Proofs from THE BOOK Lecture Notes

Taught by Saarik Kalia

1 Euclid's Theorem

Theorem. *There are infinitely many prime numbers.*

Definition. An integer $p > 1$ is *prime* if and only if there exist no integers $a, b > 1$ so that $p = ab$.

Basic facts about primes and factorization:

- The only positive factors of a prime p are 1 and p.
- Every integer $N > 1$ has a prime factor.
- The only factor of 1 is itself. (1 is not considered to be prime.)

Proof. We show that for any finite list of primes, there exists another prime, and so there must be infinitely many prime numbers. Let $p_1, p_2, \ldots, p_n$ be a finite list of primes, and set $P = p_1 p_2 \cdots p_n$. Now consider the number $Q = P + 1$. It is either prime or not prime.

- If Q is prime, then it is not in the list (as it is greater than all $p_1, \ldots, p_n$), so we have found our additional prime.
- If Q is not prime, then it has a prime factor p. Suppose p is in the list. Then p divides P (since it is the product of all the primes in the list), as well as Q. Therefore p divides their $Q - P = 1$ as well, but no prime number divides 1. Therefore p was not in the list, and we have our additional prime.

□

2 Fermat's Little Theorem

Theorem. *Let p be a prime number, and a an integer. Then*

$$a^p \equiv a \pmod{p}.$$

Definition. Let a, b, m be integers so that $a - b$ is divisble by m. Then we say a and b are *congruent modulo* m and write $a \equiv b \pmod{m}$.

Basic facts about modular arithmetic:

- If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
- If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m} \qquad \text{and} \qquad a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

Proof (Golomb). Let us consider strings of beads. Suppose we have all possible strings of p beads, where each bead is colored with one of a possible colors. Therefore there we will have a^p such strings (there are a choices of color for each bead, so we get $\underbrace{a \cdot a \cdots a}_{p \text{ times}}$ total choices). Note that we may turn each string into a necklace by tying the ends together. Now group all strings which form the same neckalce together, i.e. one can be rotated to obtain the other.

For any string which has at least two colors, we can see that its group has exactly p strings, since each rotation produces a different string. However, any string which only has one color lies in its own group, since rotating it gives back the same string. There are a such strings, one for each color, and so there are $a^p - a$ strings which are not alone in their group. Since each of these groups has p elements, then we see $a^p - a$ must be divisble by p, or in other words, $a^p \equiv a \pmod{p}$. □

3 Euler's Theorem

Theorem. *Let u, m be integers which are relatively prime. Then*

$$u^{\varphi(m)} \equiv 1 \pmod{m}.$$

Definition. Two integers a, b are *relatively prime* if and only if they have no positive common divisor except 1.

Definition. For any integer m, its *totient* $\varphi(m)$ is the number of positive integers less than or equal to m which are relatively prime to m.

Basic facts about relatively prime numbers:

- If p is prime and a is not divisble by p, then a and p are relatively prime. Therefore $\varphi(p) = p - 1$.
- If a and b are relatively prime, then $a + kb$ and b are relatively prime, for any constant k.
- If a and b are relatively prime, and c and b are relatively prime, then ac and b are relatively prime.
- If u and m are relatively prime, then there exists some integer w so that $uw \equiv 1 \pmod{m}$.

  Sketch of proof: Consider all possible values of $au + bm$, where a, b are integers. Call the smallest possible positive value $d = a_0u + b_0m$. We may write $m = qd + r$, where r is the remainder when m is divided by d and q is the quotient. Then $r = -qa_0u + (1 - qb_0)m$, so $r < d$ is a smaller possible value. Therefore r cannot be positive so $r = 0$, meaning d divides m. Similarly, d divides u. Therefore d is a common divisor of u and m, so $d = 1$. Then we can write $ua_0 \equiv 1 \pmod{m}$.

Proof. Label the positive integers relatively prime to m which are less than or equal to m as $a_1, a_2, \ldots, a_{\varphi(m)}$. Consider what happens when we multiply each of these by u, and reduce modulo m. Each ua_i is still relatively prime to m, and reducing modulo m subtracts a multiple of m, so it will still be relatively prime. Therefore $ua_i = a_j$ for some j. In fact, there cannot be another a_k so that $ua_k = a_j$. This is because multiplying by w (as above) shows that $ua_i = ua_k$ implies $a_i = a_k$. Thus multiplying by u and reducing modulo m simply sends the numbers $a_1, a_2, \ldots, a_{\varphi(m)}$ back to themselves one-to-one (in a different order). Then taking the product of this list, shows

$$ua_1 \cdot ua_2 \cdots ua_{\varphi(m)} \equiv a_1 \cdot a_2 \cdots a_{\varphi(m)} \pmod{m}$$

$$u^{\varphi(m)} \cdot a_1 \cdot a_2 \cdots a_{\varphi(m)} \equiv a_1 \cdot a_2 \cdots a_{\varphi(m)} \pmod{m}$$

$$u^{\varphi(m)} \equiv 1 \pmod{m}.$$

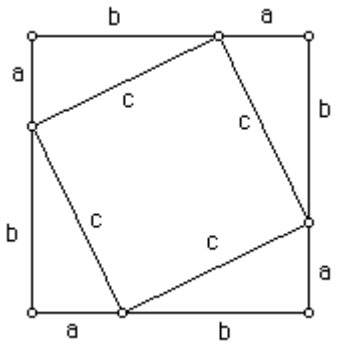
□

4 Pythagorean Theorem

Theorem. *Let a, b, and c be the lengths of sides of a right triangle, with c being the length of the side opposite to the right angle. Then*

$$a^2 + b^2 = c^2.$$

Proof. Consider the following diagram



consisting of four right triangles and a square arranged into one large square. The triangles each have area $\frac{a \cdot b}{2}$. The smaller square has area c^2, where c is the length of the hypotenuse of each of the right triangles. The large square has area $(a+b)^2$. Equating areas gives

$$(a+b)^2 = 4 \cdot \frac{a \cdot b}{2} + c^2$$

$$a^2 + 2ab + b^2 = 2ab + c^2$$

$$a^2 + b^2 = c^2.$$

□

5 Irrational Powers of Irrational Numbers

Theorem. *There exist irrational numbers a, b so that a^b is rational.*

Definition. We say a real number x is *rational* if and only if we can write $x = \frac{p}{q}$ where p, q are integers. If a number is not rational, we say it is *irrational*.

Lemma. $\sqrt{2}$ *is irrational.*

Proof. Suppose that $\sqrt{2}$ is rational, so there exist integers p, q such that $\sqrt{2} = \frac{p}{q}$ and p and q are relatively prime. Then we have $2 = \frac{p^2}{q^2}$ or equivalently $2q^2 = p^2$. We can see that p^2 is even, and so p is as well. Let us write $p = 2k$. Then we have $2q^2 = 4k^2$ or equivalently $q^2 = 2k^2$. By similar argument, q is then even, and so p and q are not relatively prime. Thus we have a contradiction, so $\sqrt{2}$ is irrational. □

Proof of Theorem. Consider the number $\sqrt{2}^{\sqrt{2}}$. This is either rational or irrational. If it is rational, then setting $a = b = \sqrt{2}$ will suffice. If it is irrational, then setting $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ will suffice because

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2$$

is rational. □

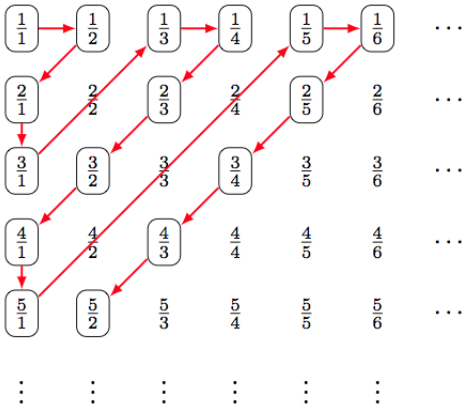
6 Cantor's Diagonalization Argument

Theorem. *The set of real numbers* $\mathbb{R}$ *is uncountable.*

Definition. A set S is *countable* if and only if each element can be assigned a unique positive integer, i.e. they can be written in a list $s_1, s_2, \ldots$ so that every element appears. If a set is not countable, we say it is *uncountable.*

Basic facts about countability:

- The set of positive integers $\mathbb{N}$ is, by definition, countable.
- The set of integers $\mathbb{Z}$ is countable, by listing them as $0, 1, -1, 2, -2, \ldots$.
- The set of rational numbers $\mathbb{Q}$ is countable, by listing them as



Proof. It suffices to show that the real numbers between 0 and 1 are uncountable, as they are a subset of $\mathbb{R}$. Suppose there exists some way to list the real numbers between 0 and 1 as $r_1, r_2, \ldots$. We will show that there exists a real number between 0 and 1 not in this list. Write each r_i in binary, and label its digits so that a_{ij} is the j^{th} digit (after the decimal point) of r_i's binary expansion. Then construct the number r whose i^{th} digit (after the decimal point) is 0 if $a_{ii} = 1$ and is 1 if $a_{ii} = 0$. Note that r then differs from each r_i in its i^{th} digit, and so r cannot be in the list. Thus we have a contradiction, so the set of real numbers are uncountable. □

7 Russell's Paradox

Theorem. *There exists no universal set, i.e. a set which contains all objects.*

Proof. Suppose there were a universal set U. Consider the set S of all objects $x \in U$ so that $x \notin x$. Since U is a universal set, then $S \in U$. Now we ask whether $S \in S$ or $S \notin S$. If $S \notin S$, then it satisfies the definition to be in S, so $S \in S$. If however $S \in S$, then by definition of S, it must satisfy the property $S \notin S$. Therefore, either way we reach a contradiction and so there can be no universal set. □

8 Sum of Squares

Theorem.

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{2}$$

Lemma.

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Proof (Gauss). Write $S = \sum_{k=1}^{n} k$. Then

$$\begin{array}{rcccccccccccc} S & = & 1 & + & 2 & + & \cdots & + & n-1 & + & n & & \\ S & = & n & + & n-1 & + & \cdots & + & 2 & + & 1 & & \\ \hline 2S & = & n+1 & + & n+1 & + & \cdots & + & n+1 & + & n+1 & = & n(n+1). \end{array}$$

Therefore $S = \frac{n(n+1)}{2}$. □

Proof of Theorem. Consider the following triangle, and its two rotations.

$$\begin{array}{ccccccccccc} & & & & 1 & & & & & & \\ & & & 2 & & & 2 & & & & \\ & & 3 & & & 3 & & & 3 & & \\ & \iddots & & \vdots & & & \vdots & & & \ddots & \\ n & & n & & & \cdots & & & n & & n \end{array}$$

$$\begin{array}{ccccccccccc} & & & & n & & & & & & \\ & & & n & & & n-1 & & & & \\ & & n & & & n-1 & & & n-2 & & \\ & \iddots & & \vdots & & & \vdots & & & \ddots & \\ n & & n-1 & & & \cdots & & & 2 & & 1 \end{array}$$

$$\begin{array}{ccccccccccc} & & & & n & & & & & & \\ & & & n-1 & & & n & & & & \\ & & n-2 & & & n-1 & & & n & & \\ & \iddots & & \vdots & & & \vdots & & & \ddots & \\ 1 & & 2 & & & \cdots & & & n-1 & & n \end{array}$$

Since each row of the first triangle has the number k repeated k times, it is clear that the sum of the entries in this triangle is $S = \sum_{k=1}^{n} k^2$. Superimposing the triangles, i.e. adding corresponding elements together, will in fact

give a triangle whose entries are all $2n+1$. This is true because the element in the j^{th} position (from the left) and i^{th} row of the first triangle is i. In the second triangle, it is $n-j+1$. And in the third triangle, it is $n-i+j$. Adding these together gives $2n+1$. Note that this triangle must have sum $3S$, since it is gotten from 3 triangles, each with original sum S. Moreover by the above lemma, the triangle has $\frac{n(n+1)}{2}$ entries. Therefore

$$3S = \frac{n(n+1)}{2} \cdot 2n+1$$

$$S = \frac{n(n+1)(2n+1)}{6}.$$

□

9 Sum of Totient Function

Theorem.

$$\sum_{d|n} \varphi(d) = n,$$

where the sum is taken over all positive integers d which divide n.

Proof. Consider the fractions

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots, \frac{n-1}{n}, \frac{n}{n}.$$

Let us reduce each of these fractions to lowest terms, and consider how many times the denominator d appears, where d is a factor of n. In order to be in lowest terms, the numerator must be relatively prime to d, so there can be at most $\varphi(d)$ such fractions. In fact, each of these fractions will appear, because multiplying the numerator and denominator by $\frac{n}{d}$ shows which original fraction they came from. Therefore, for every divisor d of n, there are $\varphi(d)$ fractions appearing in the above list. Since the list has n fractions, then we get

$$\sum_{d|n} \varphi(d) = n.$$

□

10 Basel Problem

Theorem (Euler)**.**

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Proof. Consider the function $\sin x$. It has zeroes at 0 and $\pm n\pi$ for all positive integer n. Treating it as an infinite polynomial, we may factor it as

$$\begin{aligned}\sin x &= Ax\left(1-\frac{x}{\pi}\right)\left(1+\frac{x}{\pi}\right)\left(1-\frac{x}{2\pi}\right)\left(1+\frac{x}{2\pi}\right)\left(1-\frac{x}{3\pi}\right)\left(1+\frac{x}{3\pi}\right)\cdots \\ &= Ax\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots,\end{aligned}$$

where A is some constant. Now we may compare this to its Taylor expansion

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots.$$

(This is a fact from calculus, which I will not give proof of here.) These expansions must have equal coefficients. The coefficient of the linear term in the Taylor expansion is 1. To expand our product, just as in finite products, we take all terms gotten by multiplying terms from each factor. Thus the only linear term we get comes when we choose the 1 in each factor (otherwise we have a higher power of x). Therefore the linear coefficient in our expansion is A. This shows $A = 1$, so now we have

$$\sin x = x\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots.$$

Now the cubic coefficient in the Taylor series is $-\frac{1}{3!} = -\frac{1}{6}$. The cubic terms in our expansion are gotten by choosing the x^2 term from one of the binomial factors and the 1 term from all the others. If we choose our x^2 term from the n^{th} binomial factor, then the term we get is $-\frac{x^3}{n^2\pi^2}$. Thus our total coefficient is $\sum_{n=1}^{\infty} -\frac{1}{n^2\pi^2}$, and so we have

$$\sum_{n=1}^{\infty} -\frac{1}{n^2\pi^2} = -\frac{1}{6}$$

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

□

Other Cool Theorems and Proofs

The following is a list of other statements in mathematics, either whose proof or result, is particularly interesting. I encourage you to look some of these up. (Despite what your English teacher says, Wikipedia is a great source for math.) Some of these statements and proofs will likely involve math you have not gotten to yet. That just gives you more of a reason to learn more, so you can come back to these one day and actually understand them.

- Art Gallery Problem
- Quadratic Reciprocity
- Lagrange's Four Square Theorem
- Bertrand's Postulate
- The integral of a Gaussian: $\int_{-\infty}^{\infty} e^{-x^2} = \sqrt{\pi}$
- Crystallographic Restriction Theorem
- Abel-Ruffini Theorem
- Banach-Tarsky Paradox
- Brouwer Fixed Point Theorem
- Fermat's Last Theorem (good luck understanding that proof)