А Р И Ф М Е Т И К А   О С Т А Т К О В

АР 7
24.12
1987г

Пусть $m \in \mathbb{N}$. Обозначим через $\mathbb{Z}_m$ множество $\{0,1,2,\dots,m-1\}$ остатков от деления на m, а через $\overline{n}$ остаток от деления $n \in \mathbb{Z}$ на m. Для $a,b \in \mathbb{Z}_m$ определим "сумму" и "произведение": $a+b := \overline{a+b}$, $ab := \overline{ab}$. Множество $\mathbb{Z}_m$ с этими операциями называется КОЛЬЦОМ ВЫЧЕТОВ ПО МОДУЛЮ m. Из листка АР2 следует что для любых $x,y \in \mathbb{Z}$ $\overline{x+y} = \overline{x}+\overline{y}$ и $\overline{xy} = \overline{x}\,\overline{y}$.

1. Составьте таблицы умножения и сложения для $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_9$ и найдите в этих кольцах а) все квадраты; б) все кубы.

2. а) Каким днем недели было 1 января 0001 года ?
Докажите, что существует бесконечно много натуральных чисел, не представимых в виде суммы трех б) квадратов; в) кубов натуральных чисел.

3. При каких m в кольце $\mathbb{Z}_m$ есть делители нуля?

4. Пусть $a \in \mathbb{Z}_m$. Возьмем m точек на плоскости и расставим на них элементы множества $\mathbb{Z}_m$. Соединив стрелкой точку x с точкой ax, мы получим ДИАГРАММУ УМНОЖЕНИЯ НА a. а) Нарисуйте ее для $m=10, a=4$ и $m=13, a=5$.
Пусть m простое число и $a \neq 0$. Докажите, что тогда
б) в каждую вершину диаграммы ведет не более двух стрелок;
в) в каждую вершину диаграммы ведет ровно одна стрелка;
г) диаграмма представляет собой объединение циклов;
д) все эти циклы кроме одного (нулевого) имеют одну и ту же длину.

5. (СЛЕДСТВИЯ ИЗ СВОЙСТВ ДИАГРАММ) Докажите, что при простом p
а) любой ненулевой элемент $\mathbb{Z}_p$ обратим; б) уравнение $ax=b$ в $\mathbb{Z}_p$ разрешимо, если $a \neq 0$; в) если $a \neq 0$, то существует $n \in \mathbb{N}$ тч $a^n=1$;
г) (Теорема ФЕРМА) если $a \not\vdots\, p$, то $a^{p-1}-1$ p ($a \in \mathbb{Z}$).

6. (КВАДРАТНЫЕ УРАВНЕНИЯ) Пусть p простое, $p \neq 2$. Докажите, что в $\mathbb{Z}_p$
а) уравнение $x^2=a$ имеет не более двух решений;
б) есть ровно два элемента, обратных самому себе;
в) ровно $(p+1)/2$ элементов, являющихся квадратами;
г) уравнение $x^2+ax+b=0$ разрешимо титтк a^2-4b квадрат.

7. (АРИФМЕТИЧЕСКИЕ СЛЕДСТВИЯ) Пусть p простое. Докажите, что p делит
а) числитель дроби $m/n = 1+1/2+1/3+\dots+1/(p-1)$;
б) (Теорема ВИЛЬСОНА) число $(p-1)!+1$.
<Указание: разбейте элементы $\mathbb{Z}_p$ на пары (a,a^{-1}) и вспомните 6б.>

8. (СЛЕДСТВИЯ ИЗ ТЕОРЕМЫ ФЕРМА) Пусть $p \neq 2;5$ простое. Докажите, что
а) существует число вида 111...11 кратное p;
~~б) если 2 - 1 простое число, то 2 - 2 кратно p;~~ б) все простые делители числа 2^p-1 имеют вид $q=2kp+1$
в) длина периода разложения $1/p$ в периодическую дробь делит $p-1$.

9. (КВАДРАТИЧНЫЕ ВЫЧЕТЫ) Пусть $p \neq 2$ простое число. Докажите, что в $\mathbb{Z}_p$
а) произведение двух квадратов – квадрат;
б) произведение квадрата и неквадрата – неквадрат;
в) произведение двух неквадратов – квадрат;
г) при $a \neq 0$ элемент $a^{(p-1)/2}$ равен 1 или –1 (т.е. p–1);
д) уравнения $x^{\frac{p-1}{2}}=1$ и $x^{(p-1)/2}=-1$ имеют по $(p-1)/2$ решений;
е) $a \neq 0$ является квадратом титтк $a^{(p-1)/2}=1$.

10. Для каких простых p а) –1; б)* –2; в)* –3 является квадратом в $\mathbb{Z}_p$;
г) существуют натуральные x и y $(x,y \not\vdots\, p)$ тч x^2+y^2 делится на p ?

1абв 2абв 3 4абвгд 5абвг 6абвг 7аб 8абв 9абвгде 10абвг