

## Глава 4

# Квадратични остатъци.

### 4.1 Квадратични и $k$ -степенни остатъци.

Да разгледаме общото сравнение от втора степен

$$ax^2 + bx + c \equiv 0 \pmod{n}, \quad (4.1)$$

където  $a \not\equiv 0 \pmod{n}$ . Умножавайки по  $4a$  и полагайки  $y = 2ax + b$  получаваме системата

$$\begin{cases} y^2 \equiv D \pmod{4an} \\ y \equiv b \pmod{2a}, \end{cases} \quad (4.2)$$

където  $D = b^2 - 4ac$ .

Очевидно всяко решение на (4.1) определя еднозначно решение  $y$  на (4.2). Обратно, ако  $y$  е решение на системата (4.2), то  $x = (y - b)/2a$  е решение на (4.1). Следователно въпросът за решаване на произволно сравнение от втора степен се свежда до решаване на сравнения от вида

$$x^2 \equiv a \pmod{m}. \quad (4.3)$$

Направените заключения може още да се преценират. По-точно в сила е

**Теорема 4.1.1** *Нека  $(a, m) = d$ ,  $a = da_1$ ,  $m = dm_1$  и  $d = e^2 f$ , където  $f$  е свободно от квадрати естествено число. Сравнението (4.3) има решение тогава и само тогава, когато  $(f, m_1) = 1$  и сравнението  $y^2 \equiv fa_1 \pmod{m_1}$  има решение.*

**Доказателство.** *Необходимост.* Ако  $x$  е решение на (4.3), то

$$x^2 \equiv e^2 fa_1 \pmod{e^2 fm_1},$$

откъдето следва  $e^2 \mid x^2$ , тъй като  $f$  е свободно от квадрати. Но тогава  $e \mid x$ , т.е.  $x = ey$ , което след заместване и съкращаване дава

$$y^2 \equiv fa_1 \pmod{fm_1}.$$

Следователно  $f \mid y^2$  и очевидно е изпълнено и по-слабото сравнение  $y^2 \equiv fa_1 \pmod{m_1}$ . Но  $f$  е свободно от квадрати и следователно  $f \mid y$ , т.е.  $y = fz$ .

Замествайки получаваме  $fz^2 \equiv a_1 \pmod{m_1}$ , откъдето  $(f, m_1) \mid a_1$ . Но тогава  $(m_1, a_1) = 1$  влече  $(m_1, f) = 1$ , което пък дава, че  $y^2 \equiv fa_1 \pmod{m_1}$ .

*Достатъчност.* Обратно нека  $(m_1, f) = 1$  и съществува  $y$ , за което  $y^2 \equiv fa_1 \pmod{m_1}$ . Тогава съществува и то единствено  $z$ , такова че  $fz \equiv y \pmod{m_1}$ , откъдето  $f^2z^2 \equiv fa_1 \pmod{m_1}$ . Но щом  $(m_1, f) = 1$ , то  $fz^2 \equiv a_1 \pmod{m_1}$ . Умножавайки с  $e^2f$  получаваме

$$e^2f^2z^2 \equiv e^2fa_1 \pmod{e^2fm_1},$$

т.е.

$$(efz)^2 \equiv a \pmod{m}.$$

И така въпросът за решимостта на произволно сравнение от втора степен по същество се свежда до решимостта на квадратно сравнение от специален вид, а именно

$$x^2 \equiv a \pmod{n}, \quad (a, n) = 1. \quad (4.4)$$

Цяло число  $a$ , за което (4.4) има решение се нарича квадратичен остатък по модул  $n$ , и квадратичен неостатък, ако такова решение не съществува. Въведеното понятие се обобщава със следната дефиниция:

**Дефиниция 4.1.2** Нека  $n \neq 0$  и  $k \geq 2$  са цели числа. Казваме, че цялото число  $a$ ,  $(a, n) = 1$  е  $k$ -степенен остатък (неостатък) по модул  $n$ , когато е решимо (нерешимо) сравнението

$$x^k \equiv a \pmod{n}. \quad (4.5)$$

При  $k = 2, 3, 4$  числото  $a$  се нарича съответно **квадратичен, кубичен и биквадратичен остатък**

**Теорема 4.1.3** Нека  $n \neq 0$  е цяло число, което има примитивен корен. Цялото число  $a$ ,  $(a, n) = 1$ , е  $k$ -степенен остатък по модул  $n$  тогава и само тогава, когато

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n},$$

където  $d = (\varphi(n), k)$ . В този случай сравнението (4.5) има точно  $d$  решения.

**Доказателство.** Нека  $g$  е примитивен корен по модул  $n$ . Вземайки индекси при основа  $g$  от (4.5) получаваме

$$k \cdot \text{ind } x \equiv \text{ind } a \pmod{\varphi(n)}.$$

Но съгласно Теорема 2.2.1 това сравнение има решение относно  $\text{ind } x$  тогава и само тогава, когато  $d = (\varphi(n), k)$  дели  $\text{ind } a$ . При това, ако решение съществува, то това сравнение, а следователно и (4.5) ще имат точно  $d$  решения. Нека сега  $e = \text{ind } a = d \cdot t$ . От определението за индекс получаваме, че

$$a^{\frac{\varphi(n)}{d}} = g^{\frac{e\varphi(n)}{d}} = g^{t\varphi(n)} \equiv 1 \pmod{n}.$$

Обратно, ако  $a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}$ , то

$$g^{\frac{e\varphi(n)}{d}} \equiv 1 \pmod{n},$$

откъдето  $\varphi(n)$  дели  $\frac{e\varphi(n)}{d}$ . Следователно  $d \mid \text{ind } a$ .

**Теорема 4.1.4** *Нека  $n \neq 0$  е цяло число, което има примитивен корен и  $d = (\varphi(n), k)$ . Съществуват точно  $\frac{\varphi(n)}{d}$  на брой несоразни  $k$ -ти остатъци по модул  $n$ .*

**Доказателство.** Съгласно предната теорема  $a$  е  $k$ -степенен остатък по модул  $n$  тогава и само тогава, когато

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}.$$

Но това сравнение има точно

$$\left(\frac{\varphi(n)}{d}, \varphi(n)\right) = \frac{\varphi(n)}{d}$$

решения пак съгласно горната теорема.

Да се върнем отново към квадратичните остатъци. В частност от предната теорема получаваме, че броят на квадратичните остатъци съвпада с този на неостатъците и е равен на  $\varphi(n)/2$ .

**Дефиниция 4.1.5** *Нека  $p$  е нечетно просто число. Символ на Лъожандр от  $a$  относно  $p$  се дефинира като:*

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

**Твърдение 4.1.6** *Символът на Лъожандр притежава следните свойства:*

- (1) ако  $a \equiv b \pmod{p}$ , то  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ,
- (2)  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$  (Критерий на Ойлер),
- (3)  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .

**Доказателство.** Свойство (1) е очевидно.

(2): Полагайки  $k = 2$ ,  $n = p$  в Теорема 4.1.3 получаваме, че  $d = (p-1, 2) = 2$ , откъдето следва, че  $a$  е квадратичен остатък тогава и само тогава, когато  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , откъдето и  $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$  за всяко  $(a, p) = 1$  следва твърдението.

(3): Съгласно (2)

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}.$$

Нека  $p$  е нечетно просто число и  $g$  е примитивен корен по модул  $p$ . Тъй като всяко число  $1 \leq a \leq p-1$  е степен на  $g$ , то съвкупността от квадратични остатъци съвпада с множеството от четните степени на  $g$

$$QR^+ = \{g^2, g^4, \dots, g^{p-1}\},$$

а съвкупността от квадратични неостатъци с

$$QR^- = \{g, g^3, \dots, g^{p-2}\}.$$

Очевидно горните множества описват квадратичните остатъци и неостатъци и в по-общия случай за произволно естествено число  $n$ , което има примитивен корен  $g$ .

**Пример 4.1.1** Ще покажем, че  $-1$  е квадратичен остатък по модул  $p$  тогава и само тогава, когато  $p = 4k + 1$ . Наистина съгласно критерия на Ойлер

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Следователно

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ако } p = 4k + 1, \\ -1, & \text{ако } p = 4k - 1 \end{cases}$$

**Лема 4.1.7** (Лема на Гаус) *Нека  $p$  е нечетно просто число и  $(a, p) = 1$ . Нека  $\mu$  е броя на числата в редицата  $a, 2a, 3a, \dots, \frac{p-1}{2}a$ , които са сравними по модул  $p$  с числа в интервала  $[-\frac{p-1}{2}, -1]$ , (т.е. с числата в интервала  $[\frac{p+1}{2}, p-1]$ ). Тогава*

$$\left(\frac{a}{p}\right) = (-1)^\mu.$$

**Доказателство.** Нека  $r_k \equiv ka \pmod{p}$  е минималния по абсолютна стойност остатък на  $ka$ , т.е.  $-\frac{p-1}{2} \leq r_k \leq \frac{p-1}{2}$ . Очевидно  $r_k = r_l$ , т.е.  $ka \equiv la \pmod{p}$ , е в сила тогава и само тогава, когато  $k = l$ . Аналогично, ако допуснем, че  $r_k = -r_l$ , то  $(k+l)a \equiv 0 \pmod{p}$ . Но това е невъзможно тъй като  $k+l < p$ . Следователно  $|r_k| \neq |r_l|$  за  $k \neq l$ , т.е. абсолютните стойности на остатъците  $r_k$  представляват пермутация на числата от 1 до  $\frac{p-1}{2}$ . Умножавайки ги получаваме

$$\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv \prod_{k=1}^{\frac{p-1}{2}} r_k = (-1)^\mu \prod_{k=1}^{\frac{p-1}{2}} |r_k| = (-1)^\mu \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Делейки двете страни на сравнението на  $(p-1/2)!$  получаваме

$$a^{\frac{p-1}{2}} \equiv (-1)^\mu,$$

което съгласно критерия на Ойлер дава търсеното равенство.

**Теорема 4.1.8** *Числото 2 е квадратичен остатък по модул прости числа от вида  $8t \pm 1$  и квадратичен неостатък по модул останалите нечетни прости числа, т.е.*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \quad (4.6)$$

**Доказателство.** Да отбележим първо, че за  $p = 8t \pm 1$  дясната страна на (4.6) дава точно 1, т.е. 2 е остатък, а при  $p = 8t \pm 3$  дава -1 (т.е. 2 е неостатък). За да докажем теоремата ще приложим Лемата на Гаус за  $a = 2$ . Нека  $m = \lfloor \frac{p-1}{4} \rfloor$ , т.е.  $2m \leq (p-1)/2$ , но  $2(m+1) > (p-1)/2$ . Тогава  $\mu = (p-1)/2 - m$ . В такъв случай при  $p = 8t + 1$  получаваме  $m = 4t$  и  $\mu = 2t$ . Аналогично, при  $p = 8t - 1$  имаме  $m = 2t - 1$  и  $\mu = 2t$ . Следователно  $(-1)^\mu = 1$ . При  $p = 8t \pm 3$ , обаче  $\mu = 2t + 1$  и  $\mu = 2t - 1$ , съответно. Следователно  $(-1)^\mu = -1$ , т.е. 2 е квадратичен неостатък по модул  $p$ .

**Упражнение 4.1.1** Числото  $-2$  е квадратичен остатък по модул прости числа от вида  $8t + 1$  и  $8t + 3$  и квадратичен неостатък по модул останалите нечетни прости числа  $(8t - 1$  и  $8t - 3)$ .

**Лема 4.1.9** Сравнението  $x^2 \equiv a \pmod{2^e}$ ,  $(a, 2) = 1$ ,  $e \geq 3$ , е разрешимо тогава и само тогава, когато  $x^2 \equiv a \pmod{8}$  е разрешимо.

**Доказателство.** Необходимостта е очевидна. Да покажем достатъчността. Нека  $x_0$  е решение  $x^2 \equiv a \pmod{2^e}$ ,  $e \geq 3$ , т.е.  $x_0^2 = a + c2^e$ , където  $c \in \mathbb{Z}$ . Да разгледаме  $x = x_0 + b2^{e-1}$ , където  $b = 0$  или 1 и  $b \equiv c \pmod{2}$ . Тогава за  $e \geq 3$

$$x^2 = x_0^2 + 2^e b x_0 + b^2 2^{2e-2} \equiv a + (bx_0 + c)2^e \pmod{2^{e+1}}.$$

Но  $bx_0 + c \equiv b + c \equiv 0 \pmod{2}$ , тъй като  $x_0 \equiv 1 \pmod{2}$ . Следователно

$$x^2 \equiv a \pmod{2^{e+1}},$$

откъдето твърдението следва по индукция.

**Теорема 4.1.10** Нека  $n = 2^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$  е разлагането на  $n$  на прости множители и  $(a, n) = 1$ . Сравнението  $x^2 \equiv a \pmod{n}$  е решимо тогава и само тогава, когато са изпълнени следните условия:

- (1) ако  $e = 2$ , то  $a \equiv 1 \pmod{4}$ ; ако  $e \geq 3$ , то  $a \equiv 1 \pmod{8}$ .
- (2)  $a^{\frac{p_i-1}{2}} \equiv 1 \pmod{p_i}$  за всяко  $i$ .

**Доказателство.** Съгласно Китайската теорема за остатъците даденото сравнение е еквивалентно със системата от  $k+1$  сравнения:

$$x^2 \equiv a \pmod{2^e}, x^2 \equiv a \pmod{p_1^{e_1}}, \dots, x^2 \equiv a \pmod{p_k^{e_k}}.$$

Да разгледаме  $x^2 \equiv a \pmod{2^e}$ . При  $e = 1$  то не налага никакви ограничения на  $a$ . При  $e = 2$  квадратични остатъци са само числата  $a \equiv 1 \pmod{4}$ , тъй като  $(2t+1)^2 \equiv 1 \pmod{4}$ . Аналогично при  $e = 3$  такива са само  $a \equiv 1 \pmod{8}$ , тъй като  $(8t \pm 1)^2$  и  $(8t \pm 3)^2$  дават остатък 1 при деление на 8. В такъв случай условие (1) се получава от Лема 3.1.5.

Съгласно Теорема 3.3.11 сравнението  $x^2 \equiv a \pmod{p_i^{e_i}}$  е разрешимо тогава и само тогава, когато  $x^2 \equiv a \pmod{p_i}$  е решимо. Сега условие (2) следва от критерия на Ойлер.

## 4.2 Квадратичен закон за реципрочност.

Квадратичният закон за реципрочност (Теорема 4.2.3) е формулиран от Ойлер, а доказателство, макар и в частни случаи, за първи път дава Лъжандр (1785 г.). Гаус предлага осем различни доказателства, а днес са известни над сто. Тук ще изложим едно доказателство, което се свързва с Айзенщайн - ученик на Гаус, който има значителен принос за развитието на математиката, въпреки че умира твърде млад - на 29 години. Самият Гаус го определя като един от тримата най-велики математици наред с Архимед и Нютон.

**Лема 4.2.1** *Нека  $p$  е нечетно просто число,  $(a, p) = 1$  и  $\mu$  е дефинирано както в Лема 4.3.1. Тогава*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + (a-1) \cdot \frac{p^2-1}{8} \equiv \mu \pmod{2}.$$

**Доказателство.** Да разгледаме редицата

$$a, 2a, 3a, \dots, \frac{p-1}{2}a.$$

За всяко число  $ka$  от нея е в сила  $ka = p \left\lfloor \frac{ka}{p} \right\rfloor + \rho_k$ , където  $1 \leq \rho_k \leq p-1$ . Тогава

$$\frac{p^2-1}{8} \cdot a = \sum_{k=1}^{\frac{p-1}{2}} ka = p \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \rho_k.$$

Нека с  $r_1, \dots, r_\mu$  означим тези остатъци  $\rho_k$ , които са по-големи от  $(p-1)/2$ , а с  $s_j$ ,  $1 \leq j \leq \frac{p-1}{2} - \mu$ , тези, които не надминават  $(p-1)/2$ . Тогава числата  $(p-r_1), \dots, (p-r_\mu)$ ,  $s_1, \dots, s_{\frac{p-1}{2}-\mu}$  не надминават  $(p-1)/2$  и са различни, т.е. представляват точно числата от 1 до  $(p-1)/2$ . Следователно

$$\mu p - \sum r_i + \sum s_j = 1 + 2 + \dots + \frac{p-1}{2} = \frac{p^2-1}{8}.$$

Но тъй като

$$\sum_{k=1}^{\frac{p-1}{2}} \rho_k = \sum r_i + \sum s_j = 2 \sum r_i - \mu p \equiv \frac{p^2-1}{8} - \mu p \pmod{2}$$

то

$$\frac{p^2-1}{8} \cdot a \equiv p \left( \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - \mu \right) \pmod{2},$$

откъдето и условието  $p$  нечетно просто получаваме

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - \mu \equiv (a-1) \cdot \frac{p^2-1}{8} \pmod{2}.$$

**Лема 4.2.2** (Лема на Айзенщайн) *Нека  $m$  и  $n$  са нечетни взаимнопрости числа по-големи от 1. Тогава*

$$\sum_{k=1}^{\frac{n-1}{2}} \left\lfloor \frac{km}{n} \right\rfloor + \sum_{l=1}^{\frac{m-1}{2}} \left\lfloor \frac{ln}{m} \right\rfloor = \frac{m-1}{2} \cdot \frac{n-1}{2}.$$

**Доказателство.** Да фиксираме в равнината декартова координатна система и да разгледаме в нея права зададена с уравнение  $y = \frac{m}{n}x$ . Тази права се явява диагонал на правоъгълника в първи квадрант ограничен от координатните оси и правите  $x = n/2$  и  $y = m/2$ . Ще преброим точките с естествени координати (“целите точки”) в правоъгълника по два начина. По абцисата имаме  $(n-1)/2$  естествени числа, а по ординатата -  $(m-1)/2$ . Следователно общият брой цели точки е

$$\frac{m-1}{2} \cdot \frac{n-1}{2}.$$

От друга страна това число е сума от броя на точките под диагонала и над диагонала. За всяко  $k$ ,  $1 \leq k \leq (n-1)/2$  под диагонала има точно  $\left\lfloor \frac{m}{n} \cdot k \right\rfloor$  цели точки. Следователно общият брой на точките под правата е

$$\sum_{k=1}^{\frac{n-1}{2}} \left\lfloor \frac{km}{n} \right\rfloor.$$

Аналогично над диагонала има

$$\sum_{l=1}^{\frac{m-1}{2}} \left\lfloor \frac{ln}{m} \right\rfloor$$

точки. Сумирайки получаваме твърдението на лемата.

**Теорема 4.2.3** *Ако  $p$  и  $q$  са нечетни прости число, то*

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

**Доказателство.** Полагайки  $a = q$  в Лема 4.2.1 и използвайки, че  $q-1$  е четно число получаваме

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \equiv \mu \pmod{2}.$$

В такъв случай лемата на Гаус ни дава

$$\left( \frac{q}{p} \right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor}.$$

Аналогично

$$\left( \frac{p}{q} \right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor}.$$

Умножавайки горните равенства и прилагайки лемата на Айзенщайн за  $m = p$  и  $n = q$  получаваме твърдението на теоремата.

Следващият пример илюстрира как законът за реципрочност може да се използва при пресмятане на символа на Лъожъндр.

**Пример 4.2.1** Да пресметнем

$$\left(\frac{213}{499}\right) = \left(\frac{3}{499}\right) \left(\frac{71}{499}\right).$$

Прилагайки Теорема 4.2.3 и Твърдение 4.1.6 получаваме

$$\left(\frac{3}{499}\right) = \left(\frac{499}{3}\right) (-1)^{249 \cdot 1} = -\left(\frac{1}{3}\right) = -1.$$

$$\left(\frac{71}{499}\right) = \left(\frac{499}{71}\right) (-1)^{249 \cdot 35} = -\left(\frac{2}{71}\right) = -(-1)^{\frac{71^2-1}{8}} = -1.$$

Следователно

$$\left(\frac{213}{499}\right) = 1.$$

### 4.3 Представяне в сума от квадрати.

**Лема 4.3.1** (Лема на Туе) *Нека  $n > 1$  е естествено число и  $r = \lceil \sqrt{n} \rceil$ . Тогава за всяко  $a$ ,  $(a, n) = 1$  съществуват две естествени числа  $x$  и  $y$  ненадминаващи  $r - 1$ , такива че*

$$ay \equiv x \quad \text{или} \quad ay \equiv -x \pmod{n}.$$

**Доказателство.** Да разгледаме множеството от всички числа от вида  $ay + x$ , където  $x, y \in \{0, 1, \dots, r - 1\}$ . То се състои от  $r^2 > n$  числа и следователно съществуват две двойки числа  $(x_1, y_1)$  и  $(x_2, y_2)$ , такива че

$$ay_1 + x_1 \equiv ay_2 + x_2 \pmod{n}, \quad \text{т.е.} \quad a(y_1 - y_2) \equiv x_2 - x_1 \pmod{n}.$$

Но  $0 \leq |y_1 - y_2| \leq r - 1$  и  $0 \leq |x_1 - x_2| \leq r - 1$ . При това  $x_1 \neq x_2$  влече  $y_1 \neq y_2$ . Следователно полагайки  $y = |y_1 - y_2|$  и  $x = |x_1 - x_2|$  получаваме исканото сравнение.

**Теорема 4.3.2** *Нечетното просто число  $p$  се представя като сума на два квадрата тогава и само тогава, когато  $p$  от вида  $4t + 1$ .*

**Доказателство.** *Необходимост.* Нека  $p = a^2 + b^2$ . Очевидно  $(b, p) = 1$  и следователно

$$\left(\frac{a}{b}\right)^2 \equiv -1 \pmod{p}.$$

Но това означава, че  $-1$  е квадратичен остатък по модул  $p$ , което влече  $p = 4t + 1$ .



*Достатъчност.* Нека  $p = 4t + 1$ . Тогава съществува естествено число  $z$ , такова че  $z^2 \equiv -1 \pmod{p}$ . Но съгласно лемата на Туе може да намерим естествени числа  $a, b < \sqrt{p}$ , такива че  $zb \equiv \pm a \pmod{p}$ , т.е.

$$z \equiv \pm \frac{a}{b} \pmod{p}.$$

Последното дава

$$\frac{a^2}{b^2} \equiv -1 \pmod{p}, \quad \text{т.е.} \quad a^2 + b^2 \equiv 0 \pmod{p}.$$

Вземайки предвид, че  $a^2 + b^2 < 2p$  получаваме  $a^2 + b^2 = p$ .

**Теорема 4.3.3** *Всяко цяло число, което е произведение на прости числа от вида  $p = 4t + 1$  или два пъти такова произведение се представя като сума на два квадрата.*

*Доказателство.* Доказателството следва от предната теорема,  $2 = 1^2 + 1^2$  и равенството

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Да отбележим, че условието в горното твърдение не е необходимо. Например  $18 = 3^2 + 3^2$ , но 18 не удовлетворява условието.

Темата за представянето като сума на два квадрата ще завършим с описанието на *питагоровите тройки*, т.е. с решаването в цели числа на уравнението

$$x^2 + y^2 = z^2. \quad (4.7)$$

Очевидно, че ако две от числата имат общ делител, то той дели и третото. Затова интерес представляват решенията с  $(x, y) = (x, z) = (y, z) = 1$ , които ще наричаме примитивни решения.

**Теорема 4.3.4** *Всички примитивни решения на (4.7) се дават с*

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2,$$

където  $(a, b) = 1$  като точно едното от тях е четно. (очевидно местата на  $x$  и  $y$  може да се разменят)

*Доказателство.* Тъй като се интересуваме от примитивните решения, то две от числата трябва да са нечетни, а третото четно. Допускането  $x = 2k + 1$ ,  $y = 2m + 1$ ,  $z = 2n$  дава  $x^2 + y^2 \equiv 2 \pmod{4}$ , докато  $z^2 \equiv 0 \pmod{4}$ . Следователно  $x = 2k + 1$ ,  $y = 2m$ ,  $z = 2n + 1$ . Тогава  $z + x$  и  $z - x$  са едновременно четни и следователно

$$4m^2 = y^2 = z^2 - x^2 = 4(n + k)(n - k) = 4cd, \quad \text{т.е.} \quad m^2 = cd,$$

Тъй като  $(c, d) = 1$ , то  $c = a^2$ ,  $d = b^2$  и получаваме

$$z + x = 2a^2, \quad z - x = 2b^2, \quad y = 2ab,$$

което ни дава твърдението. Условието за четностите и примитивност на решението определя изискването към  $a$  и  $b$ .

**Лема 4.3.5** Ако  $p$  е нечетно просто число, то съществуват цели числа  $x, y, t$ , такива че

$$x^2 + y^2 + 1 = tp,$$

където  $1 \leq t < p$ ,  $0 \leq x, y \leq (p-1)/2$ .

**Доказателство.** Всяко от множествата

$$\left\{ x^2 \mid 0 \leq x \leq \frac{p-1}{2} \right\} \quad \text{и} \quad \left\{ -1 - y^2 \mid 0 \leq y \leq \frac{p-1}{2} \right\}$$

се състои от две по две несравними по модул  $p$  числа, а общият им брой е  $p+1$ . Следователно съществуват  $x$  и  $y$ , такива че  $x^2 \equiv -1 - y^2 \pmod{p}$ , т.е.

$$x^2 + y^2 + 1 = tp.$$

Но

$$t = \frac{x^2 + y^2 + 1}{p} < \frac{1}{p} \left( \frac{p^2}{4} + \frac{p^2}{4} + 1 \right) < p,$$

с което лемата е доказана.

**Лема 4.3.6** Всяко просто число  $p$  може да се представи като сума от квадрати на четири цели числа.

**Теорема 4.3.7** Всяко цяло число може да се представи като сума от квадрати на четири цели числа.

## 4.4 Допълнителни задачи към Глава 4.

**Задача 4.1** Докажете, че сравнението  $x^2 \equiv -1 \pmod{n}$  е решимо тогава и само тогава, когато  $n$  е нечетно число от вида  $4t+1$ ,  $t > 0$ .

**Задача 4.2** Нека  $p$  е нечетно просто число. Докажете, че сравнението  $x^4 + 1 \equiv 0 \pmod{p}$  е решимо тогава и само тогава, когато  $p$  е от вида  $8t+1$ ,  $t > 0$ .

**Задача 4.3** Използвайки предната задача докажете, че има безброй много прости числа от вида  $8t+1$ .

**Задача 4.4** Проверете, че 666 е квадратичен остатък по модул простото число 2137.

**Задача 4.5** Докажете, че ако  $a$  и  $b$  са цели числа и  $p$  е нечетно просто число, което не дели  $a$ , то

$$\sum_{n=0}^{p-1} \left( \frac{an+b}{p} \right) = 0.$$

**Задача 4.6** Докажете, че полиномът  $x^4 + 1$  е разложим в  $\mathbb{Z}_p$  за всяко просто  $p$ .

**Задача 4.7** Докажете, че нечетното просто число  $p$  се представя като сума от вида  $p = a^2 + 3b^2$  тогава и само тогава, когато  $p$  е от вида  $6t+1$ .