MAS114: Lecture 10

James Cranch

http://cranch.staff.shef.ac.uk/mas114/

2017–2018

A better method

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

1

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form.

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form. We repeat the following steps:

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form. We repeat the following steps:

1. Find the first untouched number and mark it as a prime.

[1] An *algorithm* is a method for calculating something.

A better method

If you have to find primes, it's probably better to use this method, which works well in practice:

Algorithm (The Sieve of Eratosthenes)

[1] The *Sieve of Eratosthenes* proceeds by writing down the natural numbers from 2 up to N (for some N) in a convenient form. We repeat the following steps:

1. Find the first untouched number and mark it as a prime.
2. Mark all its multiples as being composite.

[1] An *algorithm* is a method for calculating something.

The Sieve of Eratosthenes

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

The Sieve of Eratosthenes

Here's an example, where we take $N = 100$:

	2	3	4	5	6	7	8	9	10
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

As you can see, when we find a number uncrossed, it's because it has no factors that would have caused it to be crossed out, so it's prime.

More comments

More comments

Remark

The Sieve of Eratosthenes doesn't prove that there are infinitely many primes: it just finds them.

More comments

Remark

The Sieve of Eratosthenes doesn't prove that there are infinitely many primes: it just finds them. Unless we'd found a proof of Euclid's theorem, we could have nightmares that one day we'll find ourself crossing off all the remaining naturals and not finding any more primes.

More comments

Remark

The Sieve of Eratosthenes doesn't prove that there are infinitely many primes: it just finds them. Unless we'd found a proof of Euclid's theorem, we could have nightmares that one day we'll find ourself crossing off all the remaining naturals and not finding any more primes.

Remark

There are (quite a lot of) other proofs of Euclid's theorem, but Euclid himself probably only knew the way we've discussed.

Coprimality

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, and its factors, it's going to turn out to be really useful to consider two numbers and their factors.

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, and its factors, it's going to turn out to be really useful to consider two numbers and their factors.

Definition

Let a and b be integers. A *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$.

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, and its factors, it's going to turn out to be really useful to consider two numbers and their factors.

Definition

Let a and b be integers. A *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$. The *greatest common divisor* of a and b, written $\gcd(a, b)$ (or sometimes as $\mathrm{hcf}(a, b)$ or sometimes even just (a, b) for short) is the largest common divisor of a and b.

Coprimality

Now we're going to introduce some very useful concepts. Rather than (as we were doing before) looking at one number at a time, and its factors, it's going to turn out to be really useful to consider two numbers and their factors.

Definition

Let a and b be integers. A *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$. The *greatest common divisor* of a and b, written $\gcd(a, b)$ (or sometimes as $\mathrm{hcf}(a, b)$ or sometimes even just (a, b) for short) is the largest common divisor of a and b.

Remark

That definition probably just says that a greatest common divisor is what you'd expect it to be, given the name!

Warning!

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function.

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):*

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every positive integer, and so will certainly be a common divisor.

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every positive integer, and so will certainly be a common divisor.
- *There may be lots of common divisors, but no largest one.*

Warning!

Remark

That definition is *dangerous*, because it does something I've warned you against doing several times: it defines something that looks like a function, but it doesn't prove that it is a function. There are two reasons why the gcd might not exist; we need to satisfy ourselves that neither is a problem:

- *There might be no common divisors at all (and hence no greatest common divisor):* This is not a problem: we have observed before that 1 is a divisor of every positive integer, and so will certainly be a common divisor.
- *There may be lots of common divisors, but no largest one.* That's not a problem either, here. It's easy to see that if $d \mid a$ then $|d| \leqslant |a|$, which means we can't get arbitrarily large divisors.

Finding GCDs

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important.

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we just count down from $|a|$ and stop when we reach the first common divisor.

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we just count down from $|a|$ and stop when we reach the first common divisor. For example,

$$\gcd(9, 15) =$$

$$\boxed{?}$$

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we just count down from $|a|$ and stop when we reach the first common divisor. For example,

$$\gcd(9, 15) =$$

$$\boxed{?}$$

and

$$\gcd(-30, 42) =$$

$$\boxed{?}$$

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we just count down from $|a|$ and stop when we reach the first common divisor. For example,

$$\gcd(9, 15) =$$

$$\boxed{?}$$

and

$$\gcd(-30, 42) =$$

$$\boxed{?}$$

This approach to finding greatest common divisors is pretty terrible:

Finding GCDs

As happens quite often, the remark above, which looks like a slightly pedantic point at first, really says something practically important. Indeed, it gives us a way of finding the greatest common divisor of two numbers: to find $\gcd(a, b)$ we just count down from $|a|$ and stop when we reach the first common divisor. For example,

$$\gcd(9, 15) =$$

$$\boxed{?}$$

and

$$\gcd(-30, 42) =$$

$$\boxed{?}$$

This approach to finding greatest common divisors is pretty terrible: imagine being asked to find

$$\gcd(123456789, 987654321)$$

by this approach!

Other ways

Other ways

Another way might be to work out all factors of one of the numbers (a, for example) and work out which of them are factors of b.

Other ways

Another way might be to work out all factors of one of the numbers (a, for example) and work out which of them are factors of b. That's also a pretty terrible way, because factorising numbers is hard work: it seems like a lot of work to find all factors of 123456789 still.

Other ways

Another way might be to work out all factors of one of the numbers (a, for example) and work out which of them are factors of b. That's also a pretty terrible way, because factorising numbers is hard work: it seems like a lot of work to find all factors of 123456789 still.
We will see a much better way soon, but, first, let's spot some easy properties of greatest common divisors.

Properties of the gcd

Properties of the gcd

Remark

For all integers a and b, we have

$$\gcd(a, b) = \gcd(b, a),$$

because the definition is symmetric in a and b.

Properties of the gcd

Remark

For all integers a and b, we have

$$\gcd(a, b) = \gcd(b, a),$$

because the definition is symmetric in a and b.
Also, for all positive integers a, we have

$$\gcd(a, a) = a,$$

Properties of the gcd

Remark

For all integers a and b, we have

$$\gcd(a, b) = \gcd(b, a),$$

because the definition is symmetric in a and b.
Also, for all positive integers a, we have

$$\gcd(a, a) = a,$$

and

$$\gcd(a, 1) = 1,$$

Properties of the gcd

Remark

For all integers a and b, we have

$$\gcd(a, b) = \gcd(b, a),$$

because the definition is symmetric in a and b.
Also, for all positive integers a, we have

$$\gcd(a, a) = a,$$

and

$$\gcd(a, 1) = 1,$$

and

$$\gcd(a, b) = \gcd(a, -b).$$

More properties of the gcd

More properties of the gcd

A slightly less obvious property is:

Proposition

Let a, b and k be integers. Then

$$\gcd(a, b) = \gcd(a + kb, b).$$

The Proof

The Proof

Proof.

?

□

Least common multiples

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\text{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\text{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\text{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists (and is at most ab).

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\text{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists (and is at most ab).

The last piece of terminology we might want is this:

Least common multiples

We should also mention that the greatest common divisor has a close cousin:

Definition

Given two positive integers a and b, the *least common multiple* $\text{lcm}(a, b)$ is the smallest positive integer which is a multiple both of a and b.

Remark

Given that ab is a common multiple of a and b, the least common multiple always exists (and is at most ab).

The last piece of terminology we might want is this:

Definition

Two integers a and b are said to be *coprime*, or *relatively prime*, if $\gcd(a, b) = 1$.

Division with remainder

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?
It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors.

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?
It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors. We can use it to make the numbers smaller.

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?
It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors. We can use it to make the numbers smaller.
The question is, given a and b, how small can a number of the form $a + kb$ (for k an integer) be?

Division with remainder

The above Proposition about adding on things inside the gcd looks slightly dry at first: so what if you can add multiples of one number to another number without changing their greatest common divisor?
It turns out this is the key step in a surprisingly efficient method for calculating greatest common divisors. We can use it to make the numbers smaller.
The question is, given a and b, how small can a number of the form $a + kb$ (for k an integer) be? It turns out that this is something familiar to you all:

Division with Remainder

Division with Remainder

Proposition (Division with Remainder)

Let a and b be integers, with $b > 0$. One can write

$$a = qb + r$$

for integers q (the quotient) and r (the remainder) such that $0 \leqslant r < b$. □

Division with Remainder

Proposition (Division with Remainder)

Let a and b be integers, with $b > 0$. One can write

$$a = qb + r$$

for integers q (the quotient) and r (the remainder) such that $0 \leqslant r < b$. □

Remark

It is not too hard to prove this: one can do it with two inductions, for example, (one for the negative and one for the positive integers), but I won't do so here.

Division with Remainder

Proposition (Division with Remainder)

Let a and b be integers, with $b > 0$. One can write

$$a = qb + r$$

for integers q (the quotient) and r (the remainder) such that $0 \leqslant r < b$. □

Remark

It is not too hard to prove this: one can do it with two inductions, for example, (one for the negative and one for the positive integers), but I won't do so here.

Remark

It's reasonable to ask why we had to take $b > 0$. It's true for $b < 0$, too, we just have to say that the remainder r satisfies $0 \leqslant r < -b$ instead.

Computing GCDs

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example.

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

?

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

$$\boxed{?}$$

That made the problem much smaller, and we can do the same trick repeatedly:

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

?

That made the problem much smaller, and we can do the same trick repeatedly:

?

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

$$\boxed{?}$$

That made the problem much smaller, and we can do the same trick repeatedly:

$$\boxed{?}$$

That's smaller still. Let's see what happens next:

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

?

That made the problem much smaller, and we can do the same trick repeatedly:

?

That's smaller still. Let's see what happens next:

?

Computing GCDs

This observation gives us a *really efficient* way of computing greatest common divisors. Let's illustrate it by an example. Suppose we're trying to compute $\gcd(126, 70)$. If we divide 126 by 70 we get 1 with remainder 56; in other words $126 = 70 \times 1 + 56$. That means that

?

That made the problem much smaller, and we can do the same trick repeatedly:

?

That's smaller still. Let's see what happens next:

?

As 56 is a multiple of 14, of course we get remainder 0, so we can stop here and get the greatest common divisor to be 14.

Euclid's algorithm

Euclid's algorithm

Here's the general case:

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier. By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b)$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b)$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b)$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b) = \gcd(b, r),$$

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b) = \gcd(b, r),$$

and since $b < a$ and $r < b$ we've made both numbers smaller.

Euclid's algorithm

Here's the general case:

Algorithm (Euclid's algorithm)

Suppose we must calculate the greatest common divisor of two positive integers. Call them a and b with $a > b$. If they're not in the right order, we can swap them over as we proved earlier.
By division with remainder, we can write $a = qb + r$ for some integers q and r with $0 \leqslant r < b$.
But then we have

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b) = \gcd(b, r),$$

and since $b < a$ and $r < b$ we've made both numbers smaller.
If we keep doing this repeatedly, we'll end up making one of the numbers zero and can stop.

Another example

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\gcd(556, 296)$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} & \gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} & \gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) &= \gcd(260, 296) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\gcd(556, 296)$$
$$= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260)$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} &\gcd(556, 296) \\ &= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ &= \gcd(1 \times 260 + 36, 260) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{gathered}\gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ = \gcd(1 \times 260 + 36, 260) = \gcd(36, 260)\end{gathered}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{gathered}\gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ = \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36)\end{gathered}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} &\gcd(556, 296) \\ &= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ &= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\ &= \gcd(7 \times 36 + 8, 36) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned} &\gcd(556, 296) \\ &= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ &= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\ &= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) \end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{gathered}\gcd(556, 296) \\ = \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\ = \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\ = \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8)\end{gathered}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4) \\
&= \gcd(2 \times 4 + 0, 4)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4) \\
&= \gcd(2 \times 4 + 0, 4) = \gcd(0, 4)
\end{aligned}$$

Another example

For another example, let's suppose we want the greatest common divisor of 556 and 296. We write

$$\begin{aligned}
&\gcd(556, 296) \\
&= \gcd(1 \times 296 + 260, 296) = \gcd(260, 296) = \gcd(296, 260) \\
&= \gcd(1 \times 260 + 36, 260) = \gcd(36, 260) = \gcd(260, 36) \\
&= \gcd(7 \times 36 + 8, 36) = \gcd(8, 36) = \gcd(36, 8) \\
&= \gcd(4 \times 8 + 4, 8) = \gcd(4, 8) = \gcd(8, 4) \\
&= \gcd(2 \times 4 + 0, 4) = \gcd(0, 4) = 4.
\end{aligned}$$

Is this good?

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is.

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. Proving it is (slightly) beyond the scope of this course, but one good answer is that if you're trying to work out $\gcd(a, b)$ and $b < a$, then the number of steps you need is always less than five times the number of digits of b.

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. Proving it is (slightly) beyond the scope of this course, but one good answer is that if you're trying to work out $\gcd(a, b)$ and $b < a$, then the number of steps you need is always less than five times the number of digits of b.

So working out $\gcd(123456789, 987654321)$ will take less than $5 \times 9 = 45$ steps

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. Proving it is (slightly) beyond the scope of this course, but one good answer is that if you're trying to work out $\gcd(a, b)$ and $b < a$, then the number of steps you need is always less than five times the number of digits of b.

So working out $\gcd(123456789, 987654321)$ will take less than $5 \times 9 = 45$ steps (actually, this one takes a lot less than 45 steps, if you try it).

Is this good?

Remark

One might reasonably wonder just *how fast* Euclid's algorithm really is. Proving it is (slightly) beyond the scope of this course, but one good answer is that if you're trying to work out $\gcd(a, b)$ and $b < a$, then the number of steps you need is always less than five times the number of digits of b.

So working out $\gcd(123456789, 987654321)$ will take less than $5 \times 9 = 45$ steps (actually, this one takes a lot less than 45 steps, if you try it). Compared with the other methods we discussed, this makes it seem really good.