4. Number Theory (Part 1)

Terence Sim

God made the integers, all else is the work of man.

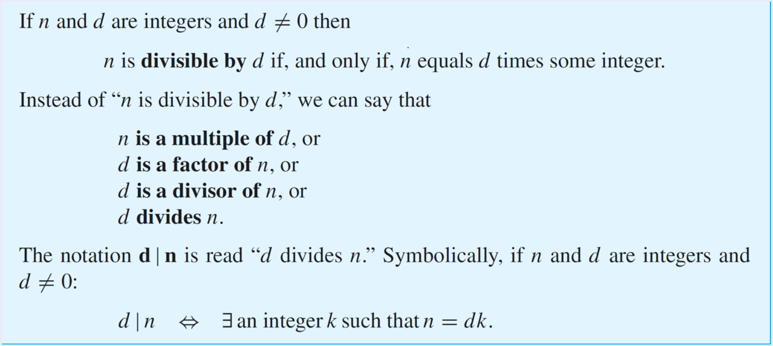
Leopold Kronecker,
1823 — 1891

Reading

Sections 4.1 — 4.7 of Epp

4.1. Recap

Definition 1.3.1 (Divisibility)



If n and d are integers and $d \neq 0$ then

n is **divisible by** d if, and only if, n equals d times some integer.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d} \mid \mathbf{n}$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Reminder: No division is actually performed when we say: $d \mid n$.

Theorem 4.1.1 (Linear Combination)

$$\forall a, b, c \in \mathbb{Z}, \text{ if } a \mid b \text{ and } a \mid c, \text{ then } \forall x, y \in \mathbb{Z}, a \mid (bx + cy)$$

That is, if a divides both b and c, then a divides their linear combination.

Note that this statement was called Proposition 1.3.2 in `Week1_Proofs.pdf`

Since it is useful, we promote it to a theorem.

Proof.

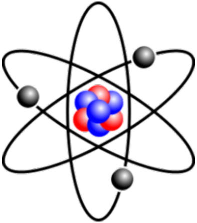
1. Take any $a, b, c \in \mathbb{Z}$.
2. If $a \mid b$ and $a \mid c$:
3. Let $k \in \mathbb{Z}$ such that $b = ak$. (by definition of divisibility)
4. Let $m \in \mathbb{Z}$ such that $c = am$. (by definition of divisibility)
5. Take any $x, y \in \mathbb{Z}$.
6. Then $bx + cy = (ak)x + (am)y = a(kx + my)$. (by basic algebra)
7. Note that $kx + my \in \mathbb{Z}$. (by closure of addition and multiplication over integers)
8. Thus $a \mid bx + cy$. (by definition of divisibility) $\blacksquare$

4.2. Primes

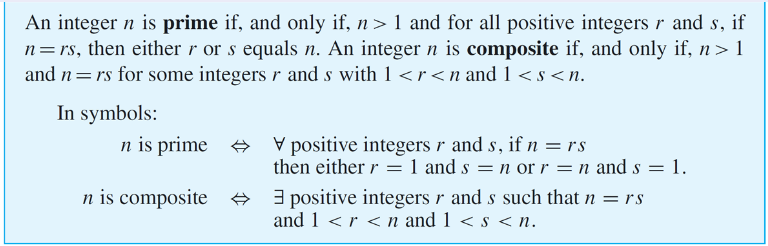
Prime numbers are to integers what atoms are to materials.

They are the indivisible building blocks of integers.

We will learn some key properties and see some applications of prime numbers.



Definition 4.2.1 (Prime number)



An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

n is composite $\Leftrightarrow$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

- 1 is neither prime nor composite.
- The first few primes are: $2, 3, 5, 7, 11, 13, 17, 19$.
- The first few composites are: $4, 6, 8, 9, 10, 12, 14, 15$.

Every integer $n > 1$ is either prime or composite.

4.2.1. Prime properties

Primes have interesting properties, some of which we will now study. We begin with the property that if one prime divides another, then they must be equal.

Proposition 4.2.2

For any two primes p and p', if $p \mid p'$ then $p = p'$.

Note that this property does not hold for composites, e.g. $4 \mid 8$ but $4 \neq 8$.

Proof:

1. For any primes p and p':
2.   If $p \mid p'$:
3.   Let $k \in \mathbb{Z}$ such that $p' = pk$, by definition of divisibility.
4.   Then $p = 1$ or $p = p'$, since p' is prime.
5.   Also, $p > 1$, since p is prime.
6.   Therefore, by Elimination on Lines 4, 5, $p = p'$. ■

The next property of primes sets the stage for the important fact that prime numbers do not end; ever larger primes exist.

Proposition 4.7.3 (Epp)

For any $a \in \mathbb{Z}$ and any prime p, if $p \mid a$ then $p \nmid (a+1)$.

Proof: (by Contradiction)

1. Suppose not. Then there exist $a \in \mathbb{Z}$ and prime p such that $p \mid a$ and $p \mid (a+1)$.
2. Then $p \mid a(-1) + (a+1)(1)$, by Theorem 4.1.1.
3. Then $p \mid 1$, by basic algebra.
4. By Theorem 4.3.1 (Epp), this implies $p \leq 1$, which contradicts the fact that $p > 1$.
5. Thus by the Contradiction Rule, the statement is true. ■

The statement to be proven takes the form:

$$S = \forall x(\forall y(P(x,y) \to Q(x,y)))$$

Thus, its negation is:

$$\begin{aligned}
\sim S &\equiv \sim(\forall x(\forall y(P(x,y) \to Q(x,y)))) \\
&\equiv \exists x \sim (\forall y(P(x,y) \to Q(x,y))) \text{ (by Theorem 3.2.1 (Epp))} \\
&\equiv \exists x(\exists y \sim (P(x,y) \to Q(x,y))) \text{ (by Theorem 3.2.1 (Epp))} \\
&\equiv \exists x(\exists y \sim (\sim P(x,y) \vee Q(x,y))) \text{ (Implication law)} \\
&\equiv \exists x \exists y\ P(x,y) \wedge \sim Q(x,y) \text{ (De Morgan's \& Double negative laws)}
\end{aligned}$$

The last line above is the form used in Line 1 of the proof.

Theorem 4.7.4 (Epp): Infinitude of Primes.

The set of primes is infinite.

Proof: (by Contradiction)

1. Suppose the set of primes is finite: a total of k primes.
2. Then we may list all the primes: $p_1, p_2, p_3, \ldots, p_k$
3. Let N be the product of all primes plus 1: $N = p_1 p_2 p_3 \cdots p_k + 1$.
4. Clearly, $N > 1$, and thus by Theorem 4.3.4 (Epp), there exists a prime q such that $q \mid N$.

. . .

proof cont'd

5. Now, q must be one of the primes in our list: $p_1, p_2, p_3, \ldots, p_k$

6. So $q \mid p_1 p_2 p_3 \cdots p_k$ because q is one of the factors in the product.

7. Then by Proposition 4.7.3 (Epp), $q \nmid N$, which contradicts Line 4 which says $q \mid N$.

8. Thus by the Contradiction Rule, the statement is true. $\blacksquare$

- This proof shows that if you form the product of all primes up to some point and add 1, the result, N, is divisible by a prime not in the list.
- Note that this does not mean that N is prime. As an exercise, try to find an N constructed in this way that is not prime.

So now we know that primes do not end. Ever larger primes can always be found.

But they seem fewer and fewer as we examine larger integers.

> For example, there are 4 primes under 10, but 25 primes under 100. To get the thousandth prime, you need to search up to about 8000; to get the millionth prime, your search goes to about 15.5 million.

The Prime Number Theorem tells us that the number of primes less than or equal to integer x is approximately $x/\log(x)$.

Watch this video: `http://tinyurl.com/nrwal9x`

Theorem 4.2.3

If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that: $p \mid x_1 x_2 \ldots x_n$,

then $p \mid x_i$, for some x_i $(1 \leq i \leq n)$.

For example, consider $2 \times 3 \times 6 = 36$:

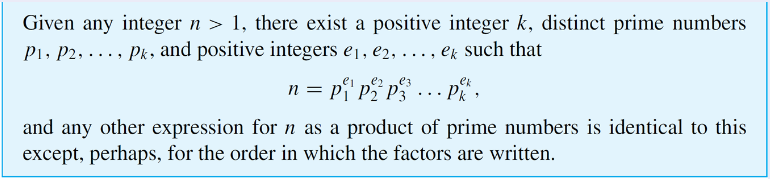
Clearly, 3 is prime, and $3 \mid 36$ and $3 \mid 6$.

However, the theorem does not hold for composites, e.g. 4 is composite and $4 \mid 36$. But $4 \nmid 2$, and $4 \nmid 3$ and $4 \nmid 6$.

This theorem shows that a prime factor of a product must be completely "inside" one of the factors of the product. The prime cannot be "split" into several of the factors.

Proof deferred.

Theorem 4.3.5 (Epp): Unique Prime Factorization



Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

That is, every positive integer greater than 1 can be uniquely factorized into a product of prime numbers.

This is also called *The Fundamental Theorem of Arithmetic*.

It is standard practice to sort the primes from smallest to largest. Examples:

$$24 = 2 \times 2 \times 2 \times 3 = 2^3 \cdot 3.$$

$$90 = 2 \times 3 \times 3 \times 5 = 2 \cdot 3^2 \cdot 5.$$

Example

Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14$$

Does $17 \mid m$?

Since 17 is a prime factor of the right hand side, it must also divide the product on the left hand side.

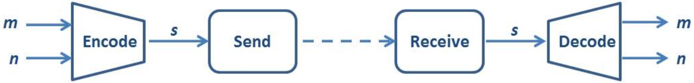
Then by Theorem 4.2.3, 17 must divide one of the factors on the left hand side. This must be m because the other factors are not divisible by 17.

Thus, $17 \mid m$.

4.2.2. An application

Suppose you wish to send a message consisting of two positive integers m, n to a friend. Unfortunately, the Send device can only send a single integer, however large, but not two. The Receive device is likewise limited to receiving only a single integer.

You thus need a way to encode, i.e. convert, your m, n into s, as well as a way to decode. This is shown in the diagram below.



How would you encode?

1. Suppose you encode m, n by inserting a 0 between their decimal representations, e.g.

   1234 and 768 gets encoded to 12340768

   Clearly, this won't work if m or n contains 0.
2. Suppose you try $s = m + n$. This doesn't work either. Why?
3. Next, you try $s = 1000m + n$. Will this work?
4. Clearly, $s = mn$ also doesn't work.
5. Luckily, you remember CS1231, so you try $s = 2^m 3^n$.

   This works because the prime factorization of s guarantees that we can get back m and n uniquely!

Question: how would you handle negative m and n?

Python code for encode and decode:

```
def encode(m, n):
    return 2**m * 3**n

def decode(s):
    # Repeatedly divide s by 2, and count number of times
    # this can be done. Do the same for 3.

    m = 0
    while isEven(s):
        s = s / 2
        m = m + 1

    n = 0
    while isColorful(s):
        s = s / 3
        n = n + 1

    return m,n
```

Python code cont'd

```
def isEven(x):
    # x is even if its remainder is 0
    # when divided by 2
    return x % 2 == 0

def isColorful(x):
    # x is colorful if its remainder is 0
    # when divided by 3
    return x % 3 == 0
```

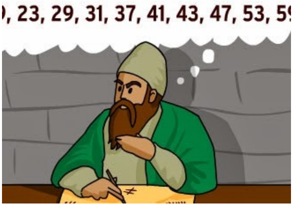
4.2.3. Primality test

This is a test to see if an integer n is prime.

The most straightforward method is Trial Division, i.e. test if n is divisible by all integers k between 2 and $\sqrt{n}$ (rounded up). If n is not divisible by all such k, then n is prime, otherwise, composite.

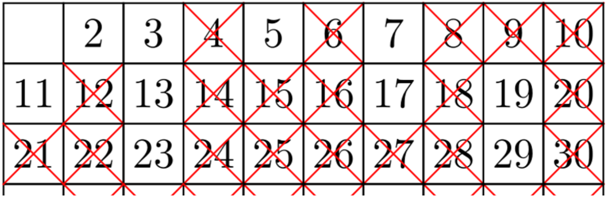
This test is easy to code, but is slow. It can be sped up using only k which are primes, but this requires a list of such primes to begin with.

The side benefit of Trial Division is that you also get all the factors of n, if n is composite.



Of course, one way to check if a number n is prime is to see if n can be found in a list, L, of primes. To generate L, an ancient method called the Sieve of Eratosthenes may be used:

1. Start by listing all integers greater than 1. Call this list C. Also, let L be an empty list.
2. Take the first number $p = 2$ in C, and add it to L. This is the first prime.
3. In C, cross out all multiples of p.
4. Let p be the next uncrossed number in C. This is the next prime. Add it to L, and repeat from Step 3.



	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~~

A more sophisticated method is the Miller-Rabin probabilistic test. More correctly, it tests for compositeness.

An integer, suspected of being a composite, is “put on trial”. The Judge (algorithm) randomly picks a person (another integer) and asks a series of questions concerning the Suspect.

If the person provides sufficient evidence, the person is then called a *Witness* and the Suspect is guilty of being a Composite, and the trial ends.

If not, then another random person is picked, and the trial is repeated several times. If no Witness emerges, then the Suspect is probably a Prime.

Thus the Miller-Rabin test can make errors: a composite may be passed off as a prime. Such a composite is called a *pseudoprime*. But the probability of error can be made small.

Still, in some applications, having a non-zero probability of getting a pseudoprime is unacceptable, e.g. in Cryptography. In this case, other primality tests are needed.

Furthermore, the Miller-Rabin test does not tell you the factors of the composite; it merely tells you if the integer is composite or probably prime.

Primality testing is still an active research area.

4.2.4. Open Questions

There are several Open Questions concerning prime numbers, i.e. questions for which answers are still lacking or unproven. Proving any of these will earn you a Ph.D. immediately, and land you a professorship at a prestigious university.

We mention two Open Questions:

Goldbach's Conjecture: Every even integer greater than 2 can be written as a sum of two primes.

Examples: $4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5.$

This Conjecture has been shown to be true for integers up to 4×10^{18}, but this is still far from proving it for *all* even integers.

Twin Primes Conjecture: There are infinitely many primes p such that $p + 2$ is also a prime.

Examples: $(3, 5)$, $(11, 13)$, $(41, 43)$.

Twin primes are primes separated by a gap of 2. In 2013, Yitang "Tom" Zhang, a hitherto unknown mathematician, rocked the world of mathematics by making in a big leap in proving the Twin Primes Conjecture.

He proved that there are infinitely many primes whose gap is at most 70 million. Although this gap is much larger than 2, Zhang's work sparked a revival in research in this area. A year later, through the efforts of many researchers, this gap is now reduced to 246.

Zhang, who had struggled to secure an academic job since getting his Ph.D. in 1991, and at one time even worked as a restaurant delivery worker, quickly got promoted to Full Professor.

Watch this video: `http://tinyurl.com/mv2xuq7`