

Китайская теорема об остатках

1. Дана таблица из 4 строк и 7 столбцов. Строки соответствуют остаткам по модулю 4 (от 0 до 3), а столбцы — остаткам по модулю 7 (от 0 до 6). Впишите в клетки этой таблицы числа от 0 до 27.
2. Рассмотрим таблицу, подобную описанной в предыдущей задаче, для остатков по двум взаимно простым модулям m и n . Впишем в неё числа от 0 до $mn - 1$. Докажите, что в каждой клетке окажется... (a) не более одного числа; (b) ровно одно число.
3. Сколько пятизначных чисел... (a) кончаются на 7 и кратны 9; (b) имеют остаток 17 по модулю 24 и остаток 29 по модулю 125?
4. В армии китайского императора менее миллиона солдат. Он приказал солдатам встать в шеренги по 101 и посчитал, сколько солдат остались лишними. Потом приказал им встать в шеренги по 103 и посчитал, сколько лишних. Наконец, приказал встать по 107 и вновь посчитал лишних. Докажите, что теперь он может однозначно определить численность армии.

Китайская теорема об остатках. Пусть m_1, m_2, \dots, m_N — взаимно простые числа, a_1, a_2, \dots, a_N — произвольные целые числа. Тогда среди любых $m_1 m_2 \dots m_N$ последовательных целых чисел найдётся ровно одно число x , для которого $x \equiv_{m_1} a_1, x \equiv_{m_2} a_2, \dots, x \equiv_{m_N} a_N$.

5. Докажите китайскую теорему об остатках: (a) для $N = 3$; (b) для произвольного N .
6. *Как разделить секрет?* Пароль от ядерного чемоданчика — десятизначное число. Семерым министрам выданы остатки от деления этого пароля на семь простых чисел: 97, 101, 103, 107, 109, 113, 127. Докажите, что если любые 5 министров захотят открыть чемоданчик, то сумеют сделать это с первого раза, а если всего четверо, то не смогут.

Это прекрасно, что такие числа существуют, но как их найти?

7. Найдите какое-нибудь число, которое...
 - (a) кратно 5, 7 и имеет остаток 1 по модулю 3;
 - (b) кратно 3, 7 и имеет остаток 1 по модулю 5;
 - (c) кратно 3, 5 и имеет остаток 1 по модулю 7;
 - (d) имеет остаток a по модулю 3, b по модулю 5 и c по модулю 7.
8. Докажите, что для всякого n найдутся n последовательных чисел, ни одно из которых не является степенью простого.