УДК 681.3.06, 65.012

В.Я. Певнев

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

RSA И ПРОСТЫЕ ЧИСЛА

Рассматривается проблема построения простых чисел. Указаны главные недостатки существующих подходов к нахождению простых чисел. Рассмотрен алгоритм построения системы асимметричного шифрования RSA. Показана зависимость системы RSA от правильности нахождения функции Эйлера. Представлен пример определения простоты числа, основанный на правильности определения нахождения функции Эйлера. Показана возможность формирования прямого и обратного чисел, исходя из простоты проверяемого числа. Сформулировано утверждение о необходимости условия простоты чисел с использованием пары прямого и обратного чисел во множестве ненулевых элементов кольца Z(p-1).

Ключевые слова: *простые числа, алгоритм RSA, функция Эйлера, прямое число, обратное число, простые сомножители.*

Введение

В теории чисел одной из основных проблем, имеющих многовековую историю, является проблема нахождения простых чисел (ПЧ). Первым алгоритмом, который дошел до наших дней, является решето Эратосфена [1]. Сложность нахождения ПЧ обусловлено тем, что математики не могут найти закона их распределения на числовой оси.

Современные алгоритмы нахождения ПЧ достаточно просты и состоят из двух частей. Это определение кандидатов на ПЧ и проверка выбранных кандидатов на простоту.

Большинство алгоритмов в качестве кандидатов выбирают нечетные числа или числа специального вида (Ферма, Мерсенна, Кармайкла).

Проблема построения детерминированного алгоритма проверки простоты натуральных чисел, имеющего приемлемую полиномиальную временную оценку, является одной из важнейших проблем теории чисел. Для проверки на простоту, ввиду отсутствия эффективных детерминированных алгоритмов, чаще всего используют вероятностные алгоритмы (Ферма, Соловея-Штрассена, Миллера-Рабина).

Анализ основных достижений и литературы. Наиболее известной по представлению материалов, касающихся нахождению и распределению ПЧ, является книга К. Прахара, изданная в 1957 году в Германии [2]. Наиболее полными работами по современным методам нахождению ПЧ и факторизации являются [1, 3, 4]. В работах [5 – 7] рассматриваются как закономерности в распределения ПЧ, так и некоторые их свойства.

В абсолютном большинстве алгоритмов нахождения ПЧ процесс начинается с вычисления числа заданной размерности. После этого построения полученное число проверяется на простоту различными тестами, и если оно проходит эти проверки, то объявляется ПЧ. Недостатком подобного подхода является избирательное определение ПЧ. Шаг между двумя кандидатами при определении ПЧ достаточно большой и много простых чисел просто выпадает из процесса их нахождения.

В [5 – 7] предложен и теоретически обоснован принципиально новый подход к построению ПЧ. Он основан на выделении множества псевдопростых чисел (ППЧ), которые могут стать ПЧ. Причем с ростом размерности искомого ПЧ количество ППЧ, предлагаемых для проверки, уменьшается. При этом ни одно ПЧ не пропускается.

Целью работы является разработка детерминированного полиномиального алгоритма определения ПЧ. **Постановка задачи.** Применить теоретическое обоснование асимметричного алгоритма RSA для определения простоты чисел.

Материалы и результаты исследований

На сегодняшний день главным «потребителем» ПЧ являются асимметричные алгоритмы шифрования. Самым известным и наиболее распространенным является алгоритм RSA. Напомним читателю данный алгоритм.

1. Выбираются два больших простых числа P и Q.
2. Выбранные числа перемножаются между собой, образуя основание системы $N = P * Q$.
3. Вычисляется функция Эйлера $\varphi(N) = (P-1)*(Q-1)$.
4. Произвольно выбирается открытый ключ K_o при соблюдении условий $K_o<\varphi(N)$, $НОД(K_o, \varphi(N))=1$.
5. Вычисляется закрытый ключ $K_з=f(K_o, \varphi(N))$.
6. Рекомендуется сделать проверку правильности выбора ключей $K_o*K_з \equiv 1 \bmod \varphi(N)$.
7. Производится шифрование текста C следующим образом:

$E = C^{K_o} \bmod N$.

8. Расшифрование зашифрованного текста E осуществляется следующим образом:

$C = E^{K_з} \bmod N$.

Алгоритм достаточно прост, и в нем имеется лишь одно слабое звено – это нахождение ПЧ. С точки зрения теории эта задача достаточно проста. Необходимо разделить проверяемое число на все ПЧ, меньшие квадратного корня из данного числа. Но здесь вступают в силу неопровержимые законы математики, и в частности проклятие размерности. На первом миллиарде ПЧ более 50 миллионов. И с увеличением искомого числа количество простых чисел также растет. Следует отметить, что в современных асимметричных системах шифрования размер ключа в 300 десятичных знаков вызывает усмешку у специалистов, т.к. используются ключи размером в 4 килобита и более.

Законы распределения ПЧ достаточно сложны для того, что гарантированно определить местоположение такого числа. В работе [7] показана практическая, теоретически обоснованная, возможность определения минимального расстояния между двумя соседними ПЧ. С помощью предложенного подхода можно резко уменьшить количество проверяемых чисел на простоту, при этом ни одно ПЧ не будет пропущено.

Следующим этапом поиска ПЧ будет определение простоты проверяемого числа. Как было указано выше, ни один из существующих точных алгоритмов за приемлемое время решить данную проблему не может. Следует отметить тот факт, что в [8] приведен детерминированный полиномиальный алгоритм AKS определения простоты чисел, однако его сложность составляет $O(\log^{18} n)$ [9]. Этот факт делает данный алгоритм неудобным для практического применения.

Недостатком применения вероятностных алгоритмов проверки чисел на простоту является достаточно большое количество повторений одного и того же шага. В большинстве алгоритмов в качестве инструмента проверки произвольно выбирается какое-либо число z. И проверка будет продолжаться до достижения заранее определенной вероятности простоты проверяемого числа. Увеличением скорости проверки может быть выбор числа z как произведения множества простых чисел. Причем на каждом шаге эти множества будут непересекаемыми. Эффективность такого выбора проверяющего числа хорошо видна на примере алгоритма Эвклида для нахождения НОД.

Алгоритм RSA использует достаточно интересное свойство, называемое в криптографии обратным числом. Следует отметить свойство пары прямого и обратного числа это ее уникальность. Уникальность состоит в том, что ни одно из этих чисел не встречается ни в одной из остальных пар при фиксированном φ(N). Можно также сказать, что любая из этих пар опосредственно связана с каждым из сомножителей числа N.

Рассмотрим пример применения алгоритма RSA.

1. Выбираем числа 5, 143
2. N = 715
3. φ (N) = 4*142 =568
4. Ко = 7
5. Кз = 487
6. Кз * Ко ≡ 3409 mod (568) ≡ 1 mod (568)
7. $E = C^{Ko} \bmod (N) = 3^7 \bmod (715) = 42$
8. $C = E^{Kз} \bmod (N) = 42^{487} \bmod (715) = 653$

Результат, полученный после расшифрования шифртекста, не совпадает с исходным. Наиболее вероятная ошибка заключается в неправильном определении закрытого ключа. Но в предложенном алгоритме в п.6 была проверена правильность выбора пары ключей, и эта проверка успешна прошла. Отбрасывая ошибки в ходе вычислений, остается сделать вывод, что были неправильно определены числа, образующие основание системы RSA. Число 5 сомнений не вызывает, а число 143 раскладывается на два сомножителя 11 и 13.Если повторить проведенную процедуру, то она примет следующий вид.

1. 143 = 11* 13
2. Выбираем ПЧ =5
3. N = 715
4. φ (N) = 10*12*4 = 480
5. Ко = 7
6. Кз = 343
7. Кз * Ко ≡ 2401 mod (480) ≡ 1 mod (480)
8. $E = C^{Ko} \bmod (N) = 3^7 \bmod (715) = 42$
9. $C = E^{Kз} \bmod (N) = 42^{343} \bmod (715) = 3$

В данной версии полученный текст «3» совпадает с исходным.

Таким образом, можно сделать вывод, что в первом примере была произведена удачная попытка применения полиномиального алгоритма определения простоты числа, которая подтвердила составной характер числа 143.

Сформулируем данный алгоритм.

1. Выбирается число P, которое необходимо проверить на простоту.
2. Выбирается ПЧ малого размера Q.
3. Выбранные числа перемножаются между собой, образуя число N = P * Q.
3. Вычисляется функция Эйлера

$$\varphi(N) = (P-1)*(Q-1).$$

4. Произвольно выбирается число К при соблюдении условий $K<\varphi(N)$, НОД(К, φ(N))=1.
5. Вычисляется обратное к числу К число К1.
6. Проверяется правильность выбора пары $K*K1 \equiv 1 \bmod \varphi(N)$.
7. Производится вычисления числа Е с использованием произвольного числа С следующим образом:

$E = C^K \bmod N$.

8. Вычисление числа С1 осуществляется следующим образом:

$C1 = E^{K1} \bmod N$.

9. Если С = С1, то выбранное нами число (п.1) простое, иначе составное.

Исходя из представленного алгоритма, получаем:

$$C1 = E^{K1} \bmod N = (C^K \bmod N)^{K1} \bmod N = C^{K*K1} \bmod N. \quad (1)$$

С точки зрения теории чисел, определяющим для получения прямого и обратного чисел необходимо только одно число. В системе RSA в качестве такого числа выбирается функция Эйлера. Если взять простое число P, то функция Эйлера будет равна P-1. Исходя из этого, можно выбрать открытый ключ и вычислить закрытый во множестве ненулевых элементов кольца Z(p-1). В качестве ПЧ выбираем число P=2657. В табл. 1 представлены различные пары прямых и обратных чисел в кольце Z (2656).

Таблица 1

Пары прямых и обратных чисел в кольце Z (2656)

P	P-1	K	K1	K*K1	C
2657	2656	3	1771	5313	3
		5	2125	10625	3
		9	2361	21249	3
		13	613	7969	3
		15	2479	37185	3

Как видно из табл. 1, в том случае если число простое, то вне зависимости от пары, получается один и тот же ответ, совпадающий с исходным.

В том случае, если число составное, ответ будет иным. Это хорошо видно из примера применения алгоритма RSA. Исходя из того, что C = C1, формула (1) приобретает следующий вид:

$$C^{K*K1} \equiv C \bmod P.$$

Разделив обе части сравнения на C получаем:

$$C^{K*K1-1} \equiv 1 \bmod P. \quad (2)$$

В переводе на привычный математикам язык, полученная формула (2) приобретет такой вид:

$$a^{(k*k1)-1} \equiv 1 \bmod P. \quad (3)$$

Данная формула практически полностью повторяет малую теорему Ферма [1], за исключением показателя степени. Получив данную формулу можно сформулировать следующее утверждение.

Утверждение. Необходимым условием простоты числа P является выполнение сравнения

$$a^{(k*k1)-1} \equiv 1 \bmod P,$$

где k и k1 – пара прямого и обратного чисел во множестве ненулевых элементов кольца Z(p-1).

Доказательством данного утверждения, на взгляд автора, можно считать весь предыдущий материал, изложенный в данной работе.

Выводы

В статье предлагается методика определения простоты чисел на основе алгоритма RSA. Основываясь на особенностях функции Эйлера, предлагается построить алгоритм определения простоты чисел. Используя данный подход, сформулировано утверждение о необходимом условии определения простоты исследуемого числа.

Список литературы

1. *Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.*
2. *Прахар К. Распределение простых чисел / К. Прахар. – М.: Мир, 1967. – 513 с.*
3. *Крэндалл Р. Простые числа: Криптографические и вычислительные аспекты / Р. Крэндалл, К. Померанс. – М.: УРСС: Кн. «ЛИБРОКОМ»,. 2011. – 664 с.*
4. *Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов. – Казань: Казан. ун., 2011. – 190 с.*
5. *Певнев В.Я. Генератор простых чисел / В.Я. Певнев // Кафедра систем інформації: Зб. наукових праць. – Х.: ТОВ «Щедра садиба плюс», 2014. – С. 140-146.*
6. *Певнев В.Я. Теоретическое обоснование методики построения псевдопростых чисел / В.Я. Певнев // Радіоелектронні і комп'ютерні системи. – 2016. – № 6(80). – С. 210-213.*
7. *Певнев В.Я. Методика построения псевдопростых чисел / В.Я. Певнев // Системи обробки інформації. – Харків: ХУПС, 2016. – Вип. 3(140). – С. 30-32.*
8. *Agrawal M. PRIMES is in P / M. Agrawal, N. Kayal, N. Saxena // Annals of Mathematics. – 2004. – V. 160. – P. 781-793.*
9. *Venturi D. Lecture Notes on Algorithmic Number Theory / D. Venturi. – Springer-Verlag, New-York, Berlin, 2009. – 217 p.*

Поступила в редколлегию 10.06.2016

Рецензент: д-р техн. наук, проф. А.А. Серков, Национальный технический университет «ХПИ», Харьков.

RSA І ПРОСТІ ЧИСЛА

В.Я. Певнєв

Розглядається проблема побудови простих чисел. Вказані головні недоліки існуючих підходів до знаходження простих чисел. Розглянутий алгоритм побудови системи асиметричного шифрування RSA. Показана залежність системи RSA від правильності знаходження функції Ейлера. Представлений приклад визначення простоти числа, заснований на правильності визначення знаходження функції Ейлера. Показана можливість формування прямого і зворотного чисел, виходячи з простоти числа, що перевіряється. Сформульовано твердження про необхідність умови простоти чисел з використанням пари прямого і зворотного чисел в безлічі ненульових елементів кільця Z(p-1).

Ключові слова: *прості числа, алгоритм RSA, функція Ейлера, пряме число, зворотне число, прості співмножники.*

RSA AND PRIME NUMBERS

V.Ya. Pevnev

The problem of construction of prime numbers is examined. The main lacks of the existent going are indicated near finding of prime numbers. The algorithm of construction of the system of asymmetric encipherement of RSA is considered. Dependence of the system of RSA is rotined on the rightness of finding of function of Euler. The example of determination of simplicity of number, based on the rightness of determination of finding of function of Euler, is presented. Possibility of forming of direct and reverse numbers is rotined, coming from simplicity of the checked up number. Assertion about the necessity of condition of simplicity of numbers is formulated with the use of pair of direct and reverse numbers in the great number of unzero elements of ring of Z(p-1).

Keywords: *prime numbers, algorithm of RSA, function of Euler, direct number, reverse number, simple factors.*