Делимость
8 класс "В"
30 ноября 2011 г.

В арифметике по модулю мы научились выполнять три основные операции: $+, -, \times$*, и до сих пор молчаливо обходили вопрос существования операции деления.*

В обычной арифметике деление определялось как операция обратная умножению, если $5 \cdot 2 = 10$*, то* $10 : 2 = 5$*. Назовем частным от деления числа* a *на* d *по модулю* m *такое число* b*, что* $a \equiv bd \pmod{m}$*.*

1. Найдите частное от деления a на d

a) mod 5

	0	1	2	3	4
0					
1			3	2	
2			1		
3					
4					

b) mod 6

	0	1	2	3	4	5
0						
1		1				
2						
3						
4						
5						

Из задачи 1 следует, что деление в арифметике по модулю осуществимо не всегда (но гораздо чаще, чем деление нацело в обычной арифметике, $1 : 3 \equiv 2 \pmod{5}$*).*

2. Если 1 делится на a по модулю m, то и любое число b делится на a по модулю m.

Число a *называется* **обратимым в арифметике по модулю** m*, если существует такое число* a^{-1}*, что* $aa^{-1} \equiv 1 \pmod{m}$*. Число* a^{-1} *называется* **обратным к числу** a **по модулю** m*.*

3. Найдите обратные числа по модулю 7 к числам $1, 2, 3, 4, 5, 6$.

Число $a \neq 0$ называется **делителем нуля в арифметике по модулю** m, если существует отличное от нуля число b, что $ab \equiv 0 \pmod{m}$.

4. Найдите делители нуля в арифметике по модулю 8.

5. Докажите, что число не может быть одновременно и обратимым и делителем нуля.

6. Докажите, что, если число обратимо, то обратное к нему единственно.

7. Докажите, что если m — составное число, то найдется число a, являющееся делителем нуля по модулю m.

8. Докажите, что если a — не делитель нуля, то

a) $a^2, a^3, a^4, \ldots$ — тоже не являются делителями нуля;

b) среди чисел $a^2, a^3, a^4, \ldots$ должна найтись единица.

9. Докажите, что если m — простое число, все числа отличные от нуля, обратимы.

10. Докажите, что если m — составное число, все числа взаимно простые с m, обратимы.

11. Докажите **малую теорему Ферма**: если p — простое, то $n^p \equiv n \pmod{p}$.

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

13. Докажите **китайскую теорему об остатках**: для любых попарно взаимно простых чисел m_1, m_2,..., m_n и любых натуральных $r_1 < m_1$,..., $r_n < m_n$ найдется такое число N, что $N \equiv r_1 \pmod{m_1}$,..., $N \equiv r_n \pmod{m_n}$