

Announcements

- No Recitation tomorrow or next Friday
- Recitations start back after spring break

February 23, 2012

Prof. Rodger

TABLE 1 The Sieve of Eratosthenes.

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

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

Chap 4.3 - 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:

- 105 =
- 641 =
- 221 =
- 1024 =

The Sieve of Erastosthenes

Erastosthenes
(276-194 B.C.)



- The *Sieve of Erastosthenes* 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.
 - Delete all the integers, other than 2, divisible by 2.
 - Delete all the integers, other than 3, divisible by 3.
 - Next, delete all the integers, other than 5, divisible by 5.
 - Next, delete all the integers, other than 7, divisible by 7.
 - Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

continued →

TABLE 1 The Sieve of Eratosthenes.

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

The Sieve of Erastosthenes

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 .

In previous example, why did we use only 2, 3, 5 and 7?

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, \dots, 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, \dots, 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, \dots, 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)

Mersenne Primes



Marin Mersenne
(1588-1648)

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

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, and $2^7 - 1 = 127$ are Mersenne primes.
- $2^{11} - 1 = 2047$ is not a Mersenne 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 Mersenne primes.
- As of mid 2011, 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.
- The *Great Internet Mersenne Prime Search (GIMPS)* is a distributed computing project to search for new Mersenne Primes.

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

Generating Primes

- Finding large primes with hundreds of digits is important in cryptography.
- There is no simple function $f(n)$ such that $f(n)$ is prime for all positive integers n .
- Consider
 - $f(n) = n^2 - n + 41$ is prime for all integers $1, 2, \dots, 40$.
 - But $f(41) = 41^2$ is not prime.
- Fortunately, we can generate large integers which are almost certainly primes. See Chapter 7.

Distribution of Primes

- Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the *prime number theorem* was proved which gives an asymptotic estimate for the number of primes not exceeding x .

Prime Number Theorem: The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. ($\ln x$ is the natural logarithm of x)

- The theorem tells us that the number of primes not exceeding x , can be approximated by $x/\ln x$.
- The odds that a randomly selected positive integer less than n is prime are approximately $(n/\ln n)/n = 1/\ln n$.

Conjectures about Primes

Many conjectures about them are unresolved, including:

- *Goldbach's Conjecture:* Every even integer n , $n > 2$, is the sum of two primes. It has been verified by computer for all positive even integers up to $1.6 \cdot 10^{18}$. The conjecture is believed to be true by most mathematicians.
- There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer. But it has been shown that there are infinitely many primes of the form $n^2 + 1$, where n is a positive integer or the product of at most two primes.
- *The Twin Prime Conjecture:* The twin prime conjecture is that there are infinitely 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. The current world's record for twin primes (as of mid 2011) consists of numbers $65,516,468,355 \cdot 2^{33,333} \pm 1$, which have 100,355 decimal digits.

Greatest Common Divisor

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?

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

Greatest Common Divisor

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

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

Solution:

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

Solution:

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of a and b are:

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

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

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

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

$\gcd(120, 500) =$

- 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 $\text{lcm}(a, b)$.

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

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

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

Least Common Multiple

Example: $\text{lcm}(30, 35) =$

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

LCM and GCD relation

Theorem 5: Let a and b be positive integers. Then
 $ab = \text{gcd}(a,b) \cdot \text{lcm}(a,b)$

Example: $\text{gcd}(20,15) \cdot \text{lcm}(20,15)$

Proof:

Euclidean Algorithm



Euclid
(325 B.C.E. – 265 B.C.E.)

- The Euclidean algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that $\text{gcd}(a,b)$ is equal to $\text{gcd}(a,c)$ 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

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

continued →

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

procedure $\text{gcd}(a, b)$: positive integers)

$x := a$

$y := b$

while $y \neq 0$

$r := x \bmod y$

$x := y$

$y := r$

return x { $\text{gcd}(a,b)$ is x }

Correctness of Euclidean Algorithm

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 .
- Suppose that d divides both b and r .
- Therefore, $\gcd(a, b) = \gcd(b, r)$.

Correctness of Euclidean Algorithm

- 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:

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

gcds as Linear Combinations

Étienne Bézout
(1730-1783)



Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.
(proof in exercises of Section 5.2)

Definition: 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 . The equation $\gcd(a, b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b .
 - $\gcd(6, 14) =$

Finding gcds as Linear Combinations

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

Solution: First use the Euclidean algorithm to show $\gcd(252, 198) = 18$

- Now working backwards, from iii and i above
- Substituting the 2nd equation into the 1st yields:
- Substituting $54 = 252 - 1 \cdot 198$ (from i)) yields:
 -
- This method illustrated above is a two pass method. It first uses the Euclidean algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers.

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

$$sa + tb = 1.$$

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 the proof of the uniqueness of prime factorizations.

Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).

- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

Theorem 7: Let m be a positive integer and let a , b , and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof:

Uniqueness of Prime Factorization

- We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique. (This is part of the fundamental theorem of arithmetic. The other part, which asserts that every positive integer has a prime factorization into primes, will be proved in Section 5.2.)

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

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

- 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 the assumption that p_{i_1} and q_{j_k} are distinct primes.

- Hence, there can be at most one factorization of n into primes in nondecreasing order. ◀

Chap 4.4 - Linear Congruences

Definition: A congruence of the form

$$ax \equiv b \pmod{m},$$

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

- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Definition: An integer \bar{a} such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse of a modulo m* .

Example: What is the inverse of 3 modulo 7?

- One method of solving linear congruences makes use of an inverse \bar{a} , if it exists. Although we can not divide both sides of the congruence by a , we can multiply by \bar{a} to solve for x .

Inverse of a modulo m

- The following theorem guarantees that an inverse of a modulo m exists whenever a and m are relatively prime. Two integers a and b are relatively prime when $\gcd(a,b) = 1$.

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 . (This means that there is a unique positive integer \bar{a} less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to \bar{a} modulo m .)

Proof: Since $\gcd(a,m) = 1$, by Theorem 6 of Section 4.3, there are integers s and t such that $sa + tm = 1$.



Finding Inverses

- The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

Example: Find an inverse of 3 modulo 7.

Solution: Because $\gcd(3,7) = 1$, by Theorem 1, an inverse of 3 modulo 7 exists.

- Using the Euclidian algorithm to find gcd: $7 = 2 \cdot 3 + 1$.
- From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7.
- Hence, -2 is an inverse of 3 modulo 7.
- Also every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, -9 , 12, etc.

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that $\gcd(101,4620) = 1$.

Working Backwards:

