УДК 681.3.06, 65.012

В. Я. ПЕВНЕВ

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ МЕТОДИКИ ПОСТРОЕНИЯ ПСЕВДОПРОСТЫХ ЧИСЕЛ

Рассматривается проблема построения простых чисел. Предлагается новый подход, который основывается на построении псевдопростых чисел. Вводится новое понятие факториала простых чисел. Для теоретического обоснования данной методики формулируются и доказываются теоремы. На основе представленных теорем производится поиск псевдопростых чисел на выделенном диапазоне числовой оси. Рассматривается возможность увеличения диапазона поиска за счет использования составных чисел. Для уменьшения количества составных чисел предлагается разбиение диапазона поиска на определенное количество частей. Выдвигается гипотеза о зеркальности и повторяемости псевдопростых чисел.

Ключевые слова: *простые числа, псевдопростые числа, простые сомножители, факториал простых чисел, диапазон поиска, составное число.*

Введение

Все более ускоряющее развитие инфокоммуникационных технологий ставит все более серьезные задачи для обеспечения информационной безопасности пользователей. Любой компьютер, находящийся в сети, становиться доступным из любой точки земного шара. Назойливо предлагается использование внешних хранилищ данных, при этом никто не дает гарантий обеспечение их конфиденциальности. В этих условиях простому пользователю остается надеяться только на себя.

Одним и самым простым и надежным способом обеспечения конфиденциальности является криптографическая защита. На сегодня стойкость криптосистем обуславливается секретностью ключа. В асимметричных системах шифрования эта секретность напрямую зависит от размера ключа. В основу системы RSA положена задача факторизации, относящаяся к классу NP-полных задач. Размер ключей составляет 2048 и более бит. И здесь возникает другая задача – нахождение простого числа (ПЧ) большой размерности.

В теории чисел одной из основных проблем, имеющих многовековую историю, является проблема ПЧ. Первым алгоритмом, который дошел до наших дней, является решето Эратосфена [1]. Этим алгоритмом пользуются и по сей день. Сложность работы с ПЧ обусловлено тем, что математики не могут найти закона их распределения по числовой оси.

Анализ основных достижений и литературы. Для построения больших ПЧ во многих источниках используется следующий метод [1]. Строится последовательность простых чисел $\mathbf{p_1 < p_2 < p_3 < \ldots}$, пока не найдется простое число необходимой величины. Простое нечетное число $\mathbf{p_1}$ выбирается произвольно. После того, когда будет построено простое $\mathbf{p_{i-1}}$, выбирается случайное $\mathbf{r}$, $1 \le \mathbf{r} \le \mathbf{p_{i-1}} - 1$. Пусть $\mathbf{r} = 2\mathbf{s}\cdot\mathbf{t}$, $\mathbf{t}$ – нечетно. Тогда в качестве кандидата на очередное простое $\mathbf{p_i}$ берется

$$\mathbf{n} = 2\mathbf{r}\mathbf{p_{i-1}} + 1 = 2^{s+1} * \mathbf{p_{i-1}}\cdot\mathbf{t} + 1.$$

Далее n проверяется на простоту известными методами. Недостаток такого подхода очевиден – вероятность угадывания ПЧ при больших числах (>200D) слишком мала.

Другая группа методов [2, 3] основывается на выборе арифметической последовательности либо сумме произведений простых чисел с единицей. Главный недостаток всех рассмотренных методов - получение прогнозируемых ПЧ, которые достаточно легко повторить. Если полученные таким образом ПЧ использовать в качестве ключей в системах шифрования, то возникает возможность построения пула ключей, наиболее часто используемых пользователями. Это ведет к достаточно быстрой их компрометации. Об этой проблеме уже открыто заявляют специалисты в области защиты информации [4].

Цель роботы. Целью роботы является продолжение теоретических и экспериментальных исследований законов распределения ПЧ.

Постановка задачи. Усовершенствовать теоретическую основу методики построения множества псевдопростых чисел (ППЧ).

1. Материалы и результаты исследований

При определении простоты числа большинство методов более или менее явно производит проверку взаимной простоты между проверяемым числом и ПЧ, меньшими квадратного корня проверяемого числа. Одним из способов уменьшения количества проверяемых чисел - это удаление из их последовательности заведомо составных. В работе [5] представлены и доказаны теоремы о возможности использования непересекающихся множеств ПЧ для определения ППЧ. В предлагаемой работе доказываются теоремы для общего случая.

Теорема 1. Сумма (разность) произведений двух непересекающихся множества простых чисел есть взаимно простое число с каждым из элементов этих множеств.

$$\text{НОД}\left(\left(\prod_{i=1}^{k} a_i \pm \prod_{j=1}^{l} b_j\right),\ \forall x \in X = A \bigcup B\right) = 1,$$

где $a \in A; |A| = k;$

$b \in B; |B| = l;$

$A \subset P;$

$B \subset P;$

$A \bigcap B = 0;$

P – множество ПЧ.

Доказательство теоремы 1.

Рассмотрим любой элемент **a** принадлежащий множеству **A** $\mathbf{a} \in$ **A**. Очевидно, что для любого **a** верны выражения

$$\text{НОД}\left(\prod_{i=1}^{k} a_i,\ \forall\, a \in A\right) = a,$$

$$\text{НОД}\left(\prod_{j=1}^{l} b_j,\ \forall\, a \in A\right) = 1.$$

Следовательно, основываясь на вышеприведенных рассуждениях,

$$\text{НОД}\left(\left(\prod_{i=1}^{k} a_i \pm \prod_{j=1}^{l} b_j\right),\ \forall a \in A\right) = 1.$$

Аналогичное доказательство можно привести для любого элемента **b** принадлежащего множеству **B** $\mathbf{b} \in$ **B** и в результате получим, что

$$\text{НОД}\left(\left(\prod_{i=1}^{k} a_i \pm \prod_{j=1}^{l} b_j\right),\ \forall\, b \in B\right) = 1.$$

Т.к. элемент **x** принадлежит объединению двух непересекающихся множеств ПЧ **A** и **B**, то можно констатировать, что теорема доказана.

Прежде чем рассмотреть следствие, введем новое понятие «факториал простых чисел» и обозначим его следующим образом $\boldsymbol{\pi}(\mathbf{n})!$. Данная запись обозначает произведение всех ПЧ не больших **n.** Например $\boldsymbol{\pi}(7)! = \boldsymbol{\pi}(8)! = \boldsymbol{\pi}(9)! = \boldsymbol{\pi}(10)! = 2*3*5*7 = 210$. Фактически, как это принято в теории чисел, $\boldsymbol{\pi}(\mathbf{n})$ означает количество ПЧ на интервале от 1 до **n**, т.е. их количество в произведении.

Следствие теоремы 1. Если взять $\boldsymbol{\pi}(\mathbf{n})!$ и прибавить к нему 1, то полученное число будет взаимно простым со всеми ПЧ, не большими **n**. В научной литературе такие числа часто называют ППЧ. Исходя из теоремы 1, следующим взаимно простым будет число, полученное как сумма $\boldsymbol{\pi}(\mathbf{n})!$ и первого ПЧ большего **n**. Если к $\boldsymbol{\pi}(\mathbf{n})!$ прибавить следующее ПЧ, то вновь получиться ППЧ. Постепенно наращивая значения индекса ПЧ, можно получить возможное место нахождение ППЧ.

Теорема 2. На интервале между $\boldsymbol{\pi}(\mathbf{n})!$ +1 и прибавляемыми ПЧ все числа будут составными, кроме чисел, получившихся в результате сложения, причем максимальное ПЧ должно быть меньше квадрата первого прибавляемого ПЧ.

Доказательство теоремы 2.

Рассмотрим ПЧ $\mathbf{a_i}$, принадлежащее множеству ПЧ **A**.

$$a_i \in A;\quad |A| = B;\ B >> \pi(n),$$

где **B** – мощность множества **A**.

Доказательство начнем с условия теоремы. Если рассмотреть число, равное сумме $\boldsymbol{\pi}(\mathbf{n})!$ и произведения двух ПЧ, больших **n**, то оно, согласно теореме 1, будет ППЧ. Это число может быть ПЧ. Предположим, что минимальное ПЧ, большее **n**, равно **a**. Тогда минимальным произведением двух ПЧ, не входящих в **n**, может быть числом $\mathbf{a^2}$. Т.о. максимальное ПЧ, которое можно использовать для определения ППЧ должно быть меньше числа $\mathbf{a^2}$.

Рассмотрим первую часть теоремы. Для определения простоты числа рассматриваются числа, меньшие или равные корню квадратному из этого числа. Если ни одно из рассматриваемых чисел не будет делителем, то число признается простым. Это означает, что на интервале от числа **a** до числа $\mathbf{a^2}$ будут только простые или составные числа, в которых как минимум один из сомножителей меньше

или равен **n.** Все ПЧ, согласно теореме 2, участвующие в формировании интервала определения, находятся на числовой оси между числами **a** и $\mathbf{a}^2$. Оставшиеся числа являются составными.

Доказательство завершено.

Замечание к теор. 2. Приведенный диапазон касается однозначного определения ППЧ. Если прибавляемое ПЧ будет больше $\mathbf{a}^2$, то часть чисел, которые окажутся внутри интервала между суммой **π**(**n**)! и двумя соседними ПЧ, могут оказаться ППЧ. Для того, чтобы этого не произошло необходимо построить все возможные комбинации ПЧ, больших **n**, включая и их степенные значения.

Как доказано в теор.2, для однозначного определения ППЧ величина добавляемого ПЧ не должна превосходить квадрата первого ПЧ, большего **n**. Много это или мало? При рассмотрении больших чисел **n** > 200 **D** это будет относительно небольшое число. Например **π**(**1000**)! будет соответствовать числу 416 **D.** Диапазон рассматриваемых ПЧ будет равен 1018081. На этом интервале необходимо будет проверить 79682 ППЧ, что составляет менее 8 процентов. Следует отметить и возможность увеличение проверяемого интервала, согласно теор.1, за счет вычитания из **π**(**n**)!. В этом случае диапазон проверяемых чисел увеличивается до 2036162, а их количество- до 944648. Для увеличения ППЧ возможно использовать не только простые числа, но и их комбинации. При этом в эти комбинации не должны входить числа, являющиеся сомножителями **π**(**n**)!.

Рассмотрим число **π**(**11**)! =2310, и следующее за ним число **π**(**13**)! =30030. Для того, чтобы найти все ПЧ на интервале от 2310 до 30030 необходимо взять ПЧ от 13 до 28720. Таких чисел 3123. Кроме этого все возможные комбинации составят еще 2001. Итого получается 5124 числа, которые необходимо проверить. Для определения ПЧ, при условии определения всех ПЧ меньших 2310, требуется найти еще 2785 ПЧ. Если учесть то, что на выделенном интервале находится 2905 ПЧ (включая число 2311), то КПД предлагаемого метода в данном примере – 56,7 процента.

Для уменьшения количества предварительных вычислений можно предложить следующий метод. Разбиваем интервал от 2310 до 30030 на двенадцать равных частей.

Часть первая от **π**(**11**)! до 2* **π**(**11**)! (от 2310 до 4620).

Часть вторая от 2* **π**(**11**)! до 3* **π**(**11**)! (от 4620 до 6930).

Часть двенадцатая от 12* **π**(**11**)! до **π**(**13**)! (от 27720 до 30030).

В каждой из приведенных частей выполняются одинаковые действия с одинаковыми множествами чисел: используется 336 ПЧ и 203 составных чисел.

При использовании данного метода возможен независимый поиск ПЧ в любой части выделенного интервала, или, другими словами, возможно распараллеливание вычислительного процесса.

Выводы

В статье представлено теоретическое обоснование методики поиска ППЧ. Использование сформулированных и доказанных теорем позволяет уменьшить количество рассматриваемых вариантов при нахождении ПЧ.

Введенное понятие факториала простых чисел позволяет более компактно излагать представленные теоретические рассуждения и наглядно показывать практическое применение теоретического материала.

В статье явно не показаны свойства ППЧ, которые можно выявить, используя доказанные теоремы. Это повторяемость и зеркальность отображения множества ППЧ. В некотором смысле, основываясь на этих свойствах, можно предположить о некоторой закономерности расположения ПЧ на числовой оси. Но данный вопрос предполагает проведения большого количества экспериментальных исследований и выходит за рамки представленной статьи.

Литература

1. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Текст] / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

2. Couvreur, C. An introduction to fast generation of large primes [Text] / C. Couvreur, J. J. Quisquater // Philips J. Res. –1982. – V. 37. – P. 231–264.

3. Mihailescu, P. Fast generation of provable primes using search in arithmetic progressions [Text] / P. Mihailescu // Advances in cryptology– CRYPTO '94 -Santa Barbara, CA, 1994. – P. 282–293.

4. Mimoso, M. Prime Diffie-Hellman Weakness May Be Key to Breaking Crypto [Электронный ресурс] / M. Mimoso. – Режим доступа: https:// threatpost.com/prime-diffie-hellman-weakness-may-be-key-to-breaking-crypt/115069/#sthash.wnLEv2zR.dpuf. - 18.10.2015.

5. Певнев, В. Я. Генератор простых чисел [Текст] / В. Я. Певнев // Кафедра систем інформації : Зб. наукових праць. – Х. : ТОВ «Щедра садиба плюс», 2014. - С. 140-146.

6. Певнев, В. Я. Методика построения псевдопростых чисел [Текст] / В. Я. Певнев // Системи обробки інформації. – Х. : ХУПС ім. І. Кожедуба. 2016. – Вип. 3(140). - С. 30-32

References

1. Vasilenko, O. N. *Teoretiko-chislovye algoritmy v kriptografii*. Moskow, MCNMO Publ., 2003. 328 p.

2. Couvreur, C., Quisquater, J. J. An introduction to fast generation of large primes. *Philips J. Res*., 1982, vol. 37, pp. 231–264.

3. Mihailescu, P. Fast generation of provable primes using search in arithmetic progressions. *Advances in cryptology–CRYPTO '94 -Santa Barbara*, CA, 1994, pp. 282–293.

4. Mimoso, M. *Prime Diffie-Hellman Weakness May Be Key to Breaking Crypto*. Available at: https://threatpost. com/prime-diffie-hellman-weakness-may-be-key-to-breaking-crypto/115069/#sthash. wnLEv2zR.dpuf (accessed 18.10.2015).

5. Pevnev, V. Ja. Generator prostyh chisel. *Kafedra sistem informacii. Zbirnik naukovih prac'*, Kharkov, TOV «Shhedra sadiba pljus» Publ., 2014, pp. 140-146.

6. Pevnev, V. Ja. Metodika postroenija psevdo-prostyh chisel. *Sistemi obrobki informacii*. Kharkov, HUPS im. I. Kozheduba Publ., 2016, no. 3(140), pp. 30-32.

Поступила в редакцию 22.03.2016, рассмотрена на редколлегии 14.04.2016

ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ МЕТОДИКИ ПОБУДОВИ ПСЕВДОПРОСТИХ ЧИСЕЛ

В. Я. Пєвнєв

Розглядається проблема побудови простих чисел. Пропонується новий підхід, який ґрунтується на побудові псевдопростих чисел. Вводиться нове поняття факторіала простих чисел. Для теоретичного обґрунтування даної методики формулюються та доводяться теореми. На основі представлених теорем проводиться пошук псевдопростих чисел на виділеному діапазоні числової осі. Розглядається можливість збільшення діапазону пошуку за рахунок використання складених чисел. Для зменшення кількості складених чисел пропонується розбиття діапазону пошуку на певну кількість частин. Було висунуто гіпотезу про дзеркальність та повторність псевдопростих чисел.

Ключові слова: прості числа, псевдопрості числа, прості множники, факторіал простих чисел, діапазон пошуку, складно число.

THE THEORETICAL JUSTIFICATION FOR METHODOLOGY OF CONSTRUCTING PSEUDO-PRIMES

V. Ja. Pevnev

The problem of constructing primes is considering. The new approach, which is based on the construction of the candidates for pseudo-prime is proposed. The new definition of the factorial of primes is introduced. For the theoretical foundation of this methodology the theorems are formulated and proved. On a base of introduced theorems the search of pseudo-primes on a dedicated range of integer axis is conducted. The opportunity of increasing of search range using composite numbers is considered. To reduce the number of composite numbers decomposition of the search range for a certain number of parts is proposed. The hypothesis of symmetry and repetition of pseudo-primes is introduced.

Keywords: primes, pseudo-prime, prime factors, factorial primes, the search range, a composite number.

Певнев Владимир Яковлевич – канд. техн. наук, доцент, доцент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», e-mail: pevnevvy@mail.ru.

Pevnev Vladimir Jakovlevich – PhD, associate professor, assistant professor of the Department of Computer Systems and Networks of the National Aerospace University. N. E. Zhukovsky "KhAI", e-mail: pevnevvy@mail.ru.