Number Theory:
Primes and Greatest Common Divisors

CS261 Mathematical Foundations of CS
Professor Leah Buechley
Spring 2024
University of New Mexico

Primes and Greatest Common Divisors

Section 4.3

Section Summary[3]

Prime Numbers and their Properties.

Greatest Common Divisors and Least Common Multiples.

The Euclidian Algorithm.

Primes

Definition: A positive integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*. A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2.$
- $641 = 641.$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37.$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \; 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$

The Sieve of Eratosthenes [1]

Erastothenes

(276-194 B.C.)

The *Sieve of Eratosthenes* can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Next, delete all the integers, other than 5, divisible by 5.
d. Next, delete all the integers, other than 7, divisible by 7.
e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

$\{2,3,5,7,11,15,1719,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,$
$97\}$

The Sieve of Eratosthenes 2

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

1	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

Integers divisible by 3 other than 3 receive an underline.

1	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

Integers divisible by 5 other than 5 receive an underline.

1	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

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	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

If an integer n is a composite integer, then it has a prime divisor less than or equal to $\sqrt{n}$.

To see this, note that if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i.

Access the text alternative for slide images.

Infinitude of Primes

Euclid

(325 B.C.E. – 265 B.C.E.)

Theorem: There are infinitely many primes. (Euclid)

Proof: Assume finitely many primes: $p_1, p_2, \ldots, p_n$

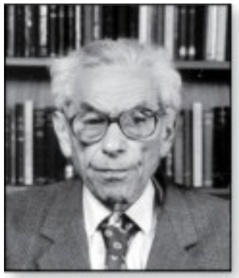
Let $q = p_1 p_2 \cdots p_n + 1$

Either q is prime or by the fundamental theorem of arithmetic it is a product of primes.

- But none of the primes p_j divides q since if $p_j \mid q$, then p_j divides $q - p_1 p_2 \cdots p_n = 1$.
- Hence, there is a prime not on the list $p_1, p_2, \ldots, p_n$. It is either q, or if q is composite, it is a prime factor of q. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ are all the primes.

Consequently, there are infinitely many primes.

This proof was given by Euclid *The Elements*. The proof is considered to be one of the most beautiful in all mathematics. It is the first proof in *The Book,* inspired by the famous mathematician Paul Erdős' imagined collection of perfect proofs maintained by God.



Paul Erdős

(1913-1996)

Greatest Common Divisor [1]

Definition: Let *a* and *b* be integers, not both zero. The largest integer *d* such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of *a* and *b*. The greatest common divisor of *a* and *b* is denoted by gcd(*a*,*b*).

One can find greatest common divisors of small numbers by inspection.

Example: What is the greatest common divisor of 24 and 36?

Solution: gcd(24, 36) = 12

Example: What is the greatest common divisor of 17 and 22?

Solution: gcd(17,22) = 1

Greatest Common Divisor 2

Definition: The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1.

Example: 17 and 22.

Definition: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd\left(a_i, a_j\right) = 1$ whenever $1 \leq i < j \leq n$.

Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: Because gcd(10,17) = 1, gcd(10,21) = 1, and gcd(17,21) = 1, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because gcd(10,24) = 2, 10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

Suppose the prime factorizations of *a* and *b* are:

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,bn)},$$

This formula is valid since the integer on the right (of the equals sign) divides both *a* and *b*. No larger integer can divide both *a* and *b*.

Example: $120 = 2^3 \cdot 3 \cdot 5 \qquad 500 = 2^2 \cdot 5^3$

$$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

Definition: The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. It is denoted by lcm(*a*,*b*).

The least common multiple can also be computed from the prime factorizations.

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,bn)},$$

This number is divided by both *a* and *b* and no smaller number is divided by *a* and *b*.

Example: $\operatorname{lcm}\left(2^3 3^5 7^2, 2^4 3^3\right) = 2^{\max(3,4)}\ 3^{\max(5,3)}\ 7^{\max(2,0)} = 2^4\ 3^5\ 7^2$

The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

ab = gcd(*a*,*b*) ·lcm(*a*,*b*)

(*proof is Exercise* 31)

Euclidean Algorithm 1

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(*a*,*b*) is equal to gcd(*a*,*c*) when $a > b$ and *c* is the remainder when a is divided by *b*.

Euclid
(325 B.C.E. – 265 B.C.E.)

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$ — Divide 287 by 91
- $91 = 14 \cdot 6 + 7$ — Divide 91 by 14
- $14 = 7 \cdot 2 + 0$ — Divide 14 by 7

Stopping condition

gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7

Euclidean Algorithm 2

The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while   y ≠ 0
      r := x mod y
      x := y
      y := r
return x {gcd(a,b) is x}
```

In Section 5.3, we'll see that the time complexity of the algorithm is $O(\log b)$, where $a > b$.

Correctness of Euclidean Algorithm [1]

Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a,b) = \gcd(b,r)$.

Proof:

- Suppose that d divides both a and b. Then d also divides $a - bq = r$ (by Theorem 1 of Section 4.1). Hence, any common divisor of a and b must also be any common divisor of b and r.
- Suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of a and b must also be a common divisor of b and r.
- Therefore, $\gcd(a,b) = \gcd(b,r)$.

Correctness of Euclidean Algorithm 2

Suppose that a and b are positive integers with $a \geq b$.

Let $r_0 = a$ and $r_1 = b$.

Successive applications of the division algorithm yields:

$$
\begin{array}{ll}
r_0 = r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 = r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\
\cdot & \\
\cdot & \\
\cdot & \\
r_{n-2} = r_{n-1} q_{n-1} + r_2 & 0 \leq r_n < r_{n-1}, \\
r_{n-1} = r_n q_n. &
\end{array}
$$

Eventually, a remainder of zero occurs in the sequence of terms: $a = r_0 > r_1 > r_2 > \cdots \geq 0$. The sequence can't contain more than a terms.

By Lemma 1

$$\gcd(a,b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.