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:

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

$641 = 641$

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

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

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 $2 \leq j \leq k$. 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 $2 \leq a \leq b < k + 1$. 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. ⊠

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 $n = ab$.

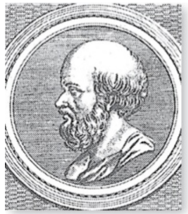
Either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$: if this is not the case, i.e. $a > \sqrt{n}$ and $b > \sqrt{n}$, $ab > n$, which is a contradiction.

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

Then either a is prime, or a has a prime factor that is smaller than $\sqrt{n}$.

In either case the theorem follows. $\boxtimes$

The Sieve of Erastosthenes



Erastothenes

(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:

{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

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

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.
  - 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. $\boxtimes$

Summary

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

<u>Theorem:</u> If $2^n - 1$ is prime, then n is prime.

Proof by contradiction:

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

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

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

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

$$= 2^a 2^{a(b-1)} - 2^a 2^{a(b-2)} + 2^a 2^{a(b-2)} - 2^a 2^{a(b-3)} \dots + 2^a - 1$$

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

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

therefore $2^{ab} - 1$ is not prime