

Number Theory and Cryptography

Chapter 4

With Question/Answer Animations

Chapter Summary

4.1 Divisibility and Modular Arithmetic

4.2 Integer Representations and Algorithms

4.3 Primes and Greatest Common Divisors

4.4 Solving Congruences

4.5 Applications of Congruences

4.6 Cryptography

Primes and Greatest Common Divisors

Section 4.3

Section Summary

- Prime Numbers and their Properties
- Conjectures and Open Problems About Primes
- Greatest Common Divisors (gcd)
- Least Common Multiples (lcm)
- The Euclidian Algorithm
- gcd as Linear Combination

Primes

Definition: $p \in \mathbb{Z}, > 1$ is *prime* if the only positive factors of p are 1 and p .

(If $n \in \mathbb{Z}, > 1$ is not prime, then it is *composite*.)

Examples:

7 is prime

9 is composite

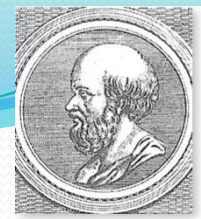
What about 37, 43, 51, 59, 67, 143, 561?

The Fundamental Thm of Arithmetic

Theorem: $\forall n \in \mathbb{Z}, > 1 \exists!$ product expression of primes whose factors are nondecreasing.

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$
- What about 37, 43, 51, 59, 67, 143, 561?



The Sieve of Erastosthenes

- The *Sieve of Erastosthenes* can be used to find all primes not exceeding a specified $n \in \mathbb{Z}^+$. For example, $n = 100$.
 - a. Delete all multiples of 2 (except 2), then multiples of 3, then multiples of 5, and finally 7,
 - b. the primes up to $n = 100$ are
{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,
47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}

Note that we can stop at 7 because it is the largest prime smaller than

$$\sqrt{100} = 10$$

The process is best illustrated using an animation. Pictures after deleting multiples of 2, 3, 5 and 7 appear on the next 4 pages.

*Integers divisible by 2 other than 2
receive an underline.*

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	9	<u>10</u>
11	<u>12</u>	13	<u>14</u>	15	<u>16</u>	17	<u>18</u>	19	<u>20</u>
21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	27	<u>28</u>	29	<u>30</u>
31	<u>32</u>	33	<u>34</u>	35	<u>36</u>	37	<u>38</u>	39	<u>40</u>
41	<u>42</u>	43	<u>44</u>	45	<u>46</u>	47	<u>48</u>	49	<u>50</u>
51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	57	<u>58</u>	59	<u>60</u>
61	<u>62</u>	63	<u>64</u>	65	<u>66</u>	67	<u>68</u>	69	<u>70</u>
71	<u>72</u>	73	<u>74</u>	75	<u>76</u>	77	<u>78</u>	79	<u>80</u>
81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	87	<u>88</u>	89	<u>90</u>
91	<u>92</u>	93	<u>94</u>	95	<u>96</u>	97	<u>98</u>	99	<u>100</u>

*Integers divisible by 3 other than 3
receive an underline.*

1	2	3	<u>4</u>	5	<u><u>6</u></u>	7	8	<u>9</u>	<u>10</u>
11	<u><u>12</u></u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u><u>18</u></u>	19	<u>20</u>
<u>21</u>	<u><u>22</u></u>	23	<u><u>24</u></u>	25	<u>26</u>	<u>27</u>	<u>28</u>	29	<u><u>30</u></u>
31	<u>32</u>	<u>33</u>	<u>34</u>	35	<u><u>36</u></u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u><u>42</u></u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u><u>48</u></u>	49	<u>50</u>
<u>51</u>	<u>52</u>	53	<u><u>54</u></u>	55	<u>56</u>	<u>57</u>	<u>58</u>	59	<u><u>60</u></u>
61	<u>62</u>	<u>63</u>	<u>64</u>	65	<u><u>66</u></u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u><u>72</u></u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u><u>78</u></u>	79	<u>80</u>
<u>81</u>	<u>82</u>	83	<u><u>84</u></u>	85	<u>86</u>	<u>87</u>	<u>88</u>	89	<u><u>90</u></u>
91	<u>92</u>	<u>93</u>	<u>94</u>	95	<u><u>96</u></u>	97	<u>98</u>	<u>99</u>	<u>100</u>

*Integers divisible by 5 other than 5
receive an underline.*

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<u>21</u>	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>
<u>51</u>	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>
<u>81</u>	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
91	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>

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

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<u>21</u>	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	<u>49</u>	<u>50</u>
<u>51</u>	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	<u>77</u>	<u>78</u>	79	<u>80</u>
<u>81</u>	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
<u>91</u>	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>

Why we can stop at \sqrt{n}

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 .

Infinitude of Primes



Euclid

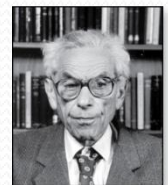
(325 B.C.E. – 265 B.C.E.)

Theorem: \exists infinitely many primes. (Euclid)

Proof: Assume finitely many primes: p_1, p_2, \dots, p_n

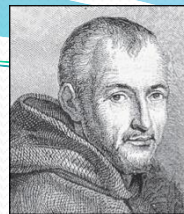
- Let $q = p_1 p_2 \cdots p_n + 1$
- By the fundamental theorem of arithmetic either q is prime or it is a product of primes.
 - But none of the primes p_j divides q since if $p_j \mid q$, then p_j divides $q - p_1 p_2 \cdots p_n = 1$.
 - Hence, \exists prime not on the list p_1, p_2, \dots, p_n , contradicting the assumption that p_1, p_2, \dots, p_n are all the primes.

This proof was given by Euclid in *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)

Mersene Primes



Marin Mersenne
(1588-1648)

Definition: Prime numbers of the form $2^p - 1$, where p is prime, are called *Mersene primes*.

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, and $2^7 - 1 = 127$ are Mersene primes.
- $2^{11} - 1 = 2047$ is not a Mersene prime since $2047 = 23 \cdot 89$.
- There is an efficient test for determining if $2^p - 1$ is prime.
- The largest known prime numbers are Mersene primes.
- As of mid 2011, 47 Mersene primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.
- The *Great Internet Mersene Prime Search (GIMPS)* is a distributed computing project to search for new Mersene Primes.

<http://www.mersenne.org/>

While no new Mersene Primes have been found, important results were added just a few weeks ago (April 8, 2018).

Distribution of Primes

- Mathematicians have been interested in the distribution of prime numbers for several centuries.
- Let $f(n) = \#\text{primes} \leq n$.
- In the 19th century, an asymptotic estimate for f was found:

Prime Number Theorem: $f(n)$ is $\Theta(n/\ln n)$

In other words, chance that randomly selected $x \in \{1, \dots, n\}$ is prime is approximately $(n/\ln n)/n = 1/\ln n$.



Primes & Arithmetic Progressions

Euclid's proof that $\exists \infty$ many primes can be easily adapted to show that $\exists \infty$ many primes in $4k + 3$, $k = 1, 2, \dots$. See Exercise 55

- In 19th century Dirichlet showed every arithmetic progression $ka + b$, $k = 1, 2, \dots$, $\gcd(a, b) = 1$ contains ∞ many primes.
- Do \exists arithmetic progressions made up entirely of primes?
 - 5, 11, 17, 23, 29 is an arithmetic progression of five primes.
 - 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 is an arithmetic progression of ten primes.
- In the 1930s, Erdős conjectured and in 2006, Green and Tao proved that $\forall n \in \mathbb{Z}, > 1, \exists$ arithmetic progression of length n made up entirely of primes.

Generating Primes

- Large prime generation is of theoretical & practical interest
 - Primes with 100's of digits are important in cryptography (Sect 4.6)
- So far, \nexists simple function $f(n)$ such that $f(n)$ is prime $\forall n \in \mathbb{Z}^+$.
 - e.g., $f(n) = n^2 - n + 41$ is prime for $n = 1, 2, \dots, 40$. But not for 41.
- More specifically, \nexists polynomial with integer coefficients such that $f(n)$ is prime $\forall n \in \mathbb{Z}^+$. (See supplementary Exercise 23.)
- Fortunately, we can generate large integers which are almost certainly primes. See Chapter 7.

Conjectures about Primes

Even though primes have been studied extensively for centuries, many conjectures about them are unresolved, including:

- *Goldbach's Conjecture*: Every $n \in \mathbb{Z}, > 2$, even, is the sum of two primes. It has been verified by computer for $n \leq 1.6 \cdot 10^{18}$.
- $\exists \infty$ many primes of the form $n^2 + 1, n \in \mathbb{Z}^+$. But it has been shown that $\exists \infty$ many primes or the product of at most two primes of that form.
- *The Twin Prime Conjecture*: $\exists \infty$ many pairs of twin primes. Twin primes are pairs of primes that differ by 2. Examples are 3 and 5, 5 and 7, 11 and 13, etc.
- Discovered in September 2016, the current world's record for twin primes are $2996863034895 \cdot 2^{1290000} \pm 1$, [\[17\]](#) with 388,342 decimal digits.

Greatest Common Divisor

Definition: $a, b \in \mathbb{Z}$, not both zero. The *greatest common divisor* of a and b

$$\gcd(a, b) = \max(d \in \mathbb{Z}, d \mid a, d \mid b)$$

One can find the gcd of small numbers by inspection.

Example: What is the gcd of 24 and 36?

Solution: $\gcd(24, 36) = 12$

Example: What is the gcd of 17 and 22?

Solution: $\gcd(17, 22) = 1$

Greatest Common Divisor

Definition: a and b are *relatively prime* if $\gcd(a, b) = 1$.

Example: 17 and 22

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

Example: Determine if 10, 17 & 21 are prp.

Solution: $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, $\gcd(17, 21) = 1$, so 10, 17, and 21 are prp.

Example: Determine whether 10, 19, and 24 are prp.

Solution: $\gcd(10, 24) = 2$, so 10, 19, and 24 are not prp.

Finding gcd using Prime Factorizations

Suppose the prime factorizations of a and b are:

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

Then:

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

- Formula is valid since integer on right (of = sign) divides both a and b . No larger integer can divide both a and b .

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

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

- Finding gcd this way is not efficient because \nexists efficient algorithm for finding prime factorization

Least Common Multiple

Definition: $a, b \in \mathbb{Z}$, not both zero. The *least common multiple* of a & b
 $\text{lcm}(a, b) = \min\{d \in \mathbb{Z}, a \mid d, b \mid d\}$

- The lcm can also be computed from the prime factorizations.

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

Example:

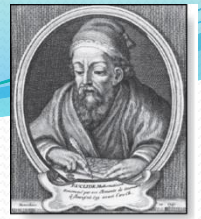
$$\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$$

- The gcd and the lcm are related by:

Theorem 5: Let $a, b \in \mathbb{Z}^+$. Then

$$ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$$

(*proof is Exercise 31*)



Euclidean Algorithm

- The Euclidian algorithm is an efficient method for computing the gcd.
- It is based on the idea that $\text{gcd}(a, b) = \text{gcd}(b, c)$ when $a > b$ and c is the remainder when a is divided by b .



Euclidean Algorithm

- The Euclidian algorithm is an efficient method for computing the gcd.
- It is based on the idea that $\text{gcd}(a, b) = \text{gcd}(b, c)$ when $a > b$ and c is the remainder when a is divided by b .

Example: Find $\text{gcd}(91, 287)$:

- $287 = 91 \cdot 3 + 14$

Divide 287 by 91

- $91 = 14 \cdot 6 + 7$

Divide 91 by 14

- $14 = 7 \cdot 2 + 0$

Divide 14 by 7

Stopping
condition

So $\text{gcd}(287, 91) = \text{gcd}(91, 14) = \text{gcd}(14, 7) = 7$

Euclidean Algorithm

- 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, it is shown that the complexity is $O(\log b)$, where $a > b$.

Correctness of Euclidean Algorithm

Lemma 1: Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. 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

- Suppose that $a, b \in \mathbb{Z}^+, a \geq b$.
 Let $r_0 = a$ and $r_1 = b$.
 Successive applications of the division algorithm yields:

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

- Eventually, a remainder of zero occurs in the sequence of terms:

$$a = r_0 > r_1 > r_2 > \dots \geq 0.$$

- The sequence can't contain more than a terms.

- By Lemma 1

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

- \therefore gcd is the last nonzero remainder in the sequence of divisions.





gcd as Linear Combination

Bézout's Theorem: If $a, b \in \mathbb{Z}^+$, then $\exists s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$,

i.e., the gcd of a and b can be written as a *linear combination* of a and b with *integer coefficients*.

(proof in exercises of Section 5.2)

- $s, t \in \mathbb{Z}$ are *Bézout coefficients*.

Example: $\gcd(6, 14) = 2 = (-2) \cdot 6 + 1 \cdot 14$

Finding gcds as Linear Combinations

- We illustrate the two pass method for finding the Bézout coefficients.
 - It first uses the Euclidian algorithm to find the gcd;
 - then works backwards to express the gcd as a linear combination of the original two integers.
- A one pass method, the *extended Euclidean algorithm*, is developed in the exercises.

Finding gcds as Linear Combinations

Example: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution: Use the Euclidean algorithm:

i. $252 = 1 \cdot 198 + 54$

ii. $198 = 3 \cdot 54 + 36$

iii. $54 = 1 \cdot 36 + 18$

iv. $36 = 2 \cdot 18$

- Solve for the remainders in i to iii

i. $54 = 252 - 1 \cdot 198$

ii. $36 = 198 - 3 \cdot 54$

iii. $18 = 54 - 1 \cdot 36$

- Substituting the 2nd equation into the 3rd yields:
 - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting the 1st equation into this new equation yields:
 - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

Consequences of Bézout's Theorem

Lemma 2: If a , b , and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof: Assume $\gcd(a, b) = 1$ and $a \mid bc$

- Since $\gcd(a, b) = 1$, by Bézout's Theorem there are integers s and t such that

$$sa + tb = 1.$$

- Multiplying both sides of the equation by c , yields $sac + tbc = c$.
- From Theorem 1 of Section 4.1:
 $a \mid tbc$ (part ii) and a divides $sac + tbc$ since $a \mid sac$ and $a \mid tbc$ (part i)
- We conclude $a \mid c$, since $sac + tbc = c$. ◀

Lemma 3: If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i .
(*proof uses mathematical induction; see Exercise 64 of Section 5.1*)

- Lemma 3 is crucial in proof of the uniqueness of prime factorizations.

Uniqueness of Prime Factorization

Given $n \in \mathbb{Z}^+$, then the prime factorization of n , where the primes are in nondecreasing order, is unique.


Proof: (by contradiction) Suppose that the positive integer n can be written as a product of primes in two distinct ways:

$$n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots q_t$$

- Remove all common primes from the factorizations to get

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

- By Lemma 3, it follows that p_{i_1} divides q_{j_k} , for some k , contradicting assumption that p_{i_1} and q_{j_k} are distinct primes.

$\therefore \exists$ at most one factorization of n into primes in nondecreasing order. 

Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Sec 4.1).
- But dividing by an integer **relatively prime** to the modulus does produce a valid congruence:

Theorem 7: Let $m \in \mathbb{Z}^+$ and let $a, b, c \in \mathbb{Z}$. If

$$ac \equiv bc \pmod{m} \text{ and } \gcd(c, m) = 1,$$

then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c, m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$. ◀

Example: $24 \equiv 6 \pmod{9}$, $\gcd(2, 9) = 1$, so $12 \equiv 3 \pmod{9}$