Таким же образом происходит обращение к процедуре *UPDATE_USER*, но без использования *ResultSet* (Рисунок 5).

```
public void updateUser(int userId, String newName) throws SQLException {
        String sql = "BEGIN PS_UPDATE_USER(?,?); END;";
        CallableStatement statement = connection.prepareCall(sql);
        statement.setInt(1, userId);
        statement.setString(2, newName);
        statement.executeUpdate();
        /*Высвобождение ресурсов.*/
}
```

Рис.5 – Реализация обращения к процедуре *UPDATE_USER*

Литература

1. Этапы разработки и внедрения информационно-аналитической системы [Электронный ресурс] – Режим доступа: http://www.prj-exp.ru/dwh/dwh_stages_of_development.php [Дата обращения 27.01.2017].

2. Джейсон, К. Oracle Certified Professional™ Подготовка администраторов баз данных [Текст] / Джейсон К., Ульрике Шв. – М.:Лори, 2009. - 868 с.

3. CREATE SYNONYM [Электронный ресурс] – Режим доступа: https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_7001.htm [Дата обращения 07.02.2017].

4. Хабибуллин, И. Ш. Java 7 [Текст] / И. Ш. Хабибуллин. – СПб.:БХВ-Петербург, 2012. – 768 с.

О.В. Прохорова

ПРОВЕРКА БОЛЬШИХ ЧИСЕЛ НА ПРОСТОТУ

(Самарский государственный технический университет)

Раскладывание числа на простые сомножители практикуется достаточно широко, например, в алгоритме RSA, где стойкость схемы RSA зависит от того, как быстро можно разложить большое составное число на 2 простых сомножителя. Процедура такого разложения занимает относительно много времени в силу большого числа итераций подбора, что является большим минусом в применении.

Предлагаемая автором методика проверки больших чисел на простоту основывается на применении сформулированных правил генерации простых чисел, 3 теорем и алгоритма. Представим правила сцепления цифр в числа:

1. Сцепляются два числа. Самая правая цифра есть только нечетное число, за исключением цифры 5, т.е. последней цифрой справа могут быть только: 1, 3, 7, 9. Слева это любые числа, начина с 0 и далее. Для двух разрядного числа и левой цифре 0 правая цифра 5 допускается.

2. Для каждого сцепленного числа $X = \{a_1 \cdot a_2 \cdot \ldots \cdot a_n\}$ находится отображение b = F(X) = F{a1 a2 a3 … an} , где ai – есть цифры числа X, b – есть

одна цифра, полученная последовательным сложением всех цифр числа X. Таким образом из сцепленных чисел формируется множество значимых чисел, обозначаемое буквой ψ. В это множество не входят также числа, состоящие из повторяющихся цифр за исключением числа 11. Числа множества ψ подчиняются следующему правилу:

$$b = F(X) = \sum_{i=1}^{n} a_i, \quad b \in H, \quad H = \{1, \ 2, \ 4, \ 5, \ 7, \ 8\} \quad .$$

3. Для каждого значимого числа $X \in \psi$ формируется множество его делителей, обозначаемое Q(X). Множество Q(X) формируется из значимых чисел меньших X / 2, полученных ранее, возрастающих по величине и по которым принято заключение об их простоте (см. теоремы 1- 2). Возможные делители есть простые числа: { 3,7, 11, 13, 17, 19, …}.

4. В множество $\psi^*(X)$ простых чисел включаются лишь те числа из множества $\psi(X)$, для которых Q(X) есть пустые множества.

Рассмотрим применимость предложенных правил генерации последовательности простых чисел на примерах. Результаты приведены в таблицах. В первом столбце по строкам таблицы располагаются цифры от 0 до 9. В столбцах первой строки располагаются цифры 1, 3, 7, 9.

1. На пересечении строки и столбца помещается число в соответствии с первым правилом - конкатенации (сцепления) чисел, а именно, сцепления числа строки и цифры столбца, при этом учитываются правила 1 и 2. Множество чисел ψ начинается с известных простых чисел 01, 07, затем дополняется числами 11, 13, 17 и т.д. Числа 02, 03 и 05 вводятся в окончательно сформированное множество $\psi^*(X)$ дополнительно, поскольку они являются простыми, но не генерируются рассматриваемым методом. В таблицу не входят числа, нарушающие правила. Например, число 21 имеет сумму цифр равную 3, что не допускается по правилу 2.

2. Построенная такая таблица дает множество чисел $\psi(X)$= {1, 2, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, **49**, 53, 59, 61, 67, 71, 73, 79, 83, 89, **91**, 97}.

3. Множества Q(X) для всех чисел кроме 49 и 91 есть пустые множества, а Q(49) = {7}, Q(91) = {7, 13}. Значит, числа 49 и 91 являются составными, т.к. они имеют делители.

4. Массив $\psi^*(X)$= { 02, 03, 05, 07, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97} есть массив простых чисел , число 01 – не простое по определению, поэтому исключено из множества.

5. Продолжая генерировать числа, увеличиваем левое число для сцепления. Оно уже будет иметь 2 разряда , в начале с единицей слева, т.е. это

будут числа {10, 11,12,13,14,15,16,17,18,19}, а справа те же цифры столбца 1,3,7, 9.

Таблица. Генерация простых чисел X < 100

	1		7	
	1	3	7	9
		3		9
	1		7	
	1	3	7	**9**
		3		9
	1		7	
	1	3		9
		3		9
	1		7	

По аналогии генерируются простые числа и далее. Анализ результатов генерирования последовательности простых чисел по представленной методике дает основание для формулирования теорем. Отметим, что числа размерности более 1 оканчивающиеся на четную цифру или цифру 5 не рассматриваются на простоту, т.к. они заведомо составные.

Теорема 1. Необходимым условием простоты числа $X \in \psi$ размерности более 1, которое не состоит из повторяющихся цифр за исключение числа 11, является выполнение требования:

$$b = F(X) = \sum_{i=1}^{n} a_i, \quad b \in H, \quad H = \{1, \ 2, \ 4, \ 5, \ 7, \ 8\}. \qquad 1)$$

Теорема 2. Достаточны условием простоты числа $X \in \psi^*$ является пустота множества его делителей Q(X).

Теорема 3. Достаточным условием того, что число разрядности более единицы, есть составное число, является выполнение требования:

$$b = F(X) = \sum_{i=1}^{n} a_i, \quad b \in Z \text{, где } \quad Z = \{ \ 3, \ 6, \ 9\}. \qquad 2)$$

Доказательство теорем подтверждается простыми действиями с числами согласно сформулированным правилам.

Пример 1. Проверим число X = 156789 на простоту. Решение задачи отобразим в виде таблицы.

X - делимое	(X)	Q(X) - делитель	Частное	Остаток от деления
156789		3	**52263**	0
52263		3	17421	0
17421		3	5807	0
5807		-	-	-

Подводим итог решения. Число 156789 является составным, оно имеет делителями простые числа: { 3, 5807 }, т.е. число X = 156789 не простое, что и требовалось проверить. Интересно то, что поиск делителей заканчивается, когда сумма цифр числа, характеризующего частное будет одним из цифр множества H. В данном примере это цифра 2.

Пример 2. Проверим число X = 2 147 483 647 на простоту.

Для этого найдем сумму цифр числа X до тех пор , пока не останется одна цифра. Получим b = 1, что удовлетворяет теореме 1. Проверка условия теоремы 2 дала тоже положительный результат, т.к. делители не были обнаружены. Для этого использовалось правило 2.

Предложенная автором методика генерации последовательности простых чисел имеет преимущество по сравнению с существующими алгоритмами в силу элементарности проверки любого числа на простоту и разложения большого числа на простые сомножители, что особенно важно в современной криптографии.

Литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. С. 75 - 79.

2. Прохорова О.В. Генерация последовательности простых чисел. Журнал ВАК - Естественные и технические науки, № 8 Москва: Спутник +, 2015.- С. 68 – 72.