Степанов Алексей Владимирович

ПЕРЕКЛАДЫВАЕМ КАМУШКИ ИЛИ ВОЗВОДИМ ДВОЙКУ В СТЕПЕНЬ

От редакции. В этом номере помещена статья Л.Б. Горелик об исследовательских работах в ИУМК «Математика в школе – XXI век». Когда с этими исследовательскими работами познакомился А.В. Степанов – автор серии статей по языкам разметки в «парном» вузовском журнале «Компьютерные инструменты в образовании», он предложил несколько своих работ, которые показались редколлегии журнала настолько интересными, что одну из них решили опубликовать в том же номере журнала.

Цель работы. На примере одной задачи обсудить идею сравнений по модулю p, операцию умножения по модулю p, цикличность этой операции при простом p и в результате использовать компьютерный перебор для получения некоторых решений исходной задачи.

Постановка задачи. Возьмем n камушков, где n – некоторое нечетное число, и разложим их в две кучки. В одной из кучек обязательно получится четное число камушков. Из этой кучки переложим половину камушков в другую. Продолжим процесс. Будем считать, что в этой игре для одного участника мы выиграли, если в некоторый момент в одной из кучек останется ровно один камушек. Ваша задача, выяснить, при каких n мы победим, независимо от разбиения на кучки. Числа n, обладающие указанным свойством, будем называть хорошими. Для решения поставленной задачи вам разрешается использовать подсказки мудрецов и помощь компьютера.

Подсказки мудрецов. Предположим, что в некоторый момент количество камушков в первой кучке равно k, а НОД$(n, k) > 1$. Докажите, что в этом случае мы не выиграем. Таким образом, для гарантированной победы n, по крайней мере, должно быть простым.

Сколько камушков было в первой кучке на предыдущем шаге:

если $k > n/2$;

если $k < n/2$?

Заметьте, что остаток от деления этого числа на n в обоих случаях одинаков.

Для того чтобы решать задачу дальше, необходимо иметь некоторые сведения о равноостаточности или сравнимости по модулю n (слово «модуль» в этом контексте не имеет ничего общего с абсолютной величиной числа). Будем говорить, что целые числа a и b сравнимы по модулю n, если они имеют одинаковый остаток от деления на n или, что то же самое, $a - b$ делится нацело на n. В этом случае пишем $a \equiv b \bmod n$.

Докажите основные свойства сравнимости: если $a \equiv b \bmod n$, а $c \equiv d \bmod n$, то $a + c \equiv b + d \bmod n$ и $ac \equiv bd \bmod n$. Сравнимость по модулю обсуждается во многих книгах и брошюрах.

Докажите, что мы выиграем за m шагов тогда и только тогда, когда $k \equiv \pm 2m \bmod n$.

Таким образом, для гарантированной победы необходимо и достаточно, чтобы любое число от 1 до $n - 1$ было бы сравнимо с $\pm 2m$ по модулю n. Проверьте это свойство для чисел $n = 13$ и $n = 17$.

Надеюсь, решая эту задачу, вы обратили внимание на то, что последовательнось остатков от деления $2m$ на n зацикливается и все дело в длине этого цикла. Имеет место следующее утверждение.

Теорема. Пусть n – простое число, а $1 \le t \le n - 1$. Существует целое положительное число m такое, что $tm \equiv 1 \bmod n$. Наименьшее такое m называется порядком числа k по модулю n. Порядок любого числа по модулю n является делителем числа $n - 1$.

Докажите, что мы гарантировано победим тогда и только тогда, когда порядок двойки по модулю n равен $n - 1$ или $(n - 1)/2$.

Докажите, что мы гарантировано победим, если $n = 2p + 1$, где p – простое число.

С математической точки зрения задача решена. Мы научились отличать хорошие n от плохих и можем привести достаточное количество примеров хороших чисел. Для того, что выписать эти самые примеры, воспользуйтесь помощью компьютера и выполните следующие задания.

Задания

1. Напишите программу, которая выписывает простые числа n вида $2p + 1$, где p тоже простое.

2. Как вы видели на примере из пункта 5, не все хорошие числа имеют вид $2p + 1$, где p простое. Найдите хотя бы одно хорошее число, большее 1000, которое не представляется в таком виде.

***Степанов Алексей Владимирович,
доцент кафедры Высшей
математики №2 СПбГЭТУ
«ЛЭТИ».***