24. Сравнения

Говорят, что числа a и b *сравнимы по модулю* m, если их разность делится на m. (Числа предполагаются целыми; мы считаем, что модуль m полложителен.) Обозначение: $a \equiv b \pmod{m}$.

24.1. Доказать, что $a \equiv b \pmod{m}$ в том и только том случае, когда a и b дают одинаковые остатки при делении на m.

24.2. Найти положительное целое число, которое сравнимо с -1 по любому из модулей $1, 2, 3, 4, 5, 6, 7$.

24.3. Доказать, что сравнения по одному модулю можно складывать и перемножать: если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a + c \equiv b + d \pmod{m}$ и $ac \equiv bd \pmod{m}$.

24.4. Доказать, что если $a \equiv b \pmod{m}$, то $a^n \equiv b^n \pmod{m}$ при $n = 1, 2, 3, 4, \ldots$.

24.5. Доказать, что $a^n \equiv b^n \pmod{(a-b)}$ при $n = 1, 2, 3, 4, \ldots$ (и при любых $a \neq b$).

24.6. Какие остатки может давать точный квадрат при делении на 3, 5 и 7?

24.7. Найти остатки от деления 16^{101} и 18^{101} на 17.

24.8. Доказать, что четырёхзначное число $abcd$ сравнимо с $a+b+c+d$ по модулю 9 и с $-a + b - c + d$ по модулю 11.

24.9. Известно, что $7a \equiv 3 \pmod{13}$. Найти остаток от деления a на 13. (Сколько есть возможностей?)

24.10. Известно, что $8a \equiv 4 \pmod{14}$. Найти остаток от деления a на 14. (Сколько есть возможностей?)

24.11. Доказать, что $1^{99} + 2^{99} + 3^{99} + 4^{99} + 5^{99} + 6^{99}$ делится на 7.

24.12. Доказать, что если $ac \equiv bc \pmod{mc}$, то $a \equiv b \pmod{m}$.

24.13. Найти остаток от деления $(n^2 - 1)^{101}(n + 1)^{100}$ на n.

* * *

24.14. Доказать, что $7777^{2222} + 2222^{7777}$ делится на 9.

24.15. Найти остаток от деления числа 1234567891011 ... 99100 на 9.

24.16. Доказать, что $1^{100} + 2^{100} + 3^{100} + 4^{100} + 5^{100} + 6^{100}$ делится на 7.

24.17. При каких n число $11^{2n} + 12^{n}$ делится на 133?

24.18. Известно, что сумма двух точных квадратов делится на 21. Доказать, что она делится на 441.

В этом листке мы после некоторого перерыва снова возвращаемся к арифметике остатков; новшество состоит в использовании обозначения для сравнений.

В задаче 24.3 можно немного упростить вычисления, изменяя только один из операндов. Задача 24.5 — переформулировка задачи 24.4, а также задачи о том, что $a^n - b^n$ делится на $a - b$.

Задачи 24.9 и 24.10 показывают, что иногда деление однозначно, а иногда нет. Короткое решение задачи 24.9: если $7a \equiv 3 \pmod{13}$, то $14a \equiv 6 \pmod{13}$, но $14a \equiv a \pmod{13}$.

В задаче 24.11 группируются пары с противоположным знаком. В аналогичной дополнительной задаче 24.16 это уже не проходит. Можно либо явно всё вычислить, либо использовать стандартное решение: если умножить все основания степеней на 2 (скажем), то сумма умножится на 2^{100}, но также и не изменится (слагаемые переставятся). Общий ответ: $1^n + 2^n + \ldots + 6^n$ (по модулю 7) равно либо 6 (при n, кратном 6, малая теорема Ферма), либо 0 (при остальных n).

В задаче 24.17 требуется два перехода: от числа к сумме его цифр и затем к числу $1 + 2 + 3 + \ldots + 99 + 100$, с которым уже легко разобраться.

В задаче 24.18 можно отдельно понять, что a и b делятся на 7 и на 3, анализируя возможные остатки точных квадратов.