Материал за упражнения по Теория на числата

Велико Дончев

25.02.2015г.

Допълнителен материал по Алгебра 2 и Висша алгебра

1 Предмет на теорията на числата. Дялове.

Класическата теория на числата е клон на математиката, който изследва свойствата на целите числа. Някои математици наричат класическата (елементарна) теория на числата "кралица на математиката". "Кралицата" се занимава с привидно прости математически структури (целите числа) и ги изследва със скромен математически апарат. Често теоремите и доказателствата са по идея достъпни дори за ученици, но в същото време от векове стоят неразрешени проблеми, привидно "очевидни". Пример за това е например хипотезата на Голдбах, според която

"Всяко четно число, по- голямо от 2, може да се представи като сума на две прости числа"

Компютърно е проверено (от T. Oliveira e Silva), че хипотезата е вярна за $n \leq 4.10^{17}$ и все пак не е ясно дали е вярна въобще.

От сравнително по-скоро теорията на числата се занимава с по-широк клас проблеми, които естествено възникват при изучаването на целите числа. Тя се разделя на няколко подобласти, в зависимост от методите които се използват и типовете въпроси които се разглеждат.

- В *елементарната теория на числата*, целите числа се изучават без да се използват методи от други области на математиката. Тя се занимава с въпроси като делимост, използване на алгоритъма на Евклид за намиране на най-голям общ делител, разлагане на целите числа като произведение на прости, изследване на съвършените числа, сравнения и други. Някои от важните открития в тази област включват: малката теорема на Ферма, теоремата на Ойлер, китайската теорема за остатъците и закона за квадратичната реципрочност. Изучаване на свойствата на мултипликативните функции като например функцията на Мьобиус и функцията на Ойлер, целочислени редици, функцията факториел и числата на Фибоначи също попадат в тази област.

- В *аналитичната теория на числата* се използват средствата на диференциалното и интегрално смятане и комплексния анализ, за да отговаря на въпроси за целите числа. Законът за разпределение на простите числа и свързаната с него хипотеза на Риман са области от аналитичната теория на числата.

- В *алгебричната теория на числата*, понятието число се разширява. Много от теоремите от елементарната теория на числата се обобщават и за други (по- абстрактни) алгебрични структури, например за полиноми.

В курса по Алгебра-2 ще засегнем предимно класическия дял. Резултатите от елементарната теория на числата, ще имат директно приложения в абстрактните алгебрични структури. От друга страна, познания по елементарна теория на числата са необходима база за навилизане както в теорията на кодирането, така и в криптографията.

2 Естествени и цели числа

Както се преподава в учищиле, естествените числа са тези, с които броим.

$$\mathbb{N} = \{1, 2, 3, ...\}$$

Има много начини за дефиниране на множеството на естествените числа, както и операциите в тях, но това излиза извън рамките на курса по Алгебра–2. Един от тях е чрез аксиомите на Пеано – виж [1]. Друг е теоретико множествен.

$\mathbb{N}$ се разширявя с добавяне на нула 0, така че $a + 0 = a$ за всяко $a \in \mathbb{N}$, и с добавяне на отрицателните цели числа: в разширената съвкупност за всяко $a \in \mathbb{N}$ съществува еднозначно определен елемент $-a$, такъв че $a + (-a) = 0$. Полученото множество се нарича пръстен на целите числа $\mathbb{Z}$ и притежава следните свойства:

За всеки $a, b, c \in \mathbb{Z}$ са в сила

1. a + b = b + a
2. (a + b) + c = a + (b + c)
3. a + 0 = a
4. a + (-a) = 0
5. ab = ba
6. (ab)c = a(bc)
7. a(b + c) = ab + ac
8. 1a = a

Следното важно твърдение няма да доказваме, т.к. доказателството му предполага работа с конструкцията на ествените числа.

Твърдние 2.1. *Всяко непразно множество от естествени числа има най- малък елемент*

Въз основа на това твърдение ще докажем важната

Теорема 2.1. *За всеки две цели числа a и $b, b \neq 0$, съществуват еднозначно определени $q, r \in \mathbb{Z}$, такива че*

$$a = bq + r, \quad 0 \leq r \leq |b| \tag{1}$$

Числата q и r се наричат съответно частно и остатък при деление на a на b.

Доказателство:
Нека първо $b > 0$. Да разгледаме множеството

$$M = \{a - bx \big| x \in \mathbb{N}, a - bx \geq 0\}$$

Множеството M не е празно: в него има поне един елемент: $-a^2$. Наистина,

$$a - b(-a^2) = a + ba^2 \geq 0.$$

Прилагаме 2.1 за M: съществува най-малък елемент $r \geq 0$. Нека q е стойността, за която

$$a - bq = r \Leftrightarrow a = bq + r.$$

Остана да докажем, че $r < b$ и че това представяне е единствено. Да допуснем, че $r \geq b$. Тогава

$$0 \leq r - b = a - bq - b = a - b(q+1) \in M.$$

Но $r > r - b \geq 0$, което противоречи на избора на r. Сега за да докажем единствеността да допуснем, че

$$a = bq + r = bq_1 + r_1.$$

Тогава получаваме, че $r - r_1 = b(q_1 - q)$. Но понеже $0 \leq r, r_1 < b$, то $|r - r_1| < b$. Следователно развенството $r - r_1 = b(q_1 - q)$ е възможно само ако и двете страни са равни на 0, т.е. $r = r1, q = q1$, тоест представянето е единствено.

Нека $b < 0$. Тогава $-b > 0$ и имаме, че съществуват Q и r такива, че

$$a = (-b)Q + r$$

Да положим $q = -Q$. Получаваме $a = (-b)(-q) + r = bq + r$.

Следствие 2.1.1. *За всеки две цели числа a и $b \neq 0$ съществуват $k, l \in \mathbb{Z}$, че*

$$kb \leq a < lb, \quad |k - l| = 1.$$

Доказателство: Имаме, че съществуват q, r, че $a = qb + r$. Понеже $0 \leq r < b$, то $qb \leq a < qb + b = q(b+1)$. Числата k и l са q и $q + 1$.

3 Делимост

Дефиниция 3.1. *Казваме, че цялото число $b \in \mathbb{Z} \backslash \{0\}$ дели $a \in \mathbb{Z}$ ако съществува $q \in \mathbb{Z}$, такова, че $a = bq$. Бележим $b|a$.*

Формулираме някой основни свойства на делимостта, които са директни следствия на дефиницията. Нека $a, b \in \mathbb{Z} \backslash \{0\}$. В сила са:

1. $b|a$ тогава и само тогава когато остатъкът r при деление на b на a е 0;
2. Ако $b|a$, то $-b|a$;

3. $a|0$;

4. От $a|b$ и $b|a$ следва, че $a = \pm b$;

   Наистина, имаме, че съществуват цели, ненулеви q_1, q_2, че $a = bq_1 = (aq_2)q_1 = aq_1q_2$. Но последното е възможно само ако $q_1q_2 = 1$, т.е. $q_1 = q_2 = 1$ или $q_1 = q_2 = -1$. Следователно, $a = b$ или $a = -b$.

5. От $a|b$ и $b|c$ следва, че $a|c$;

   Наистина, имаме, че $b = q_1a$, $c = q_2b$. Следователно $c = (q_1q_2)a$, което доказва следствието.

6. Нека $a|b_1$ и $a|b_2$. Тогава за произволни $k_1, k_2 \in \mathbb{Z}$, $|k_1b_1 + k_2b_2$.

   Наистина, $b_1 = aq_1, b_2 = aq_2$. Следователно $k_1b_1 + k_2b_2 = k_1q_1a + k_2q_2a = (k_1q_1 + k_2q_2)a$.

7. Нека $a|b$. Следователно $|a| \leq |b|$.

8. Нека $a|b$, но $a \nmid c$. Тогава $a \nmid b + c$.

Дефиниция 3.2. *Казваме, че едно естествено число p е просто ако се дели само на $\pm 1, \pm p$.*

Известен метод за намиране на първите n прости числа е Решето на Ератостен. Алгоритъм за компютърно реализиране:

1. Инициализираме един масив от n елемента с нули. По-късно, когато задраскаме някое число, на съответната позиция в масива ще записваме 1. i показва кое е първото незадраскано или немаркирано число. Започваме от 2.

2. Увеличаваме i докато съответния елемент от масива стане 0. Тогава числото i е просто (и го извеждаме).

3. Маркираме с 1 всички стойности в масива за $k = 2i, 3i, \ldots$ – всички кратни на i стойности.

4. Ако $i <= n$, то се връщаме на стъпка 2, иначе приключваме.

Задачи от делимост:

1. Напишете програма, която проверява дали едно число е просто.

2. Напишете програма, която намира простите числа в интервала $[a; b]$.

3. Едно число се нарича съвършено ако е равно на сумата от положителните си делители (без самото то). Първото съвършено число е $6 = 1.2.3 = 1 + 2 + 3$. Напишете програма за намиране на $n-$тото съвършено число. До какво n програмата ще смята за разумно време?

4. Нека n е естествено. Покажете, че $n(n + 1)$ се дели на 2.

   От всеки две последователни естествени число, точно едното е четно, а другото нечетно. Следователно $2|n(n + 1)$.

5. Нека n е естествено. Докажете, че $n^2 + 1$ и n са с различна четност;

6. Нека n е естествено. Докажете, че n^2+1 не се дели на 3.

   n може да дава остатък или 0,1,2 при деление на 3. Нека първо $n = 3k$ - имаме, че $n^2+1 = 9k^2+1$. $9k^2$ се дели на 3, но 1 не, следователно $3 \nmid n^2+1$. Нека $n = 3k+1$. $n^2+1 = 9k^2+6k+2$. Понеже $3 \nmid 2$, то $3 \nmid n^2+1$. Накрая, нека $n = 3k+2$. $n^2+1 = 9k^2+6k+5$. Аналогично, понеже $3 \nmid 5$, то $3 \nmid n^2+1$.

7. Нека n е естествено число. Покажете, че n^5-n се дели на 30.

8. Нека n е естествено число. Покажете, че n^3+11n се дели на 6.

4 Най- голям общ делител (НОД) и най- малко общо кратно (НОК).

Дефиниция 4.1. *Най- голям общ делител (НОД) на целите числа a, b наричаме цяло число d (което бележим с (a, b)), такова, че:*

1. $d|a$, $d|b$.   (d е делител на a, b).

2. Ако $d_1|a$ и $d_1|b$, то $d_1|d$.   (d е най- малкият по модул измежду всички).

Ясно е, че НОД е определен с точност до знак. Наистина, ако d_1, d_2 изпълняват 1. и 2., то $d_1|d_2$, $d_2|d_1$, т.е. $d_1 = \pm d_2$.

Твърдние 4.1. *(Тъждество на Безу) Всеки две цели числа a, b имат НОД $d = (a, b)$ и съществуват $u, v \in \mathbb{Z}$, такива, че*

$$d = ua + vb. \tag{2}$$

Дефиниция 4.2. *Казваме, че две ненулеви цели числа a, b са взаимнопрости ако $(a, b) = 1$.*

Твърдние 4.2. *Нека $(a, b) = 1$ и $a|bc$. Тогава $a|c$.*

Доказателство: От това, че $(a, b) = 1$ веднага получаваме (Безу) че съществуват цели u, v, такива, че

$$au + bv = 1.$$

Да умножим това равенство по c

$$acu + bcv = c.$$

Имаме, че лявата част се дели на a, следователно и дясната част се дели на a.

Твърдние 4.3. *Нека $(a, b) = 1$ и $a|c, b|c$. Тогава $ab|c$.*

Доказателство: По условие $c = qb$. Но $a|qb$ и $(a, b) = 1$ по условие, следователно от 4.2 следва, че $a|q$. Следователно $q = ap$ и $c = pab$, т.е. $ab|c$.

Лема 4.1. *За всеки $a, b, q \in \mathbb{Z}$ имаме $(a, b - qa) = (a, b)$.*

Доказателство: Нека $d = (a, b - qa)$. Съществуват $u, v \in \mathbb{Z}$, че

$$d = ua + v(b - qa) = (u - qv)a + vb$$

От последното представне следва, че d е НОД също и за a, b.

Твърдние 4.4. *Ако $a = bq + r, 0 \leq r < |b|$, то $(a, b) = (b, r)$.*

Доказателство: Имаме, че $(b, r) = (b, a - bq)$. От 4.1 следва че $(b, a - bq) = (a, b)$.

Последното твърдение ни позволява да построим алгоритъм за пресмятане на (a, b) чрез последователно делене с остатък.

Алгоритъм на Евклид за намиране на НОД(a, b):

$$\begin{aligned}
a &= bq + r, \quad 0 \leq r < |b| \\
b &= rq_1 + r_1, \quad 0 \leq r_1 < r \\
r &= r_1q_2 + r_2, \quad 0 \leq r_2 < r_1 \\
&\dots\dots\dots\dots\dots\dots\dots\dots \\
r_{i-1} &= r_iq_{i+1} + r_{i+1}, \quad 0 \leq r_{i+1} < r_i \\
r_i &= r_{i+1}q_{i+2} + 0.
\end{aligned}$$

Ясно е, че при тази поредица от деления понеже $|b| > r > r_1 > ... > r_k > ...$,то на някоя стъпка ще получим деление без остатък. Прилагайки 4.4 получаваме

$$(a, b) = (b, r) = (r, r_1) = ... = (r_i, r_{i+1}).$$

Но $r_{i+1}|r_i$, следователно $(a, b) = r_{i+1}$. Извода, до който стигаме, е че

Твърдние 4.5. *Последният ненулев остатък, който получим при алгоритъма на Евклид е търсеният най- голям общ делител на числата a и b.*

Наблюдение: Връщайки се "отзад напред" в алгоритъма на Евклид можем да получим и някоя двойка коефициенти на Безу. Наистина, имаме $d = r_{i+1} = r_{i-1} - r_iq_{i+1}$. Да изразим в това равенство r_i от предходното уравнение: $d = r_{i-1} - (r_{i-2} - r_{i-1}q_i)q_{i+1} = (1 + q_iqi + 1)r_{i-1} - q_{i+1}r_{i-2}$. Продължаваме като изразим r_{i-1} и така нататък докато накрая не изразим и $r = a - bq$ и го заместим. По този начин ще получим тъждество на Безу. Прецизното описване и компютърно реализиране на този алгоритъм може да се намери в [1] и се предоставя на читателя като задача в тази глава.

Пример 4.1. *Да се намери НОД(174,48) и съответни коефициенти на Безу.*

Правим прав ход по Евклид за намиране на НОД:

$$\begin{aligned}
174 &= 3 \times 48 + 30 \\
48 &= 1 \times 30 + 18 \\
30 &= 1 \times 18 + 12 \\
18 &= 1 \times 12 + 6 \\
12 &= 2 \times 6 + 0
\end{aligned}$$

Следователно $(174, 48) = 6$. Изразяваме последователно

$$\begin{aligned}
6 &= 18 - 1 \times 12 && = \\
&= 18 - 1 \times (30 - 1 \times 18) && = \\
&= 2 \times 18 - 1 \times 30 && = \\
&= 2 \times (48 - 1 \times 30) - 1 \times 30 && = \\
&= 2 \times 48 - 3 \times 30 && = \\
&= 2 \times 48 - 3 \times (174 - 3 \times 48) && = \\
&= 11 \times 48 - 3 \times 174
\end{aligned}$$

Следователно

$$6 = (48, 174) = \underbrace{11}_{\text{u}} \times 48 + \underbrace{(-3)}_{\text{v}} \times 174$$

Дефиниция 4.3. *Най- малко общо кратно (НОК) на целите числа a, b наричаме цяло число d (което бележим с $[a, b]$), такова, че:*

1. $a|d$, $b|d$,
2. Ако $a|d_1$ и $b|d_2$, то $d|d_1$.

Твърдние 4.6. *За всеки две цели числа в сила $(a, b)[a, b] = ab$.*

Доказателството се предоставя на читателя.

Дефиниция 4.4. *Най- голям общ делител (НОД) на целите числа $a_1, a_2, \ldots, a_k$ наричаме цяло число d (което бележим с $(a_1, \ldots, a_k)$), такова, че:*

1. $d|a_i, \quad i = 1, \ldots, k,$
2. *Ако* $d_1|a_i, \quad i = 1, \ldots, k,$ *то* $d_1|d$.

Дефиниция 4.5. *Най- малко общо кратно (НОК) на целите числа $a_1, a_2, \ldots, a_k$ наричаме цяло число d (което бележим с $[a_1, \ldots, a_k]$), такова, че:*

1. $a_i|d, \quad i = 1, \ldots, k,$
2. *Ако* $a_i|d_i, \quad i = 1, \ldots, k,$ *то* $d|d_1$.

Твърдние 4.7. *В сила са рекурентните зависимости:*

$$(a_1, a_2, \ldots, a_k) = (a_1, (a_2, \ldots, a_k)),$$

$$[a_1, a_2, \ldots, a_k] = [a_1, [a_2, \ldots, a_k]].$$

1 Линейни Диофантови Уравнения

Дефиниция 4.6. *Линейно Диофантово Уравнение (ЛДО) за k неизвестни цели числа наричаме уравнение от вида*

$$a_1x_1 + \ldots a_kx_k = b, \tag{3}$$

където $a_1, \ldots, a_k, b$ са цели числа.

От линейната алгебра знаем, че ако в (3) коефициентите са от поле, то имаме $k-1$-мерно афинно пространство от решения (ако поне един от коефициентите $a_1, \ldots, a_k$ е различен от 0). Целите числа *не са поле* и следователно такъв резултат тук не можем да формулираме.

Твърдние 4.8. *Уравнение (3) има решение т.с.т.к. $(a_1, \ldots, a_k)|b$.*

Едно примерно решение се дава, използвайки тъждеството на Безу. Нека $b = b_1d, d = (a_1, \ldots, a_k)$. От Безу имаме, че

$$d = u_1a_1 + \ldots + u_ka_k.$$

Да умножим това равенство по b_1. Получаваме, че $(u_1b_1, \ldots, u_kb_1)$ е решение на ЛДО.

Ако $k = 2$ и x_0, y_0 е някое решение, то всички решения се дават с

$$x = x_0 + \frac{b}{(a,b)}t, \quad y = y_0 - \frac{a}{(a,b)}t, \quad t \in \mathbb{Z}.$$

Пример 4.2. *Да се реши уравнението $12x + 15y = 21$.*

Решение: $3 = (12, 15)|21$. Следователно уравнението има решение и

$$3 = -1 \times 12 + 1 \times 15, \quad \times 7$$

Получаваме, че $(x_0, y_0) = (-7, 7)$ е решение. Тогава всички решения са $x = 5t - 7, y = 7 - 4t, \quad t \in \mathbb{Z}$.

Пример 4.3. *Да се реши в цели числа системата уравнения*

$$a)\left|\begin{array}{ll} 2x + 3y & = 5 \\ 4x + 8y & = 12 \end{array}\right. \qquad b)\left|\begin{array}{ll} 2x + 3y & = 5 \\ 4x + 8y + 2z & = 12 \end{array}\right.$$

*a)*Първо проверяваме дали двете уравнения по отделно имат решение. Да, $1 = (2, 3)|5$ и $4 = (4, 8)|12$). Всички решения на първото уравнение (виж горната задача) са: $x = 3t - 5, y = 5-2t, \quad t \in \mathbb{Z}$. Заместваме този резултат във второто уравнение: $4(3t-5)+8(5-2t) = 12 \Leftrightarrow -4t = -8$, т.е. $t = 2$ и $x = 1, y = 1$ е единствено решение.

b) След решаване на първото уравнение, като заместим във второто получаваме $-4t + 2z = -8$. Решенията на това уравнение са $t = 4 + q, z = 4 + 2q, \quad q \in \mathbb{Z}$. Окончателно, $x = 3q + 7, y = -3 - 2q, z = 4 + 2q, \quad q \in \mathbb{Z}$.

Теорема 4.1. *Основна теорема на аритметиката. Нека $n \in \mathbb{N}$. Тогава съществува естествено число k, прости числа $p_1, \ldots, p_k$ и естествени $s_1, \ldots, s_k$, че*

$$n = p_1^{s_1} \ldots p_k^{s_k}.$$

Теорема 4.2. *Теорема за представяне на естествени числа в бройна система. За всяко естествено число n и всяко ествествено $k \geq 2$ (k-бройната система) съществува единствено представяне*

$$n = k^q a_q + k^{q-1} a_{q-1} + \ldots + k^1 a_1 + k^0 a_0,$$

където $q \in \mathbb{N}, q \geq 1$ и $0 \leq a_q, a_{q-1}, \ldots, a_1, a_0 < k$. Пишем $n = \overline{a_q a_{q-1} \ldots a_1 a_0}^{(k)}$ и казваме, че цифрите на n в $k-$бройна система са $a_q, a_{q-1}, \ldots, a_1, a_0$.

Признаци за делимост (в десетична бройна система) и доказателство на някои от тях. Останалите са за упражнение на читателя.

- на 2 - Ако числото е четно
- на 3 - Ако сборът на цифрите на даденото число се дели на 3.

  Наистина, нека $n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0$. Понеже за $j \geq 1$ имаме $3 | 10^j - 1 = \underbrace{9 \ldots 9}_{j}$ представяме n във вида

  $$n = a_k(10^k) + \ldots + 9a_1 + (a_0 + a_1 + \ldots + a_k),$$

  от където $3|n \Leftrightarrow 3|(a_0 + a_1 + \ldots + a_k)$, което е сборът от цифрите на n. Да забележим, че всъщност от тук следва и по-силното твърдение, признака за делимост на 9.
- на 4 - Ако числото образувано от последните две цифри се дели на 4.

  Следва от факта, че $4|10^k - 1$ за $k \geq 2$.
- на 5 - Ако числото завършва на 5 или 0.
- на 6 - Ако числото се дели на 2 и на 3 (за това вече има признаци)
- на 8 - Ако числото, образувано от последните три цифри се дели на 8.
- на 9 - Ако сборът на цифрите на даденото число се дели на 9.
- на 10 - Ако последната цифра на даденото число е 0.
- на 11 - Ако разликата от сборовете на цифрите на четни и нечетни позиции се дели на 11.
- на 13 - Ако сборът на последната цифра на даденото число умножена с 4 и останалите цифри се дели на 13.
- на 17 - Ако разликата на последната цифра, умножена по 5, и останалите цифри се дели на 17.
- на 19 - Ако сборът на последната цифра на даденото число умножена по 2 и останалите цифри се дели на 19.
- на 23 - Ако сборът на последната цифра на даденото число умножена по 7 и останалите цифри се дели на 23.
- на 25 - Ако последните две цифри на даденото число се делят на 25.
- на 50 - Ако последните две цифри на даденото число се делят на 50.
- на 125 - Ако последните три цифри на даденото число се делят на 125.

...

5 Функцията $\varphi(n)$

Дефиниция 5.1. *Аритметична функция f наричаме функция, дефинирана върху естествените числа*

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

Дефиниция 5.2. *Аритметичната функция f наричаме мултипликативна, ако за всеки две взаимно прости m, n*

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

Дефиниция 5.3. *Функция на Ойлер $\varphi(n)$, дефинирана за всяко естествено n наричаме*

$$\varphi(n) := |\{1 \leq a \leq n \big| (a, n) = 1\}|,$$

тоест $\varphi(n)$ е броят на естествените числа, по - малки от n и взаимно прости с n.

Задача Докажете, че ако p е просто, то $\varphi(p^k) = p^{k-1}(p-1)$.

Тврърдние 5.1. *φ е мултипликативна.*

Тврърдние 5.2. *Нека $n = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ е каноничното разлагане на числото n. Тогава*

$$\varphi(n) = n\big(1 - \frac{1}{p_1}\big) \dots \big(1 - \frac{1}{p_k}\big).$$

Задача Да се намиери $\varphi(a)$ за $a = 17, 26, 36, 128$.

Решение: Числото 17 е просто и $\varphi(17) = 17 - 1 = 16$. Разлагаме канонично числото 26: $26 = 2.13$ и следователно $\varphi(26) = \varphi(2)\varphi(13) = 1.12 = 12$. За 36 имаме $\varphi(36) = \varphi(2^2.3^2) = 36(1 - \frac{1}{2})(1 - \frac{1}{3}) = 36.\frac{1.2}{2.3} = 12$. Последно, $128 = 2^7$ и следователно $\varphi(128) = 2^{7-1}(2-1) = 64$.

Задача Да се пресметне $\varphi(\varphi(6!))$.

Решение Имаме, че $6! = 720 = 2^4 3^2 5$. $\varphi(720) = \varphi(2^4 3^2 5) = \varphi(16)\varphi(9)\varphi(5) = 8.6.4 = 192$. Остана да пресметнем $\varphi(192) = \varphi(2^6.3) = \varphi(2^6)\varphi(3) = 32.2 = 64$.

Задача Да се реши уравнението $\varphi(n) = 6$.

Решение: Нека $n = 2^e p_1^{k_1} \dots p_m^{k_m}, e \geq 0, k_i \geq 0, i = 1 \dots m$ е разлагането на n в прости множители. Да допуснем, че има поне два прости множителя, различни от 2, които влизат в разлагането. Имаме $k \geq 2, k_1, k_2 \geq 1$. Понеже функцията на Ойлер е мултипликативна, то $\varphi(n) = 2^{e-1}(2-1)p_1^{k_1-1}(p_1-1)p_2^{k_2-2}(p_2-1)\varphi(p_3^{k_3} \dots p_m^{k_m})$. Но $p_1, p_2 > 2$ и следователно $p_1 - 1$ и $p_2 - 1$ са две четни числа, което означава, че $4|\varphi(n) = 6$, противоречие. Следователно в разлагането на n има най-много едно просто число, различно от 2, а следователно и $k \leq 1$.

1сл. $k = 0$. В този случай $n = 2^e, \varphi(n) = 2^{e-1} = 6$, което е невъзможно.

2сл. $k = 1$. В този случай $n = 2^e p_1^{k_1}, e \geq 0$.

2.1 Ако допуснем, че $e = 0$, то $\varphi(n) = p_1^{k_1-1}(p_1 - 1) = 2.3$. Ако $k_1 = 1$, то $p_1 - 1 = 6$, т.е. $p_1 = 7$. Ако $k_1 \geq 2$, то 6 се дели на степен на просто число, следователно $k_1 = 2$. Но тогава p_1 трябва да е 3, т.е. $n = 3^2 = 9$.

2.2 Нека сега $e \geq 1$. Имаме, че $\varphi(n) = 2^{e-1}p_1^{k_1-1}(p_1 - 1) = 6$. Ако $e \geq 2$, то 6 би се деляло на 4 (веднъж от 2^{e-1}, веднъж от $(p_1 - 1)$), което е противоречие. Следователно $e = 1$ и $\varphi(n) = \varphi(p_1^{k_1})$ и от предните разсъждения следва, че останалите две решения са $n = 2.7 = 14$ и $n = 2.3^2 = 18$.

6 Сравнения

Дефиниция 6.1. *Нека $n \neq 0$ е цяло число. Казваме, че целите числа a, b са сравними по модул n и бележим с*

$$a \equiv b \pmod{n},$$

ако разликата $a - b$ се дели на n.

В сила са следните свойства

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ т.с.т.к. $b \equiv a \pmod{n}$,
3. Ако $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$, то $a \equiv c \pmod{n} =$,
4. Ако $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a \pm c \equiv b \pm d \pmod{n}$,
5. Ако $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $ac \equiv bd \pmod{n}$,
6. Ако $ma \equiv mb \pmod{n}$ и $(m, n) = d$, то $a \equiv b \pmod{n/d}$,
7. Ако $a \equiv b \pmod{n}$ и $(a, n) = d$, то $d|b$.

Дефиниция 6.2. *При фиксирано n, за всяко цяло число a с $\overline{a}$ бележим остатъка при деление на n. За всяко n със $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots \overline{n-1}\}$ бележим всички остатъци по модул n. Имаме $\overline{a} \in Z_n$.*

Дефиниция 6.3. *Всяка система от n на брой несравними помежду си по модил n числа наричаме пълна система от отстатъци по модул n.*

Твърдние 6.1. *За всяка система остатъци $a_1, \ldots, a_n$ по модул n имаме, че $\overline{a_1}, \ldots, \overline{a_n}$ изчерпват Z_n.*

Дефиниция 6.4. *Линейно сравнение с едно неизвестно $x \in \mathbb{Z}$ наричаме сравнение от вида*

$$ax + b \equiv 0 \pmod{n}, \tag{4}$$

където a, b, n са цели числа. Всеки две негови решения x_1, x_2, за които $x_1 \equiv x_2 \pmod{n}$ смятаме за неразличими (по модул n).

Теорема 6.1. *Сравнението $ax + b \equiv 0 \pmod{n}$ има решение т.с.т.к. $d = (a, n)|b$. В този случай, сравнението има точно d решения (в смисъла на последната дефиниция) и те са:*

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d},$$

където $x_0 \equiv -b_1 a_1^{\varphi(n_1)-1} \pmod{n_1}$ и $a_1 = a/d, b_1 = b/d, n_1 = n/d$.

Пример 6.1. *Да се решат в цели числа следните уравнения и системи:*

$$a)2x \equiv 3 \pmod{14} \quad b)2x \equiv 6 \pmod{14}$$

$$c)\left|\begin{array}{l} 3x \equiv -1 \pmod 7 \\ 4x \equiv 5 \pmod{11} \end{array}\right. \qquad d)\left|\begin{array}{l} 3x \equiv -1 \pmod 7 \\ 4x \equiv 8 \pmod{32} \end{array}\right.$$

Забележка: Във формулата, изложена по-горе сравнението е записано във вида $ax + b \pmod n$, а в задачата сравненията са записани във вида $ax = b \pmod n$. Какво се променя във формулата за решение?

(a) $2 = (2, 14)$ не дели 3, следователно сравнението няма решение.

(b) $2 = (2, 14)|6$ и нека $a_1 = 2/2 = 1$, $b_1 = 6/2 = 3$, $n_1 = 14/2 = 7$. Имаме. че $-(-b_1 a_1^{\varphi(n_1)-1}) = 3$. Следователно $x_0 = 3, x_1 = 3 + 7 = 10$ са решенията в $\mathbb{Z}_{14}$, а всички решения са $x = 3 + 14t$ и $x = 10 + 14t$ за $t \in \mathbb{Z}$.

(c) Първо проверяваме дали двете уравнения по отделно имат решение. Наистина, $(3, 1)|7, (4, 11)|5$. Решенията на първото уравнение са $x = 2 + 7q, \quad q \in \mathbb{Z}$. Заместваме този резултат във второто уравнение. Получаваме $4(2+7q) \equiv 4 \pmod{11}$, което е еквивалентно на $6q \equiv 5 \pmod{11}$. Всички решения на последното сравнение са $q = 1 + 11z, \quad z \in \mathbb{Z}$. Окончателно, всички решения на задачата са $x = 9 + 77z, \quad z \in \mathbb{Z}$.

(d) От *(c)*, решенията на първото уравнение са $x = 2 + 7q, \quad q \in \mathbb{Z}$. Заместваме този резултат във второто уравнение. Получаваме $4(2+7q) \equiv 8 \pmod{32}$, което е еквивалентно на $28q \equiv 0 \pmod{32}$. Това уравнение има $4 = (28, 32)$ решения в $\mathbb{Z}_{32}$. Те са:

$$q = 0 + 32t,\ 8 + 32t,\ 16 + 32t,\ 24 + 32t, \quad t \in \mathbb{Z}$$

Съответно за x имаме 4 серии от решения:

$$x = 2 + 224t,\ 58 + 224t,\ 114 + 224t,\ 170 + 224t, \quad t \in \mathbb{Z}$$

Теорема 6.2. *(Ойлер-Ферма) Нека* $(a, m) = 1$. *Тогава*

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Ако $m = p$ *е просто*

$$a^{p-1} \equiv 1 \pmod p, \quad a^p \equiv a \pmod p$$

Пример 6.2. *Да се намери остатъкът при деление на* 19^{20} *на* 17.

Имаме, че $19 \equiv 2 \pmod{17} \mid \uparrow^4 \Rightarrow 19^4 \equiv 16 \equiv -1 \pmod{17} \uparrow^5 \Rightarrow 19^{20} \equiv -1 \equiv 16 \pmod{17}$. Остатъкът при деление на 19^{20} на 17 е 16.

Пример 6.3. *Да се намери остатъкът при деление на* $5^{2013} + 4^{2013}$ *на* 28.

Решение: Имаме, че $(5, 28) = 1$ така че по теорема на Ойлер-Ферма получаваме, че $5^{\phi(28)} \equiv 1 \pmod{28}$, $\phi(28) = 12$. Да вдигнем последното сравнение на степен 167 (най-близката, с която няма да надминем 2013). Получаваме, че $5^{2004} \equiv 1 \pmod{28}$. Остава да пресметнем остатъкът на 5^9. Имаме, че $5^2 \equiv -3 \pmod{28}$ следователно $5^8 \equiv 81 \equiv -3 \pmod{28}$. Окончателно, $5^{2013} = 5^{2004+8+1} \equiv 1.-3.5 \equiv 13 \pmod{28}$.

Да забележи, че $4^4 = 256 \equiv 4 \pmod{28}$. Вдигаме на 4 степен: $4^{16} \equiv 4^4 \equiv 4(\mod 28)$. Ясно е, че $4^{1024} \equiv 4^{256} \equiv 4^{64} \equiv 4^{16} \equiv 4^4 \equiv 4 \pmod{28}$. От тук $4^{2000} = 4^{1024+3.256+3.64+16} \equiv 4^3.4^3.4 = 4^{4.2} \equiv 16 \pmod{28}$. Но $4^3 = 64 \equiv 8 \pmod{28}$. Следователно $4^6 = 64 \equiv 8 \pmod{28}$. И така, $4^{2000} \equiv 8 \pmod{28}$. От тук лесно получаваме, че $4^{2013} = 4^{2000+2.6+1} \equiv 16.8^2.4 = 4^6 \equiv 8 \pmod{28}$.

Забележка: Задачата е давана на първо контролно по Алгебра-2 на спец. Компютърни науки, 2013г.

Следователно $5^{2013} + 4^{2013} \equiv 13 + 8 = 21 \pmod{28}$.

Теорема 6.3. *(Уилсън) За всяко просто p е в сила*

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Литература

[1] Николай Манев, *Записки по теория на числата*,

[2] Стефка Буюклиева, *Елементарна теория на числата с алгоритми*, 2001

[3] Пламен Сидеров, *Записки по алгебра: Групи, пръстени, полиноми*, 2013, Веди

[4] Стефан Додунеков, Керопе Чакърян *Задачи по теория на числата*, 1999, Регалия-6