^{x+1}k$.

Но ако $k > 1$, то 1, k и m са различни делители на m. Тогава

$$\sigma(m) \geq 1 + k + m = 1 + k + (2^{x+1}-1)k = 1 + 2^{x+1}k > 2^{x+1}k,$$

което противоречи на равенството $\sigma(m) = 2^{x+1}k$. Следователно $k = 1$, $m = (2^{x+1}-1)k$ и $\sigma(m) = 2^{x+1} = m + 1$. От последното равенство следва, че m е просто число.

Простите числа от вида $2^k - 1$ се наричат числа на Мерсен. Първите четири числа на Мерсен са $2^2-1 = 3$, $2^3-1 = 7$, $2^5-1 = 31$ и $2^7-1 = 127$. Тогава съгласно Теорема 5 първите четири четни съвършени числа са $2(2^2-1) = 6$, $2^2(2^3-1) = 28$, $2^4(2^5-1) = 496$ и $2^6(2^7-1) = 4064$.

Въпреки привидната си простота, два важни въпроса стоят открити:

(1) не е известно дали има нечетни съвършени числа,

(2) не е известно дали четните съвършени числа са краен брой (по-точно, не е известно дали числата на Мерсен са безбройно много).

24. Функцията $[x]$

Функциите $[x]$ и $\{x\}$

Дефиниция 1. Функцията, която на всяко реално число x съпоставя най-голямото цяло число, което не надминава x, се нарича *цяла част на x* и стойностите ѝ се означават с $[x]$.

Например имаме $[n] = n$ за всяко цяло число n, $\left[\dfrac{2}{3}\right] = 0$, $[-1.25] = -2$, $[\pi] = 3$ и т.н. Лесно се вижда, че $[n + x] = n + [x]$ за всяко цяло n и реално x.

От Дефиниция 1 следва, че $[x]$ е равно на единственото цяло число n, за което $n \leq x < n + 1$. Да отбележим още, че $[x]$ е единственото цяло число, за което $x - 1 < [x] \leq x$.

Ако a и $b > 0$ са цели числа и $a = bq + r$ по теоремата за деление с частно и остатък, то

$$\left[\frac{a}{b}\right] = \left[\frac{bq+r}{b}\right] = \left[q + \frac{r}{b}\right] = q + \left[\frac{r}{b}\right] = q,$$

защото $0 \leq \frac{r}{b} \leq \frac{b-1}{b} < 1$.

Дефиниция 2. Функцията, която на всяко реално число x съпоставя числото $x - [x]$, се нарича *дробна част на* x и стойностите ѝ се означават с $\{x\}$.

От Дефиниции 1 и 2 следва, че $x = [x] + \{x\}$ за всяко реално число x.

Свойства на $[x]$

Теорема 1. За всеки две реални числа a и b е в сила неравенството

$$[a] + [b] \leq [a + b].$$

Доказателство: От $[a] \leq a$ и $[b] \leq b$ следва, че $[a] + [b] \leq a + b$. Следователно $[a] + [b]$ е цяло число, което не надминава $a + b$. Тъй като $[a + b]$ е най-голямото такова цяло число, получаваме $[a] + [b] \leq [a + b]$.

Теорема 2. За всяко реално число x и всяко естествено число n е в сила равенството

$$\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right].$$

Доказателство: Имаме

$$\frac{x}{n} = \frac{[x] + \{x\}}{n} = \frac{[x]}{n} + \frac{\{x\}}{n} = \left[\frac{[x]}{n}\right] + \frac{k}{n} + \frac{\{x\}}{n},$$

където k е цяло число и $0 \leq k \leq n - 1$ (всъщност k е остатъкът при деление на $[x]$ на n). Тъй като

$$\frac{k}{n} + \frac{\{x\}}{n} = \frac{k + \{x\}}{n} < \frac{n - 1 + 1}{n} = 1,$$

получаваме $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$.

Теорема 3. Ако m и n са естествени числа, то числото $\left[\frac{m}{n}\right]$ е равно на броя на естествените числа, ненадминаващи m и кратни на n.

Доказателство: Както отбелязахме по-горе, $\left[\frac{m}{n}\right] = q$, където $m = nq + r$ по теоремата за деление с частно и остатък. От друга страна, естествените числа, ненадминаващи m и кратни на n са $n, 2n, \ldots, qn$ – точно q на брой.

Теорема 4. За всяко реално число x е в сила равенството

$$\left[x + \frac{1}{2}\right] = [2x] - [x].$$

Доказателство: Ще разгледаме два случая.

Случай 1. Ако $0 \le \{x\} < \frac{1}{2}$, то

$$\left[x + \frac{1}{2}\right] = \left[[x] + \{x\} + \frac{1}{2}\right] = [x],$$

защото $0 < \{x\} + \frac{1}{2} < 1$. От друга страна,

$$[2x] - [x] = [2([x] + \{x\})] - [x] = [2[x] + 2\{x\}] - [x] = 2[x] - [x] = [x],$$

защото $0 \le 2\{x\} < 1$.

Случай 2. Ако $\frac{1}{2} \le \{x\} < 1$, то

$$\left[x + \frac{1}{2}\right] = \left[[x] + \{x\} + \frac{1}{2}\right] = [[x] + 1 + (\{x\} + \frac{1}{2} - 1)] = [x] + 1,$$

защото $0 \le \{x\} - \frac{1}{2} < 1$. От друга страна,

$$[2x] - [x] = [2([x] + \{x\})] - [x] = [2[x] + 2\{x\}] - [x] = 2[x] + 1 - [x] = [x],$$

защото $1 \le 2\{x\} < 2$.

Теорема 5. За всеки три естествени числа a, b и c е в сила равенството

$$\left[\frac{\left[\frac{c}{a}\right]}{b}\right] = \left[\frac{c}{ab}\right].$$

Доказателство: Твърдението следва директно то Теорема 2, но ще приведем и друго доказателство.

Нека $c = qa + r$ и $q = q_1 b + r_1$ съгласно теоремата за деление с частно и остатък. Тогава $\left[\frac{c}{a}\right] = q$ и $\left[\frac{q}{b}\right] = q_1$, т.е. лявата страна е равна на q_1.

Имаме $c = qa + r = a(q_1 b + r_1) + r = abq_1 + ar_1 + r$ и следователно е достатъчно да докажем, че $ar_1 + r$ е остатъкът при деление на c на ab. Последното следва от $0 \le ar_1 + r \le a(b-1) + (a-1) = ab - 1 < ab$.

Теорема 6. За всеки две реални числа a и b е в сила неравенството

$$[2a] + [2b] \ge [a] + [b] + [a + b].$$

Доказателство: Нека $a = [a] + \alpha$ и $b = [b] + \beta$, където $\alpha = \{a\}$ и $\beta = \{b\}$ за краткост. Тогава $0 \le \alpha < 1$, $0 \le \beta < 1$ и

$$\begin{aligned} [2a] + [2b] &= [2[a] + 2\alpha] + [2[b] + 2\beta] = 2[a] + 2[b] + [2\alpha] + [2\beta], \\ [a] + [b] + [a + b] &= [a] + [b] + [a] + [b] + [\alpha + \beta]. \end{aligned}$$

Следователно е достатъчно да докажем, че

$$[2\alpha] + [2\beta] \ge [\alpha + \beta].$$

Ако $0 \le \alpha + \beta < 1$, дясната страна е равна на 0, а лявата е неотрицателна, т.е. неравенството е изпълнено. Ако $1 \le \alpha + \beta < 2$, то дясната страна е равна на 1, а лявата е поне 1, защото поне едно от числата α и β е по-голямо или равно на $\frac{1}{2}$.

Теорема 7. Ако p е просто, а n е естествено число, то степенният показател на p в каноничното разлагане на $n!$ е

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots .$$

Доказателство: Да отбележим първо, че последната сума е крайна, защото от известно място нататък (даже отначало, ако $p>n$) всички събираеми са равни на 0.

Нека t_i, $i=1,2,3,\ldots$, е броят на числата измежду $1,2,\ldots,n$, които се делят на p^i. Тогава търсеният степенен показател е $t_1+t_2+t_3+\cdots$ (ако $k\in\{1,2,\ldots,n\}$ се дели на p^i, но не се дели на p^{i+1}, то е преброено в тази сума точно i пъти – по веднъж в $t_1,t_2,\ldots,t_i$) и е достатъчно да намерим последната сума. От Теорема 3 обаче следва, че $t_i=\dfrac{n}{p^i}$, с което доказателството е завършено.

Теорема 2 има многобройни приложения. Да разгледаме два прости примера.

Пример 1. Да намерим каноничното разлагане на 10!. Тъй като простите делители на 10! са 2, 3, 5 и 7, съответните степенни показатели се намират с помощта на Теорема 2:

$$\left[\frac{10}{2}\right]+\left[\frac{10}{2^2}\right]+\left[\frac{10}{2^3}\right]=5+2+1=8,$$

$$\left[\frac{10}{3}\right]+\left[\frac{10}{3^2}\right]=3+1=4,\ \left[\frac{10}{5}\right]=2,\ \left[\frac{10}{7}\right]=1.$$

Следователно $10!=2^8.3^4.5^2.7$.

Пример 2. Числото $\dfrac{(m+n)!}{m!n!}$ е цяло за произволни естествени m и n, защото за всяко просто p и за всяко естествено i имаме

$$\left[\frac{m+n}{p^i}\right]\geq\left[\frac{m}{p^i}\right]+\left[\frac{n}{p^i}\right]$$

съгласно Теорема 1 от предишния въпрос. Действително, от последното неравенство следва, че степенният показател на p в разлагането на $(m+n)!$ е по-голям или равен на съответния показател в $m!n!$. Аналогично се доказва (с помощта на Теорема 6 от предишния въпрос), че числото $\dfrac{(2m)!(2n)!}{m!n!(m+n)!}$ е цяло за произволни естествени m и n.

25. Метод на безкрайното спускане. Решения в цели числа на уравненията $x^2+y^2=z^2$ и $x^4+y^4=z^2$

Методът на безкрайното спускане[3] е използван строго за пръв път от Ферма, но подобни подходи са могат да се намерят още при Евклид. По същество този метод е близък до индукционно разсъждение.

Задача 1. Да се докаже, че уравнението $x^3+2y^3=4z^3$ няма други решения в цели числа, освен $x=y=z=0$.

Решение. Ясно е, че x е четно число. Да положим $x=2x_1$ и да заместим в уравнението. Получаваме $4x_1^3+y^3=2z^3$, откъдето следва, че $y=2y_1$ е четно число. Тогава $2x_1^3+4y_1^3=z^3$ и значи и $z=2z_1$ е четно число, т.е. $x_1^3+2y_1^3=4z_1^3$.

Получихме уравнение от същия вид и е ясно, че можем да продължим по същия начин. Това означава, че всяко от числата x, y и z се дели на произволно висока степен на 2, което е възможно само при $x=y=z=0$.

[3] Infinite descent

Не е трудно да се съобрази, че вариант на горното разсъждение е следното: да допуснем, че има ненулеви решения и да изберем решение, при което $|x| > 0$ е възможно най-малко (съобразете, че можем да считаме, че $x \neq 0$). Тогава ще получим решение с $|x|/2$, което портиворечи на допускането.

Задача 2. Да се докаже, че уравнението $x^2 + y^2 = 3(a^2 + b^2)$ няма други решения в цели числа, освен $x = y = a = b = 0$.

Решение. От $3|x^2+y^2$ следва, че $3|x$ и $3|y$, откъдето получаваме уравнението $3(x_1^2+y_1^2) = a^2+b^2$. Аналогично имаме $3|a$ и $3|b$, $x_1^2 + y_1^2 = 3(a_1^2 + b_1^2)$ и т.н. Следователно всяко от числата x, y, a и b се дели на произволно висока степен на 3, което е възможно само при $x = y = a = b = 0$.

Да разгледаме задачата за намиране на целите решения на уравнението $x^2 + y^2 = z^2$. Тройките $(a, 0, a)$ и $(0, a, a)$ са тривиални решения и по-нататък ще се интересуваме само от ненулевите решения.

Ако (a, b, c) е решение, за което $a = da_1$, $b = db_1$ и $c = dc_1$, където $d > 1$ е естествено число, то (a_1, b_1, c_1) също е решение. Следователно можем да считаме, че $(a, b, c) = 1$. Всяко такова решение се нарича *примитивна питагорова тройка*. Очевидно е, че в примитивна питагорова тройка всеки две числа са взаимно прости (в противен случай общият им делител ще дели и третото число поради равенството $a^2 + b^2 = c^2$).

Ясно е, че ако (a, b, c) е приметивна питагорова тройка, то едно от числата a и b е четно, а другото и c са нечетни. Нека a е четно, а b и c са нечетни.

Лема 1. Ако $a^2 = mn$, където m и n са взаимно прости естествени числа, то m и n са точни квадрати.

Доказателство: За произволно просто число p да означим съответно с a_p, m_p и n_p степенните показатели на p в каноничните разлагания на a, m и n. Тогава от равенството $a^2 = mn$ получаваме $2a_p = m_p + n_p$.

Следователно числата m_p и n_p имат еднаква четност. Ясно е, че те не могат да бъдат нечетни, защото тогава m и n няма да са взаимно прости. Тогава m_p и n_p са четни, което означава, че m и n са точни квадрати. Нещо повече, не е възможно едновременно m_p и n_p да са положителни (четни). Следователно $m_p = 0$ или $n_p = 0$.

От равенството

$$a^2 = (c - b)(c + b)$$

следва, че числата $b - c$ и $b + c$ имат най-голям общ делител 2 (защото техният най-голям общ делител дели сумата и разликата им) и произведението им е точен квадрат. Съгласно Лема 1 можем да запишем

$$c - b = 2u^2,\ c + b = 2v^2,$$

където u и v са естествени числа. Решаваме тази система относно b и c получаваме

$$b = v^2 - u^2,\ c = u^2 + v^2,$$

откъдето намираме и $a = 2uv$. Лесно се вижда, че $(u, v) = 1$.

Обратно, чрез непосредствена проверка се убеждаваме, че всяка тройка от вида $(2uv, v^2-u^2, u^2+v^2)$ действително е решение на уравнението $x^2 + y^2 = z^2$. Следователно е в сила следната теорема.

Теорема 1. Ако (a, b, c) е примитивна питагорова тройка, то

$$a = 2uv,\ b = v^2 - u^2,\ c = u^2 + v^2,$$

където u и v са взаимно прости естествени числа.

Да разгледаме едно класическо приложение на Теорема 1.

Теорема 2. Уравнението $x^4 + y^4 = z^2$ няма решения в естествени числа.

Доказателство: Да допуснем, че разглежданото уравнение има решения в естесвени числа и нека (x_0, y_0, z_0) е решение, за което естесвеното число z_0 е възможно най-малко. Ясно е, че $(x_0, y_0, z_0) = 1$. Ще достигнем до противоречие, като конструираме решение с по-малко z.

Тъй като $(x_0^2)^2 + (y_0^2)^2 = z_0^2$ и $(x_0, y_0, z_0) = 1$, числата x_0^2, y_0^2 и z_0 образуват питагорова тройка. Следователно съществуват естествени числа u и v, за които

$$x_0^2 = 2uv,\ y_0^2 = u^2 - v^2,\ z_0 = u^2 + v^2.$$

Тъй като $(x_0, y_0) = 1$, числата u и v са от различна четност. Тогава v е четно, а u – нечетно (в другия случай получаваме $y_0^2 \equiv -1 (\mathrm{mod}\ 4)$, което е невъзможно).

От $x_0^2 = 2uv$ следва съгласно Лема 1, че $v = 2a^2$ и $u = b^2$ за някои естествени числа a и b.

От равенството $y_0^2 + v^2 = (u^2 - v^2) + v^2 = u^2$ следва, че (y_0, v, u) е примитивна питагорова тройка. Тогава съществуват естествени числа p и q, за които

$$y_0 = p^2 - q^2,\ v = 2pq,\ u = p^2 + q^2.$$

Следователно $a^2 = pq$, откъдето съгласно Лема 1 имаме $p = s^2$ и $q = t^2$.

В крайна сметка получаваме

$$b^2 = u = p^2 + q^2 = s^4 + t^4,$$

т.е. тройката (s, t, b) е решение на уравнението. Остава да отбележим, че

$$b \leq b^2 = u < u^2 + v^2 = z_0,$$

с което доказателството е завършено.

Следствие 1. Уравнението $x^{4k} + y^{4k} = z^{4k}$ няма решения в естествени числа за никое естествено k.

26. Диофантови уравнения

Да разложим на множители

Задача 1. Да се намерят всички двойки цели числа x и y, за които $x^2 + x = 4y^2 + 4y + 3xy$.

Задача 2. (Олимпиада в Румъния, 2001) Да се намерят всички цели числа m и n, за които $9m^2 + 3n = n^2 + 8$.

Задача 3. Да се докаже, че уравнението $4xy - x - y = z^2$ няма решение в цели числа.

Задача 4. (ЗМС 2005) Да се реши в цели числа уравнението $z^2 + 1 = xy(xy + 2y - 2x - 4)$.

Задача 5. Да се намерят всички прости числа p и q, за които числото $16p^2 + 13q^2 + 5p^2q^2$ е точен квадрат.

Да разгледаме дискриминантата

Задача 6. Да се реши в цели числа уравнението $2x^2 - 2xy + 3y^2 = 2x + 2y - 1$.

Задача 7. (ПМТ Казанлък 1981) Да се намерят всички двойки цели числа a и b, за които $7a + 14b = 5a^2 + 5ab + 5b^2$.

Задача 8. (Областен кръг 2004) Да се реши в цели числа уравнението $x^3 + 10x - 1 = y^3 + 6y^2$.

Задача 9. Да се реши в цели числа уравнението $x^2 + x + 4 = y^2$.

Използване на оценки

Задача 10. Да се намерят всички цели стойности на x, за които числото $\sqrt{(x+1)(x+2)(x+3)(x+4)}$ е рационално.

Задача 11. Да се намерят всички тройки естествени числа $(x; y; z)$, за които числото $x^2 + y^2 + z^2 + 2xy + 2x(z-1) + 2y(z+1)$ е точен квадрат.

Задача 12. Да се реши в цели числа уравнението $x^3 = y^3 + 2y^2 + 1$.

Задача 13. (Пловдив, 2004) Да се намерят всички двуцифрени числа a и b, за които числата $a+b$ и $102a+b$ са точни квадрати.

Задача 14. (БОМ2005) Да се намерят всички прости числа p, за които числото p^2-p+1 е точен куб.

Задача 15. Да се реши в цели числа уравнението $x^3+x^2y+xy^2+y^3=8(x^2+xy+y^2+1)$.

Задача 16. (Московска олимпиада, 1997) Да се реши в естествени числа уравнението $a!+b!+c!=d!$.

Задача 17. (Областен кръг, 2002) Да се реши в естествени числа уравнението $x!+y!=15.2^{z!}$.

Използване на подходящи модули

Задача 18. Да се докаже, че уравнението $x^3+y^3+z^3=4$ няма решение в цели числа.

Задача 19. (БОМ 1998) Да се докаже, че уравнението $m^2=n^5-4$ няма решение в цели числа.

Задача 20. (Математика 1981) Да се докаже, че уравнението $x^4+4=y^7$ няма решения в цели числа.

Задача 21. Да се намери най-малката възможна стойност на израза $f(x,y)=|5x^2+11xy-5y^2|$, където x и y са цели числа, които не са едновременно равни на 0.

Задача 22. (НОМ 1979) Да се докаже, че уравнението $y^3=x^2+5$ няма решения в цели числа.

Отговори, упътвания и решения

Да разложим на множители

1. *Упътване.* Разгледайте уравнението като квадратно относно x и получете разлагането $(x+y+1)(x-4y)=0$. *Отговор.* $(x;0)=(4a;a)$ и $(-a-1;a)$, където a е произволно цяло число.

2. *Упътване.* Представете уравнението във вида $(6m-2n+3)(6m+2n-3)=23$. *Отговор.* $(2;7)$, $(2;-4)$, $(-2;-4)$ и $(-2;7)$.

3. *Решение.* След умножение по 4 даденото уравнение се представя във вида $(4x-1)(4y-1)=(2z)^2+1$. Числото $4x-1$ има поне един прост делител от вида $4k+3$, защото в противен случай самото то ще е от вида $4k+1$. Следователно числото $(2z)^2+1$ има прост делител от вида $4k+3$, което е невъзможно (виж Задача 13 от "Теореми на Ферма и Ойлер").

4. *Решение.* След полагането $x=u-1$, $y=v+1$ получаваме $z^2+1=(u^2-1)(v^2-1)$. Тъй като числата от вида t^2+1 не се делят на 4 (Защо?), заключаваме, че u, v и z са четни числа.

Нека $|u|>1$. Тогава $u^2-1\equiv -1 \pmod 4$ и следователно u^2-1 има прост делител p от вида $4k+3$. Следователно $z^2+1\equiv 0 \pmod p$, което е невъзможно. Аналогично се отхвърля и случая $|v|>1$. Тъй като u и v са четни числа, остава $u=v=0$, откъдето $z=0$. Окончателно $x=-1$, $y=1$, $z=0$.

5. *Решение.* Нека $n^2=16p^2+13q^2+5p^2q^2$. Ако p и q са нечетни, то $p^2\equiv q^2\equiv 1 (\mathrm{mod}\ 4)$ и получаваме, че $n^2\equiv 2 (\mathrm{mod}\ 4)$, което е невъзможно. Следователно поне едно от числата p и q е четно, т.е. $p=2$ или $q=2$.

При $p=2$ получаваме $n^2=64+33q^2$. При $q=2$ получаваме $n=14$. При $q\neq 2$ записваме равенството във вида $(n-8)(n+8)=33q^2$. Следователно едно от числата $n-8$ и $n+8$ се дели на q^2, а другото е делител на 33 (ако $q|n-8$ и $q|n+8$, то $q|16$, което е невъзможно). Тогава $n-8=1,3,11,33$ или $n+8=1,3,11,33$, откъдето $n=9,11,19,41,25$. Директна проверка показва, че решения се получават само при $n=19$ (тогава $q=3$) и при $n=41$ (тогава $q=7$).

При $q=2$ имаме $n^2=52+36p^2$, откъдето следва, че n е четно число. Полагаме $n=2n_0$ и получаваме $n_0^2=13+9p^2$, което записваме във вида $(n_0-3p)(n_0+3p)=13$. Оттук $n_0-3p=1$ и $n_0+3p=13$, т.е. $n_0=7$, $p=2$. Отново получихме решението $p=q=2$, $n=14$.

Отговор. $(p;q)=(2;2)$, $(2;3)$ и $(2;7)$.

Да разгледаме дискриминантата

6. *Упътване.* Разгледайте уравнението като квадратно относно x. Дискриминантата е неотрицателна само за краен брой цели стойности на y. *Отговор.* $x=y=1$.

7. *Упътване.* Разгледайте уравнението като квадратно относно b. *Отговор.* $(-1;3)$, $(0;0)$ и $(1;2)$.

8. *Упътване.* Означете $k = x - y$ (k е нечетно число) и запишете уравнението като квадратно относно y във вида $(3k-6)y^2 + (3k^2+10)y + k^3 + 10k - 1 = 0$. Докажете, че дискриминантата $D = -3k^4 + 24k^3 - 60k^2 + 252k + 76$ е отрицателна при $k \leq -1$ и при $k \geq 7$. *Отговор.* $(6;5)$ и $(2;-3)$.

9. *Решение.* Да запишем даденото уравнение във вида $x^2 + x + 4 + a - y^2 = a$, където a е реален параметър, който ще бъде определен по-късно. Лявата страна е квадратен тричлен на x, чиято дискриминанта е $4y^2 - 4a - 15$. Следователно е удобно да изберем $a = -\dfrac{15}{4}$ и така да намерим разлагане на лявата страна.

Получаваме

$$(x + y + \frac{1}{2})(x - y - \frac{1}{2}) = -\frac{15}{4} \iff (2x + 2y + 1)(2x - 2y - 1) = -15,$$

откъдето намираме осем решения. *Отговор.* $(-4;4)$, $(-4;-4)$, $(3;4)$, $(3;-4)$, $(-1;2)$, $(-1;-2)$, $(0;2)$ и $(0;-2)$.

Използване на оценки

10. *Решение.* Ако $\sqrt{(x+1)(x+2)(x+3)(x+4)} = y$ е рационално, то x и y са цели решения на уравнението

$$\begin{aligned}(x+1)(x+2)(x+3)(x+4) = y^2 &\iff (x^2+5x+4)(x^2+5x+6) = y^2 \\ &\iff (x^2+5x+5)^2 - 1 = y^2.\end{aligned}$$

Последното равенство е възможно само при $y = 0$ (Защо?), откъдето получаваме $x \in \{-1, -2, -3, -4\}$.

11. *Упътване.* Докажете, че $(x+y+z-1)^2 < x^2+y^2+z^2+2xy+2x(z-1)+2y(z+1) < (x+y+z+1)^2$. *Отговор.* $(x;y;z) = (a;a;b)$, където a и b са произволни естествени числа.

12. *Решение.* Очевидно имаме $x \geq y+1$. Тогава $y^3+2y^2+1 = x^3 \geq (y+1)^3$, откъдето получаваме $y^2 + 3y \leq 0$. Следователно $y \in \{-3, -2, -1, 0\}$ и директната проверка дава решенията $(x;y) = (-2;-3)$, $(1;-2$ и $(1;0)$.

13. *Решение.* Ако $a + b = u^2$ и $102a + b = v^2$, то $u < 14$ и $v < 101$. Тогава от $101a = v^2 - u^2 = (v-u)(v+u)$ и факта, че 101 е просто числа, следва, че 101 дели $v-u$ или $v+u$. Но $0 < v-u < 101$ и $0 < v+u < 200$, т.е. $u + v = 101$ и $v - u = a$. Оттук $u = \frac{101-a}{2}$, $(101-a)^2 = 4(a+b) \iff (103-a)^2 = 4(b+102)$. Следователно $b+102$ е точен квадрат и тъй като числото b е двуцифрено, получаваме следните възможности $b + 102 = 121, 144, 169$ или 196. Оттук получаваме решенията $(a;b) = (81;19)$, $(79;42)$, $(77;67)$, $(75;94)$.

14. *Решение.* Нека $p^2 - p + 1 = a^3$, т.е. $p(p-1) = (a-1)(a^2+a+1)$. Очевидно $1 < a < p$ и значи p е делител на a^2+a+1. Следователно $a^2+a+1 = bp$, $p-1 = b(a-1)$ и оттук $a^2+a+1 = b[b(a-1)+1]$. Лесно се проверява, че $b > 2$ и тогава

$$a + 1 < \frac{a^2+a+1}{a} < b^2 < \frac{a^2+a-1}{a-1} \leq a + 3,$$

откъдето $b^2 = a + 2$. Сега $a^2 + a + 1 = (a+2)(a-1) + b$, което показва, че $b = 3$, $a = 7$ и $p = 19$.

15. *Решение.* Да представим даденото уравнение във вида $(x^2+y^2)(x+y-8) = 8(xy+1)$. Оттук следва, че x и y са с еднаква четност.

Ако x и y са нечетни, то дясната страна се дели на 16, $x^2 + y^2$ се дели на 2, но не и на 4 и следователно $x + y - 8$ се дели на 8. Полагаме $x + y - 8 = 8k$, където k е цяло число, и получаваме $k(x^2 + y^2) = xy + 1$. Но $2|xy| \leq x^2 + y^2 \leq |k(x^2 + y^2)| = |xy + 1| \leq |xy| + 1$, откъдето $|xy| \leq 1$. Следователно $|x| = |y| = 1$, което не дава решение.

Нека $x = 2x_1$ и $y = 2y_1$, където x_1 и y_1 са цели числа. Тогава $(x_1^2 + y_1^2)(x_1 + y_1 - 4) = 4x_1y_1 + 1$, откъдето следва, че $x_1^2 + y_1^2$ и $x_1 + y_1 - 4$ са нечетни числа. При $|x_1 + y_1 - 4| \geq 3$ получаваме $|4x_1y_1| + 1 \geq |4x_1y_1 + 1| = |x_1^2 + y_1^2||x_1 + y_1 - 4| \geq 3(x_1^2 + y_1^2) \geq 6|x_1y_1|$, което е невъзможно.

Следователно $|x_1 + y_1 - 4| = 1$, т.е. $x_1 + y_1 = 3$ или 5. В първия случай получаваме $x_1^2 + y_1^2 + 4x_1y_1 + 1 = 0 \iff (x_1 + y_1)^2 + 2x_1y_1 + 1 = 0$, откъдето $x_1y_1 = -5$, което е невъзможно. При

$x_1 + y_1 = 5$ аналогично имаме $x_1 y_1 = 4$, откъдето $x_1 = 4$, $y_1 = 1$ или $x_1 = 1$, $y_1 = 4$. Окончателно получаваме, че решенията са $(x; y) = (8; 2)$ и $(2; 8)$.

16. *Решение.* Без ограничение на общността можем да считаме, че $a \leq b \leq c$. От уравнението следва, че $d > c$. Тогава при $c > 2$ имаме $d! \geq (c+1)! = (c+1)c! > 3c! \geq a! + b! + c!$, т.е. уравнението няма решение при $c > 2$. Следователно $a \leq b \leq c \leq 2$ и с непосредствена проверка установяваме, че уравнението има единствено решение $a = b = c = 2$, $d = 3$.

17. *Решение.* При $x \geq 6$ и $y \geq 6$ лявата страна се дели на 9, а дясната само на 3. Следователно без ограничение на общността можем да считаме, че $y \leq 5$ и $y \leq x$. Да запишем уравнението във вида $\dfrac{x!}{y!} + 1 = \dfrac{15.2^{z!}}{y!}$.

При $z = 1$ получаваме $x = 4$, $y = 3$, а при $z = 2$ уравнението няма решение. При $z \geq 3$ числителят на $\dfrac{15.2^{z!}}{y!}$ се дели на 2^6, а знаменателят се дели на 2 или 2^3. Следователно числото $\dfrac{x!}{y!} + 1$ е четно, т.е. $\dfrac{x!}{y!}$ е нечетно. Последното е възможно само при $x = y + 1$ нечетно или при $x = y$. И в двата случая лесно се вижда, че уравнението няма решение.

Отговор. $(x; y; z) = (4, 3, 1)$.

Използване на подходящи модули

18. *Упътване.* Използвайте, че кубовете на целите числа са сравними с 0 и ± 1 по модул 9.

19. *Упътване.* Разгледайте уравнението по модул 11.

20. *Решение.* Да допуснем, че уравнението има решение в цели числа. Ако x е четно числа, от уравнението следва, че y^7 се дели на 4, но не и на 8, което е невъзможно. Следователно x и y са нечетни числа. Тъй като $y^7 = x^4 + 4 = (x^2 + 2)^2 - 4x^2 = (x^2 - 2x + 2)(x^2 + 2x + 2)$ и $(x^2 + 2x + 2, x^2 - 2x + 2) = 1$, заключаваме, че $x^2 + 2x + 2 = y_1^7$ и $x^2 - 2x + 2 = y_2^7$, където y_1 и y_2 са нечетни числа, за които $y_1 y_2 = y$.

Да разгледаме по модул 7 горните уравнения, записани във вида $(x+1)^2 + 1 = y_1^7$ и $(x-1)^2 + 1 = y_2^7$. Ако $y_1 \equiv y_2 \equiv 1 (\mathrm{mod}\ 7)$, то $x + 1$ и $x - 1$ се делят на 7, което е невъзможно. Следователно едно от числата y_1 и y_2 дава остатък, различен от 1 при деление на 7. Нека това е y_1. Имаме $(x+1)^2 = (y_1 - 1)(y_1^6 + y_1^5 + \cdots + y_1 + 1)$. От представянето $y_1^6 + y_1^5 + \cdots + y_1 + 1 = (y_1^6 - 1) + (y_1^5 - 1) + \cdots + (y_1 - 1) + 7$ се вижда, че $d = (y_1 - 1, y_1^6 + y_1^5 + \cdots + y_1 + 1)$ дели 7, откъдето следва, че $d = 1$. Тогава $y_1 - 1 = a^2$ и $y_1^6 + y_1^5 + \cdots + y_1 + 1 = b^2$, където a и b са цели числа, за които $ab = x + 1$.

Тъй като y_1 е нечетно число, то a е четно. Получаваме $y_1 \equiv 1 (\mathrm{mod}\ 4)$, откъдето $b^2 \equiv 7 (\mathrm{mod}\ 4)$ – противоречие.

21. *Решение.* Ще докажем, че търсената стойност е 5. Числото $5x^2 + 11xy - 5y^2$ е четно точно когато x и y са четни числа (Проверете!). Сега от равенството $f(2x, 2y) = 4f(x, y)$ следва, че търсената най-малка стойност е нечетно число. Тъй като $f(1, 0) = 5$, достатъчно е да покажем, че $f(x, y)$ не приема стойности 1 и 3.

Имаме $f(x, y) = 1 \iff 5x^2 + 11xy - 5y^2 = \pm 1 \iff (10x + 11y)^2 - 221y^2 = \pm 20$, откъдето получаваме $t^2 \equiv \pm 7 (\mathrm{mod}\ 13)$ за цялото число $t = 10x + 11y$. След повдигане на шеста степен и прилагане на теоремата на Ферма получаваме $1 \equiv t^{12} \equiv 7^6 (\mathrm{mod}\ 13)$, което е невъзможно, защото $7^6 \equiv -1 (\mathrm{mod}\ 13)$. Следователно равенството $f(x, y) = 1$ е невъзможно.

Аналогично се вижда, че равенството $f(x, y) = 3$ води до сравнението $t^2 \equiv \pm 5 (\mathrm{mod}\ )13)$, което е невъзможно.

22. *Решение.* Да допуснем, че уравнението има решение. Ако y е четно число, то $x \equiv 3 (\mathrm{mod}\ 4)$, което е невъзможно. Следователно y е нечетно, а x е четно число.

Ако $y \equiv 3 (\mathrm{mod}\ 4)$, то $x \equiv 2 (\mathrm{mod}\ 4)$, което е невъзможно. Нека $y \equiv 1 (\mathrm{mod}\ 4)$. От представянето $x^2 + 4 = (y-1)(y^2 + y + 1)$ следва, че $y^2 + y + 1$ дели $\left(\dfrac{x}{2}\right)^2 + 1$ ($y^2 + y + 1$ е нечетно и значи е взаимно просто с 4). Но $y^2 + y + 1 \equiv 3 (\mathrm{mod}\ 4)$, т.е. $\left(\dfrac{x}{2}\right)^2 + 1$ има прост делител от вида $4k + 3$ (ако всички прости делители на $y^2 + y + 1$ са от вида $4k + 1$, то и $y^2 + y + 1$ е от този вид), което е невъзможно.