Московский государственный технический университет им. Н.Э. Баумана

Факультет ИУ "Информатика и системы управления"

Кафедра ИУ-3 "Информационные системы и телекоммуникации"

Методические указания к лабораторной работе №3

по курсу "Моделирование информационных процессов и систем"

“Изучение свойств поведения систем при помощи языка спецификаций TLA+”

для студентов, обучающихся по направлению

2304000062

Продолжительность 4 часа.

Составили: *Ошкало Д.В.*

Москва 2016

# Цель работы

Ознакомление студентов с методами и средствами анализа поведения систем при помощи языка TLA+.

# Задание

В данной лабораторной работе необходимо ознакомиться с языком TLA+, средой разработки спецификаций TLA+ Toolbox и их использованием при изучении поведения систем.

# Порядок выполнения работы

## Подготовка к выполнению задания

Перед тем, как приступить к выполнению задания данной лабораторной работы, следует установить и настроить необходимые программные инструментальные средства:

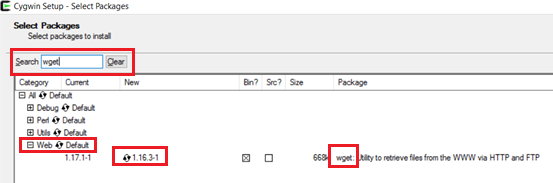
1. Скачать установочный пакет TLAPS – набора инструментов для доказательства свойств системы, выраженных при помощи формул темпоральной логики (<https://tla.msr-inria.inria.fr/tlaps/dist/current/tlaps-1.4.3-i686-cygwin-inst.exe>).
2. Установить Cygwin (Unix-подобную оболочку и интерфейс командной строки для ОС Windows) версии 1.7.24 или более поздней (https://cygwin.com/install.html). Данная оболочка будет использоваться в качестве платформы для установки пакета инструментов TLAPS. Обязательно необходимо установить 32-битную версию эмулятора, даже в том случае, если на Вашей рабочей машине установлена 64-битная версия ОС Windows, иначе TLAPS не будет работать корректно. Процесс установки подробно описан ниже.

В начальный момент установки необходимо выбрать опцию «Установить из Интернета».

Далее нужно будет выбрать корневую директорию установки и директорию, в которую будут загружаться установочные файлы в процессе установки.

После этого, не меняя установок соединения (оставить активной опцию «Direct Connection»), нужно выбрать один из репозиториев, с которого будет произведена загрузка установочных файлов. Выбрать можно любой.

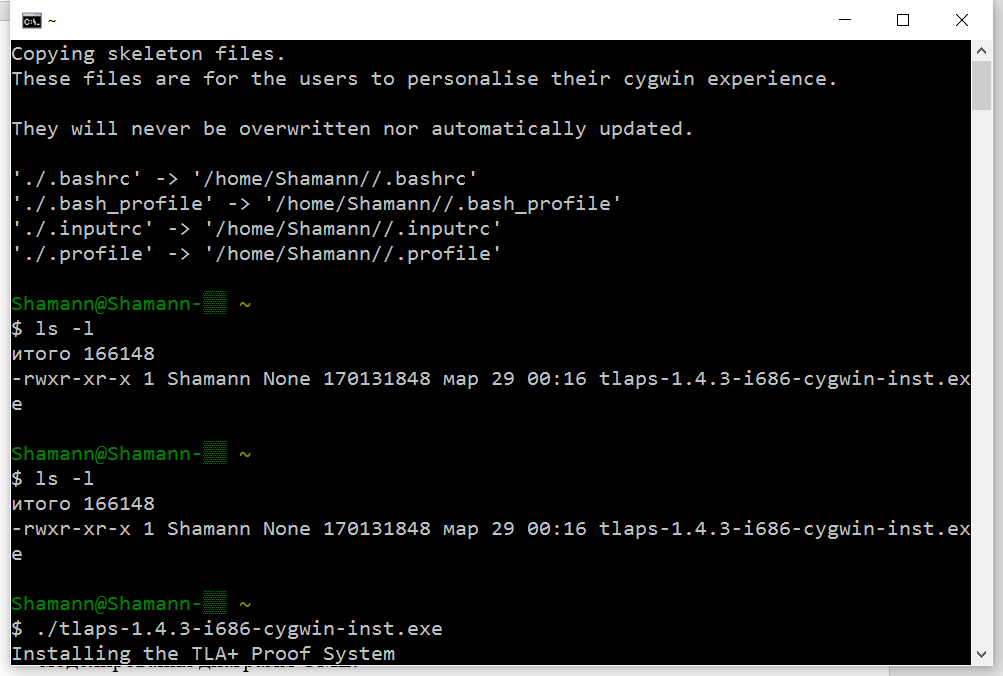
Далее Вам будет предложено выбрать дополнительные пакеты, которые можно установить. Необходимо выбрать следующие модули: Devel/make, Perl/perl, Web/wget. Эти утилиты нужны для того, чтобы распаковать и установить пакет инструментов TLAPS. Для быстрого поиска этих модулей можно воспользоваться строкой поиска в верхней части окна.



Для выбора модуля необходимо щелкнуть левой кнопкой мыши в колонке «New» на поле «Skip», после чего появится номер версии. Аналогичные действия нужно проделать для всех модулей.

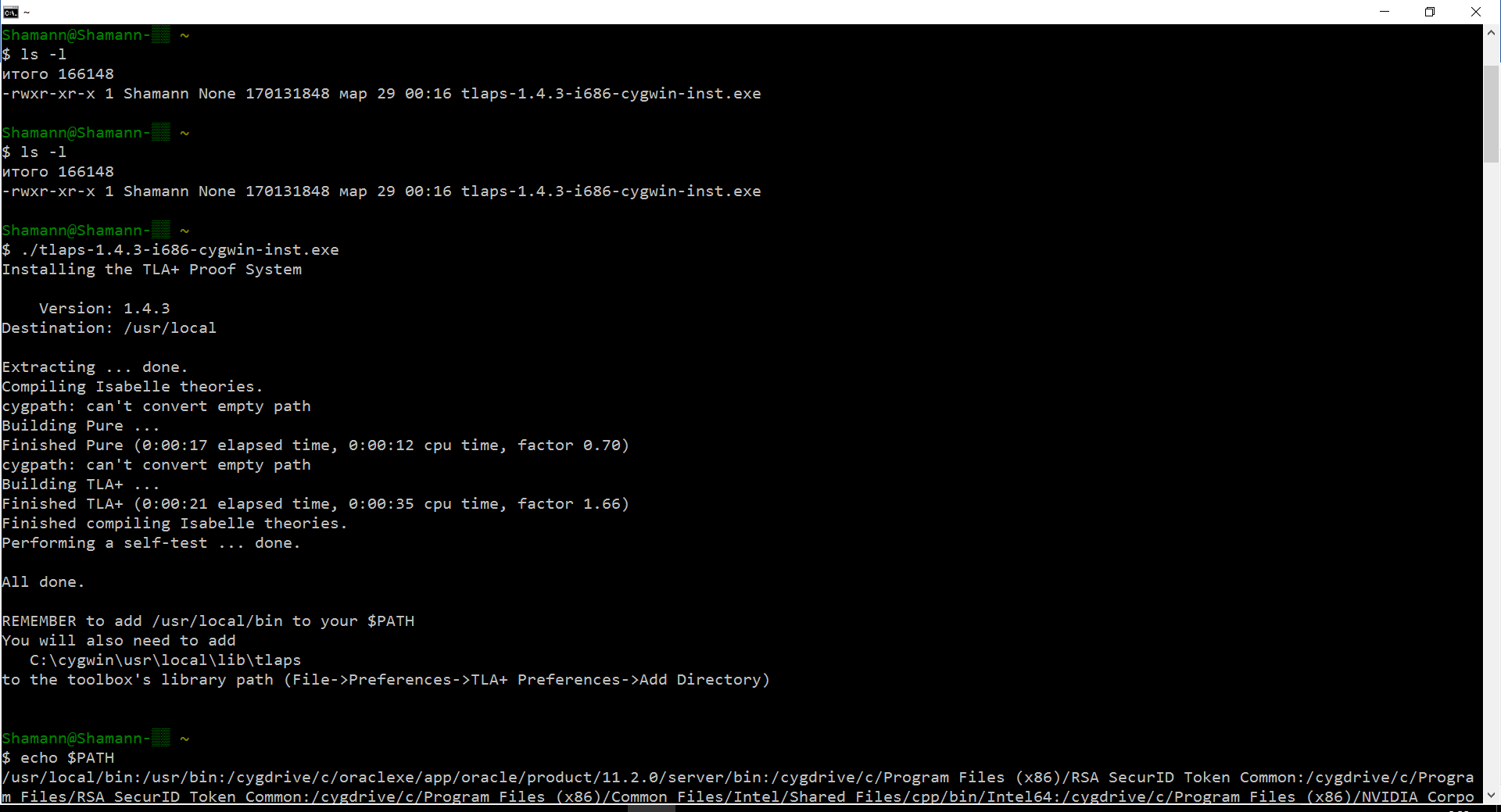
После выбора дополнительных модулей запустится процесс установки.

1. По окончании установки запустите Cygwin. Откроется окно с интерфейсом командной строки UNIX.

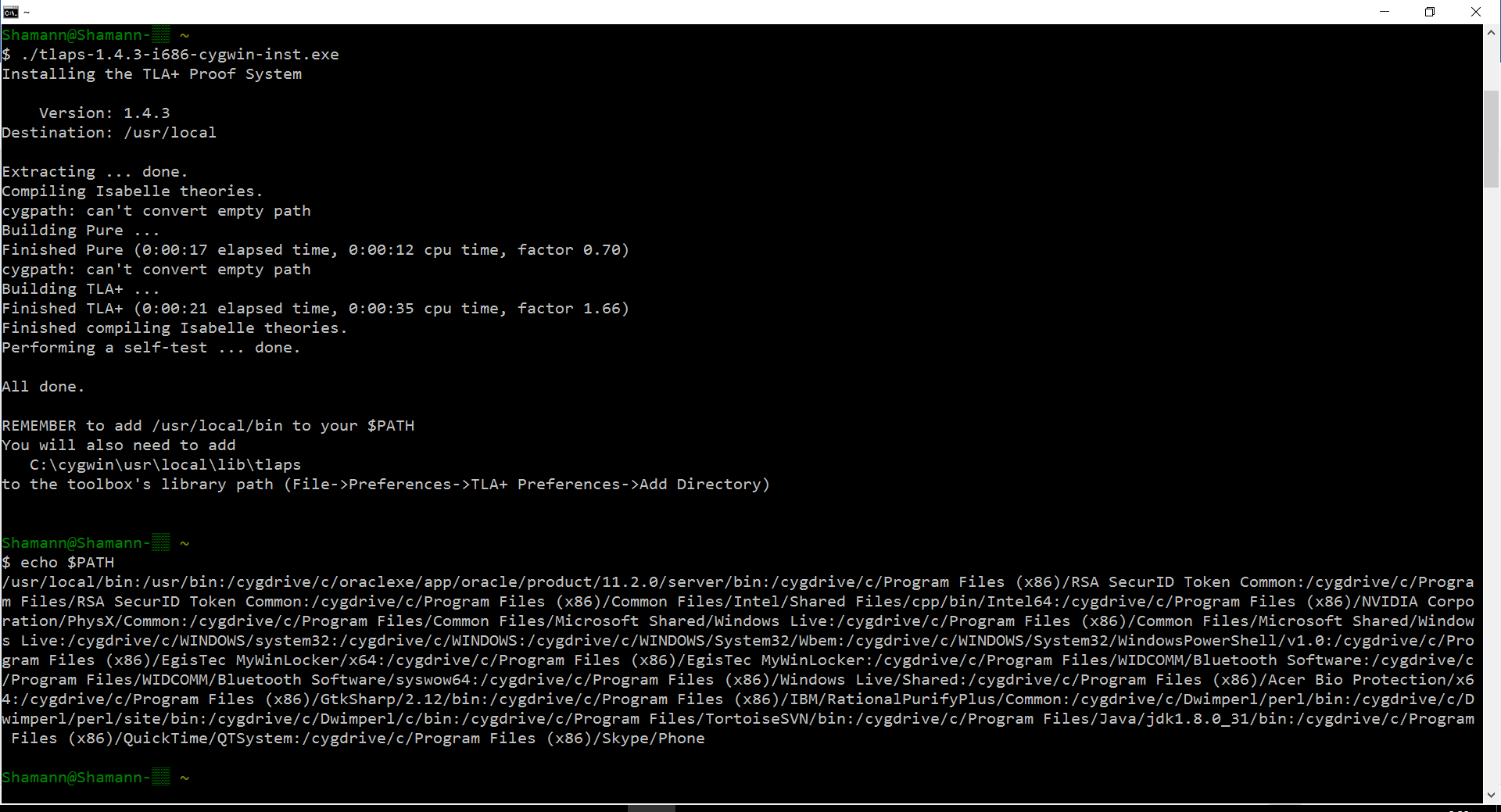


Наберите команду pwd для определения своего текущего расположения, после чего проверьте содержимое домашней директории, набрав команду ls.

Физически домашняя директория, в которой Вы в данный момент расположены, находится в каталоге [путь установки Cygwin]\home\[имя пользователя Windows]. В этот каталог Вам необходимо скопировать установочный пакет, который Вы скачали, выполняя задание пункта 1. Убедитесь в том, что пакет действительно появился в каталоге, набрав команду ls -l в Cygwin.

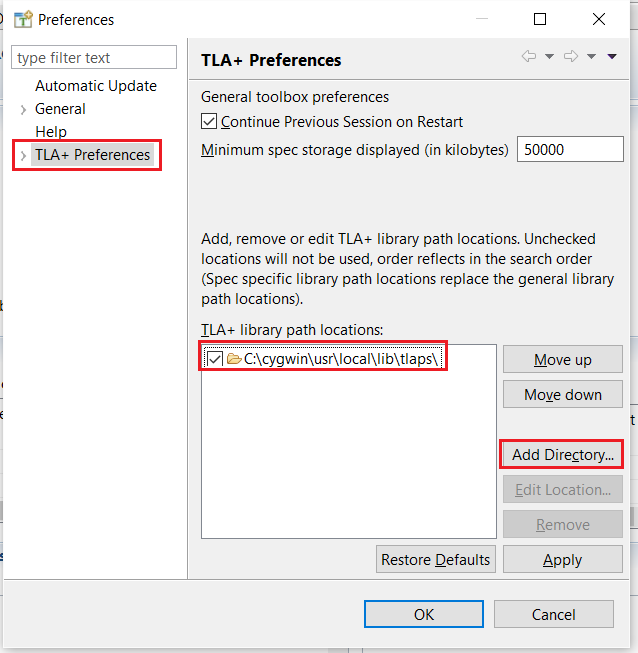


Далее необходимо запустить установку пакета TLAPS, набрав команду ./[наименование пакета]



После запуска команды начнется процесс распаковки и установки набора инструментов TLAPS. По окончании установки будет предложено добавить путь /usr/local/bin в переменную среды PATH. Сначала выведите на экран значение этой переменной, набрав команду echo $PATH. Значение этой переменной представляет собой набор путей, разделенных символом двоеточия. Если указанного пути в этой переменной нет, добавьте его, используя команду PATH=/usr/local/bin:$PATH. После этого снова выполните команду echo $PATH, чтобы убедиться, что значение переменной PATH действительно изменено.

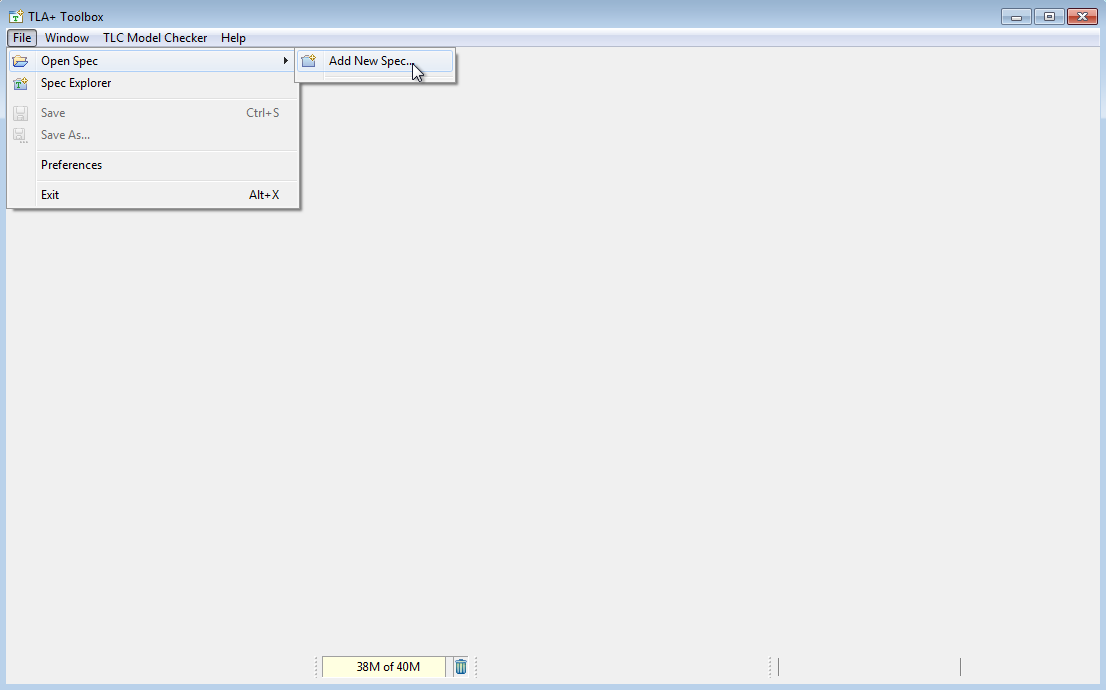
1. Скачать программу TLA+ Toolbox по ссылке <https://tlaplus.codeplex.com>. По окончании загрузки распаковать архив с приложением.
2. Открыть установленное приложение, выбрать пункт меню File->Preferences, в появившемся окне выбрать пункт TLA+ Preferences, после чего нажать кнопку «Add Directory…» и указать [путь установки Cygwin]\usr\local\lib\tlaps.



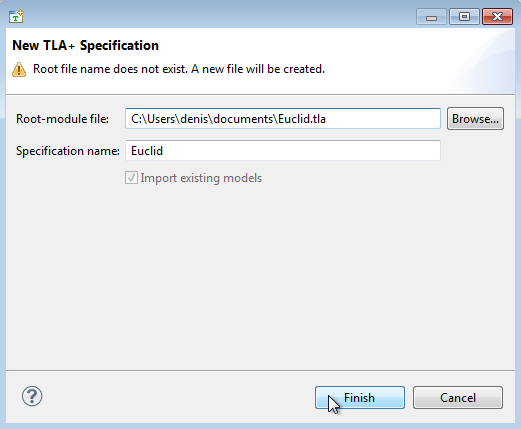
## Использование TLA+ Toolbox

В качестве примера работы с приложением рассмотрим доказательство корректности алгоритма Евклида нахождения наибольшего общего делителя. Для того, чтобы выполнить процедуру формального доказательства, необходимо составить спецификацию алгоритма в терминах языка TLA+, после чего в этих же терминах с использованием формул временной модальной логики сформулировать свойство корректности. По окончании работы с примером настоятельно рекомендуется перейти к рекомендуемым источникам для ознакомления с языком TLA+, используемыми в нем конструкциями и способами построения доказательств.

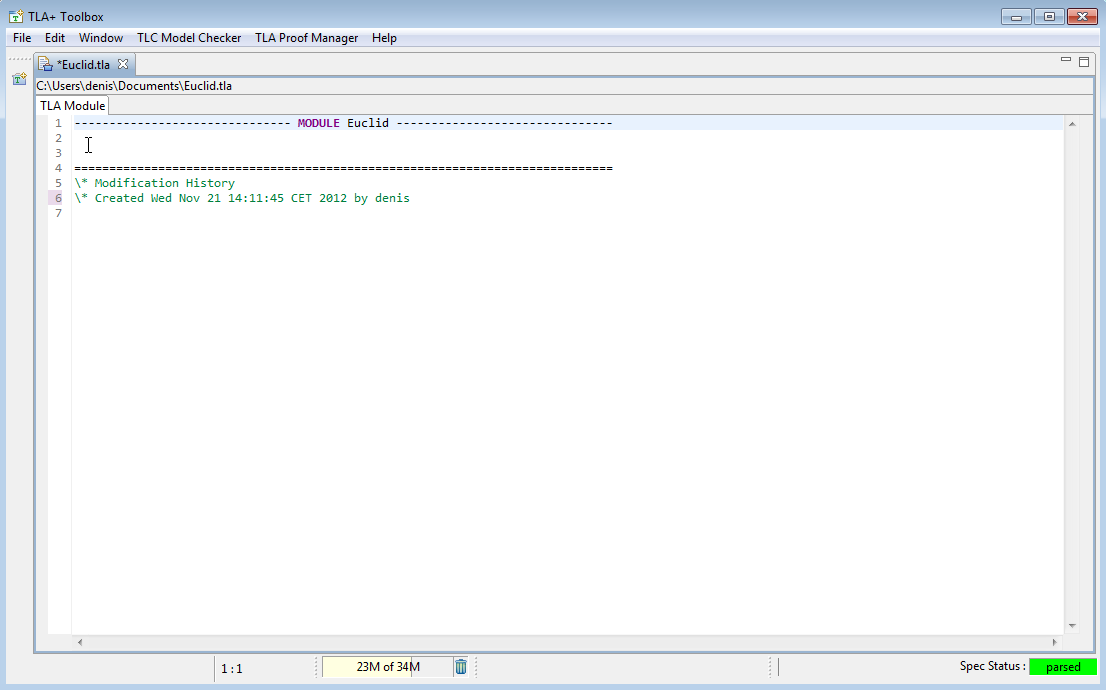
Вернемся к нашему примеру. Сначала создадим новую спецификацию в приложении.



Далее выберите папку, в которой будет располагаться Ваш проект, и укажите имя файла Вашей спецификации, а также расширение .tla.



В результате откроется окно спецификации.



Для исследования алгоритма нам понадобятся арифметические операции. Чтобы использовать их в спецификации, импортируем стандартный модуль TLAPS, указав в спецификации

-------------------- MODULE Euclid --------------------

EXTENDS Integers

=======================================================

Далее нужно определить наибольший общий делитель двух чисел. Для этого определим предикат «q делится на p» следующим образом: q делится на p в том и только том случае, когда существует некоторое целое число d в интервале от 1 до q такое, что q = p \* d. Добавим это определение в спецификацию:

p | q == \E d \in 1..q : q = p \* d

Определим множество делителей числа q как множество целых чисел от 1 до q таких, что выполняется описанное выше условие:

Divisors(q) == {d \in 1..q : d | q}

Определим максимальный элемент на множестве целых чисел:

Maximum(S) == CHOOSE x \in S : \A y \in S : x >= y

Теперь определим наибольший общий делитель как пересечение множеств всех делителей чисел p и q:

GCD(p,q) == Maximum(Divisors(p) \cap Divisors(q))

Для удобства определимся, что мы работаем с положительными целыми числами:

Number == Nat \ {0}

Для описания алгоритма Евклида добавим в спецификацию определение двух констант, определяющих числа, поступающие на вход алгоритма, и двух переменных:

CONSTANTS M, N

VARIABLES x, y

Зададим начальное состояние алгоритма как

Init == (x = M) /\ (y = N)

Каждое следующее состояние системы, согласно работе алгоритма, определим

Next == \/ /\ x < y

/\ y' = y - x

/\ x' = x

\/ /\ y < x

/\ x' = x-y

/\ y' = y

Работа алгоритма начинается с инициализации начального состояния и выполнения перехода в следующее состояние с перерасчетом переменных до тех пор, пока их значение между текущим и предыдущим состояниями алгоритма не будет неизменно. Таким образом, спецификация алгоритма будет выглядеть следующим образом (двойными скобками << >> обозначается условие неизменности значений переменных):

Spec == Init /\ [][Next]\_<<x,y>>

Также необходимо убедиться, что значения чисел, поступивших на вход алгоритма, больше нуля:

ASSUME NumberAssumption == M \in Number /\ N \in Number

Теперь сформулируем свойство корректности алгоритма:

ResultCorrect == (x = y) => x = GCD(M, N)

Процедуру доказательства данного свойства сформулируем в виде следующей теоремы:

THEOREM Correctness == Spec => []ResultCorrect

Доказательство такой теоремы возможно благодаря тому, что существует инвариант – условие, которое выполняется в каждом из состояний алгоритма:

InductiveInvariant == /\ x \in Number

/\ y \in Number

/\ GCD(x, y) = GCD(M, N)

Сформулируем теорему о том, что данное условие выполняется в начальном состоянии алгоритма:

THEOREM InitProperty == Init => InductiveInvariant

BY NumberAssumption DEF Init, InductiveInvariant

В итоге спецификация должна выглядеть следующим образом:

-------------------- MODULE Euclid --------------------

EXTENDS Integers

p | q == \E d \in 1..q : q = p \* d

Divisors(q) == {d \in 1..q : d | q}

Maximum(S) == CHOOSE x \in S : \A y \in S : x >= y

GCD(p,q) == Maximum(Divisors(p) \cap Divisors(q))

Number == Nat \ {0}

CONSTANTS M, N

VARIABLES x, y

Init == (x = M) /\ (y = N)

Next == \/ /\ x < y

/\ y' = y - x

/\ x' = x

\/ /\ y < x

/\ x' = x-y

/\ y' = y

Spec == Init /\ [][Next]\_<<x,y>>

ResultCorrect == (x = y) => x = GCD(M, N)

InductiveInvariant == /\ x \in Number

/\ y \in Number

/\ GCD(x, y) = GCD(M, N)

ASSUME NumberAssumption == M \in Number /\ N \in Number

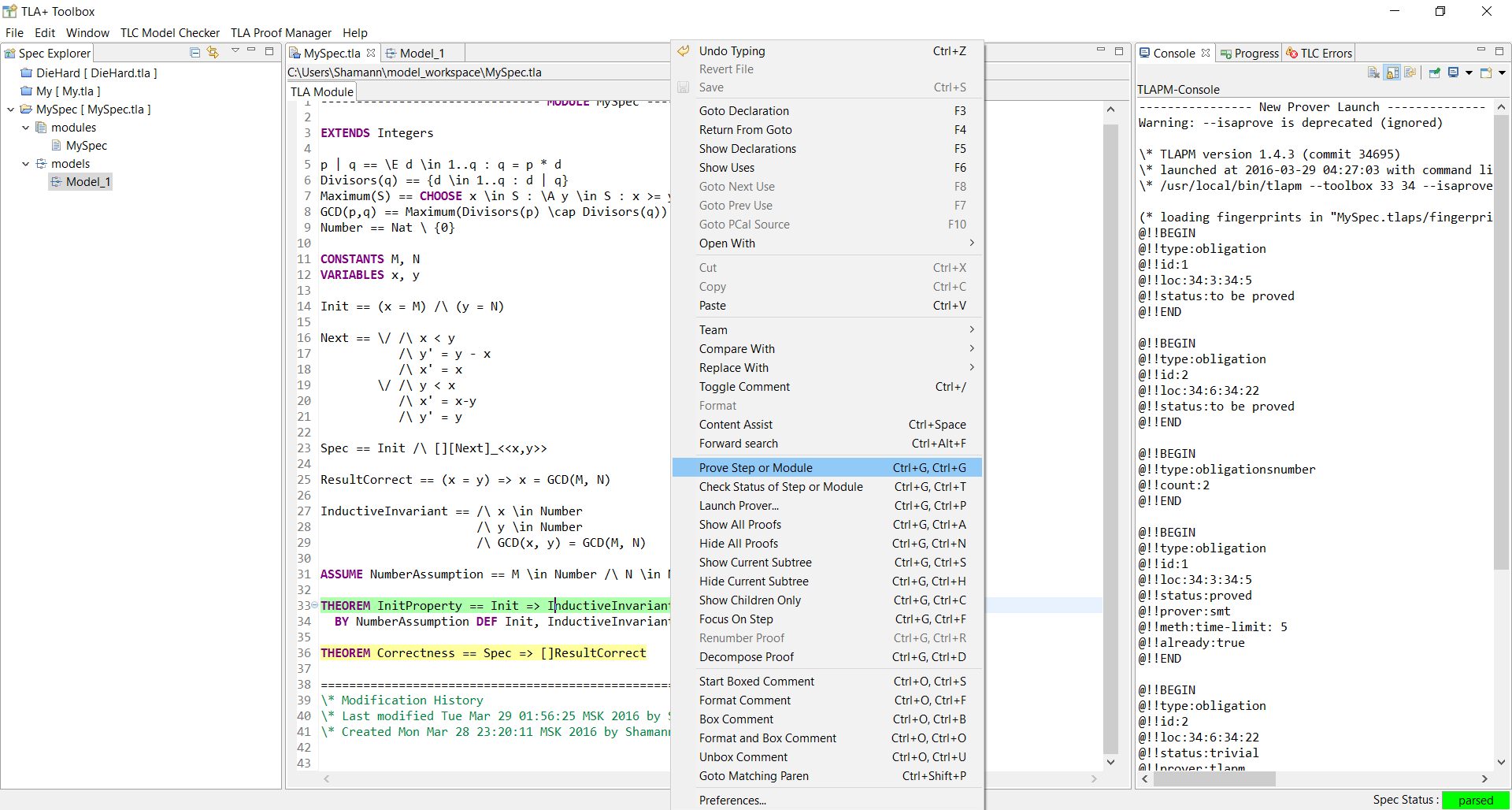
THEOREM InitProperty == Init => InductiveInvariant

BY NumberAssumption DEF Init, InductiveInvariant

THEOREM Correctness == Spec => []ResultCorrect

=======================================================

Запустить процедуру доказательства теоремы можно, вызвав контекстное меню в спецификации на той строчке, с которой начинается теорема, и выбрав пункт меню «Prove Step or Module»

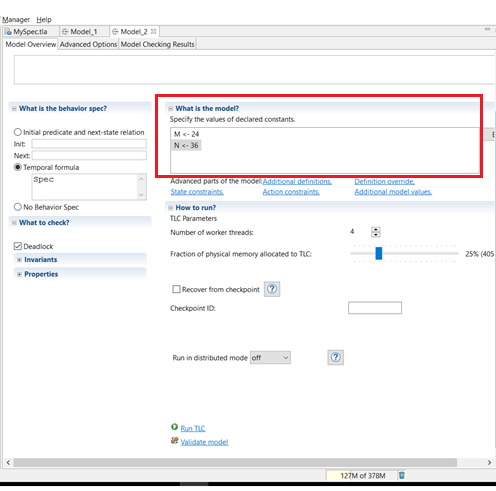


## Запуск моделей

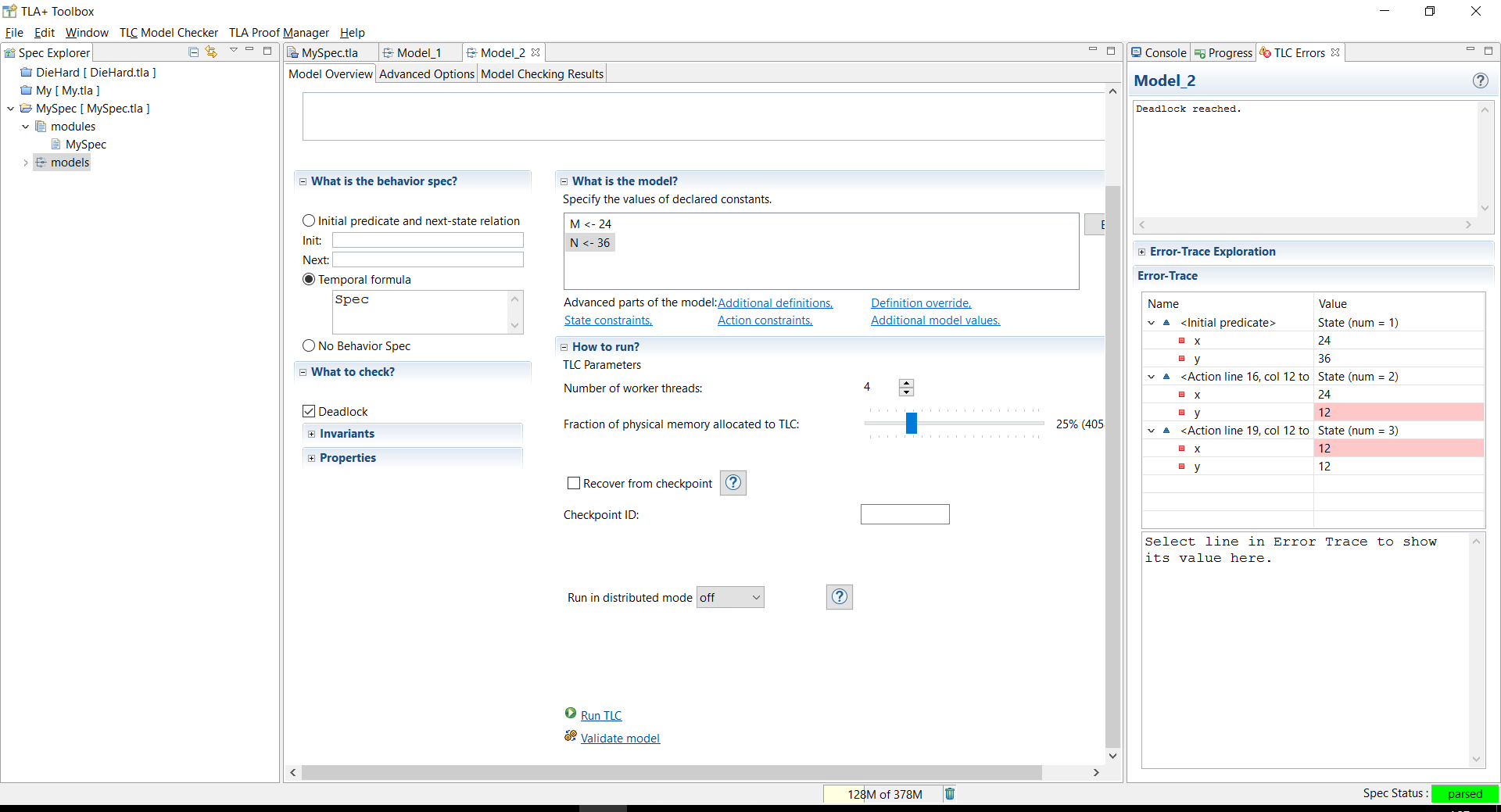
После составления спецификации можно создать тестовую модель, которую можно запустить до выполнения некоторого условия (в виде темпоральной формулы или deadlock) и посмотреть на значения переменных внутри каждого состояния.

Для создания модели необходимо вызвать контекстное меню на компоненте models и выбрать пункт «New Model», после чего модель создастся автоматически.

Т.к. в нашей спецификации определены две константы, для запуска модели необходимо указать их значения.



После запуска модели (Run TLC), появится список состояний модели со значениями переменных в каждом из них.



## Задание для самостоятельного изучения

Используя приложение TLA+ Toolbox Вам необходимо ознакомиться со спецификациями протокола PAXOS и изучить его свойства. Спецификации протокола доступны по ссылке

<https://github.com/fintler/tlaplus/tree/master/examples/Paxos>

Необходимо сначала ознакомиться с самим протоколом (см. список источников), после чего, изучив конструкции языка TLA+, подробно рассмотреть предлагаемые спецификации, описанные в них свойства и механизмы из доказательства, оценить адекватность спецификации реальной работе протокола.

# Отчет о лабораторной работе

## Содержание отчета

Титульный лист.

Цель работы.

Результаты проведенных опытов и проделанной работы.

Анализ полученных результатов и выводы.

## Требования к оформлению отчета

Отчет должен быть предоставлен в формате MS Word или OpenOffice.

Отчет должен быть набран с использованием стилей как минимум для основного текста, заголовков разделов.

Отчет должен содержать номера страниц.

Заголовки разделов должны быть иметь иерархическую нумерацию.

Таблицы, рисунки, листинги, графики должны быть подписаны.

# Литература

TLA+:

1. <http://research.microsoft.com/en-us/um/people/lamport/tla/tla.html>
2. Книга Lamport L. [Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers](http://research.microsoft.com/en-us/um/people/lamport/tla/book.html#download). 2002.
3. <http://research.microsoft.com/en-us/um/people/lamport/tla/hyperbook.html> (настоятельно рекомендуется изучить этот учебник, скачав его по ссылке <http://research.microsoft.com/en-us/um/people/lamport/tla/hyperbook.zip>)
4. <http://research.microsoft.com/en-us/um/people/lamport/pubs/tlaps.pdf>
5. <http://www.sts.tu-harburg.de/teaching/ws-08.09/VSS/06-TLA.pdf>
6. http://www.loria.fr/~merz/talks/argentina2005/handout.pdf

Paxos:

1. <https://it.mail.ru/video/104/>
2. http://research.microsoft.com/en-us/um/people/lamport/pubs/paxos-simple.pdf