Делимость и малая теорема Ферма

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

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

mod 5

b

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

mod 6

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$^{\vee}$ 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 такое, что $ab \equiv 0 \pmod m$.*

4 Найдите делители нуля в арифметике по модулю 8.

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

6$^{\vee}$ Докажите, что число не может быть одновременно и обратимым и делителем нуля.

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 a$^{\vee}$ Докажите, что если a взаимно просто с m, то числа a, $2a$, $3a$, ... $(m-1)a$ дают разные остатки по модулю m.

b Докажите, что если p — простое число, все числа, отличные от нуля, обратимы.

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

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

---

11 Найдите остаток от деления a 2^{100} на 101; b 3^{102} на 101;
c 8^{900} на 29; d 3^{2012} на 43; e 8^{1543} на 48.

12$^{\vee}$ Докажите, что если p простое и $p > 2$, то $7^p - 5^p - 2$ делится на $6p$.

13 Докажите, что $m^5n - mn^5$ кратно 30 при любых целых m и n.

14* Пусть p — простое число, отличное от 2, 3 и 5. Докажите, что число, записанное $p-1$ единицей, кратно p. (Например, 111111 кратно 7.)
