Session 58: Primes

- Primes
- Basic Theorems on Primes

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. The integer 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: If *n* is an integer greater than 1, then *n* can be written as the product of primes.

Examples:

Proof of Fundamental Theorem of Arithmetic

Proof: (strong induction) Let P(n) be the proposition that n can be written as a product of primes.

- BASIS STEP: P(2) is true since 2 itself is prime.
- INDUCTIVE STEP: The inductive hypothesis is P(j) is true for all integers j with $2 \le j \le k$. To show that P(k + 1) must be true under this assumption, two cases need to be considered:
 - If k + 1 is prime, then P(k + 1) is true.
 - Otherwise, k + 1 is composite and can be written as the product of two positive integers a and b with $2 \le a \le b < k + 1$. By the inductive hypothesis a and b can be written as the product of primes and therefore k + 1 can also be written as the product of those primes.

Hence, it has been shown that every integer greater than 1 can be written as the product of primes. \square

Trial Division

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

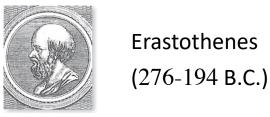
Proof:

If n is composite it can be written as n = ab.

Either $a \le \sqrt{n}$ or $b \le \sqrt{n}$: if this is not the case, i.e. $a > \sqrt{n}$ and $b > \sqrt{n}$, ab > n, which is a contradiction.

W.l.o.g. assume $a \le \sqrt{n}$.

Then either a is prime, or a has a prime factor that is smaller than \sqrt{n} . In either case the theorem follows.



The Sieve of Erastosthenes

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:

{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 Erastosthenes

TAB	LE	1 Th	e Sie	eve of	f Era	tosth	enes													
Integers divisible by 2 other than 2											Integers divisible by 3 other than 3									
receive an underline.										re	receive an underline.									
1	2	3	4	5	<u>6</u>	7	8	9	<u>10</u>	1	2	3	4	5	<u>6</u>	7	8	9	<u>10</u>	
11	12	13	14	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>	23	<u>24</u>	25	<u>26</u>	27	<u>28</u>	29	<u>30</u>	<u>21</u>	22	23	<u>24</u>	25	<u>26</u>	<u>27</u>	28	29	<u>30</u>	
31	<u>32</u>	33	<u>34</u>	35	<u>36</u>	37	<u>38</u>	39	<u>40</u>	31	<u>32</u>	<u>33</u>	34	35	<u>36</u>	37	<u>38</u>	<u>39</u>	<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>	<u>51</u>	<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>	64	65	<u>66</u>	67	<u>68</u>	<u>69</u>	70	
71	<u>72</u>	73	<u>74</u>	75	<u>76</u>	77	<u>78</u>	79	<u>80</u>	71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>	
81	<u>82</u>	83	84	85	86	87	88	89	90	81	82	83	84	85	<u>86</u>	<u>87</u>	88	89	<u>90</u>	
91	<u>92</u>	93	<u>94</u>	95	<u>96</u>	97	<u>98</u>	99	100	91	<u>92</u>	<u>93</u>	<u>94</u>	95	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>	
Inte	Integers divisible by 5 other than 5										Integers divisible by 7 other than 7 receive									
	receive an underline.									I	iteger	s divi	sible	by 7 c	other	than	7 rec	eive		
rece	0				her ti	han 5	ī				iteger n und									
<i>rece</i>	0		derlin			han 5 7		9	10		0		; inte		in co		re pri	me.	10	
	eive a	n und		ie. 5	<u>6</u> 16	7	<u>8</u> 18	<u>9</u> 19		а	n und	erline	; inte	egers 5	<i>in co</i> <u>6</u>	lor ar	e pri		<u>10</u> 20	
1	eive a	n und	derlin 4 14	ie.	<u>6</u>		<u>8</u>		10 20 30	1 11	2 12	erline 3	; inte 4 14	egers	in co	lor ai 7	8 18	me. <u>9</u>	$\frac{10}{20}$	
1	2 12 22	3 13 23	4 14 24	5 15 25	6 16 26	7 17	8 18 28	19	<u>20</u> <u>30</u>	1	2 12 22	3 13 23	4 14 24	$\frac{5}{5}$ $\frac{15}{25}$	in co <u>6</u> 16 26	7 17	8 18 28	9 19 29	<u>20</u> <u>30</u>	
1 11 <u>21</u>	2 12 22 22 32	3 13 23 33	4 14 24 34	5 15 25 35	6 16 26 36	7 17 <u>27</u> 37	$\frac{8}{18}$ $\frac{28}{28}$ $\frac{38}{8}$	19 29	20 30 40	1 11 21	2 12 22 22 32	3 13	### ### ### ### ######################	5 15 25 35	in co. 6 16 26 36	7 17 27 37	8 18 28 38	9 19 29 39	<u>20</u> <u>30</u> <u>40</u>	
1 11 21 31 41	2 12 22 22 32 42	3 13 23 33 43	4 14 24 24 34 44	5 15 25 25 45	6 16 26 36 46	7 17 <u>27</u> 37 47	$\frac{8}{18}$ $\frac{18}{28}$ $\frac{38}{48}$	19 29 39 49	20 30 40 50	1 11 21 31 41	2 12 22 22 32 42	3 13 23 33 43	4 14 24 24 34 44	5 15 25 35 45	6 16 26 36 46	7 17 27 37 47	8 18 28 38 48	9 19 29 39 49	<u>20</u> <u>30</u> <u>40</u> <u>50</u>	
1 11 21 31 41 51	2 12 22 22 32 42 52	3 13 23 33 43 53	4 14 24 34 44 54	5 15 25 25 45 55	6 16 26 36 46 56	7 17 <u>27</u> 37 47 <u>57</u>	$\frac{8}{18}$ $\frac{18}{28}$ $\frac{38}{48}$ $\frac{48}{58}$	19 29 39 49 59	20 30 40 50 60	1 11 21 31 41 51	2 12 22 22 32 42 52	3 13 23 33 43 53	4 14 24 34 44 54	5 15 25 25 45 55	6 16 26 36 46 56	7 17 27 37 47 57	8 18 28 38 48 58	9 19 29 39 49	20 30 40 50 60	
1 11 21 31 41 51 61	2 12 22 22 32 42 52 62	3 13 23 33 43 53 63	4 14 24 34 44 54 64	5 15 25 25 35 45 55 65	6 16 26 36 46 56 66	7 17 27 37 47 57 67		19 29 39 49 59	20 30 40 50 60 70	1 11 21 31 41 51	2 12 22 22 32 42 52 62	3 13 23 33 43 53 63	4 14 24 34 44 54 64	5 15 25 25 45 55 65	6 16 26 36 46 56 66	7 17 27 37 47 57	8 18 28 38 48 58	9 19 29 39 49 59	20 30 40 50 60 70	
1 11 21 31 41 51 61	2 12 22 32 42 52 62 72	3 13 23 33 43 53 63 73	4 14 24 34 44 54 64 74	5 15 25 25 45 55 65 75	6 16 26 36 46 56 66 76	7 17 27 37 47 57 67	8 18 28 38 48 58 68 78	19 29 39 49 59 69 79	20 30 40 50 60 70 80	1 11 21 31 41 51 61	$ \begin{array}{c} 2 \\ 12 \\ 22 \\ 32 \\ 42 \\ 52 \\ 62 \\ 72 \\ \end{array} $	3 13 23 33 43 53 63 73	4 14 24 34 44 54 64 74	5 15 25 25 45 55 65 75	in co.	7 17 27 37 47 57 67	8 18 28 38 48 58 68	9 19 29 39 49 59 69	20 30 40 50 60 70 80	
1 11 21 31 41 51 61	2 12 22 22 32 42 52 62	3 13 23 33 43 53 63	4 14 24 34 44 54 64	5 15 25 25 35 45 55 65	6 16 26 36 46 56 66	7 17 27 37 47 57 67		19 29 39 49 59	20 30 40 50 60 70	1 11 21 31 41 51	2 12 22 22 32 42 52 62	3 13 23 33 43 53 63	4 14 24 34 44 54 64	5 15 25 25 45 55 65	6 16 26 36 46 56 66	7 17 27 37 47 57	8 18 28 38 48 58	9 19 29 39 49 59	20 30 40 50 60 70	

Infinitude of Primes



Euclid (325 b.c.e. – 265 b.c.e.)

Theorem: There are infinitely many primes (Euclid).

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

- 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.
 - 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 $p_1, p_2,, p_n$.
 - It is either q, or if q is composite, it is a prime factor of q.
 - This contradicts the assumption that $p_1, p_2,, p_n$ are all the primes.
- Consequently, there are infinitely many primes.

Summary

- Primes
- Basic Theorems on Primes
 - Fundamental Theorem of Arithmetic
 - Trial Division
- Sieve of Erastosthenes
- Euclid's Theorem

Theorem: If
$$2^{n} - 1$$
 is prime, dhen n is prime.

Proof by contradiction:

assume n is not prime, then $n = a \cdot b$ for some $a, b > 1$

$$2^{ab} - 1 = 2^{a} 2^{a(b-1)} - 1 \qquad \left[2^{2} 2^{a(b-1)} - 2^{a \cdot a(b-1)}, 2^{a \cdot a \cdot b \cdot a}, 2^{ab} \right]$$

$$= 2^{a} 2^{a(b-1)} + 2^{a} 2^{a(b-2)} - 2^{a} 2^{a(b-2)} - 1$$

$$= 2^{a} 2^{a(b-1)} + 2^{a} 2^{a(b-2)} + \dots + 2^{a} 2^{a(b-2)} - 2^{a} 2^{a(b-2)} - \dots - 2^{a} 2^{a(b-b)} - 1$$

$$= 2^{a} 2^{a(b-1)} + 2^{a} 2^{a(b-2)} + 2^{a} 2^{a(b-2)} - 2^{a} 2^{a(b-2)} + 2^{a} 2^{a(b$$