Лекция 9

Тестове за прости числа

9.1 Псевдопрости числа

За създаването на асиметрични криптосистеми се нуждаем от големи прости числа. При това тези прости числа трябва да са случайни, т.е. да нямат някакъв специален вид. Най-общо такива числа могат да се получат като се генерира някаква случайна q-ична редица от цифри $a_0, a_1, \ldots, a_m$ и направим проверка дали тази редица представя просто число, т.е. дали $a_0 + a_1 q + \ldots + a_m q^m$ е просто число. Да предположим че сме доказали следната теорема: "Ако n е просто число, то е вярно $S(n)$.", където $S(n)$ е лесно проверимо аритметично твърдение. Ако разполагаме с голямо n, за което трябва да проверим дали от е просто или съставно, то можем да проверим твърдението $S(n)$. Ако $S(n)$ не е изпълнено, то числото n е съставно; ако $S(n)$ е изпълнено, то n може да е просто или съставно. В този случай ще наречем n *S-псевдопросто число* (или *псевдопросто по отношение на S*). Например в сила е теоремата: "Ако n е просто, то $n = 2$ или n е нечетно число". Твърдението $S(n)$: ($n = 2$ или n е нечетно) се проверява лесно за всяко n. Ясно е, че този тест не е много убедително силно свидетелство за това, че n е просто. За да бъде понятието псевдопросто число полезно, то псещдопростите не трябва да бъдат "малко" на брой.

Много по-смислено твърдение $S(n)$ получаваме от малката теорема на Ферма:

$S(n)$: Ако n е просто число и a не се дели на n, то

$$a^{n-1} \equiv 1 \pmod{n}. \tag{9.1}$$

Ще казваме, че съставното число е *псевдопросто на Ферма при основа a*, ако е в сила сравнението (9.1). Лесно се проверява, че $n = 91 = 7 \cdot 13$ е псевдопросто на Ферма при основа 3, а $n = 341 = 11 \cdot 31$ е псевдопросто на Ферма при основа 2. Основа $a = 1$ е очевидно безинтересна; освен това нечетните числа n удовлетворяват (9.1) за $a = n - 1$, затова по-нататък ще предполагаме, че $1 < a < n - 1$. Следната теорема е доказана от Ердьош [23].

Теорема 9.1. *За всяко фиксирано цяло число $a \geq 2$ броят на псевдопростите числа на Ферма при основа a, които са по-малки или равни на x е $o(\pi(x))$ за $x \to \infty$.*

Изразено по-друг начин, псевдопростите числа на Ферма са малко в сравнение с простите числа.[1] Така използването на малката теорема на Ферма са различаване на прости от съставни числа би могла да се окаже полезна. Това е известно много преди доказателството на Ердьош.

Числото $n \in \mathbb{Z}^+$ ще наричаме *псевдопросто на Ферма*, ако сравнението (9.1) е изпълнено за всички цели числа a, $1 < a < n-1$, за които $\gcd(a, n) = 1$. Всяко просто число е псевдопросто на Ферма. Съгласно Теоремата на Ердьош за всяка фиксирана основа a псевдопростите числа на Ферма при основа a, които не са прости числа, са относително редки. Въпреки това съществуват безброй много от тях.

Теорема 9.2. *За всяко $a \geq 2$ съществуват безброймнго псевдопрости числа на Ферма при основа a.*

Доказателство. Ще докажем, че ако p е нечетно просто число, неделящо $a^2 - 1$, то $n = \dfrac{a^{2p} - 1}{a^2 - 1}$ е псевдопросто при основа a. Ясно е, че

$$n = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1},$$

откъдето следва, че n е съставно число. От малката теорема на Ферма слд повдигане в квадрат получаваме $a^{2p} \equiv a^2 \pmod{p}$. Така p дели $a^{2p} - a^2$. Тъй като по условие p не дели $a^2 - 1$ и тъй като

$$n - 1 = \frac{a^{2p} - a^2}{a^2 - 1}$$

получаваме, че p дели $n - 1$. Очевидно $n - 1$ е четно (сума на четен брой събираеми с една и съща четност). Следователно $2p$ дели $n - 1$ и $a^{2p} - 1$ дели $a^{n-1} - 1$. В същото време $a^{2p} - 1$ се дели на n, тъй като $a^{2p} - 1 = n(a^2 - 1)$. Оттук следва, че

$$a^{n-1} \equiv 1 \pmod{n}.$$

□

В търсенето на бърз и прост метод за различаване на нечетните прости числа можем да разгледаме комбиниране на няколко проверки на (9.1) за различни основи a. Така 341 е псевдопросто на Ферма при основа 2, но не е псевдопросто на Ферма при основа 3. Не е трудно да се докаже, че ако за нечетното, съставно число n съществува поне една основа a, за която не е изпълнено (9.1), то това сравнение не се изпълнява поне за половината основи, които са взаимнопрости с n.

Теорема 9.3. *Нека n е нечетно съставно число и нека съществува a, $1 < a < n - 1$, $\gcd(a, n) = 1$, за което $a^{n-1} \not\equiv 1 \pmod{n}$. Тогава*

$$|\{b \mid \gcd(b, n) = 1, 1 \leq b < n, b^{n-1} \equiv 1 \pmod{n}\}| \leq \frac{|\mathbb{Z}_n^*|}{2} = \frac{\varphi(n)}{2}.$$

Доказателство. Нека $b_1, \ldots, b_k$ са всички остатъци по модул n, за които е изпълнено $\gcd(b_i, n) = 1$ и $b_i^{n-1} \equiv 1 \pmod{n}$. Да положим $a_i = ab_i \pmod{n}$. лесно се проверява, че:

[1] Ако заменим условието (9.1) с $a^n \equiv a \pmod{n}$, то ще получим потенциално по-широк клас от псевдопрости на Ферма при основа a. Аналог на Теорема 9.1 в този случай е доказан в [36].

- остатъците a_i са различни;
- остатъците a_i с взаимнопрости с m;
- за всяко a_i, $i = 1, \ldots, k$, е изпълнено

$$a_i^{n-1} \equiv (ab_i)^{n-1} \equiv a^{n-1} b_i^{n-1} \equiv a^{n-1} \not\equiv \pmod{n}.$$

Оттук следва, че елементите на $\mathbb{Z}_n^*$, чийто ред не дели $(n-1)$ са поне толкова на брой, колкото са елементите, чийто ред дели $n-1$. □

Съществуват числа като, например, $561 = 3 \cdot 11 \cdot 17$, които са псеводпрости на Ферма при всяка основа a. Те са забелязани от Кармайкъл през 1910. Едно съставно число n, за което $a^n \equiv a \pmod{n}$ за всяка основа a се нарича *число на Кармайкъл*.

Ако е известно разлагането на n на прости множители, то може лесно да се определи дали то е число на Кармайкъл.

Теорема 9.4. *(критерий на Корселт) Едно съставно число n е число на Кармайкъл тогава и само тогава, когато е положително, свободно от квадрати и за всеки прост делител p на n, $p-1$ дели $n-1$.*

Доказателство. Нека n е число на Кармайкъл. По дефиниция то е съставно. Нека p е прост делител на n. От $p^n \equiv p \pmod{n}$ следва, че p^2 н дели n. така n е свободно от квадрати. Нека a е примитивен елемент по модул p. От $a^n \equiv a \pmod{n}$ следва $a^n \equiv a \pmod{p}$ и $a^{n-1} \equiv 1 \pmod{p}$. Тъй като a е от ред $p-1$, получаваме, че $p-1$ дели $n-1$.

Сега да допуснем, че n е съставно, свободно от квадрати и за всяко просто p, делящо n, имаме, че $p-1$ дели $n-1$. Ще покажем, че $a^n \equiv a \pmod{n}$ за всяко цяло число a. Тъй като n е свободно от квадрати, достатъчно е да покажем че $a^n \equiv a \pmod{p}$ за всяко цяло число a и за всеки прост делител p на n. Ако a не се дели на p, то $a^{p-1} \equiv 1 \pmod{p}$ и тъй като $p-1$ дели $n-1$ имаме $a^{n-1} \equiv 1 \pmod{p}$ и $a^n \equiv a \pmod{p}$. Но последното сравнение е тривиално изпълнено, ако p дели a. Така то е изпълнено във всички случаи. □

Забележка 9.5. Корселт доказва този критерий през 1899, но първият пример на такива числа е намерен от Кармайкъл 11 години по-късно.

Съществуват безброй много числа на Кармайкъл [2]. През 1956 г. Ердьош дава евристичен аргумент в подкрепа на факта, че съществуват безброй много числа на Кармайкъл и те не са много редки. Ако $C(x)$ означава броя на числата на Кармайкъл ненадхвърлящи x, Ердьош предполага, че за всяко $\varepsilon > 0$ съществува такова число $x_0(\varepsilon)$, че $C(x) > x^{1-\varepsilon}$ за всяко $x \geq x_0(\varepsilon)$. През 1994 Алфорд, Гранвил и Померанс не само доказват, че съществуват безброй много числа на Кармайкъл, но и дават оценка за техния брой.

Теорема 9.6. *(Alford, Granville, Pomerance) Съществуват безброймного числа на Кармайкъл. По-специално, за достатъчно големи x, броят $C(x)$ начислата на кармайкъл, ненадхвърлящи x, удовлетворява $C(x) > O(x^{2/7})$.*

Засега няма оценки за това, какво означава "достатъчно големи x" в условето на теоремата. Предполага се, че това е 96-тото число на Кармайкъл 8719309. От числови изследвания изглежда правдоподобно да е изпълнено $C(x) > 1/3$ за всички $x \geq 10^{15}$. Известно е, че за $x = 10^{15}$ съществуват $105212 < 10^5$ числа на Кармайкъл. Макар Ердьош да е предположил $C(x) > x^{1-\varepsilon}$ за $x \geq x_0(\varepsilon)$, към настоящия момнет не известно x, за което $C(x) > \sqrt{x}$.

Нежелателните ефекти от съществуването на числата на Кармайкъл могат да бъдат избягнати, ако използваме следното твърдение $S(n)$:

$S(n)$: Ако n е просто число и a не се дели на n, то

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}, \tag{9.2}$$

където (a/n) е символът на Льожандр.

Нека n нечетно съставно число и нека

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n},$$

където $\gcd(a, n) = 1$, а (a/n) е символът на Якоби. Тогава казваме, че n е *псевдопросто на Ойлер при основа* a. Ако n е псевдопросто на Ойлер при основа a, то е и псевдопросто на Ферма при същата основа. Обратното не е вярно; непосредствено се проверява, че $3^{90} \equiv 1 \pmod{91}$, но $3^{45} \equiv 27 \neq \pm 1 \pmod{91}$.

Оказва се, че за всички нечетни съставни n съществува основа a, за която (9.2) не е изпълнено. С други думи не съществува нечетно съставно n, което да е псевдопросто на Ойлер при всички допустими основи a, което от своя страна означава, че по отношение на (9.2) нямаме аналог на числата на Кармайкъл. В този случай можем да формулираме наблюдение, аналогично на Теорема 9.3.

Теорема 9.7. *Нека n е нечетно съставно число. Тогава*

$$|\{b \mid \gcd(b, n) = 1, 1 \leq b < n, b^{n-1} \equiv (b/n) \pmod{n}\}| \leq \frac{|\mathbb{Z}_n^*|}{2} = \frac{\varphi(n)}{2}.$$

Доказателство. Доказателството е аналогично на доказателството на Теорема 9.3 с тази разлика, че трябва да покажем, че съществува цяло число a', $1 \leq a' < n$, $\gcd(a', n) = 1$, за което $a'^{(n-1)/2} \not\equiv (a'/n) \pmod{n}$.

Най-напред ще разгледаме случая, когато n не е свободно от квадрати, т.е. съществува такова просто число p, че p^s дели n, $s \geq 2$. Да положим $n = p^s n'$ и $a' = 1 + n/p = 1 + p^{s-1}n'$. Сега имаме

$$\left(\frac{a'}{n}\right) = \left(\frac{a'}{p^s}\right)\left(\frac{a'}{n'}\right) = \left(\frac{a'}{p}\right)^s \left(\frac{a'}{n'}\right) = \left(\frac{1}{p}\right)^s \left(\frac{1}{n'}\right) = 1.$$

От друга страна,

$$a'^{(p-1)/2} = \left(1 + \frac{n}{p}\right)^{(n-1)/2} \equiv 1 + \frac{n(n-1)}{p} \not\equiv 1 \pmod{n}.$$

Изразът вляво не е сравним с 1 (mod n), тъй като в противен случай бихме имали, че $(n-1)/2p \in \mathbb{Z}$, т.е. p дели $n-1$, което е противоречие.

Нека сега n е свободно от квадрати и нека $n = pn'$, където p е просто число. Да фиксираме квадратичен неостатък s по модул p и да разгледаме системата:

$$\left| \begin{array}{ll} a' \equiv a & (\mathrm{mod}\ p) \\ a' \equiv 1 & (\mathrm{mod}\ \frac{n}{p}) \end{array} \right. .$$

Такова a' съществува съгласно Китайската теорема за остатъците. за символа на Якоби получаваме

$$\left(\frac{a'}{n}\right) = \left(\frac{1}{n/p}\right)\left(\frac{s}{p}\right) = -1.$$

Но ако $a'^{(n-1)/2} \equiv -\ (\mathrm{mod}\ n)$, то $a'^{(n-1)/2} \equiv -1\ (\mathrm{mod}\ n/p)$, което противоречи на $a' \equiv 1$ (mod n/p). □

9.2 Тест на Рабин-Милър

Тестът на Рабин-Милър се основава на простия факт, че за всеки полином $f(x)$ от степен k над крайно поле $\mathbb{F}_q$ уравнението $f(x) = 0$ има не повече от k корена (с отчитане на кратностите). В частност, ако p е просто число, сравнението $x^2 \equiv 1\ (\mathrm{mod}\ p)$ има точно две решения – $x = \pm 1$. Използвайки Китайската теорема за остатъците можем да докажем нещо повече.

Лема 9.8. Естественото число n е просто тогава и само тогава, когато сравнението $x^2 \equiv 1\ (\mathrm{mod}\ n)$ има точно две решения $x = \pm 1$.

Ще казваме, че x е нетривиален квадратен корен от 1 по модул n, ако $x^2 \equiv 1$ (mod n), но $x \not\equiv \pm 1$ (mod n). Така например, 6 нетривиален квадатен корен подул 35, тъй като $6^2 \equiv 1$ (mod 35) и $6 \not\equiv \pm 1$ (mod 35). От горната лема веднага следва, че ако съществува нетривиален квадратен корен по модул n, то n е съставно число.

Ако за $n = 1387$ положим $x = 2^{(n-1)/2} = 2^{693}$ лесно проверяваме, че

$$x^2 = (2^{693})^2 \equiv 1 \pmod{1397},$$

но $x = 2^{693} \equiv 512 \not\equiv 1$ (mod 1397).

Нека n е нечетно просто число от вида $n = 1 + 2^k m$, където m е нечетно число. Тогава за произволен елемент b от $\mathbb{Z}_n^*$ от ред t имаме, че или t е нечетно, или $b^{t/2} = -1$. Оттук лесно получаваме, че

$$\begin{array}{l} \text{или } a^t \equiv 1 \pmod{n}, \\ \text{или } a^{2^i t} \equiv -1 \pmod{n} \text{ за някое } 0 \le i \le j-1. \end{array}$$

Редицата от елементи на $\mathbb{Z}_n^*$

$$(b^d, b^{2m}, b^{4m}, \ldots, b^{2^{j-1}m}, b^{2^j m})$$

има един от следните два вида

$$(1, 1, 1, \ldots, 1, 1), \quad (?, ?, \ldots, -1, 1, \ldots, 1, 1).$$

Тук с "?" сме означили число $\neq \pm 1$. Ако редицата е от вида

$$(?, ?, \ldots, ?, 1, \ldots, 1, 1), (?, ?, ?, \ldots, ?, -1), (?, ?, ?, \ldots, ?, ?),$$

то n със сигурност е съставно число.

Теорема 9.9. *Нека $n \geq 3$ е нечетно число и $a \in \mathbb{Z}_n^*$. нека $n-1 = 1 + 2^k m$, където m е нечетно число. Ако кое да е от следните условия е в сила, то числото n е съставно.*

(*i*) $a^{n-1} \not\equiv 1 \pmod{n}$;

(*ii*) $a^{n-1} \equiv 1 \pmod{n}$, $a^m \not\equiv 1 \pmod{n}$ *и никое от числата в редицата*

$$(a^m, a^{2m}, \ldots, a^{2^k m} m)$$

не е $\equiv -1 \pmod{n}$.

Доказателство. Ако (*i*) е в сила, то n е съставно съгласно малката теорема на Ферма.

Нека е изпълнено (*ii*) и нека b е най-малкото число в редицата

$$(a^m, a^{2m}, \ldots, a^{2^k m} m),$$

което не е сравнимо с $1 \mod n$. Тогава $b^2 \equiv 1 \pmod{n}$, но $b \not\equiv \pm 1 \pmod{n}$. тогава $b+1$ и $b-1$ са нетривиални множители на n, □

Горната теорема води до следния тест за простота.

1) $n = 1 + 2^k m$ – нечетно число;
   b – случайно цяло число $1 < b < n-1$;

2) $i = 0$, $y = b^m \pmod{n}$;

3) `if` $i = 0$, $y = 1$ или $n-1$
   `then return` "n is probably prime";
   `if` $y > 0$, $y \neq 1$ `goto` 5);

4) $i \leftarrow i+1$; `if` $i < k$ $y \leftarrow y^2 \pmod{n}$; `goto` 3);

5) `return` "n is composite;

Теорема 9.10. *Нека $n > 9$ е нечетно съставно число. Тогава n преминавате теста (тестът дава на изхода, че n е вероятно просто) за най-много $(n-1)/4$ основи b, $1 < b < n-1$.*

Доказателство. Нека α и q са естествени числа. Броят на различните решения на

$$x^{q-1} \equiv 1 \pmod{p^\alpha}$$

е $\gcd(q-1, \varphi(p^\alpha) = \gcd(q-1, p^{\alpha-1}(p-1))$. Нека $n-1 = 2^k m$, където m е нечетно число. за да бъде n силно псевдопросто при основа b трябва да е изпълнено

- $b^m \equiv 1 \pmod{n}$ textcyrili
- $b^{2^i m} \equiv -1 \pmod{n}$ за някое $0 \leq i < k-1$.

И в двата случая $b^{n-1} \equiv 1 \pmod{n}$.

Нека $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. Съществуват

$$\gcd(n-1, p_i^{\alpha_i - 1}(p_i - 1)) = \gcd(n-1, p_i - 1)$$

решения на

$$x^{n-1} \equiv 1 \pmod{p_i^{\alpha_i}}, \;\; i = 1, \dots, s.$$

Съгласно Китайската теорема за остатъците имаме точно

$$\prod_{i=1}^{s} \gcd(n-1, p_i - 1)$$

решения на системата

$$\Big| \; x^{n-1} \equiv 1 \pmod{p_i^{\alpha_i}}, \;\; i = 1, \dots, s,$$

а следователно и на сравнението $x^{n-1} \equiv 1 \pmod{n}$.

Разглеждаме три случая:

(a) Разлагането на n съдържа проста степен $p_r^{\alpha_r}$ с експонента $\alpha_r \geq 2$;

(b) $n = p_1 p_2$, p_1, p_2 – прости числа;

(c) $n = p_1 p_2 \dots p_s$, p_i – прости числа и $s \geq 3$.

(a) Имаме

$$\frac{p_r - 1}{p_r^{\alpha_r}} = \frac{1}{p_r^{\alpha_r - 1}} - \frac{1}{p_r^{\alpha_r}} \leq \frac{1}{3} - \frac{1}{9} \leq \frac{2}{9},$$

откъдето получаваме

$$\prod_{i=1}^{s} \gcd(n-1, p_i - 1) \leq \prod_{i=1}^{s} (p_i - 1) \leq \prod_{i \neq r} (p_i - 1) \cdot (\frac{2}{9} p_r^{\alpha_r}) \leq \frac{2}{9} n < \frac{n-1}{4}$$

за $n \geq 9$.

(b) Нека $p_1 < p_2$. Тогава $p_2 - 1$ дели $n - 1 = p_1(p_2 - 1) + (p_1 - 1)$, което е невъзможно.

(c) ...

Следствие 9.11. Нека $n > 9$ е нечетно съставно число и нека b се избира по случаен начин измежду $2, 3, \dots, n-2$. Тогава вероятността n да премине през теста на Рабин-Милър е по-малка от $1/4$.

9.3 Тестът за простота на **Agrawal, Kayal** и **Saxena**

През август 2002 M. Agrawal, N. Kayal и N. Saxena анонсират детерминистичен тест за простота, който е полиномиален по време. Към този момент беше известно, че такива тестове съществуват , ако е изпълнена разширената хипотеза на Риман. Тестът на Рабин-Милър, за който очакваното време за изпълнение при вход съставно число е полиномиално. Съществува вероятностен алгоритъм, който доказва, че простите числа са прости с полиномиално очаквано време за изпълнение е алгоритъмът на Adleman–Huang. Освен това съществуваше детерминистичен "почти полиномиален" по време тест със сложност $(\ln)^c \ln\ln\ln n$. Показателят расте толкова бавно, че за практически цели мохзе да се счита за ограничен. тестът на AKS е важен не само защото окончателно решава теоретичния въпрос за доказване на простотата на дадено число, но и защото сам по себе си е твърде прост. Все още е неясно дали тестът ще може да се използва за практически, но някои негови варианти имат добри шансове за това.