Лекция 7

Факти от теория на числата

7.1 Алгоритъм на Евклид

Най-големият общ делител на две нотрицателни цели числа пресмятаме с помощта на алгоритъма на Евклид. Нека $a \geq b \geq 0$. Идеята на алгоритъма е следната: ако $b = 0$, имаме $\gcd(a, 0) = a$. В противен случай можем да разделим a на b с остатък

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

и да забележим, че $\gcd(a, b) = \gcd(b, r)$. така задачата за намиране на $\gcd(a, b)$ се свежда до по-малката задача за намиране на $\gcd(b, r)$. Тази идея е развита в следната теорема.

Теорема 7.1. *Нека a, b са цели числа, за които $a \geq b \geq 0$. Дефинираме числата $r_0, r_1, \ldots, r_{l+1}$ и $q_1, \ldots, q_l$, $l \geq 0$, както следва:*

$$\begin{array}{rcl}
a & = & r_0, \\
b & = & r_1, \\
r_0 & = & r_1 q_1 + r_2, \ \ 0 < r_2 < r_1, \\
 & \vdots & \\
r_{i-1} & = & r_i q_i + r_{i+1}, \ \ 0 < r_{i+1} < r_i \\
 & \vdots & \\
r_{l-2} & = & r_{l-1} q_{l-1} + r_l, \ \ 0 < r_l < r_{l-1} \\
r_{l-1} & = & r_l q_l, \ \ r_{l+1} = 0.
\end{array}$$

По дефиниция, $l = 0$ ако $b = 0$ и $l > 0$ в противен случай. Тогава $r_l = \gcd(a, b)$. Освен това, ако $b > 0$ $\log b / \log \phi + 1$, където $\phi = (+\sqrt{5})/2$.

Доказателство. За първото твърдение е достатъчно да забележим, че

$$\gcd(a, b) = \gcd(r_0, r_1) = \ldots = \gcd(r_{l-1}, r_l) = \gcd(r_l, r_{l+1}) = \gcd(r_l, o) = r_l.$$

За втората част да допуснем, че $b > 0$ и $l > 0$. Ако $l = 1$ твърдението очевидно е вярно. Да приемем, че $l > 1$. Твърдим, че за $i = 0, 1, \ldots, l-1$ имаме $r_{l-i} \geq \phi^i$. Твърдението ще е доказано като положим $i = l-1$ илогаритмуваме от двете страни.

За $i = 0$ и $i = 1$ имаме $r_l \geq 1 = \phi^0$ и $r_{l-1} \geq r_l + 1 \geq 2 \geq \phi^1$. За $i = 2, \ldots, l-1$ използваме индукция и факта, че $\phi^2 = \phi + 1$. Имаме

$$r_{l-i} \geq r_{l-(i-1)} + r_{l-(i-2)} \geq \phi^{i-1} + \phi^{i-2} = \phi^{i-2}(1+\phi) = \phi^i,$$

което доказва теоремата.

Теорема 7.2. *Времето за изпълнение на алгоритъма на Евклид е* $O(\operatorname{len}(a)\operatorname{len}(b))$.

Доказателство. Нека $b > 0$. Времето за изпълнение е $O(\tau)$, където $\tau = \sum_{i=1}^{l} \operatorname{len}(r_i)\operatorname{len}(q_i)$. Тъй като $r_i \leq b$ за $i = 1, \ldots, l$, имаме

$$\tau \leq \operatorname{len}(b)\sum_{i=1}^{l}\operatorname{len}(q_i) \leq \operatorname{len}(b)\sum_{i=1}^{l}(\log_2 q_i + 1) = \operatorname{len}(b)(l + \log_2(\prod_{i=1}^{l} q_i)).$$

Да отбележим, че

$$a = r_0 \geq r_1 q_1 \geq r_2 q_2 q_1 \geq \ldots \geq r_l q_l \ldots q_1 \geq q_l \ldots q_1.$$

Освен това $l \leq \log b / \log \phi + 1$. Комбинирайки това с полученото по-горе, получаваме

$$\tau \leq \operatorname{len}(b)(\log b/\log\phi + 1 + \log_2 a) = O(\operatorname{len}(a)\operatorname{len}(b)),$$

което доказва теоремата. □

Нека a и b са неотрицателни цели числа и нека $d = \gcd(a, b)$. Известно е, че съществуват цели числа s и t, такива че $as + bt = d$. Числата s и t могат да бъдат пресметнати с резширения алгоритъм на Евклид.

Теорема 7.3. *Нека* $a, b, r_0, r_1, \ldots, r_{l+1}$ *и* $q_1, \ldots, q_l$ *са като в Теорема 7.1. Дефинираме целите числа* $s_0, s_1, \ldots, s_{l+1}$ *и* $t_0, t_1, \ldots, t_{l+1}$ *както следва*

$$s_0 := 1, s_1 := 0; t_0 := 0, t_1 := 1,$$

иза $i = 1, \ldots, l$

$$s_{i+1} = s_{i-1} - s_i q_i,\ t_{i+1} = t_{i-1} - t_i q_i.$$

Тогава

(*i*) *за* $i = 0, \ldots, l+1$ *е изпълнено* $s_i a + t_i b = r_i$*; по-специално* $s_l a + t_l b = \gcd(a, b)$.

(*ii*) *за* $i = 0, \ldots, l$ *е изпълнено* $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$*;*

(*iii*) $i = 0, \ldots, l+1$ *е изпълнено* $\gcd(s_i, t_i) = 1$*;*

(*iv*) *за* $i = 0, \ldots, l$ *е изпълнено* $t_i t_{i+1} \leq 0$ *и* $|t_i| \leq |t_{i+1}|$*; за* $i = 0, \ldots, l$ *е изпълнено* $s_i s_{i+1} \leq 0$ *и* $|s_i| \leq |s_{i+1}|$*;*

(*v*) за $i = 1, \ldots, l+1$ е изпълнено $r_{i-1}|t_i| \leq a$ и $r_{i-1}|s_i| \leq b$.

Доказателство. (i) Индукция по i. За $i = 0, 1$ твъдението е ясно. За $i = 1, \ldots, l$ имаме

$$\begin{aligned} s_i a + t_i b &= (s_{i-2} - s_{i-1} q_{i-1}) a + (t_{i-2} - t_{i-1} q_{i-1}) b \\ &= (s_{i-2} a + t_{i-2} b) - (s_{i-1} a + t_{i-1} b) q_i \\ &= r_{i-2} - r_{i-1} q_{i-1} \quad (\text{ по индукция }) \\ &= r_i. \end{aligned}$$

(ii) Отново индукция по i:

$$\begin{aligned} s_i t_{i+1} - t_i s_{i+1} &= s_i (t_{i-1} - t_i q_i) - t_i (s_{i-1} - s_i q_i) \\ &= -(s_{i-1} t_i - t_{i-1} s_i) \\ &= -(-1)^{i-1} = (-1)^i. \end{aligned}$$

(iii) следва от (ii).

(iv) И двете твърдения се доказват с индукция по i. Твърдението, включващо t_i е вярно за $i = 0$; за $i = 1, \ldots, l$ имаме $t_{i+1} = t_{i-1} - t_i q_i$ и тъй като по индукционното допускане t_{i-1} и t_i имат противоположни знаци и $|t_i| \geq |t_{i-1}|$ следва, че $|t_{i+1}| = |t_{i-1} + |t_i| q_i \geq |t_i|$ и знакът на t_{i+1} е противополжен на този на t_i. Доказателството на твърдението за числата s_i е същото с разликата, че индукцията започва от $i = 1$.

(v) От уравненията

$$\begin{aligned} s_{i-1} a + t_{i-1} b &= r_{i-1}, \\ s_i a + t_i b &= r_i \end{aligned}$$

получаваме

$$a = |t_i r_{i-1} - t_{i-1} r_i| \geq |t_i| r_{i-1},$$

от което следва неравенството, включващо t_i Неравенството, включващо s_i следва по подобен начин от горната система. □

Теорема 7.4. *Времето за изпълнение на разширения алгоритъм на Евклид е* $O(\operatorname{len}(a)\operatorname{len}(b))$.

Доказателство. Ще допуснем, че $b > 0$. Достатъчно е да анализираме цената за пресмятане на редиците $\{s_i\}$ и $\{t_i\}$. Да разгледаме редицата $\{t_i\}$. Цента за прсмыатането ѝ е $O(\tau)$, където $\tau = \sum_{i=1}^{l} \operatorname{len}(t_i)\operatorname{len}(q_i)$. Имаме $t_1 = 1$ и от Теорема 7.3(v) следва, че $|t_i| \leq a$ за $i = 2, \ldots, l$. Както в доказателството на Теорема 7.2 получаваме

$$\begin{aligned} \tau &\leq \operatorname{len}(q_1) + \operatorname{len}(a) \sum_{i=2}^{l} \operatorname{len}(q_i) \\ &\leq \operatorname{len}(q_1) + \operatorname{len}(a)(l - 1 + \log_2(\prod_{i=1}^{l} q_i)) \\ &= O(\operatorname{len}(a)\operatorname{len}(b), \end{aligned}$$

като използвахме, че $\prod_{i=2}^{l} q_i \leq b$. Аналогичен аргумент показва, че всички s_i могат да бъдат пресметнати за време $O(\operatorname{len}(a)\operatorname{len}(b))$, а всъщност и за време $O(\operatorname{len}(b)^2)$. □

7.2 Сравнения

Нека $a, b, m \in \mathbb{Z}$, $m \neq 0$. Казваме, че *a е сравнимо с b по модул m*, ако m дели $b - a$. Това записваме като $a \equiv b \pmod{m}$. Ясно е, че ако $a \equiv b \pmod{m}$, то съществува цяло число c, за което $a = b + cm$. Освн това за всяко цяло число a съществува единствено цяло число b, за което $a \equiv b \pmod{m}$ и $0 \leq b < m$. Това число означаваме с $b = a \mod m$. Следващото твърдение показва, че за фиксирано m релацията $\equiv$ върху $\mathbb{Z}$ е релация на еквивалентност.

Теорема 7.5. *Нека $m > 0$ е цяло число. За всички $a, b, c \in \mathbb{Z}$ е в сила:*

(i) $a \equiv a \pmod{m}$*;*

(ii) от $a \equiv b \pmod{m}$ *следва* $b \equiv a \pmod{m}$*;*

(iii) от $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$ следва $a \equiv c \pmod{m}$.

Важно свойство на сравнениият е добрата им съгласуваност с операциите събиране и умножение.

Теорема 7.6. *За всички цели положителни цели числа m и всички $a, a'b, b' \in \mathbb{Z}$, от $a \equiv a' \pmod{m}$ и $b \equiv b' \pmod{m}$ следва*

$$a \pm b \equiv a'' \pm b' \pmod{m},$$

и

$$a \cdot b \equiv a' \cdot b' \pmod{m}.$$

Нека $m > 0$ е цяло число и нека $a \in \mathbb{Z}$. Казваме, че a' е мултипликативен обратен по модул m, ако $aa' \equiv 1 \pmod{m}$. Не е трудно да се покаже, че a има мултипликативен обратен тогава и само тогава, когато $\gcd(a, m) = 1$. От това наблюдение следва и закон за съкращаване на двете страни на сравнение.

Теорема 7.7. *Нека $a, m, x, x' \in \mathbb{Z}$ като $m > 0$. Ако a е взаимнопросто с m, то $ax \equiv ax' \pmod{m}$ тогава и само тогава, когато $x \equiv x' \pmod{m}$. По-общо, ако $d = \gcd(a, m)$, то $ax \equiv ax' \pmod{m}$ тогава и само тогава, когато $x \equiv x' \pmod{m/d}$.*

Сега ще разгледаме въпроса за решаване на линейни сравнения, т.е. сравнения от вида $ax \equiv b \pmod{m}$. Да разясним какво разбираме под различни решения на едно сравнение. Най-общо, нека $f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ и нека $(a_1, \ldots, a_n)$ ерешение на това сравнение: $f(a_1, \ldots, a_n) \equiv 0 \pmod{m}$. Ако $(b_1, \ldots, b_n)$ е n-орка,з а която $b_i \equiv a_i \pmod{m}$ за $i = 1, \ldots, n$, то $f(b_1, \ldots, b_n) \equiv 0 \pmod{m}$. Такива решения наричаме еквивалентни и няма да считаме за различни.

Теорема 7.8. *Нека a и $m > 0$ са цели числа. Сравнението $ax \equiv b \pmod{m}$ има решение тогава и само тогава, когато $d = \gcd(a, m)$ дели b. Ако d дели m сравнението има точно d решения. Ако x_0 е едно решение, то всички останали решения се задават с $x_0 + k \cdot \dfrac{m}{d}$.*

Доказателство. Нека x_0 е решнеие на сравнението $ax \equiv b \pmod{m}$. Тогава $ax_0 - b = my_0$ за някакво цяло число y_0, или, $ax_0 - my_0 = b$. Тъй като m дели лявата страна, то m дели d.

Обратно, нека d дели b. Съществуват цели числа x_0' и y_0', за които $ax_0' - my_0' = d$. Да положим $b' = b/d$ и да умножим двете страни на последното равенство по b': $a(x_0'b') - db' = m(y_0b')$. Сега $x_0 = x_0'b'$ е решение на $ax \equiv b \pmod{m}$.

Да предположим, че x_0 и x_1 са решения. От $ax_0 \equiv b \pmod{m}$ и $ax_1 \equiv b \pmod{m}$ получаваме $a(x_1 - x_0) \equiv 0 \pmod{m}$. Така m дели $a(x_1 - x_0)$ и $m' = m/d$ дели $x_1 - x_0$, т.е. $x_1 = x_0 + km'$ за някакво цяло число k. Не е трудно да се провери, че числата $x_0, x_0 + m', \ldots, x_0 + (d-1)m'$ са нееквивалентни решения. Ако $x_1 = x_0 + km'$ е някакво решение, то можем да запишем $k = rd + s$, $0 \leq s < d$, и $x_1 = (x_0 + sm') + rm$. Следователно x_1 е еквивалентно на $x_0 + sm'$. □

Следствие 7.9. *Ако a и m са взаимнопрости, то $ax \equiv b \pmod{m}$ има точно едно решение. В частност, ако p е просто число и $a \not\equiv 0 \pmod{p}$, то сравнението $ax \equiv b \pmod{m}$ има точно едно решение.*

Следствие 7.10. *Ако p просто число и p не дели цялото число a, то $a^{p-1} \equiv 1 \pmod{p}$.*

Доказателство. Разглеждаме сравненията $ax \equiv b \pmod{p}$ за $b = 1, \ldots, p-1$. Всяко от тези сравнения има единствено решение x_b и тези решения са две по две различни: ако допуснем, че $ax_0 \equiv b \pmod{p}$ и $ax_0 \equiv c \pmod{p}$, то $(a-b)x_0 \pmod{p}$ и $a \equiv b \pmod{p}$. Сега умножаваме почленно сравненията $ax_b \equiv b \pmod{p}$ за $b = 1, \ldots, p-1$ и получаваме

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p},$$

и тъй като $\gcd(p, (p-1)!) = 1$, получаваме $a^{p-1} \equiv 1 \pmod{p}$. □

Получените резултати могат да бъдат интерпретирани в термините на пръстена $\mathbb{Z}_m = \mathbb{Z}/(m)$. Така елемнтът $\overline{a} \in \mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\overline{0}\}$ е единица (има мултипликативен обратен) тогава и само тогава, когато $\gcd(a, m) = 1$. В $\mathbb{Z}_m^*$ има точно $\varphi(m)$ единици. $\mathbb{Z}_m$ е поле тогава и само тогава, когато m е просто число.

Следствие 7.11. Ако $\gcd(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Теорема 7.12. *(Китайска теорема за остатъците) Нека $m = m_1 m_2 \ldots m_t$, където $\gcd(m_i, m_j) = 1$ за $i \neq j$. Нека $b_1, b_2, \ldots, b_t$ са цели числа и да разгледаме системата от сравнения*

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \ldots, x \equiv m_t \pmod{m_t}.$$

тази система винаги има решение и всеки две решения се различават с кратно на m.

Доказателство. Да положим $n_i = m/m_i$ за $i = 1, \ldots, t$. Ясно , че $\gcd(m_i, n_i) = 1$. Затова съществуват цели числа s_i, t_i, за които $r_i m_i + s_i n_i = 1$. Ако положим $e_i = s_i n_i$. Тогава $e_i \equiv 1 \pmod{m_i}$ и $e_i \equiv 0 \pmod{m_j}$ за $j \neq i$. Непосредствено се проверява, че $x_0 = \sum_{i=1}^{t} b_i e_i$ е решение на системата.

Да предположим, че x_1 е друго решение. Тогава $x_1 - x_0 \equiv 0 \pmod{m_i}$ за $i = 1, \ldots, t$. С други думи, всяко от числата m_i дели $x - 1 - x_0$ и тъй като по условие тези числа са взаимнопрости, то $x_1 - x_0$ се ели и на $m = m_1 \ldots m_t$. □

Последната теорема допуска обобщения. Нека $S = R_1 \oplus \ldots \oplus R_t$ е директна сума на пръстени. Операциите в r се задават с

$$\begin{array}{rcl}(r_1',\ldots,r_t') + (r_1'',\ldots,r_t'') &=& (r_1'+r_1'',\ldots,r_t'+r_t''),\\ (r_1',\ldots,r_t')(r_1'',\ldots,r_t'') &=& (r_1'r_1'',\ldots,r_t'r_t''),\end{array}$$

където $r_i', r_i'' \in R_i$. Нулата и единицата на S са съответно $(0,\ldots,0)$ и $(1,\ldots,1)$. Групата от обратимите елементи на S по отношение на умножението означаваме с $S^\times$. яно, че

$$S^\times = R_1^\times \times R_2^\times \times \ldots \times R_t^\times.$$

Нека $m_1,\ldots,m_t$ са взаимнопрости цели числа и нека $\psi_i : \mathbb{Z} \to \mathbb{Z}_{m_i}$ е естественият хомоморфизъм. Разглеждаме изображение

$$\psi : \left\{\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t}\\ \psi(n) & \to & (\psi_1(n),\psi_2(n),\ldots,\psi_t(n)).\end{array}\right.$$

Ясно е, че $\psi(n) = (\psi_1(\overline{b}_1),\ldots,\psi_1(\overline{b}_t))$ тогава и само тогава, когато $\psi_i(n) = \overline{b}_i$ за всички i, т.е. $n \equiv b_i \pmod{m_i}$. Китейската теорема за остатъците гарантира, че такова n съществува. Следователно ψ е епиморфизъм. равенството $\psi(n) = 0$ е изпълнено тогава и само тогава, когат $m = m_1 \ldots m_t$ дели n. Следователно $\ker\psi = (m)$. От теоремата за хомоморфизмите получаваме следната теорема.

Теорема 7.13. *Нека* $m = m_1 \ldots m_t$, $\gcd(m_i, m_j) = 1$, *са цели числа. Изображението*

$$\psi : \mathbb{Z}_m = \mathbb{Z}/(m) \to \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_t}$$

е изоморфизъм. По-специално

$$\mathbb{Z}_m^\times \cong \mathbb{Z}_{m_1}^\times \times \ldots \times \mathbb{Z}_{m_t}^\times.$$

Ако $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ е разлагането на m на прости множители,то от теорема 7.13 получаваме:

$$\begin{array}{rcl}\mathbb{Z}_m &\cong& \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \ldots \oplus \mathbb{Z}_{p_t^{\alpha_t}},\\ \mathbb{Z}_m^\times &\cong& \mathbb{Z}_{p_1^{\alpha_1}}^\times \times \mathbb{Z}_{p_2^{\alpha_2}}^\times \times \ldots \times \mathbb{Z}_{p_t^{\alpha_t}}^\times.\end{array}$$

7.3 Структура на групата $\mathbb{Z}_m^*$

Теорема 7.14. *Групата* $\mathbb{Z}_p^\times$ *е циклична.*

Първо доказателство. За всеки делител d на $p-1$ означаваме с $\psi(p)$ броя на елементите в $\mathbb{Z}_p^\times$ от ред d. Елементите, удовлетворяващи $x^d = 1$ в $\mathbb{Z}_p^\times$ образуват подгрупа от ред d. Така имаме $\sum_{c|d} \psi(c) = d$.

Прилагайки формулата за обръщане на Мьобиус получаваме $\psi(d) = \sum_{c|d} \mu(c) d/c$. Дясната част на това равенство е равна на $\varphi(d)$. В частност $\psi(p-1) = \varphi(p-1) > 1$ за $p > 2$. така показахме, че в групата има елементи от ред $p-1$ (всъщност броят им е $\varphi(p-1)$).

Второ доказателство. Нека $p-1 = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_t^{\alpha_t}$ е разлагането на $p-1$ на прости множители. разглеждаме сравненията

$$(1)\ x^{q_i^{\alpha_i - 1}} \equiv 1 \pmod p \text{ и } (2)\ x^{q_i^{\alpha_i}} \equiv 1 \pmod p.$$

Всяко решение на (1) е решение на (2) и (2) има повече решения от (1). Нека g_i е решение на (2), което не е решение на (1), т.е. елемтът g_i поражда в $\mathbb{Z}_p^\times$ подгрупа от ред $q_i^{\alpha_i}$. Оттук следва, че $g + g_1 g_2 \dots g_t$ поражда подгрупа от ред $q_1^{\alpha_1} q_2^{\alpha_2} \dots q_t^{\alpha_t} = p-1$.

Трето доказателство. По теоретико-грпови съображения $\psi(d) \leq \varphi(d)$ за всяко d делящо $p-1$. Сумите $\sum_{d|p-1} \psi(d)$ и $\sum_{d|p-1} \varphi(d)$ са равни на $p-1$, откъдето $\psi(d) = \varphi(d)$ за всички делители d на $p-1$. Оттук $\psi(p-1) > 1$ за $p > 2$. □

Цялото число a наричаме примитивен корен по модул p, ако $\overline{a}$ поражда групата $\mathbb{Z}_p^\times$. Еквивалентно, a е примитивен корен по модул p, ако $p-1$ е най-малкото цяло ползохително число, за което $a^{p-1} \equiv 1 \pmod p$. Не съществува прост начин за намиране на примитивни корени по модул зададено просто число. Знаменитата хипотеза на Артин твърди, че ако $a > 1$ не е точен квадрат, то съществуват безброй ного прост числа, по модул които a е примитивен корен.

Пончтието примитивен корен се обобщава по очевиден начин. Нека $a, m \in \mathbb{Z}$. Ще казваме, че a е примитивен корен по модул m, ако класът от остатъци a поражда $\mathbb{Z}_m^\times$. Това е еквивалентно на изискването a и m да са взаимно прости и $\varphi(m)$ да е най-малкото цяло положително число,за което $a^{\varphi(m)} \equiv 1 \pmod m$. Казваме, че a е от ред e по модул m, ако e енай-малкото цяло положително число, за което $a^e \equiv 1 \pmod m$. С други думи, това означава, че e е редът на a в $\mathbb{Z}_m^\times$.

В общия случай $\mathbb{Z}_m^\times$ не е циклична група. (Например $\mathbb{Z}_8^\times$ не е циклична: $3^2 = 5^= 7^2 = 1 \pmod 8$. Така в нея няма елемент от ред 4.)

Сега ще обобщим Теорема 7.14. При това се оказва, че трябва да разглеждаме простото число 2 отделно от нечетните прости числа. Ще формулираме няколко необходими помощни резултати.

Лема 7.15. *Нека p е просто число и $1 \leq k \leq p-1$. Тогава $\binom{p}{k}$ се дели на k.*

Лема 7.16. *Ако $l \geq 1$ и $a \equiv b \pmod{p^l}$, то $a^p \equiv b^p \pmod{p^{l+1}}$.*

Лема 7.17. *Ако $l \geq 2$ и $p \neq 2$, то $(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}$ за всички $a \in \mathbb{Z}$.*

Теорема 7.18. *Ако p е нечетно просто число, а $l \in \mathbb{Z}^+$, то групата $\mathbb{Z}_{p^l}^\times$ е циклична.*

Доказателство. Нека $g \in \mathbb{Z}$ е примитивен корен по модул p. Тогава $g + p$ също е примитивн корен по модул p. Ако $g^{p-1} \equiv 1 \pmod{p^2}$, то

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \pmod{p^2}.$$

Тъй като p^2 не дели $(p-1)g^{p-2}p$, можем да предполагаме, че g е такъв примитивен корен за който $g^{p-1} \not\equiv 1 \pmod{p^2}$.

Твърдим, че такъв елемент g ще е примитивен корен по модул p^l. За доказателство на това е достатъчно да покажем, че ако $g^n \equiv 1 \pmod m$, то $\varphi(p^l) = p^{l-1}(p-1)|n$.

Нека $g^{p-1} = 1 + ap$, където p не дели a. Съгласно Лема 7.17 p^{l-1} е редът на елемента $1 + ap$ по модул p^l. Тъй като $(1 + ap)^n \equiv 1 \pmod{p^l}$, то $p^{l-1}|n$.

Нека $n = p^{l-1}n'$. Тогава

$$g^n = (g^{p^{l-1}})^{n'} \equiv g^{n'} \pmod{p}$$

и затова $g^{n'} \equiv 1 \pmod{p}$. Тъй като g е примитивен корен по модул p, то $p - 1$ дели n'. С това доказахме, че $p^{l-1}(p - 1)$ дели n. □

Теорема 7.19. *Числото 2^l не притежава примитивни корени за $l \geq 3$. За всяко $l \geq 3$ множеството $\{(-1)^a 5^b \mid a = 0, 1, 0 \leq b 2^{l-2}\}$ е пълна система от остатъци по модул 2^l. Оттук следва, че за $l \geq 3$ групата $\mathbb{Z}_{2^l}^{\times}$ е директно произведение на циклична група от ред 2 и циклична група от ред 2^{l-2}.*

Следствие 7.20. *Числото m има примитивни корени тогава и само тогава, когато то е от вида $2, 4, p^a$ или $2p^a$, където p е нечетно просто число.*

Нека $m, n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ и $\gcd(a, m) = 1$. Ще казваме, че a е *n-ти степенен остатък по модул m*, ако сравнението $x^n \equiv a \pmod{m}$ има решение.

Теорема 7.21. *Ако $m \in \mathbb{Z}^+$ има примитивни корени и $\gcd(a, m) = 1$, a е n-ти степенен остатък по модул m тогава и само тогава, когато*

$$a^{\varphi(m)/d} \equiv 1 \pmod{m}, \text{ където } d = \gcd(n, \varphi(m)).$$

Доказателство. Нека g е примитивен корен по модул m и $a \equiv g^b \pmod{m}$, $x \equiv g^y \pmod{m}$. Тогава сравнението $x^n \equiv a \pmod{m}$ е еквивалентно на сравнението $g^{ny} \equiv g^b \pmod{m}$, което на свой ред е еквивалентно на $ny \equiv b \pmod{\varphi(m)}$. Последното сравнение има решение тогав и само тогава, когато d дели b. Освен това, ако сравнението има едно решение, то то има точно d решения.

Ако d дели b, то $a^{\varphi(m)/d} \equiv g^{b\varphi(m)/d} \equiv 1 \pmod{m}$. Обратно, ако $a^{\varphi(m)/d} \equiv 1 \pmod{m}$, то $g^{b\varphi(m)/d} \equiv 1 \pmod{m}$; следователно $\varphi(m)$ дели $b\varphi(m)/d$, т.е. d дели b. □

Теорема 7.22. *Нека a е нечетно число, $e \geq 3$ и да разгледаме сравнението $x^n \equiv a \pmod{2^e}$. Ако n е нечетно число решение винаги съществува и е единствено. Ако n е четно решение съществува тогава и само тогава, когато $a \equiv 1 \pmod{4}$, $a^{2^{e-2}/d} \equiv 1 \pmod{2^e}$, където $d = \gcd(n, 2^{e-2})$. Ако съществува поне едно решение, то съществуват точно $2d$ решения.*

Теорема 7.23. *Нека p е нечетно просто число, $p \not| a$ и $p \not| n$.Тогава, ако сравнението $x^n \equiv a \pmod{p}$ е резарешимо, то разрешимо е и сравнението $x^n \equiv a \pmod{p^e}$ за всички $e \geq 1$. всички тези сравнения имат един и същи брой решения.*

Теорема 7.24. *Нека 2^l е най-високата степен на 2, която дели n. Нека a е нечетно и нека $x^n \equiv a \pmod{2^{2l+1}}$ е разрешимо. Тогава $x^n \equiv a \pmod{2^e}$ за всички $e \geq 2l + 1$. Освен това всички тези сравнения имат един и същи брой решения.*

7.4 Квадратичен закон за реципрочност

Нека $\gcd(a, m) = 1$. Числото a се нарича квадратичен остатък по модул m, ако сравнението $x^2 \equiv a \pmod{m}$ е разрешимо. В противен случай a се нарича квадратичен неостатък.

Теорема 7.25. *Нека $m = 2^e p_1^{e_1} \dots p_t^{e_t}$ е разлагането на числото m на прости множители и да пред предположим, че $\gcd(a, m) = 1$. Сравнението $x^2 \equiv a \pmod{m}$ е разрешимо тогава и само тогава са изпълнени следните условия:*

(i) *ако $e = 2$, то $a \equiv 1 \pmod{4}$;*
ако $e \geq 3$, то $a \equiv 1 \pmod{8}$.

(ii) за всяко i е в сила $a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$.

Тази теорема свежда въпроса за квадратичните остатъци до съответния въпрос за прости модули. Навсякъде по-нататък p ще е просто число.

Символът (a/p) име стойност 1, ако a е квадратичен остатък по модул p; стойност -1, ако a е квадратичен неостатък по модул p и нула, ако p дели a. Този символ се нарича символ на Льожандр и е изключително удобен инструмент при изследване на квадратичните остатъци. Следните свойстав на символа на Льожандр са очевидни.

Лема 7.26. Нека p е просто число, а a и b са цели числа. Тогава

(i) $a^{(p-1)/2} \equiv (a/p) \pmod{p}$;

(ii) $(ab/p) = (a/p)(b/p)$;

(iii) ако $a \equiv b \pmod{p}$, *to* $(a/p) = (b/p)$;

(iv) *броят на квадратичните остатъци по модул p е равен на броя на квадратичнте неостатъпо същия модул;*

(v) $(-1/p) = (-1)^{(p-1)/2}$.

Резултатът т. (v) може да бъде формулиран и по следния начин: сравнението $x^2 \equiv -1 \pmod{p}$ има решение тогава и само тогава, когато p е от вида $4k + 1$. Този факт позволява да се докаже, че съществуват безбой много прости числа от вида $4k + 1$. Да допуснем, че съществуват краен брой прости числ от този вид и това са $p_1, \dots, p_m$. Да разгледаме числото $(2p_1 \dots p_m)^2 + 1$. Нека p е прост делител на това число. Тогава -1 е квадратичен остатък по модул p и то има вида $4k + 1$. Но от друга страна p не е сред числата p_i, тъй като $(2p_1 \dots p_m)^2 + 1$ дава остатък 1 при делене на p_i, противоречие.

Този резултат води до следния по-общ въпрос: нека a е цяло число; за какви прости числа p числото a е квадратичен остатък по модул p? Ще използваме друга характеризация на символа (a/p), получена от Гаус.

Да разгледаме множеството $S = \{-(p-1)/2, \dots, -1, 1, \dots, (p-1)/2\}$. То се нарича множество от най-малки остатъци по модул p. Ако a е цяло число, което не се дели на p, ще означаваме с μ броя на тези наи-малки остатъци измежду числата $a, 2a, \dots, ((p-1)/2)a$, които са отрицателни.

Лема 7.27. $\left(\dfrac{a}{p}\right) = (-1)^{\mu}$.

Доказателство. Да означим с $\pm m_l$, $m_l > 0$, най-малкия остатък който дава la по модул p. Когато l пробягва стойности между 1 и $(p-1)/2$, то μ е броя на получените при това знаци минус. Нека l и k са цели числа, за които $1 \le l < k \le (p-1)/2$. лесно се проверява, че $m_l \ne m_k$. аистина, ако допуснем, че $m_l = m_k$, то $la \equiv \pm lk \mod p$ и $l \pm k \equiv 0 \pmod p$, което е невъзможно. Оттук следва, че множествата $\{1, 2, \ldots, (p-1)/2\}$ и $\{m_1, m_2, \ldots, m_{(p-1)/2}\}$. Умножавайки почленно сравненията

$$1 \cdot aa \equiv \pm m_1(p), 2 \cdot aa \equiv \pm m_2(p), \ldots, \frac{p-1}{2} a \equiv \pm m_{(p-1)/2}(p),$$

получаваме

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

Следователно $a^{(p-1)/2} \equiv (-1)^{\mu} \pmod p$ и оставе да приложим Лема 7.26(i). □

Пример 7.28. Използвайки лемата на Гаус лесно можем да докажем, че

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

Този факт може да се използва за да докажем съществуването на безброй много прости числа от вида $8k+7$. Достатъчно е даопуснем, че броят на тези числа е краен (да речем това са $p_1, \ldots, p_m$ и да забележим, че числото $(4p_1p_2 \ldots p_m)^2 - 2$ има прост делител от вида $8k+7$. □

Теорема 7.29. (квадратичен закон за реципрочност) *Нека p и q са нечетни прости числа. Тогава*

(i) $(-1/p) = (-1)^{(p-1)/2}$;

(ii) $(2/p) = (-1)^{(p^2-1)/8}$;

(iii) $(p/q)(q/p) = (-1)^{(p-1)(q-1)/2}$.

Доказателство. Първото доказателство е дадено от Гаус, който през живота си намира осем различни доказателства на тази теорема. Ще изложим доказателството на Айзенщайн, което може да бъде намерено и в [29].

Да разгледаме функцията $f(z) = e^{2\pi i z} - e^{-2\pi i z} = 2i \sin 2\pi z$. Тя удовлетворява тъждествата $f(z+1) = f(z)$ и $f(-z) = -f(z)$. Единствените ѝ реални нули са всички полуцели числа, т.е. ако $r \in \mathbb{R}$, $2r \notin \mathbb{Z}$, то $f(r \ne 0$.

Факт 1. Ако $n > 0$ е нечетно число, то

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)), \;\; \zeta = e^{2\pi i/n}.$$

Факт 2. Ако $n > 0$ е нечтно число, то

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

Да скицираме доказателство. В тъждеството от факт 1 полагаме $x = e^{2\pi iz}$, $y = e^{-2\pi iz}$ и получаваме

$$f(nz) + \prod_{i=0}^{n-1} f\left(z + \frac{k}{n}\right).$$

Имаме $f(z+k/n) = f(z+k/n-1) = f(z-(n-k)/n)$. Ако k пробягва стойностите от $(n+1)/2$ до $n-1$, то $n-k$ пробягва стойностите от $(n-1)/2$ до 1. Така получаваме

$$\begin{aligned}\frac{f(nz)}{f(z)} &= \prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right) \prod_{k=(n+1)/2}^{n-1} f\left(z+\frac{k}{n}\right) \\ &= \prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right) \prod_{k=(n+1)/2}^{n-1} f\left(z-\frac{n-k}{n}\right) \\ &= \prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right) f\left(z-\frac{k}{n}\right)\end{aligned}$$

Факт 3. Нека p е нечетно просто число, $a \in \mathbb{Z}$ като p не дели a. Тогава

$$\prod_{i=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{i=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Както в лемата на Гаус, нека $la \equiv \pm m_l \pmod{p}$, където $1 \le m_l \le (p-1)/2$. Така разликата на la/p и $\pm m_l/p$ е цяло число. Това означава, че

$$f(la/p) = f(\pm m_l/p) = \pm f(m_l/p).$$

Резулататът се получава като умножим левите и десните страни при l менящо се от 1 до $(p-1)/2$ и приложим лемата на Гаус.

Сега преминаваме към доказателството на самия закон за реципрочност. Нека p и q са нечетни прости числа. От факт 3 имаме

$$f(la/p) = f(\pm m_l/p) = \pm f(m_l/p).$$

Съгласно факт 2

$$\frac{f(ql/p)}{f(l/p)} = \prod_{m=1}^{(q-1)/2} f\left(\frac{l}{p}+\frac{m}{q}\right) f\left(\frac{l}{p}-\frac{m}{q}\right).$$

Обединявайки тези две тъждества получаваме

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}+\frac{m}{q}\right) f\left(\frac{l}{p}-\frac{m}{q}\right).$$

По същия начин получаваме

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{m}{q}+\frac{l}{p}\right) f\left(\frac{m}{q}-\frac{l}{p}\right).$$

Тъй като $f(m/q - l/p) = -f(l/p - m/q)$ от горните две равенства следва, че

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

а оттук и желаното

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

$\square$

Следващата теорема е една еквивалентна формулировка на закона за реципрочност.

Теорема 7.30. *Нека p и q са различни нечетни прости числа и нека $a \geq 1$ е цяло число. Тогава следните твърдения са еквивалентни:*

(i) $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

(ii) Ако $p \equiv \pm q \pmod{4a}$ и p не дели a, то $(a/p) = (b/p)$.

7.5 Символ на Якоби

Нека b е нечетно положително цяло число и нека $b = p_1 p_2 \dots p_m$, където p_i са прости числа (не непремнно различни). Символът (a/b), дефиниран с формулата

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_m}\right).$$

се нарича *символ на Якоби.*

Свойствата на символа на Якоби са близки до тези на символа на Льожандр. Ще отблежим, че може да се случи $(a/b) = 1$ без a да е квадратичен остатък по модул b. Все пак вярно е, че ако $(a/b) = -1$, то a не е квадратичен остатък по модул b.

Лема 7.31. *В сила са сравненията*

(i) ако $a_1 \equiv a_2 \pmod{b}$ *то* $(a_1/b) = (a_2/b)$;

(ii) $(a_1 a_2/b) = (a_1/b)(a_2/b)$;

(iii) $(a/b_1 b_2) = (a/b_1)(a/b_2)$.

Теорема 7.32. *В сила са следните равенства:*

(i) $(-1/b) = (-1)^{(b-1)/2}$;

(ii) $(2/b) = (-1)^{(b^2-1)/8}$;

(iii) ако числата a и b са нечетни и положителни, то

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/2}.$$

Тази теорема е извънредно полезна, тъй като тя позволява ефектвното пресмятане на (a/n) без да знаем разлагането на n на прости множители.