Большинство существующих алгоритмов точного построения минимальной сети Штейнера основаны на сведении задачи для исходного набора точек к задаче меньшей размерности и включают перебор различных вариантов. Задачу для ромба можно свести к алгоритму нахождения точки Штейнера для трех точек. Для этого необходимо на одной из сторон ромба построить правильный треугольник и воспользоваться алгоритмом для полученной вершины и двух оставшихся вершин ромба. Полученная точка будет являться одной из двух точек Штейнера, а вторая будет находиться аналогичным образом, но для противолежащей стороны.

Результатом работы является программа, разработанная на языке программирования C++, позволяющая получить координаты двух точек Штейнера для заданного ромба.

ЛИТЕРАТУРА

1. Протасов, В. Ю. Максимумы и минимумы в геометрии / В. Ю. Протасов. – М.: МЦНМО, 2005. – 56 с.

УДК 532.517

Студ. А. А. Малюш
Науч. рук. доц. А. М. Волк
(кафедра высшей математики, БГТУ)

МЕТОДЫ ИССЛЕДОВАНИЯ И РЕЖИМЫ ПЛЕНОЧНЫХТЕЧЕНИЙ

Пленочное течение жидкостей под действием силы тяжести по поверхности плоских и цилиндрических стенок используется для осуществления ряда технологических процессов. Методы исследования пленочных течений разделяются на экспериментальные и теоретические.

Математическое моделирование пленочного движения позволяет определить оптимальные режимы и нагрузками по фазам.

Для жидкой пленки толщиной dx уравнение динамического равновесия имеет вид:

$$d\tau = -\rho g dx = \mu \frac{d^2\omega}{dx^2} dx . \qquad (1)$$

Начальные условия определяются равенствами:

$$\omega = 0 \text{ при } x = 0 \text{ и } \frac{d\omega}{dx} = -\frac{\tau_{\text{м}}}{\mu} \text{ при } x = \delta. \qquad (2)$$

При заданных касательных напряжениях сил трения $\tau_м$ на границе раздела границе жидкость-газ, получим профиль скорости пленки жидкости:

$$\omega = \frac{\rho g \delta^2}{\mu}\left(\frac{x}{\delta} - \frac{1}{2}\cdot\frac{x^2}{\delta^2} - \frac{\tau_м}{\rho g \delta}\cdot\frac{x}{\delta}\right), \tag{3}$$

Находим среднюю скорость движения пленки

$$\omega_{ср} = \frac{1}{\delta}\int_0^\delta \omega dx = \frac{\rho g \delta}{\mu}\int_0^\delta\left(\frac{x}{\delta} - \frac{1}{2}\cdot\frac{x^2}{\delta^2} - \frac{\tau_м}{\rho g \delta}\cdot\frac{x}{\delta}\right)dx = \frac{\rho g \delta^2}{\mu}\left(\frac{1}{3} - \frac{\tau_м}{2\rho g \delta}\right), \tag{4}$$

Зависимости (3) и (4) позволяют определить профиль и режимы пленочного течения. Например, при $\tau_м/\rho g\delta$ = 0.5 поверхностная скорость пленки $\omega_м$= 0, но ее промежуточные слои, как следует из уравнения (3), сохраняют движение вниз.

УДК 512.624.95

Студ. И.И. Скородумов
Науч. рук. доц. Е. И. Ловенецкая
(кафедра высшей математики, БГТУ)

МАТЕМАТИЧЕСКИЕ ЗАДАЧИ АЛГОРИТМА RSA

По мере развития компьютерных сетей возникла необходимость в способе безопасного обмена конфиденциальной информацией без согласования ключей защищенными каналами связи. Благодаря этому были разработаны алгоритмы асимметричного шифрования. Одним из них является RSA[1].Они используется для создания цифровых подписей и обмена ключами симметричных шифров, т.к. шифровать сами сообщения с помощью RSA нерационально. Безопасность RSA обуславливается проблемой факторизации больших чисел (в настоящее время не существует быстрых алгоритмов разложения на простые множители больших целых чисел), а корректность шифрования следует из теоремы Эйлера о возведении в степень по модулю.

Цели работы: изучить математическое обоснование алгоритма RSA, написать свою реализацию алгоритма.

В основе алгоритма RSA лежат следующие методы и результаты теории чисел: свойства сравнений по модулю (основные действия в RSA выполняются по модулю заданного целого числа n); теорема Эйлера (гарантия корректности алгоритма); определение простоты больших чисел (для генерации достаточно большого n).

Проблемными местами безопасного использования RSA являются генерация больших простых чисел (в настоящее время исполь-