BASIC RESULTS IN NUMBER THEORY

Divisibility and Modular Arithmetic

Definition 1. Suppose a and b are integers. We say that a **divides** b, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b, and that b is a **multiple** of a.

Proposition 2. *If $a|b$ and $b|c$, then $a|c$.*
If $a \mid b$ and $a \mid c$, then $a \mid (kb + lc)$ for all $k, l \in \mathbb{Z}$.

Theorem 3. (**The Division Algorithm**) *Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.*

The Division Algorithm is not actually an algorithm!

Definition 4. Given integers a and b and $n \in \mathbb{N}$, we say that a and b are **congruent modulo** n if $n|\,(a - b)$. We express this as $a \equiv b \mod n$. If a and b are not congruent modulo n, we write this as $a \not\equiv b \mod n$.

Proposition 5. *Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.*

Congruence mod n is a relation that partitions the integers into n disjoint sets called **congruence classes**.

Base Representations

When a number $n = a_r a_{r-1} ... a_3 a_2 a_1 a_0$ is written in decimal form, each digit is the coefficient of a power of 10,

$$n = a_r 10^r + a_{r-1} 10^{r-1} + ... + a_3 10^3 + a_2 10^2 + a_1 10 + a_0.$$

Numbers can also be written in other bases, such as base 2 (binary).
Congruences are useful to prove the following divisibility tests.

Proposition 6. *Let the decimal representation of an integer n be $n = a_r a_{r-1} ... a_3 a_2 a_1 a_0$.*
n is divisible by 2 if and only $2|a_0$.
n is divisible by 2^k if and only $2^k|a_k ... a_0$.
n is divisible by 3 if and only $3|\,(a_r + ... + a_0)$.
n is divisible by 5 if and only $5|a_0$.
n is divisible by 9 if and only $9|\,(a_r + ... + a_0)$.
n is divisible by 11 if and only $11|\,(\pm a_r ... - a_3 + a_2 - a_1 + a_0)$.

To prove this for 9, note that $10 \equiv 1 \mod 9$, so $10^k \equiv 1^k \mod 9$. Thus $n \equiv 0 \mod 9$ if and only if $(a_n + ... + a_0) \equiv 0 \mod 9$.

Prime Numbers

Definition 7. A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and n. If n has more than two positive divisors, it is called **composite**. (Thus n is composite if and only if $n = ab$ for $1 < a, b < n$.)

The primes less than 100 are listed below.
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Proposition 8. *If an integer n is composite, it has a factor at most $\sqrt{n}$.*

Thus to check if p is prime, we can check whether all the primes up to $\sqrt{p}$ are divisors. This is called trial division. This is not efficient for large numbers, but the divisibility tests help for small divisors.
If many small numbers are to tested for primality, the **sieve of Eratosthenes** can be used.

Theorem 9. *There are infinitely many prime numbers.*

Proof. Assume to the contrary that there are finitely many prime numbers $p_1, ... , p_r$. Let $P = p_1 \cdot ... \cdot p_r + 1$. Now none of $p_1, ... , p_r$ can be factors of P, so it must be prime. This is a contradiction, so there are infinitely many prime numbers. □

Note that given primes $p_1, \ldots , p_r$, it is not the case that $p_1 \cdot \ldots \cdot p_r + 1$ must be prime, only that all of its prime factors are not amongst $p_1, \ldots , p_r$. Thus this is an existence proof, since it does not provide infinitely many prime numbers. Only finitely many primes are known.

The largest known prime number (as of 2020) is $2^{82589933} - 1$.

Theorem 10. (**Prime Number Theorem**) *Let p_n be the n^{th} prime number. Then $\lim\limits_{n\to\infty} \frac{p_n}{n \cdot \ln n} = 1$, so $p_n \approx n \cdot \ln n$.*

An even better approximation for p_n is $Li\,(n) = \int_2^n \frac{dx}{\ln x}$.

There are arbitrarily large intervals with no prime numbers (e.g. $[n! + 2, n! + n]$).

There are many famous conjectures related to prime numbers.

Conjecture 11. (**Goldbach's Conjecture** [1742]) *Every even integer greater than 2 is a sum of two prime numbers.*

This is due to Christian Goldbach. It is true for $n < 4 \cdot 10^{18}$.

Conjecture 12. (**Twin Prime Conjecture**) *There are an infinite number of pairs of twin primes (p and $p + 2$).*

Twin primes have the form $6k \pm 1$ (except 3 and 5).

Yitang Zhang [2013] proved that there are infinitely many pairs of primes that differ by N, where $N < 70000000$. Others soon reduced this to $N \leq 246$.

Unique Factorization of Integers

Definition 13. The **greatest common divisor** of integers a and b, denoted $gcd\,(a, b)$, is the largest integer that divides both a and b. The **least common multiple** of non-zero integers a and b, denoted $lcm\,(a, b)$, is the smallest integer in $\mathbb{N}$ that is a multiple of both a and b.

An efficient way to find the gcd is the **Euclidean algorithm**. This can also be reversed to find a linear combination of a and b equal to $gcd\,(a, b)$.

Theorem 14. (**Bezout's identity**) *If $a, b \in \mathbb{N}$, then there exist integers k and l for which $gcd\,(a, b) = ak + bl$.*

This can be used to prove the following lemma.

Lemma 15. *If $a, b, c \in \mathbb{Z}$ such that $gcd\,(a, b) = 1$ and $a|bc$, then $a|c$.*

This has a corollary that can be proved by induction.

Corollary 16. *If p is a prime and $p|a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p|a_i$ for some i.*

This is key to proving uniqueness below. The existence is proved using strong induction.

Theorem 17. (**Fundamental Theorem of Arithmetic**) *Every natural number $n > 1$ has a unique factorization into primes, $n = p_1^{n_1} \cdots p_k^{n_k}$.*

The unique prime factorizations of two integers can be easily used to find their gcd and lcm. However, finding the prime factorizations is harder than using the Euclidean Algorithm.

The Multiplication Principle (of combinatorics) can be used to prove the following.

Proposition 18. *The number of positive integer factors $\tau\,(n)$ of $n = p_1^{n_1} \cdots p_k^{n_k}$ is $\tau\,(n) = (n_1 + 1) \cdots (n_k + 1)$.*

The sum of positive integer factors $\sigma\,(n)$ of $n = p_1^{n_1} \cdots p_k^{n_k}$ is $\sigma\,(n) = \prod \frac{p_i^{n_i + 1} - 1}{p_i - 1}$.

Definition 19. A number $n \in \mathbb{N}$ is **perfect** if it equals the sum of its positive divisors less than itself.

The first few perfect numbers are 6, 26, 496, 8128, 8589869056, ...

Theorem 20. *A perfect number n is even if and only if $n = 2^{p-1}\,(2^p - 1)$, provided $2^p - 1$ is prime.*

Prime numbers of the form $2^p - 1$ are known as **Mersenne primes**. It is unknown whether there are infinitely many Mersenne primes (as of 2020, only 51 are known).

It is unknown whether there is any odd perfect number. This is the oldest unsolved problem in math, dating back to ancient Greece. No odd perfect number is less than 10^{1500}.

Fibonacci Numbers

The **Fibonacci numbers** are defined as $f_1 = f_2 = 1$ and $f_n = f_{n-1} + f_{n-2}$.

The sequence starts 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ... (You could also start with $f_0 = 0$.)

The recursive definition facilitates many proofs by induction. The sum $\sum_{k=1}^{n} f_k = f_{n+2} - 1$ can be proved this way, or using a telescoping sum.

There is an explicit formula for the Fibonacci numbers: $f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$. Thus f_n is the integer closest to $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$. The quantity $\frac{1+\sqrt{5}}{2}$ is called the **Golden Ratio**.

The explicit formula can be derived by solving the recurrence relation or using generating functions.

Using the Euclidean algorithm on any Fibonacci number always yields a quotient of 1, so this is the worst case scenario for this algorithm.

Sums of Powers

Definition 21. A **Pythagorean triple** consists of $a, b, c \in \mathbb{N}$ such that $a^2 + b^2 = c^2$. A triple with no common factor is **primitive**.

Small examples of primitive triples are $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$, $(7, 24, 25)$, $(20, 21, 29)$, $(12, 35, 37)$, and $(9, 40, 41)$.

Theorem 22. *All primitive Pythagorean triples* (a, b, c) *with* $a^2 + b^2 = c^2$ *are given by*

$$\begin{aligned} a &= m^2 - n^2 \\ b &= 2mn \\ c &= m^2 + n^2 \end{aligned}$$

where $m > n > 0$*,* m *and* n *are relatively prime, and* m *and* n *have opposite parity.*

Every integer is the sum of four squares. Integers of the form $4^a\,(8b + 7)$ are not sums of three squares.

Pierre de Fermat claimed (circa 1637) that there is no solution to $a^n + b^n = c^n$ for larger n. Fermat claimed to have proven this theorem, but that the margin of the book he was reading was too small to contain the proof. The quest to prove this motivated much of the development of the subject of number theory. Finally in 1995, after seven years of work, British mathematician Andrew Wiles announced a proof.

Theorem 23. (**Fermat's Last Theorem**) *For all numbers* $a, b, c, n \in \mathbb{N}$ *with* $n > 2$*,* $a^n + b^n \neq c^n$*.*

His paper was 125 pages long, and employed very difficult mathematics.