Занятие 9: деление по модулю и алгоритм Евклида

Пусть k, n — целые, причём $n > 0$. На множесте $\mathbb{Z}_n$ остатков по модулю n рассмотрим операцию «умножения на k» $[x] \mapsto [kx]$. Для решения некоторых сравнений нам приходилось эту операцию проводить в обратном направлении: «делить на k». Возникают естественные вопросы: в каких случаях можно делить, как это эффективно (без длительного перебора) делать и для чего ещё можно всё это применять?

Деление по модулю

1) Докажите, что при помощи умножения на k можно получить любой остаток по модулю n тогда и только тогда, когда никакой остаток нельзя «получить дважды» (т.е. из $[ka] = [kb]$ следует $[a] = [b]$).

2) Докажите, что если при помощи умножения на k можно получить любой остаток по модулю n, то операция деления на k определена однозначно (для любого остатка $[c]$ существует единственное «частное» $[x]$ такое, что $c \equiv kx \pmod{n}$).

3) Докажите, что если k и n взаимно просты, то из $ka \equiv kb \pmod{n}$ следует $a \equiv b \pmod{n}$. (Подсказка: вы это уже доказывали. Здесь утверждение находится лишь для целостности картины.)

4) Докажите, что деление на k однозначно определено тогда и только тогда, когда k и n взаимно просты. (Не забудьте про часть «только тогда»!)

5) Пусть d — НОД k и n. Докажите, что если $d \nmid a$, то не существет такого b, что $kb \equiv a \pmod{n}$.

Следствие. *Если k и n имеют НОД, равный $d > 1$, а делить на k хочется, то следует сократить всё на d и делить на k/d по модулю n/d. Если делимое не делится на d (в арифметике ВСЕХ целых чисел), то поделить его на k (по модулю n) не получится (см. 5 задачу).*

Следствие. *Частное (по модулю n) при делении числа a на число k определено тогда и только тогда, когда $d =$ НОД(k, n) делит a. При этом частное, если существует, определено однозначно с точностью до слагаемого, кратного n/d.*

Алгоритм Евклида

Мы полностью ответили на вопрос: когда можно делить на k? Осталось научиться делить на k быстро. Для этого достаточно уметь находить частное $[1]/[k]$. Этим и занимается алгоритм, названный в честь Евклида.

6) Докажите, что для любых целых чисел b и a ($a \neq 0$) существуют и единственны такие числа q и r, что $b = aq + r$ и $0 \leqslant r < |a|$. (Напомним, что q называется *частным*, а r — *остатком* при делении b на a. Для r мы будем использовать обозначение $b \bmod a$.)

7) Пусть $0 < a \leqslant b$, $d = $ НОД(a, b). Докажите: а) $d =$ НОД$(a, b - a)$; б) $d =$ НОД$(a, b \bmod a)$.

8) Пусть $0 < a \leqslant b$. Рассматривается последовательность пар чисел $(x_0, y_0), (x_1, y_1), \ldots$, где
$(x_0, y_0) = (a, b)$;
$(x_{n+1}, y_{n+1}) = (y_n \bmod x_n, x_n)$.
Докажите, что эта последовательность конечна (в некоторый момент m окажется, что $x_m = 0$, а $y_m =$ НОД(a, b)).

9) Вычислите при помощи алгоритма Евклида:
а) НОД$(91, 147)$; б) НОД$(-144, -233)$; в) НОД(F_{100}, F_{101}), где F_i — числа Фибоначчи.

10) Найдите: а) НОД$(2^{32} + 1, 2^{16} + 1)$; б) НОД$(2^{91} - 1, 2^{63} - 1)$; в) НОД$\left(n^a - 1, n^b - 1\right)$.

11) Пусть $[a]/[k] = [x]$ и $[b]/[k] = [y]$, причём $0 < a < b$. Пусть $b = aq + (b \bmod a)$. Выразите частное $[b \bmod a]/[k]$ через x, y и q.

12) Пусть $0 < k \leqslant n$, k и n взаимно просты. Заметим, что $[k]/[k] = [1]$, $[n]/[k] = [0]/[k] = [0]$. Рассмотрим рекуррентное соотношение (т.н. *расширенный алгоритм Евклида*)
$(x_0, y_0, a_0, b_0) = (k, n, [1], [0])$;
$(x_{n+1}, y_{n+1}) = (y_n \bmod x_n, x_n)$,
$(a_{n+1}, b_{n+1}) = ([y_n \bmod x_n]/[k], a_n)$.
Пусть m — номер последнего элемента в этой последовательности. Чему равно b_m?

13) Найдите $[1]/[666]$ по модулю 1543.