інформації, яку треба повторити. Перенесення виправлення цієї помилки на верхні рівні збільшує час на її усунення.

Спосіб зменшення кількості помилок, що не виявляються в MTP2 системи *SS7*

У форматі значущої сгнальної одиниці є резервне поле довжиною в два двійкових розряди, що не використовується. Якщо це поле використати для додаткової контрольної перевірки сигнальної одиниці на достовірність, а саме перевірки на парність, то в результаті 50 % всіх помилок, що не виявлялись, буде виявлено. При цьому буде використано один розряд резервного поля. Таке рішення дасть змогу підвищити достовірність передачі даних в компоненті MTP2 та зменшити час на обробку тих помилок, які виправляються протоколами більш високих рівнів.

1. Орлов С. IP поверх *SS7*. LAN, N9, 2002. http://www.osp.ru/lan/2002/09/030.htm#vr.
2. ITU-T Q-Series Recommendation. Q.703. Message transfer part. Signalling link.
3. Битнер В.И. Общеканальная система сигнализации N7. http://center.neic.nsk.su/page_rus/htm/UCH_MAT/course2/index.

А.Ковальчук
Національний університет"Львівська політехніка"

УДК 511.217

ПРОСТІ ЧИСЛА ФЕРМА І МЕРСЕННА В СИСТЕМІ RSA

Встановлено нескінченність множини простих чисел Ферма і Мерсенна за умови, що існує хоч би два відповідні прості числа.

The infinity of a set of prime numbers Fermat and Mersenne is established provided that there are even two appropriate prime numbers

У системі *RSA*, як відомо, при шифруванні інформації для досягення високої стійкості шифру використовуються великі прості числа. Такі прості числа можна вибирати, зокрема, в нескінченних підмножинах чисел Ферма і Мерсенна.

Надалі використовуватимо таке твердження.

Аксіома нескінченного зменшення (АНЗ): якщо з твердження, за яким задане додатнє ціле число має задану множину властивостей, випливає, що існує менше до-

датнє ціле число з тією ж множиною властивостей, то ніяке ціле додатнє число не може мати цю множину властивостей [1].

Прості числа Ферма

Означення 1. Якщо число $F_n = 2^{2^n} + 1$, $n \geq 0$ є просте, то назвемо його простим числом Ферма.

Розглянемо послідовність чисел Ферма $p_0 = 3$, $p_m = 2^{p_{m-1}+1} + 1$, $m \geq 1$.

Теорема 1. Кожне число p_m є простим числом Ферма.

Доведення. Нехай p – довільний простий дільник p_m. Тоді цей дільник має наступний вигляд [2]:

$$p = l_p 2^{p_{m-2}+1} + 1. \qquad (1)$$

Позначимо $a_p = 2^{p_{m-2}+1}$. З (1) тоді випливає, що $l_p | (p-1)$ і $a_p | (p-1)$. Це означає, що $2^{l_p} \equiv 1 \pmod p$, $2^{a_p} \equiv 1 \pmod p$ і $2^{l_p} \equiv 2^{a_p} \pmod p$.

I. Якщо $l_p < a_p$, то $l_p \equiv a_p \pmod{l_p}$, тобто $l_p | a_p$ і $l_p = 2^{n_p}$, де $n_p \geq 1$ - натуральне число. Виберемо $n_p = p_{m-1} - p_{m-2} - 2$. Тоді $p = 2^{p_{m-1}+1} + 1 = p_m$ - просте число Ферма.

II. Нехай $a_p < l_p$. Тоді $a_p \equiv l_p \pmod{a_p}$, $a_p | l_p$ і $l_p = L_p a_p$, де натуральне $L_p < l_p$.

Нерівність $a_p < L_p$ відповідно до АНЗ не може виконуватися.

Отже, $L_p < a_p$ і $p = L_p (a_p)^2 + 1$. Тоді, як і в п.I., знайдемо, що $L_p = 2^{N_p}$, де $N_p \geq 1$ - натуральне число. Вибравши $N_p = p_{m-1} - 2p_{m-2} - 3$, знайдемо $p = 2^{p_{m-1}+1} + 1$, тобто p_m - просте число Ферма.

III. Покажемо, що випадок $l_p = a_p$ неможливий. Дійсно, оскільки тоді дільник p має вигляд $p = (a_p)^2 + 1$ і оскільки p – довільний простий дільник p_m, то $p_m = 2^{p_{m-1}+1} + 1 = p^s$, $s \geq 1$.

Якщо $s > 1$, то $2^{p_{m-1}+1} = p^s - 1 = (p-1)(p^{s-1} + p^{s-2} + \ldots + 1)$, причому $p_{m-1} > 2$, звідки випливає, що s є парним числом, $s = 2t$, де t - натуральне число. Тобто $2^{p_{m-1}+1} = (p^t - 1)(p^t + 1)$

Отже, числа $p^t - 1$ і $p^t + 1$, відрізняючись на 2, є степенями 2. Тому $p^t - 1 = 2$, $p^t + 1 = 4$ і $p^t = 3$, $t = 1$, $p = 3$, що суперечить рівності (1). Це означає, що $s = 1$ і $p_m = (a_p)^2 + 1$, що суперечить визначенню послідовності чисел p_m. Отримані суперечності доводять, що $l_p \neq a_p$. Теорема 1 доведена.

Наслідок 1. За допомогою циркуля та лінійки можна побудувати нескінченну множину правильних n - кутників.

Доведення випливає з теореми 1 і узагальненого твердження Гаусса [6, с.41]: за допомогою циркуля та лінійки можна побудувати правильний n-кутник тільки з числом сторін $n = 2^\nu p_1 \cdot \ldots \cdot p_m$, де $p_1, \ldots, p_m$ - прості числа Ферма і $\nu \geq 0$.

Наслідок 2. Існує нескінченна множина простих чисел p, для яких кожне ціле число є лишком будь-якого непарного степеня.

Доведення випливає з теореми 1 і твердження: для того, щоб для простого числа p кожне ціле число було лишком будь-якого непарного степеня, необхідно і досить, щоб просте p було простим числом Ферма.

Оскільки кожне F_n - взаємно просте з усіма меншими F_m, то F_n завжди дає нові прості дільники. Первісним коренем для кожного F_n є число 3. Якщо б існувало ціле

число ρ, яке би було первісним коренем лише для скінченного числа F_n, то існувало б лише скінченне число простих чисел Ферма. Але ще не доведене припущення Артина стверджує, що довільне $\rho \neq \pm 1$, яке не є квадратом, первісний корінь для несінченної множини F_n.

Прості числа Мерсенна

Означення 2. Якщо число $M_n = 2^n - 1$, $n \geq 2$, є просте, то назвемо його простим числом Мерсенна.

Розглянемо послідовність чисел Мерсенна $3 \leq q_0$ - просте, $q_m = 2^{q_{m-1}} + 1$, $m \geq 1$.

Теорема 2. Кожне число q_m є простим числом Мерсенна.

Доведення. Нехай $q < q_m$ - довільний простий дільник q_m. Тоді цей дільник має вигляд

$$q = 2l_q q_{m-1} + 1. \tag{2}$$

Дійсно, якщо q ділить q_m, то $2^{q_{m-1}} \equiv 1 (\mathrm{mod}\ q)$ і степінь 2 (mod q) ділить просте q_{m-1}, тобто, ця степінь є q_{m-1}. За Малою Теоремою Ферма степінь 2 також ділить q - 1, тобто $q - 1 = 2l_q q_{m-1}$.

З (2) випливає, що $l_q | (q - 1)$ і $2q_{m-1} | (q - 1)$. Це означає виконання конгруенцій $2^{l_q} \equiv 1 (\mathrm{mod}\ q)$, $2^{q_{m-1}} \equiv 1 (\mathrm{mod}\ q)$ і $2^{l_q} \equiv 2^{q_{m-1}} (\mathrm{mod}\ q)$.

I. Нехай $l_q < 2q_{m-1}$. Тоді $l_q \equiv 2q_{m-1} (\mathrm{mod}\ q)$ і $l_q | 2q_{m-1}$. А оскільки $(2, q_{m-1}) = 1$ і число q_{m-1} за припущенням - просте, то або $l_q = 2$, або $l_q = 2q_{m-1}$, $l_q = q_{m-1}$, $l_q = 1$.

Якщо $l_q = 2$, то $q = 4q_{m-1} + 1$. Якщо $l_q = q_{m-1}$, то $q = 2(q_{m-1})^2 + 1$, а при $l_q = 2q_{m-1}$ $q = 4(q_{m-1})^2 + 1$.

Отже q_m має вигляд

$$q_m = p_1^s p_2^t p_3^r, \tag{3}$$

де $p_1 = 4q_{m-1} + 1$, $p_2 = 2(q_{m-1})^2 + 1$, $p_3 = 4(q_{m-1})^2 + 1$ і $p_1 \neq 2$, $p_2 \neq 2$, $p_3 \neq 2$ - прості числа.

Покажемо, що (3) не може існувати.

Дійсно, якщо $p_1 = 4q_{m-1} + 1$, то $(p_1 - 1)/2q_{m-1}$ і $2^{4q_{m-1}} \equiv 2^{p_1 - 1} \equiv 1 (\mathrm{mod}\ p_1)$. Тобто виконується конгруенція $2^{4q_{m-1}} \equiv 1 (\mathrm{mod}\ p_1)$, або $(2^{q_{m-1}} - 1)(2^{q_{m-1}} + 1) \equiv 0 (\mathrm{mod}\ p_1)$, де $(2^{q_{m-1}} - 1, 2^{q_{m-1}} + 1) = 1$.

Нехай $2^{q_{m-1}} \equiv 1 (\mathrm{mod}\ p_1)$. Тоді, оскільки $2^{p_1 - 1} \equiv 1 (\mathrm{mod}\ p_1)$, то $2^{q_{m-1}} \equiv 2^{p_1 - 1} (\mathrm{mod}\ p_1)$. Остання конгруенція виконується при $(2q_{m-1}, p_1 - 1) = 2q_{m-1}$ і $(2q_{m-1}, p_1) = 1$, в силу чого з цієї конгруенції випливає, що $2^1 \equiv 2^2 (\mathrm{mod}\ p_1)$,що неможливо для простого $p_1 \neq 2$.

Нехай $2^{q_{m-1}} \equiv -1 (\mathrm{mod}\ p_1)$. Тоді $2^{q_{m-1}} \equiv -2^{p_1 - 1} (\mathrm{mod}\ p_1)$ і $2^1 \equiv -2^2 (\mathrm{mod}\ p_1)$, що також неможливо для простого $p_1 \neq 2$. Отже, $l_q \neq 2$.

Нехай тепер $l_q = q_{m-1}$. Позначимо $b = (q_{m-1})^2$. Тоді $q = 2b + 1$, $(p_2 - 1)/(q_{m-1})^2 = 2$ і $2^{2b} \equiv 2^{p_2 - 1} \equiv 1 (\mathrm{mod}\ p_2)$. Звідси випливає, що $2^{2b} \equiv 1 (\mathrm{mod}\ p_2)$, тобто $(2^b - 1)(2^b + 1) \equiv 0 (\mathrm{mod}\ p_2)$, де $(2^b - 1, 2^b + 1) = 1$.

Якщо $2^b \equiv 1 (\mathrm{mod}\ p_2)$, то оскільки $2^{p_2 - 1} \equiv 1 (\mathrm{mod}\ p_2)$, отримуємо конгруенцію $2^b \equiv 2^{p_2 - 1} (\mathrm{mod}\ p_2)$, де $(b, p_2 - 1) = b$ і $(b, p_2) = 1$, з якої випливає конгруенція $2^1 \equiv 2^2 (\mathrm{mod}\ p_2)$, що неможливо для простого $p_2 \neq 2$.

Якщо ж $2^b \equiv -1 (\mathrm{mod}\ p_2)$, то $2^b \equiv -2^{p_2 - 1} (\mathrm{mod}\ p_2)$ і $2^1 \equiv -2^2 (\mathrm{mod}\ p_2)$, що також неможливо для простого $p_2 \neq 2$. Отже, $l_q \neq q_m - 1$.

Аналогічно доводиться, що $l_q \neq 2q_{m-1}$ і $l_q \neq 1$.

Отримані суперечності доводять, що не існує простого дільника q числа q_m, такого що $q < q_m$. Це означає, що q_m - просте число.

II. Нехай $2q_{m-1} < l_q$. Тоді $2q_{m-1} \equiv l_q (\mathrm{mod}\, 2q_{m-1})$. Тобто $2q_{m-1} | l_q$ і $l_q = L_q 2q_{m-1}$, де натуральне $L_q < l_q$.

Нерівність $2q_{m-1} < L_q$ відповідно до АНЗ не може виконуватися.

Отже, $L_q < 2q_{m-1}$, $L_q | (q - 1)$ і $2^{L_q} \equiv 2^{q_{m-1}} (\mathrm{mod}\, q)$. Тоді, як в п.І., аналогічно доводиться, що $L_q \neq 1, 2, q_{m-1}, 2q_{m-1}$, що є суперечністю, з якої випливає, що q_m - просте число. Теорема 2 доведена.

Наслідок 3. Досконалих парних чисел E_n - нескінченна множина, оскільки, як відомо [3, с.42], таке число має вигляд $E_n = 2^{n-1}M_n$, де M_n - просте число Мерсенна. Зауважимо, що кожне парне досконале число є значенням полінома $h(x) = 2x(4x - 1)$, оскільки при $x = 2^{n-1}$, $n \geq 2$, отримуємо що $h(2^{n-1}) = 2^{n-1}M_n$.

Наслідок 4. У зв'язку з простими числами Мерсенна і простими числами Ферма має місце наступна теорема: існує нескінченне число натуральних n, для яких кожне з чисел n і $n + 1$ має тільки один простий дільник. Доведення випливає з твердження [12, с.23]: теорема, за якою існує нескінченне число натуральних n, для яких кожне з чисел n і $n + 1$ має тільки один простий дільник рівносильна теоремі про те, що існує нескінченне число простих чисел Мерсенна, або нескінченне число простих чисел Ферма.

1. Эдвардс Г. Генетическое введение в алгебраическую теорию чисел. – М.: Мир, 1980. – 484с.
2.Трост Э. Простые числа. – М.: Госиздат. физ.-мат. л-ры, 1959. – 135 с.

Ю.Рашкевич, Д.Пелешко, М.Пасєка
Національний університет "Львівська політехніка"

УДК 621.372

ОПТИМІЗАЦІЯ ПРОЦЕСУ ПОШУКУ ІНФОРМАЦІЇ В БАЗАХ ДАНИХ СИСТЕМ УПРАВЛІННЯ НАВЧАННЯМ

Пропонується метод прискорення пошуку символьних рядків в системах зберігання даних, побудований на основі представлення слова чи фрази у вигляді дискретного сигналу.