Introduction to Number Theory (cont.)

Assylbek Issakhov,
Ph.D., professor

Primes

- Every integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself. Positive integers that have exactly two different positive integer factors are called **primes**.
- **DEFINITION 1.** An 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*.

Primes

- ***Remark:*** The integer n is *composite* if and only if there exists an integer a such that $a|n$ and $1 < a < n$.
- **THEOREM 1. (THE FUNDAMENTAL THEOREM OF ARITHMETIC)** Every 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 non-decreasing size.

Primes

- **EXAMPLE.** The prime factorizations of 100, 641, 999, and 1024 are given by

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$

$$641 = 641,$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$$

$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$$

Trial Division

- **THEOREM 2.** If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
- **EXAMPLE.** Show that 101 is prime.
- *Solution:* The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

Trial Division

- **EXAMPLE.** Find the prime factorization of 7007.
- *Solution:* To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes $2, 3$, and 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$. Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because $1001/7 = 143$.

Trial Division

- **EXAMPLE (cont.).** Find the prime factorization of 7007.
- Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Because 13 is prime, the procedure is completed. It follows that $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Consequently, the prime factorization of 7007 is $7^2 \cdot 11 \cdot 13$.

The Sieve of Eratosthenes

- The **sieve of Eratosthenes** is used to find all primes not exceeding a specified positive integer. For instance, the following procedure is used to find the primes not exceeding 100:

The Sieve of Eratosthenes

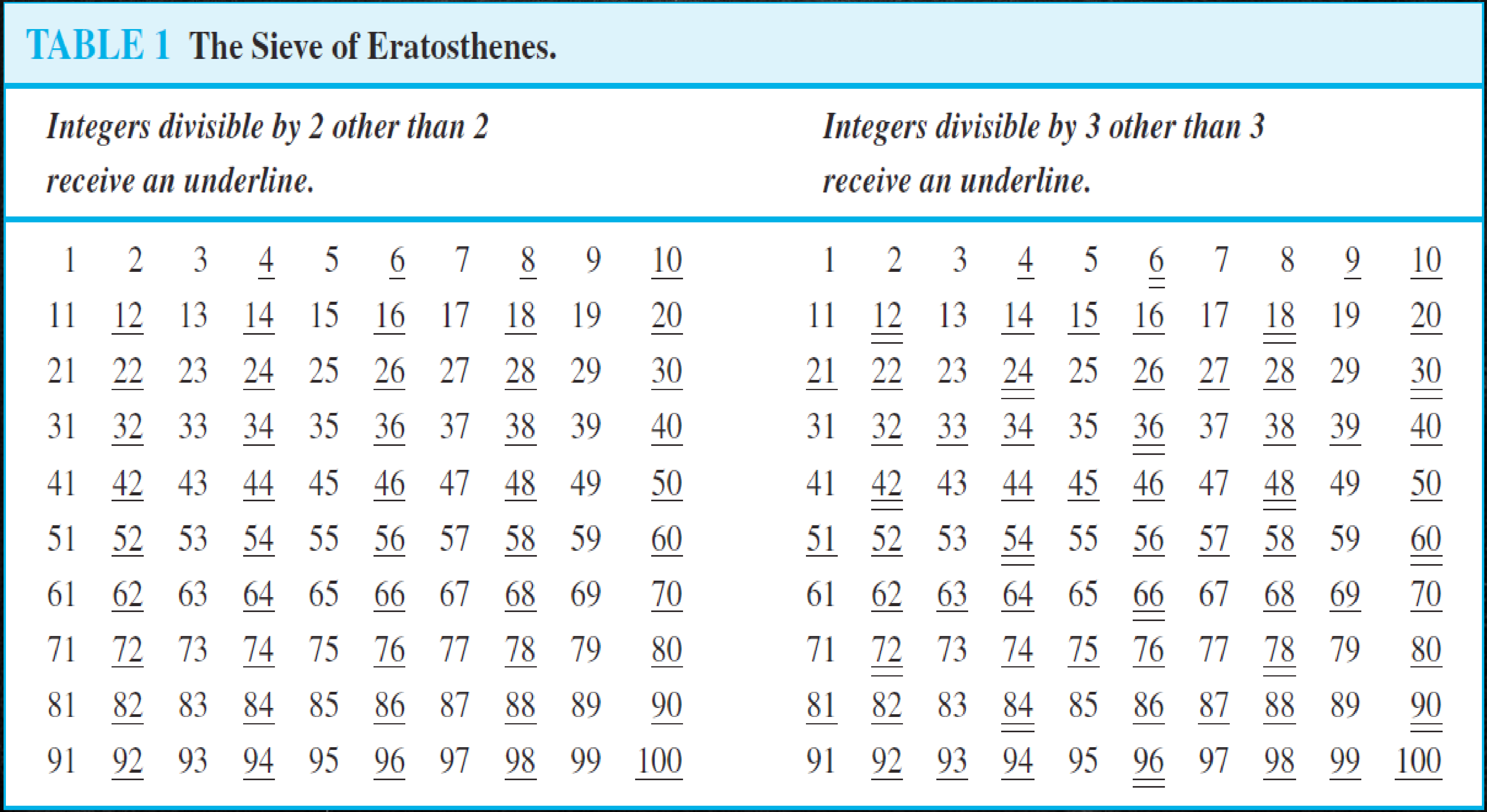


TABLE 1 **The Sieve of Eratosthenes.**

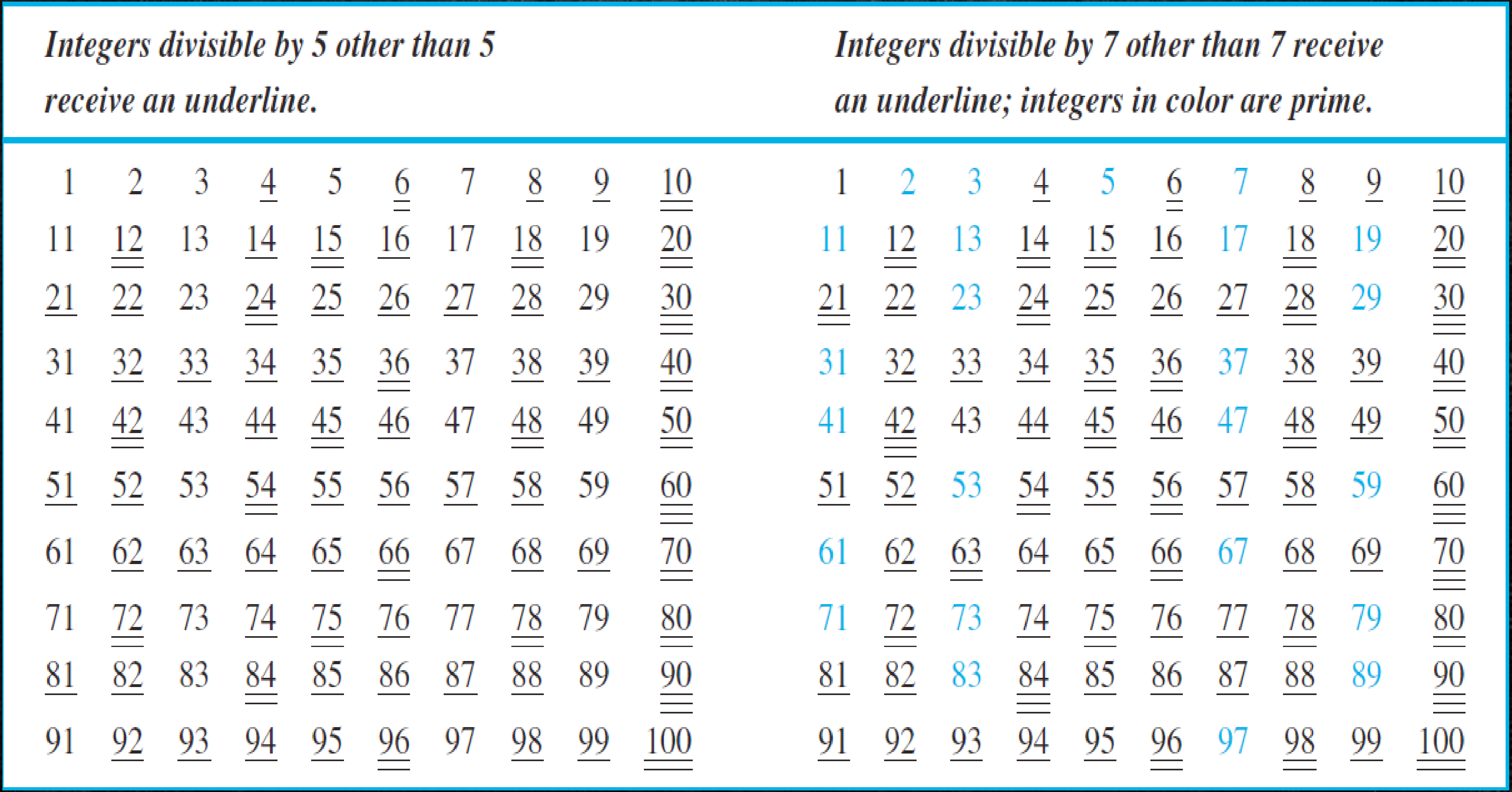
Integers divisible by 2 other than 2 receive an underline.

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

Integers divisible by 3 other than 3 receive an underline.

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

The Sieve of Eratosthenes



Integers divisible by 5 other than 5 receive an underline.

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

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

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

The Sieve of Eratosthenes

- The integers not underlined are the primes not exceeding 100. We conclude that the primes less than 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, and 97.

The Sieve of Eratosthenes

- **THEOREM 3.** There are infinitely many primes.

The Sieve of Eratosthenes

- Because there are infinitely many primes, given any positive integer there are primes greater than this integer. There is an ongoing quest to discover larger and larger prime numbers; for almost all the last 300 years, the largest prime known has been an integer of the special form $2^p - 1$, where p is also prime. (Note that $2^n - 1$ cannot be prime when n is not prime.) Such primes are called **Mersenne primes**, after the French monk Marin Mersenne, who studied them in the seventeenth century.

The Sieve of Eratosthenes

- **EXAMPLE.** The numbers

$$2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, \text{and}$$

$$2^7 - 1 = 127$$

- are Mersenne primes, while

$$2^{11} - 1 = 2047$$

- is not a Mersenne prime because $2047 = 23 \cdot 89$.

The Sieve of Eratosthenes

- Progress in finding Mersenne primes has been steady since computers were invented. As of early 2011, 47 Mersenne primes were known, with 16 found since 1990. The largest Mersenne prime known is $2^{43\,112\,609} - 1$, a number with nearly 13 million decimal digits, which was shown to be prime in 2008. A communal effort, the Great Internet Mersenne Prime Search (GIMPS), is devoted to the search for new Mersenne primes.

THE DISTRIBUTION OF PRIMES

- Theorem 3 tells us that there are infinitely many primes. However, how many primes are less than a positive number x? This question interested mathematicians for many years.
- **THEOREM 4. (THE PRIME NUMBER THEOREM)** The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)

Conjectures and Open Problems About Primes

- **EXAMPLE.** It would be useful to have a function $f(n)$ such that $f(n)$ is prime for all positive integers n. If we had such a function, we could find large primes for use in cryptography and other applications. Looking for such a function, we might check out different polynomial functions, as some mathematicians did several hundred years ago. After a lot of computation we may encounter the polynomial $f(n) = n^2 - n + 41$. This polynomial has the interesting property that $f(n)$ is prime for all positive integers n not exceeding 40.

Conjectures and Open Problems About Primes

- We have $f(1) = 41, f(2) = 43, f(3) = 47, f(4) = 53$, and so on. This can lead us to the conjecture that $f(n)$ is prime for all positive integers n. Can we settle this conjecture?
- *Solution:* Perhaps not surprisingly, this conjecture turns out to be false; we do not have to look far to find a positive integer n for which $f(n)$ is composite, because $f(41) = 41^2 - 41 + 41 = 41^2$.

Conjectures and Open Problems About Primes

- Because $f(n) = n^2 - n + 41$ is prime for all positive integers n with $1 \leq n \leq 40$. We might be tempted to find a different polynomial with the property that $f(n)$ is prime for all positive integers n.
- However, there is no such polynomial. It can be shown that for every polynomial $f(n)$ with integer coefficients, there is a positive integer y such that $f(y)$ is composite.

Greatest Common Divisors and Least Common Multiples

- The integer that divides both of two integers is called the **common divisor** of these integers.

- **DEFINITION 2.** Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b.

- The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Greatest Common Divisors and Least Common Multiples

- The greatest common divisor of two integers, not both zero, exists because the set of common divisors of these integers is nonempty and finite.
- One way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor.

Greatest Common Divisors and Least Common Multiples

- **EXAMPLE.** What is the greatest common divisor of 24 and 36?
- *Solution:* The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence,

$$\gcd(24, 36) = 12.$$

Greatest Common Divisors and Least Common Multiples

- **EXAMPLE.** What is the greatest common divisor of 17 and 22?
- *Solution:* The integers 17 and 22 have no positive common divisors other than 1, so that

$$\gcd(17, 22) = 1.$$

Greatest Common Divisors and Least Common Multiples

- Because it is often important to specify that two integers have no common positive divisor other than 1, we have Definition 3.
- **DEFINITION 3.** The integers a and b are *relatively prime* if their greatest common divisor is 1.

Greatest Common Divisors and Least Common Multiples

- Because we often need to specify that no two integers in a set of integers have a common positive divisor greater than 1, we make Definition 4.
- **DEFINITION 4.** The integers $a_1, a_2, \dots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Greatest Common Divisors and Least Common Multiples

- Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that

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

- where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary.

Greatest Common Divisors and Least Common Multiples

- Then $\text{gcd}(a, b)$ is given by

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

- where $\min(x, y)$ represents the minimum of the two numbers x and y.

Greatest Common Divisors and Least Common Multiples

- **EXAMPLE.** Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, the greatest common divisor is

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

Greatest Common Divisors and Least Common Multiples

- Prime factorizations can also be used to find the **least common multiple** of two integers.
- **DEFINITION 5.** The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b.
- The least common multiple of a and b is denoted by $lcm(a, b)$.

Greatest Common Divisors and Least Common Multiples

- The least common multiple exists because the set of integers divisible by both a and b is nonempty, and every nonempty set of positive integers has a least element. Suppose that the prime factorizations of a and b are as before. Then the least common multiple of a and b is

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

- where $max(x, y)$ denotes the maximum of the two numbers x and y.

Greatest Common Divisors and Least Common Multiples

- **EXAMPLE.** What is the least common multiple of

  $2^3 3^5 7^2$ and $2^4 3^3$?

- *Solution:* We have

$$lcm(2^3 5^5 7^2, 2^4 3^3) =$$

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

Greatest Common Divisors and Least Common Multiples

- **THEOREM 5.** Let a and b be positive integers. Then

$$ab = gcd(a, b) \cdot lcm(a, b).$$

The Euclidean Algorithm

- The Euclidean algorithm is based on the following result about greatest common divisors and the division algorithm.
- **LEMMA 1.** Let $a = bq + r$, where $a, b, q,$ and r are integers. Then

$$gcd(a, b) = gcd(b, r).$$

The Euclidean Algorithm

- Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

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

The Euclidean Algorithm

- Furthermore, it follows from Lemma 1 that
$$\begin{aligned}\gcd(a, b) &= \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots \\ &= \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) \\ &= \gcd(r_n, 0) = r_n.\end{aligned}$$
- Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

The Euclidean Algorithm

- **EXAMPLE.** Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

- *Solution:* Successive uses of the division algorithm give:
$$\begin{gathered}662 = 414 \cdot 1 + 248,\\ 414 = 248 \cdot 1 + 166,\\ 248 = 166 \cdot 1 + 82,\\ 166 = 82 \cdot 2 + 2,\\ 82 = 2 \cdot 41.\end{gathered}$$

- Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

GCDs as Linear Combinations

- **THEOREM 6. (BÉZOUT'S THEOREM)** If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb.$
- **DEFINITION 6.** If a and b are positive integers, then integers s and t such that

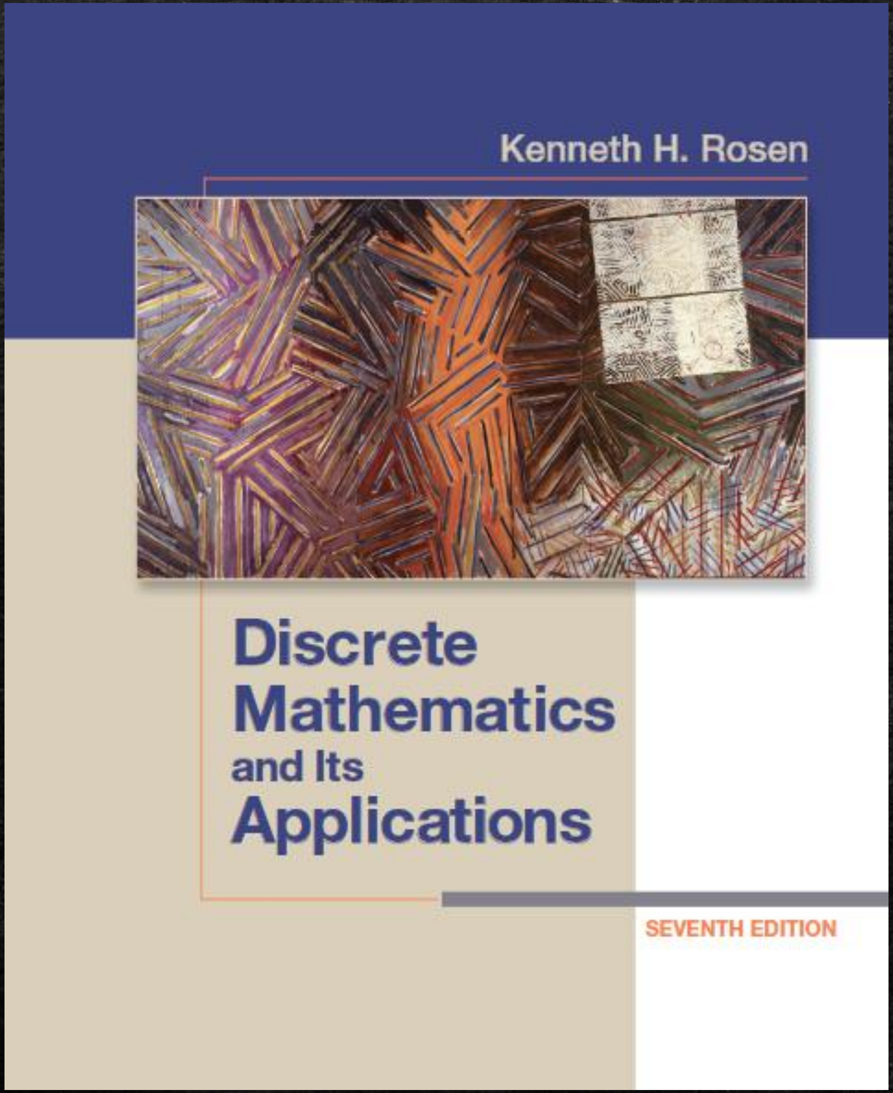
$$gcd(a,b) = sa + tb$$

- are called *Bézout coefficients* of a and b. Also, the equation $gcd(a,b) = sa + tb$ is called *Bézout's identity*.

GCDs as Linear Combinations

- **LEMMA 2.** If a, b, and c are positive integers such that $gcd(a, b) = 1$ and $a|bc$, then $a|c$.
- **LEMMA 3.** If p is a prime and $p|a_1a_2 \ldots a_n$, where each a_i is an integer, then $p|a_i$ for some i.
- **THEOREM 7.** Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc(mod\ m)$ and $gcd(c, m) = 1$, then $a \equiv b(mod\ m)$.

HOMEWORK: Exercises 2, 4, 12, 14, 20, 22, 24, 26, 28, 32, 42 on pp. 272-273;



Linear Congruences

- A congruence of the form

$$ax \equiv b(mod\, m),$$

- where m is a positive integer, a and b are integers, and x is a variable, is called a **linear congruence**.

Linear Congruences

- How can we solve the linear congruence $ax \equiv b(mod\ m)$? One method that we will describe uses an integer a' such that $aa' \equiv 1(mod\ m)$, if such an integer exists.
- Such an integer a' is said to be an **inverse** of a modulo m. Theorem 1 guarantees that an inverse of $a\ modulo\ m$ exists whenever a and m are relatively prime.

Linear Congruences

- **THEOREM 1.** If a and m are relatively prime integers and $m > 1$, then an inverse of $a\ modulo\ m$ exists. Furthermore, this inverse is unique $modulo\ m$.
- That is, there is a unique positive integer a’ less than m that is an inverse of $a\ modulo\ m$ and every other inverse of $a\ modulo\ m$ is congruent to a’ $modulo\ m$.

Linear Congruences

- Using inspection to find an inverse of $a\ modulo\ m$ is easy when m is small. To find this inverse, we look for a multiple of a that exceeds a multiple of m by 1.
- For example, to find an inverse of $3\ modulo\ 7$, we can find $k \cdot 3$ for $k = 1, 2, \ldots, 6$, stopping when we find a multiple of 3 that is one more than a multiple of 7. We can speed this approach up if we note that $2 \cdot 3 \equiv -1 (mod\ 7)$. This means that $(-2) \cdot 3 \equiv 1 (mod\ 7)$. Hence, $5 \cdot 3 \equiv 1 (mod\ 7)$, so 5 is an inverse of $3\ modulo\ 7$.

Linear Congruences

- We can design a more efficient algorithm than brute force to find an inverse of $a\ modulo\ m$ when $gcd(a, m) = 1$ using the steps of the Euclidean algorithm. By reversing these steps, we can find a linear combination $sa + tm = 1$ where s and t are integers. Reducing both sides of this equation modulo m tells us that s is an inverse of $a\ modulo\ m$.

Linear Congruences

- **EXAMPLE.** Find an inverse of $3\ modulo\ 7$ by first finding Bézout coefficients of 3 and 7.
- *Solution:* Because $gcd(3, 7) = 1$, an inverse of $3\ modulo\ 7$ exists. The Euclidean algorithm ends quickly when used to find the greatest common divisor of 3 and 7, $7 = 2 \cdot 3 + 1$. From this equation we see that $-2 \cdot 3 + 1 \cdot 7 = 1$. This shows that -2 and 1 are Bézout coefficients of 3 and 7. We see that -2 is an inverse of $3\ modulo\ 7$.

Linear Congruences

- Once we have an inverse a' of a $modulo$ m, we can solve the congruence

$$ax \equiv b\ (mod\ m)$$

- by multiplying both sides of the linear congruence by a'.

$$a'ax \equiv a'b(mod\ m),$$

$$x \equiv a'b(mod\ m).$$

Linear Congruences

- **EXAMPLE.** What are the solutions of the linear congruence $3x \equiv 4(mod\ 7)$?
- *Solution:* We know that -2 is an inverse of $3\ modulo\ 7$. Multiplying both sides of the congruence by -2 shows that

$$(-2) \cdot 3x \equiv (-2) \cdot 4(mod\ 7).$$

- Because $-6 \equiv 1(mod\ 7)$ and $-8 \equiv 6(mod\ 7)$, it follows that if x is a solution, then

$$x \equiv -8 \equiv 6(mod\ 7).$$

The Chinese Remainder Theorem

- **THEOREM 2. (THE CHINESE REMAINDER THEOREM)** Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots, a_n$ arbitrary integers. Then the system

$$\begin{gathered} x \equiv a_1 (mod\ m_1), \\ x \equiv a_2 (mod\ m_2), \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots, \\ x \equiv a_n (mod\ m_n) \end{gathered}$$

- has a unique solution modulo $m = m_1 m_2 \cdot \dots \cdot m_n$. (there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo *m* to this solution.)

The Chinese Remainder Theorem

- **EXAMPLE.** What are the solutions of the system of congruences $x \equiv 2(mod\ 3), x \equiv 3(mod\ 5), x \equiv 2(mod\ 7)$?
- *Solution*: First let

$$m = 3 \cdot 5 \cdot 7 = 105,$$

$$M_1 = \frac{m}{3} = 35,$$

$$M_2 = m/5 = 21, \text{ and}$$

$$M_3 = m/7 = 15.$$

The Chinese Remainder Theorem

- *Solution* (cont.): We see that $y_1 = 2$ is an inverse of $M_1 = 35\ modulo\ 3$, because $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 (mod\ 3)$;
- $y_2 = 1$ is an inverse of $M_2 = 21\ modulo\ 5$, because $21 \equiv 1 (mod\ 5)$;
- and $y_3 = 1$ is an inverse of $M_3 = 15 (mod\ 7)$, because $15 \equiv 1 (mod\ 7)$.
- The solutions to this system are those x such that

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \\ &\equiv 23 (mod\ 105). \end{aligned}$$

Fermat’s Little Theorem

- The great French mathematician Pierre de Fermat made many important discoveries in Number Theory. One of the most useful of these states that p divides $a^{p-1} - 1$ whenever p is prime and a is an integer not divisible by p.
- Fermat announced this result in a letter to one of his correspondents. However, he did not include a proof in the letter, stating that he feared the proof would be too long.

Fermat’s Little Theorem

- Although Fermat never published a proof of this fact, there is little doubt that he knew how to prove it, unlike the result known as Fermat’s last theorem.
- The first published proof is credited to Leonhard Euler. We now state this theorem in terms of congruences.

Fermat’s Little Theorem

- **THEOREM 3. (FERMAT’S LITTLE THEOREM)** If p is prime and a is an integer not divisible by p, then
$$a^{p-1} \equiv 1(mod\, p)$$
- Furthermore, for every integer a we have
$$a^{p} \equiv a(mod\, p)$$

Fermat's Little Theorem

- **EXAMPLE.** Find $7^{222} mod 11$.
- *Solution*:

$$7^{222} \equiv (-4)^{222} = 4^{222} = 2^{444} = (2^5)^{88} \cdot 2^4 = 32^{88} \cdot 16 \equiv (-1)^{88} \cdot 5 = 1^{88} \cdot 5 \equiv 5(mod 11)$$

- Compare with

$$7^{222} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 7^2 = 49 \equiv 5(mod 11)$$

HOMEWORK: Exercises 2, 4, 6, 10, 12, 14, 20, 34, 38, 40 on pp. 284-286;