Китайская теорема об остатках

Каким образом можно определить численность войска? Говорят, что в Китае военачальники делали так: давали несколько последовательных команд типа «В колонну по 7 становись!», «В колонну по 11 становись!», ..., и в каждом случае выясняли, сколько солдат получилось в последнем ряду. После этого — только по найденным остаткам! — вычислялось общее количество солдат с помощью *китайской теоремы об остатках*.

Вводные задачи

1. (*ВМШ-57, 2006, 7*) Олег собрал мешочек монет. Саша пересчитал их, и оказалось, что если разделить все монеты на пять равных кучек, то останется две лишние монеты. А если на четыре равные кучки — останется одна лишняя монета. В то же время монетки можно разделить на три равные кучки. Какое наименьшее число монет могло быть у Олега?

57

2. Найдите наименьшее натуральное число, дающее при делении на 2, 3, 5, 7 остатки 1, 2, 4, 6 соответственно.

209

Предварительные сведения

3. Решите сравнение: а) $4x \equiv 1 \pmod{5}$; б) $6x \equiv 2 \pmod{9}$.

а) $x \equiv 4 \pmod{5}$; б) решений нет

4. Докажите, что если натуральные числа a и m взаимно просты, то при любом целом b:
1) ровно одно из чисел $0, 1, \ldots, m-1$ удовлетворяет сравнению $ax \equiv b \pmod{m}$;
2) сравнение $ax \equiv b \pmod{m}$ имеет единственное решение вида $x \equiv c \pmod{m}$.

Определение. Пусть натуральные числа a и m взаимно просты. Единственное число x из множества $\{0, 1, \ldots, m-1\}$, удовлетворяющее сравнению $ax \equiv 1 \pmod{m}$, называется *мультипликативным обратным* по модулю m для числа a и обозначается $a^{-1} \pmod{m}$.

5. Найдите: а) $3^{-1} \pmod{7}$; б) $7^{-1} \pmod{3}$.

а) 5; б) 1

Китайская теорема об остатках

Пусть $m_1, m_2, \ldots, m_n$ — попарно взаимно простые натуральные числа (то есть $(m_i, m_j) = 1$ при $i \neq j$) и $M = m_1 m_2 \ldots m_n$. Тогда, каковы бы ни были целые числа $a_1, a_2, \ldots, a_n$, система сравнений

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \ldots \\ x \equiv a_n \pmod{m_n}. \end{cases} \qquad (1)$$

имеет единственное решение $x \equiv a \pmod{M}$, где

$$a = \sum_{i=1}^{n} a_i M_i \mu_i, \tag{2}$$

и обозначено

$$M_i = \frac{M}{m_i}, \quad \mu_i = M_i^{-1} \pmod{m_i}.$$

6. Решите задачи 1 и 2 с помощью формулы (2).

7. Пусть x' и x'' являются решениями системы (1). Докажите, что $x' \equiv x'' \pmod{M}$.

8. Докажите, что число $a_1 M_1 \mu_1$ удовлетворяет системе

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv 0 \pmod{m_2}, \\ \dots \\ x \equiv 0 \pmod{m_n}. \end{cases}$$

9. Докажите китайскую теорему об остатках.

10. При каких целых n число $n^2 + 3n + 1$ делится на 55?

$n = 55k + 6$ и $n = 55k + 46$, $k \in \mathbb{Z}$

11. (*Задачник «Кванта», M1257*) Дан многочлен $F(x)$ с целыми коэффицикнтами, причём известно, что для любого целого n число $F(n)$ делится на одно из целых чисел $a_1, a_2, \ldots, a_m$. Докажите, что из этих чисел можно выбрать одно число так, что $F(n)$ будет делиться на него при любом целом n.

12. (*Всеросс., 2008, 10, финал*) При каких натуральных $n > 1$ существуют такие натуральные $b_1, \ldots, b_n$ (не все из которых равны), что при всех натуральных k число $(b_1+k)(b_2+k)\ldots(b_n+k)$ является степенью натурального числа? (Показатель степени может зависеть от k, но должен быть всегда больше 1.)

При составных n

13. (*IMO, 1989*) Prove that for each positive integer n there exist n consecutive positive integers none of which is an integral power of a prime number.