кратно p. Значит, для чисел k, не кратных p, теорему можно формулировать следующим образом:

Теорема 1. *Если целое число k не кратно простому числу p, то k^{p-1} дает остаток 1 при делении на p.*

Доказательство. Поскольку остатки от деления на p чисел k, $2k$, $3k$, …, $(p-1)k$ – это (с точностью до перестановки) числа 1, 2, 3, …, $p-1$, то

$$k\cdot 2k\cdot 3k\cdot\ldots\cdot(p-1)k\equiv 1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)\pmod p,$$

откуда

$$k^{p-1}(p-1)!\equiv(p-1)!\pmod p.$$

Сократив на $(p-1)!$, получим желаемое:

$$k^{p-1}\equiv 1\pmod p.$$

А тот, кто не решил упражнение 4 б) и не знает, почему сравнения можно сокращать (на число, взаимно простое с модулем), пусть рассуждает следующим образом: поскольку произведение $\left(k^{p-1}-1\right)\cdot(p-1)!$ кратно p, а число $(p-1)!$ не кратно p, то число $k^{p-1}-1$ кратно простому числу p.

Упражнения

18. Найдите остаток от деления числа 3^{2000} на 43.

19. Если целое число a не кратно 17, то a^8-1 или a^8+1 кратно 17. Докажите это.

20. Докажите, что $m^{61}n-mn^{61}$ кратно 56786730 при любых целых m и n.

21. Найдите все такие простые числа p, что $5^{p^2}+1$ кратно p.

22. Пусть p – простое число, $p\neq 2$. Докажите, что число 7^p-5^p-2 кратно $6p$.

23. Если p – простое число, то сумма $1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1}$ при делении на p дает остаток $p-1$. Докажите это.

24. Шестизначное число кратно 7. Его первую цифру стерли и затем записали ее позади последней цифры числа. Докажите, что полученное число тоже кратно 7. (Например, из кратных 7 чисел 632387 и 200004 таким образом получаем числа 323876 и 42, которые тоже кратны 7.)

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

26*. Докажите, что для любого простого p число 11…1122…22…99…99, состоящее из $9p$ цифр (сначала p единиц, потом p двоек, p троек, …, наконец, p девяток), при делении на p дает такой же остаток, как и число 123456789.

Таблицы умножения

Назло ей я все-таки помножил землекопов. Правда, ничего хорошего про них не узнал, но зато теперь можно было переходить к другому вопросу.

Л.Гераскина

Рассмотрим все $n-1$ разных ненулевых остатков от деления на n. Составим таблицу умножения, написав на пересечении a-го столбца и b-й строки остаток от деления на n произведения ab. Например, при $n=5$ получим таблицу 2, при $n=11$ — таблицу 3.

Таблица 2

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Таблица 3

×	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Таблица 4

×	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Таблица 5

×	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Поскольку в обоих примерах число n простое, в каждой строке, как и в каждом столбце, возникает некоторая перестановка чисел 1, 2, …, $n-1$. Если же рассмотреть составное число, то в таблице обязательно встретится нуль. Например, при $n=4$ имеем $2\cdot 2\equiv 0$ (табл.4); не лучше ситуация и при $n=12$ (табл.5): опять в некоторых строках есть нули! И вообще, при любом составном числе $n=ab$, где $1<a$, $b<n$, на пересечении a-й строки и b-го столбца стоит остаток от деления ab на n, т.е. 0.

Итак, если n составное, то имеются *делители нуля* – ненулевые остатки a и b, произведение ab которых кратно n, иными словами, равно нулю по модулю n. Но даже при составном n в некоторых строках таблицы умножения нет нулей. В таблице 4 таковы первая и третья строки, а в