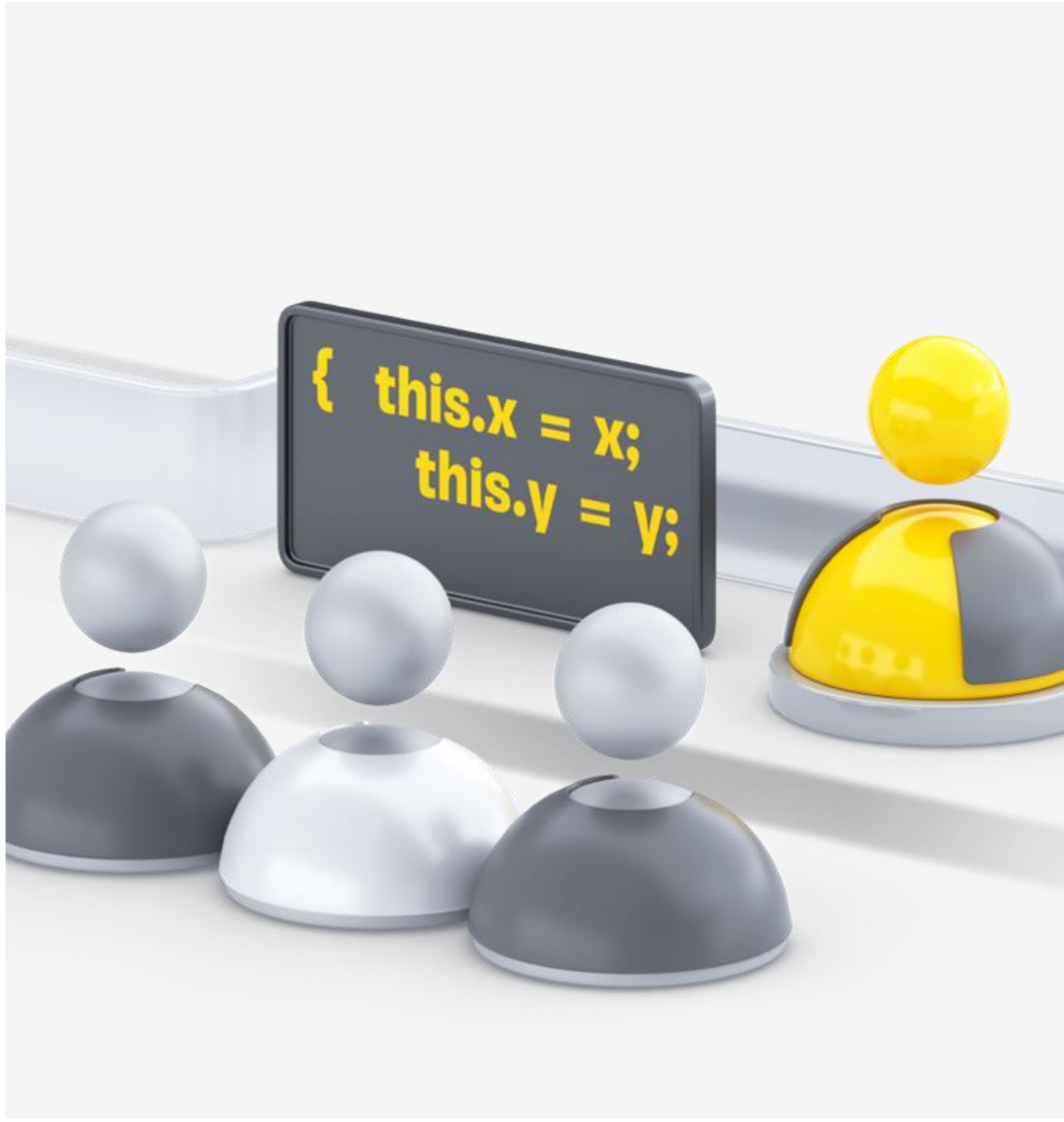
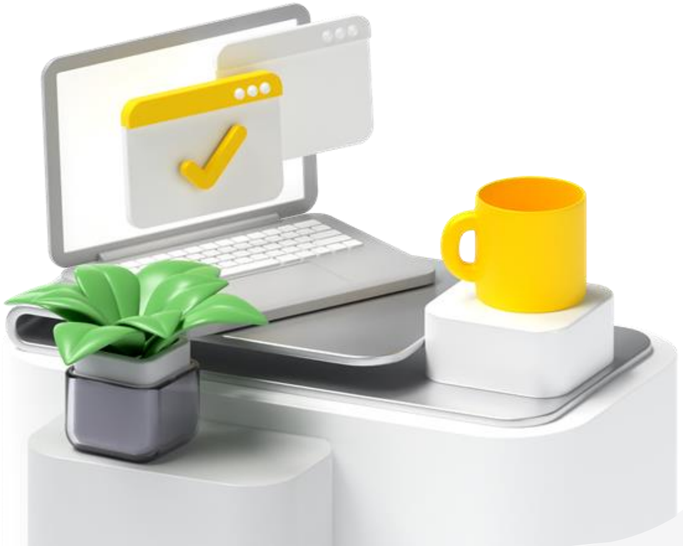
Математика



Алгоритм Евклида

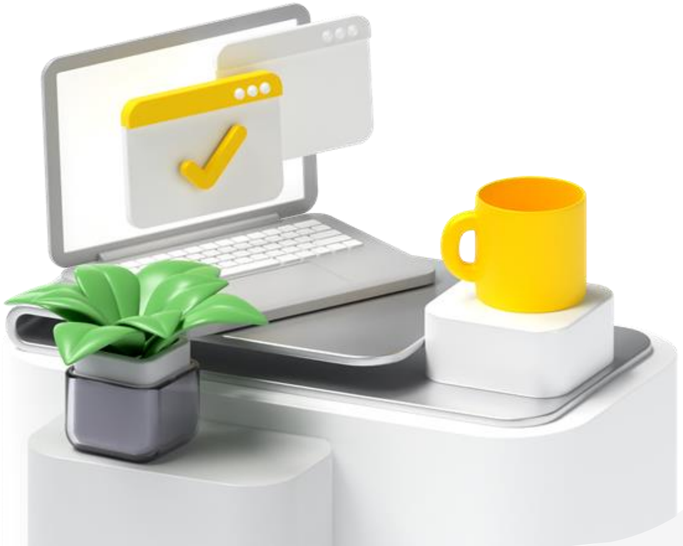
Будем из большего числа вычитать меньшее, пока не получим 0, но это можно делать быстрее



140	96	
96	1	
96	44	
88	2	
44	8	
40	5	
8	4	← последний делитель
8	2	
0		

Наименьшее общее кратное

Как найти LCM?



$$
\begin{array}{r|l}
140 & 96 \\
\underline{96} & 1 \\
96 & 44 \\
\underline{88} & 2 \\
44 & 8 \\
\underline{40} & 5 \\
8 & 4 \\
\underline{8} & 2 \\
0 &
\end{array}
$$

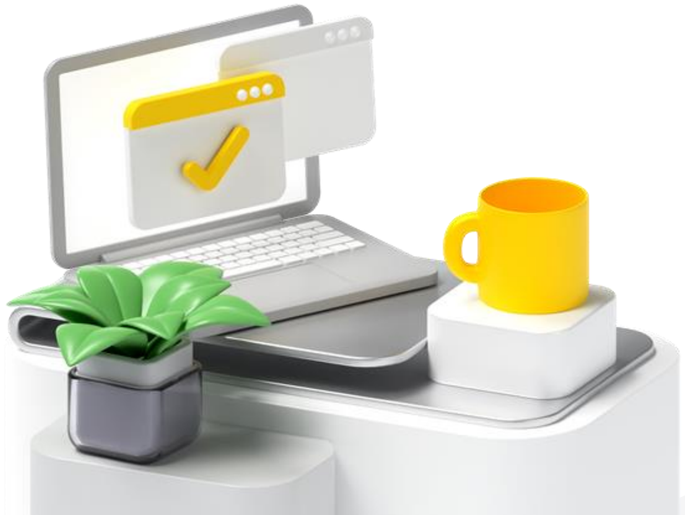
последний делитель

Факторизация

Как найти все множители числа?

Нужно ли проходить по всем числам?

Сколько всего может быть множителей у числа?



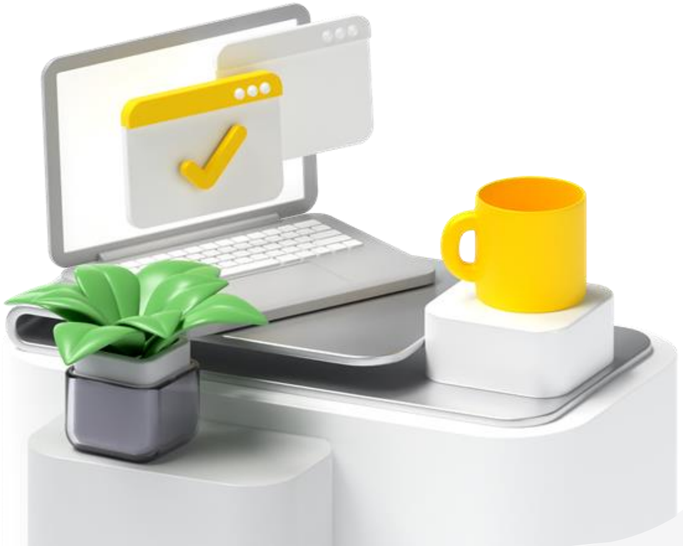
525

525 =

Решето Эратосфена

Как найти все простые числа на отрезке?

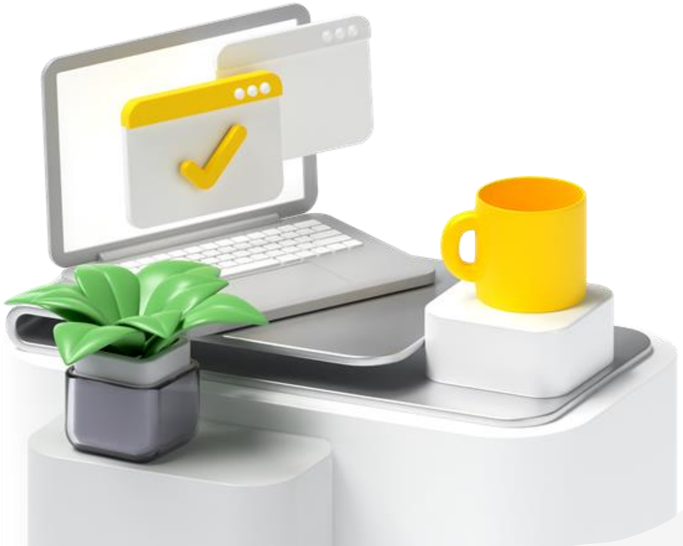
	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	



Решето Эратосфена

Как найти все простые числа на отрезке?

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	



Обратное по модулю

Как разделить число, когда мы делаем операции по модулю?

- Найти обратное число
- Умножить на него

Как найти обратное?

- Возвести число в степень
- gcd_ex

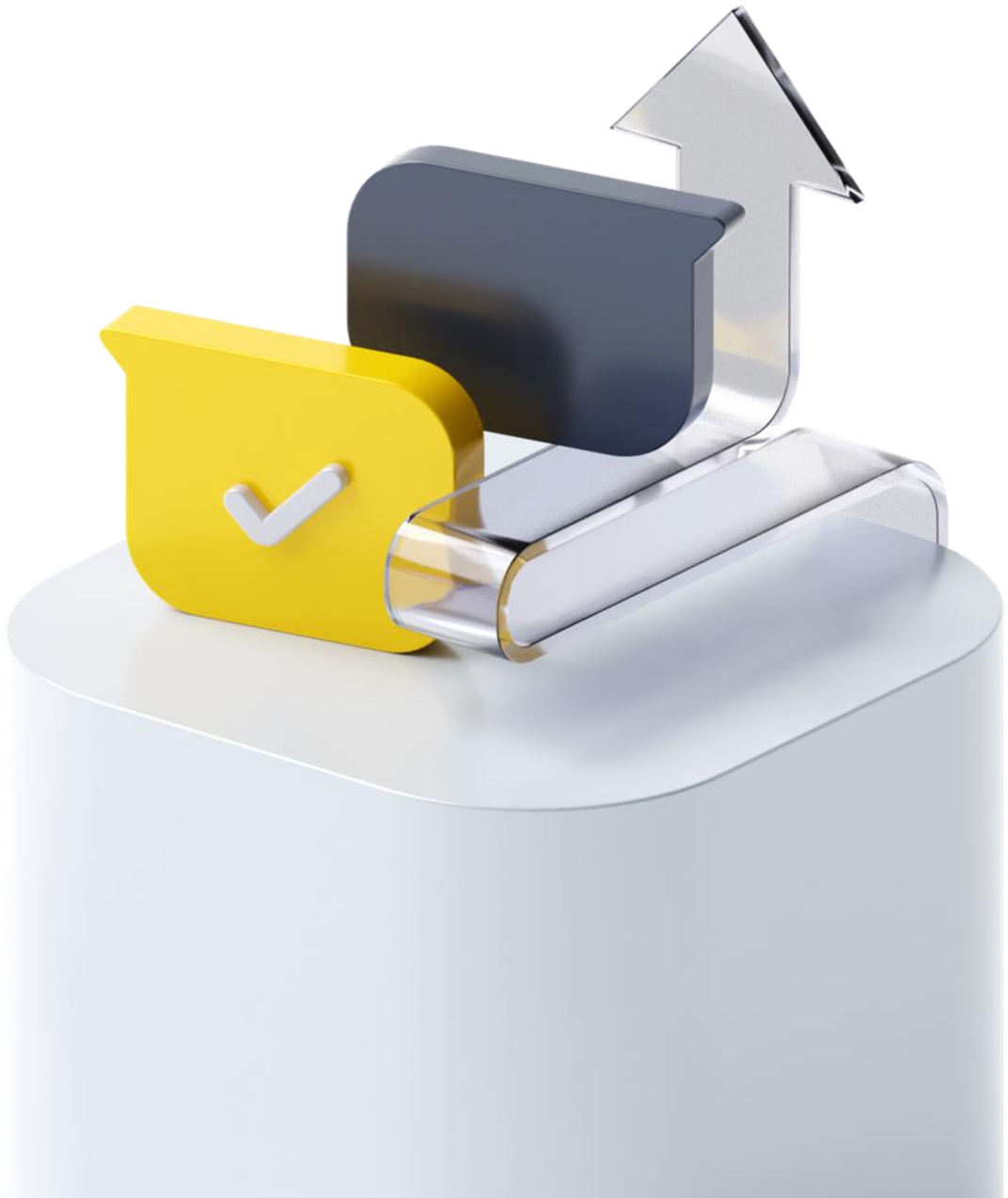
(малая) Теорема Ферма

$$a^{p-1} \equiv 1 \bmod p$$

Расширенный алгоритм Эвклида

```
int gcd(int a, int b, int &x, int &y) {
    if (a == 0) {
        x = 0;
        y = 1;
        return b;
    }
    int x1, y1;
    int d = gcd(b % a, a, x1, y1);
    x = y1 - (b / a) * x1;
    y = x1;
    return d;
}
```

Т БАНК



Спасибо за курс!