Notes on Number Theory

October 7, 2023

Contents

1 Logic

Original Statement	$P \to Q$
Contrapositive	$\neg Q \to \neg P$
Converse	$Q \to P$
Inverse	$\neg P \to \neg Q$

Table 1: The contrapositive is equivalent to the original statement; the Converse to the inverse.

2 Binomial Theorem

2.1 Proof of Binomial Theorem

The following was taken from an exercise in chapter 1 of Complex Variables and Applications from Brown and Churchill.

Use mathematical induction to verify the binomial formula. More precisely, note that the formula is true when $n = 1$. Then, then assuming it is valid when $n = m$ where m denotes any positive integer, show that it must hold when $n = m + 1$.

Suggestion: when $n = m + 1$, write

$$
\begin{aligned}
(z_1 + z_2)^{m+1} = (z_1 + z_2)(z_1 + z_2)^m = (z_1 + z_2)\sum_{k=0}^{m}\binom{m}{k} z_1^k z_2^{m-k} \\
= \sum_{k=0}^{m}\binom{m}{k} z_1^k z_2^{m+1-k} + \sum_{k=0}^{m}\binom{m}{k} z_1^{k+1} z_2^{m-k}
\end{aligned}
$$

Reaplce k by $k-1$ in the last sum. To see how this would work take this example,

$$
\sum_{k=0}^{n-1} ar^k = \sum_{k=1}^{n} ar^{k-1}
$$

So

$$
\begin{aligned}
\sum_{k=0}^{m}\binom{m}{k} z_1^{k+1} z_2^{m-k} &= \sum_{k=1}^{m+1}\binom{m}{k-1} z_1^k z_2^{m-(k-1)} \\
&= \sum_{k=1}^{m+1}\binom{m}{k-1} z_1^k z_2^{m+1-k} \\
&= \sum_{k=1}^{m}\binom{m}{k-1} z_1^k z_2^{m+1-k} + z_1^{m+1}
\end{aligned}
$$

Note that in the last operation we explicitly did the very last summation to reduce the summation back from k to m.

Then we can take the sum we didn't shift as

$$
\sum_{k=0}^{m}\binom{m}{k} z_1^k z_2^{m+1-k} = z_2^{m+1} + \sum_{k=1}^{m}\binom{m}{k} z_1^k z_2^{m+1-k}
$$

Putting these back together we get

$$
(z_1 + z_2)^{m+1} = z_2^{m+1} + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right] z_1^k z_2^{m+1-k} + z_1^{m+1}
$$

One more thing to note, is that the binomial coefficients met the following recurrence relation

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Note that

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

and

$$\binom{n}{k-1} = \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!}{(k-1)!(n-k+1)(n-k)!}$$

So

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= n!\left[\frac{1}{k(k-1)!(n-k)!} + \frac{1}{(k-1)!(n-k+1)(n-k)!}\right] \\
&= n!\left[\frac{n-k+1}{k(k-1)!(n-k+1)(n-k)!} + \frac{k}{k(k-1)!(n-k+1)(n-k)!}\right] \\
&= n!\left[\frac{n-k+1+k}{k(k-1)!(n-k+1)(n-k)!}\right] \\
&= n!\left[\frac{(n+1)n!}{k(k-1)!(n-k+1)(n-k)!}\right] \\
&= \frac{(n+1)!}{k!(n-k+1)!} \\
&= \binom{n+1}{k}
\end{aligned}$$

Using this result, we can rewrite our previous sum as

$$\begin{aligned}
(z_1+z_2)^{m+1} &= z_2^{m+1} + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right] z_1^k z_2^{m+1-k} + z_1^{m+1} \\
&= z_1^{m+1} + z_2^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k} z_1^k z_2^{m+1-k}
\end{aligned}$$

Now the magic is in seeing that the 2 stragglers are the "endpoint" terms of a binomial expansion: think how $(x+y)^2 = x^2+2xy+y^2$, the first and last term are raised to the n-th power of the binomial expansion and have a coefficient of 1 (and this pattern is seen in all such expansions). This means we can start the sum at $k=0$ by including z_1^{m+1} and end the sum at $m+1$ by addinf the z_2^{m+1} term, thus

$$(z_1+z_2)^{m+1} = \sum_{k=0}^{m+1}\binom{m+1}{k} z_1^k z_2^{m+1-k}$$

3 Modular Arithmetic

3.1 Modular Arithmetic

If $a|b$, then $b = ac$, for some integer c. That means that b/a must be an integer.

If n and d are positive integers, how many positive integers not exceeding n are divisible by d?

In order to be divisible by d, an integer must be of the form dk, for some positive integer k. So the integers divisible by d and not greater than n are the integers with k such that $0 \leq dk < n$ or $0 < k < n/d$. Thus, the number of integers divisible by d is $\lfloor n/d \rfloor$.

Theorem describing the transitive properties of division:

$$\text{If } a|b \text{ and } a|c, \text{ then } a|(b+c) \tag{3.1}$$

To prove this use the fact that $a|b$ means that $b = as$, $a|c$ means that $c = at$, and $b + c = a(s + t)$. Hence $a|(b + c)$.

$$\text{If } a|b, \text{ then } a|bc, \text{ for } c \in \mathbb{Z} \tag{3.2}$$

To prove it use the fact that $a|b$ means $b = as$, so $b * c = as * c$.

$$\text{If } a|b, \text{ and } b|c, \text{ then } a|c \tag{3.3}$$

To prove it use $b = as$, $c = bt$. Then $c = bt = ast$ and hence $a|c$.

Corollary: If a, b, and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|mb + nc$ whenever $m, n \in \mathbb{Z}$.

Use if $a|b$ and $a|c$, then $a|(b + c)$ and if $a|b$, then $a|bc$, for $c \in \mathbb{Z}$, to prove it.

3.1.1 Division Algorithm

- If $a = dq + r$ where $0 \leq r < d$ and $d > 0$
- $q = a \text{ div } d = \lfloor a/d \rfloor$
- $r = a \pmod{d} = a - dq$

For example, when 101 is divided by 11, $11|101$

$$101 = 11\dot{9} + 2$$

When -11 is divided by 3, $3| - 11$

$$-11 = 3\dot{-}4 + 1$$

3.1.2 Congruences

If a and b are congruent modulo m ($a, b \in \mathbb{Z}, m > 0$), $a \equiv b \pmod{m}$, then m divides $a - b$. Another way of seeing it is that a and b have the same remainder when divided by m.

If m divides $a - b$, then $a - b = mc$ for some integer c.

If both a and b have the same remainders when divided by m, then: $r = a - mq$ $r = b - mp$ $0 = a - mq - b + mp$ or $a - b = mq - mp = m(q - p) = mc$, where $c = q - p$.

The above also means that $a = b + mk$, for some integer k.

Equivalently, $a \equiv b \pmod{m}$ **implies that** $a \pmod{m} = a \pmod{m}$.

Theorem about multiplications and additions in congruences:
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \tag{3.4}$$

and

$$ac \equiv bd \pmod{m} \tag{3.5}$$

To prove these, you can use something like the following reasoning:
$a - b = mp$ and $c - d = mq$ $a + c - (b + d) = m(p + q)$
Since $c = d + mq$

$$ac = (b + mp)(d + mq) = bd + bmq + dmp + mmpq = bd + mc$$

Corollary detailing more forms of addition and multiplication

$$(a + b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m \tag{3.6}$$

To show this,

$a = mk + r = mk + (a \bmod m)$ hence $a \equiv (a \bmod m) \pmod{m}$ and so $b \equiv (b \bmod m) \pmod{m}$ So $a + b \equiv [(a \bmod m) + (b \bmod m)] \pmod{m}$

Because $a \equiv b \pmod{m}$ implies $a \bmod m = b \bmod m$, the above can be written as $(a + b)\text{mod} = [(a \bmod m) + (b \bmod m)] \pmod{m}$.

$$ab \bmod m = [(a \bmod m)(b \bmod m)] \bmod m \tag{3.7}$$

Following a similar logic as in the above proof, we can obtain the former equation by using $ab \equiv [(a \bmod m)(b \bmod m)] \bmod m$.