Ch 4.3 Primes and Greatest Common Divisors (R)

Primes

An integer p greater than 1 is called *prime iff* 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*.

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 nondecreasing size.

Trial Division

Accoring to Wikipedia

$\rightarrow$ Test if an integer n can be divided by each number in turn that is less than n.

Ex. $n = 12$ (1, 2, 3, 4, 6, 12). Selecting only the largest powers of primes $\rightarrow$ $12 = 3 \times 4 = 3 \times 2^2$.

Theorem 2
If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

▼ Example 3

Show that 101 is prime.

Solution:

The only primes not excceeding $\sqrt{101}$ 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.

The Sieve of Eratosthenes

$\rightarrow$ Used to find all primes not exceeding a specified positive integer.

Ex. Find all primes between 1 and 100.

1. Delete all integers divisible by 2 other than 2.
2. Delete all integers divisible by 3 other than 3. (Because 3 is the first integer greater than 2 that is left)
3. Delete all integers divisible by 5 other than 5. (Because of the same reason)
4. Do the same for 7.
5. Done. (Because all composite integers not exceeding 100 are divisible by 2, 3, 5, or 7, all remaining integers except 1 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

Theorem 3
There are infinitely many primes.

Proof. We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Let $Q = p_1 p_2 \cdots p_n + 1$.

By the fundamental theorem of arithmetic. Q is prime or else it can be written as the product of two more primes. However, none of the primes p_j divides Q, for if $p_j \mid Q$, then p_j divides $Q - p_1 p_2 \cdots p_n = 1$. Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes.

Mersenne primes

$2^p - 1$ is a prime where p is also a prime.

Theorem 4 THE PRIME NUMBBER THEOREM

The ratio of $\pi(x)$, the number of primes not exceeding x, and $\dfrac{x}{\ln x}$ approaches 1 as x grows without bound.

TABLE 2 Approximating $\pi(x)$ by $x/\ln x$.

x	$\pi(x)$	$x/\ln x$	$\pi(x)/(x/\ln x)$
10^3	168	144.8	1.161
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78,498	72,382.4	1.084
10^7	664,579	620,420.7	1.071
10^8	5,761,455	5,428,681.0	1.061
10^9	50,847,534	48,254,942.4	1.054
10^{10}	455,052,512	434,294,481.9	1.048

Goldbach's Conjecture

Every even integer n, $n > 2$, is the sum of two primes.

Twin primes

Pairs of primes that differ by 2. Ex. 3 & 5, 5 & 7, 11 & 13, 17 & 19, 4967 & 4969.

Greatest Common Divisor & Least Common Multiples

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

The integers a and b are *relatively prime* if their greatest common divisor is 1.

The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

▼ Example 13

Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution:

Because $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$ and $\gcd(17, 21) = 1$, we conclude that 10, 17, and 21 are pairwise relatively prime.

Because $\gcd(10, 24) = 2 > 1$, we see that 10, 19, and 24 are not pairwise relatively prime.

Another way to find GCD

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

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

▼ Example 14

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

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

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 $\operatorname{lcm}(a, b)$.

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

▼ Example 15

What is the least common mutliple of $2^3 3^5 7^2$ and $2^4 3^3$?

Solution:

We have $\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$.

Theorem 5

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

The Euclidean Algorithm

LEMMA 1

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

▼ Example 16

Find the greatest common divisor of 414 and 662 using the Euclidean Algorithm.

Solution:

Successive uses of the division algorithm give:

$$
\begin{aligned}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &= 82 \cdot 2 + 2 \\
82 &= 2 \cdot 41.
\end{aligned}
$$

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

ALGORITHM 1 The Euclidean Algorithm.

```
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}
```

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

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*.

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

LEMMA 3
If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

▼ Example 19

The congruence $14 \equiv 8 \pmod{6}$ holds, but both sides of this congruence cannot be divided by 2 to produce a valid congruence because $\frac{14}{2} = 7$ and $\frac{8}{2} = 4$, but $7 \not\equiv 4 \pmod{6}$.

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