Малая теорема Ферма. Теорема Вильсона

8 класс

11.10.2014

В задачах этого листика p - простое число, a - ненулевой остаток по модулю p (*без этих предположений большинство задач просто неверны*). Все остатки в условиях всех задач берутся по модулю p. Перед тем как решать задачи предлагается вспомнить следующие факты и их доказательства:
а) Остатки $0 \cdot a, 1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ образуют полную систему остатков по модулю p, т.е. выписанные остатки есть просто некоторая перестановка остатков $0, 1, 2, \ldots, p-1$; или, что то же самое, умножение на a никакие два остатка *не склеивает*.
б) Существует, и при том единственный остаток b, такой что $ab \equiv 1 \pmod{p}$. b будем называть *обратным по умножению* остатком к a.

1. (*Сокращение сравнений*) Известно, что $ax \equiv ay \pmod{p}$. Докажите, что $x \equiv y \pmod{p}$. Приведите контрпримеры к утверждению без предположений простоты p или неделимости a на p.

2. Для ненулевого остатка x рассмотрим последовательность: $x, ax, a^2x, a^3x, \ldots, a^nx, \ldots$. Докажите, что эта последовательность когда-нибудь зациклится, причём без предпериода.
   Эту последовательность будем называть *орбитой* остатка x.

3. Докажите, что орбиты любых двух ненулевых остатков x, y (т.е. множества остатков, которые можно получить из x (соответственно y) путём многократного умножения на a) либо не пересекаются вообще, либо совпадают.

4. Докажите, что орбиты любых двух ненулевых остатков x, y имеют равную длину (в смысле множества из предыдущей задачи имеют равное число элементов).

5. Покажите, что длина орбиты ненулевого остатка - делитель числа $p-1$. Выведите отсюда **малую теорему Ферма**: если p - простое, a - целое, не кратное p, то $a^{p-1} \equiv 1 \pmod{p}$.
   Эквивалентная формулировка: p - простое, a - произвольное целое $\Rightarrow a^p - a$ делится на p.

---

6. Найдите все остатки по модулю p, совпадающие со своими обратными по умножению (т.е. все остатки x, такие что $x^2 \equiv 1 \pmod{p}$).

7. Докажите **теорему Вильсона**: если p - простое, то $(p-1)! \equiv -1 \pmod{p}$.