

Иванов Сергей Георгиевич

## ИНТЕРНЕТ-ССЫЛКИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ ИЗ КОЛЛЕКЦИИ С. В. ФОМИНА

Предлагаем вашему вниманию комментарии к учебным Интернет-ресурсам, ссылки на которые любезно предоставлены профессором Мичиганского университета С.В. Фоминым.

С.В. Фомин хорошо известен в Санкт-Петербурге как талантливый популяризатор науки, много сделавший для развития олимпиадного и кружкового движения по математике в школе. В 80-х годах он вел в газете «Смена» заочную школу по информатике, которую можно считать прообразом Заочной школы современного программирования в нашем журнале.

В настоящее время С.В. Фомин работает профессором в Мичиганском университете и вновь посвящает часть своего времени работе со школьниками. Так, за последние два года он поставил курсы по дискретной математике и криптологии для абитуриентов университета.

Для этих курсов он составил любопытную подборку интернет-ссылок, о которых нам бы хотелось рассказать читателям. Ссылки указывают на англоязычные ресурсы, но мы надеемся, что это не помешает заинтересованному читателю познакомиться с ними.

В научные интересы С.В. Фомина входят комбинаторика, ее приложения, ее связь с теорией представлений, алгебраическая геометрия, и другие области математики.

Страница С.В. Фомина размещена по адресу:

<http://www.math.lsa.umich.edu/~fomin/>

На этой странице Вы найдете много интересных материалов, в том числе ссылки на различные сюжеты, не упомянутые в данной статье.



<http://www.math.lsa.umich.edu/~fomin/175.html>

*Перечисление сюжетов, связанных с криптологией и дискретной математикой.*

Некоторые из этих сюжетов сопровождаются апплетами, позволяющими проследить исследуемые закономерности и поэкспериментировать с ними. Другие сюжеты снабжены лишь формулами и комментариями.

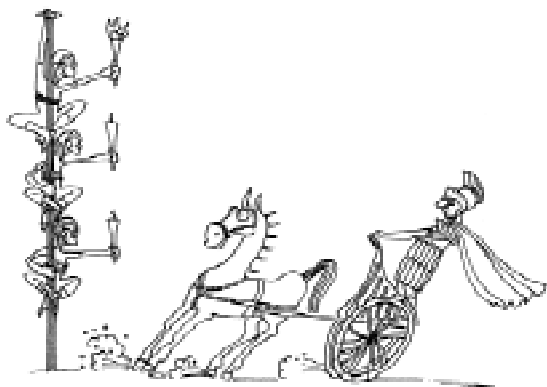
Далее я подробнее остановлюсь на тех сюжетах, которые оказались более интересными и которые ярче и доступнее проиллюстрированы.

### 1. СЮЖЕТЫ, СВЯЗАННЫЕ С ДИСКРЕТНОЙ МАТЕМАТИКОЙ

<http://www-stat.stanford.edu/~susan/surprise/Car.html>

*Апплет иллюстрирует один интересный сюжет, связанный с теорией массового обслуживания.*

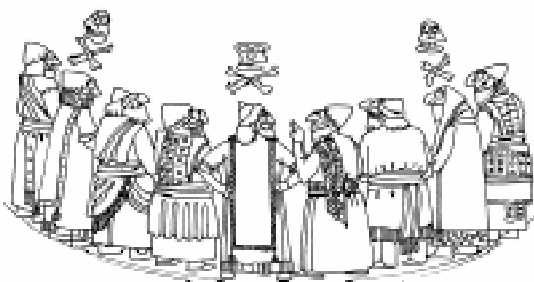
Количество остановок перед светофорами на одной и той же трассе, как известно, может оказаться больше или меньше – в зависимости от того, повезет или не повезет. В этом вы можете убедиться с помощью апплета. Также можете предположить, сколько остановок в среднем придется сделать при 2, 3, 4 или 5 светофорах, а затем экспериментально проверить свое предположение.



<http://www.cut-the-knot.com/recurrence/flavius.html>

*Апплет, моделирующий задачу Иосифа Флавия.*

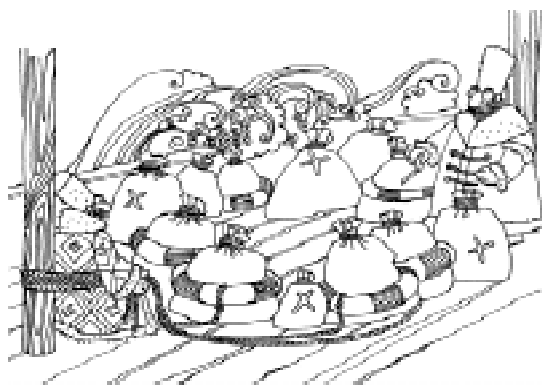
Задача опирается на довольно мрачную легенду о том, что во время войны римлян с иудеями отряд из 40 иудейских солдат был блокирован римлянами в пещере, и окруженные предпочли смерть плену. Они решили встать в круг и убивать каждого третьего (убитые при дальнейшем счете не учитываются). Но среди окруженных оказался известный историк Иосиф Флавий, который быстро догадался, куда нужно встать, чтобы остаться в живых. Впоследствии он, судя по всему, все же попал в плен, но остался в живых и донес до нас эту историю.



Апплет позволяет поэкспериментировать с этой задачей при различных значениях двух параметров: первоначальное количество воинов (не более 50) и количество живых между двумя убитыми. Цель игры – найти место Иосифа Флавия, если известно, кто из воинов будет убит первым. По ходу игры вы можете проследить, в каком порядке воины будут уходить из жизни, и узнать, действительно ли выбранный вами человек останется в живых.

Похожая идея впоследствии была реализована для других задач, уже не столь трагических. Например, в такой задаче (см. книгу Е.И. Игнатъева «В царстве смекалки»).

Во время шторма капитан приказал выбросить за борт 15 из 30 тюков с товаром, которые везли два купца (по 15 каждый). Один из купцов предложил поставить тюки по кругу случайным образом и выбрасывать за борт каждый третий. Капитан согласился, а купец поставил тюки так, что на палубе остались 15 тюков именно с его товаром. Как были расставлены тюки?



<http://www.ship.edu/~deensl/pgss/Joseph/>

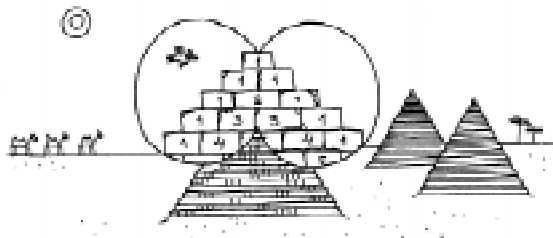
*Еще одна компьютерная реализация задачи Иосифа Флавия.*

В отличие от предшествующего варианта, здесь не ограничено количество воинов, но вместо графической демонстрации предлагается лишь таблица, показывающая, в каком порядке будут погибать воины и на каком месте следует стоять Иосифу Флавию.

<http://forum.swarthmore.edu/workshops/usi/pascal/pascal.links.html>

*О треугольнике Паскаля.*

Апплет, вопросы и ответы, биографии ученых, которые были особенно тесно связаны с этой темой.



<http://www.cecm.sfu.ca/organics/papers/granville/support/pascalform.html>

*Апплет, демонстрирующий треугольник Паскаля и остатки чисел по заданному модулю.*

Числа с различными остатками изображены прямоугольниками разного цвета, что придает апплету наглядность.

<http://www.math.uah.edu/stat/applets/>

*«Случайные» эксперименты. Игла Бюффона, испытания Бернулли и другие известные эксперименты, связанные с теорией вероятностей.*

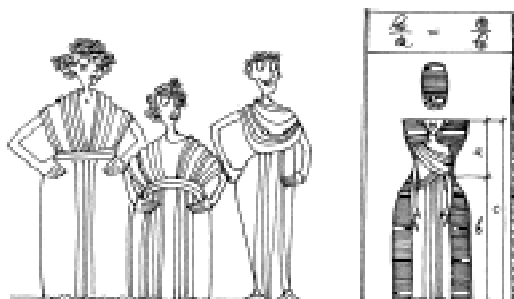
Каждый эксперимент сопровождается апплетом и подробным комментарием: в чем состоит постановка задачи и какой ответ предсказывает теория.



<http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/fib.html>

*Числа Фибоначчи и «Золотое сечение».*

Много интересной информации о математической природе этих объектов, об их связи с окружающим миром.



<http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/fibtable.html#100>

*Первые 500 чисел Фибоначчи.*

Первые 300 чисел приведены с факторизацией, то есть с разложением на простые множители.

[http://www.mi.uib.no/~ingeke/anagram/index\\_eng.html](http://www.mi.uib.no/~ingeke/anagram/index_eng.html)

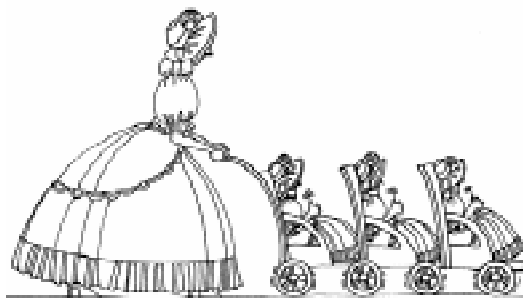
*Генератор анаграмм.*

Генерирует анаграммы на трех языках: английском, испанском и норвежском.

<http://www-stat.stanford.edu/~susan/surprise/>

*Сюрпризы теории вероятности.*

Задача о совпадении дней рождения и другие задачи, ответ в которых нередко расходится с тем, что можно было ожидать. Каждый сюжет сопровождается апплетом.



<http://www.ms.uky.edu/~mai/java/stat/brmo.html>

*Апплет «Броуновское движение».*

Случайные блуждания точки на плоскости и прямой. Теория вероятности утверждает, что точка при этом с вероятностью 1 уйдет от начала координат сколь угодно далеко, то есть дальше любого наперед заданного расстояния. Кроме того, она с вероятностью 1 вернется в начало координат, но время, которое для этого потребуется, стремится к бесконечности (точнее – математическое ожидание этого времени равно бесконечности).

Еще один интересный вывод связан с тем, что траектория точки везде непрерывна, но нигде не дифференцируема.



<http://www.math.fau.edu/Richman/Liberal/affine.htm>

*Апплет «аффинный шифр». Этот шифр обобщает шифр Цезаря.*

В данном случае номер буквы умножают на константу и прибавляют к нему другую константу (эту операцию называют аффинным преобразованием).

<http://www.trincoll.edu/depts/cpsc/cryptography/substitution.html>

*Беседа о том, что такое простой подстановочный код, с подробным примером расшифровки сообщения.*

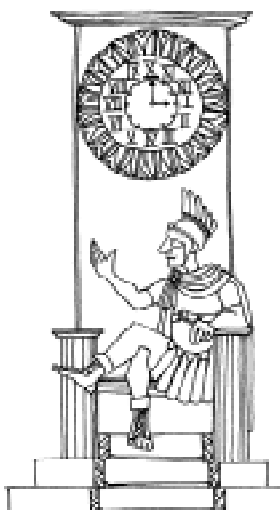


## 2. СЮЖЕТЫ, СВЯЗАННЫЕ С КРИПТОЛОГИЕЙ

<http://www.math.fau.edu/Richman/Liberal/caesar-f.htm>

*Апплет «Шифр Цезаря».*

Юлий Цезарь для зашифровки сообщений использовал циклический сдвиг буквы по алфавиту на 3 позиции, но в обобщенном варианте можно сдвигать и на другое количество позиций.



Здесь же приведены ссылки на известные литературные произведения, сюжет которых связан с расшифровкой сообщений таким способом: «Пляшущие человечки» А. Конан-Дойля и «Золотой жук» Э. По. Кроме того, вы можете поработать с апплетом, моделирующим расшифровку сообщения.

<http://raphael.math.uic.edu/~jeremy/crypt/cgi-bin/magic-gateway.cgi>

*Игра, связанная с расшифровкой подстановочного кода.*

[http://www.cut-the-knot.com/do\\_you\\_know/permutation.html](http://www.cut-the-knot.com/do_you_know/permutation.html)

*Перестановки конечного набора. Определения, примеры, апплет, вопросы для самопроверки.*

<http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/RectTran.html>

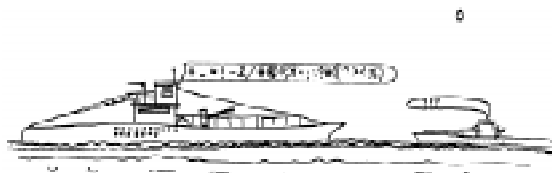
*Апплет, демонстрирующий процесс взлома перестановочного кода.*



<http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/>

*Апплет, демонстрирующий работу шифровальной машины Enigma, которую использовали в немецкой армии с начала 20-х годов до середины 40-х.*

Приведены ссылки, позволяющие познакомиться с принципами работы машины, с историей ее создания.



© Наши авторы, 2002.  
Our authors, 2002.

*Иванов Сергей Георгиевич,  
методист Центра  
профессионального обновления  
«Информатизация образования».*