Notes on Number Theory

November 10, 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 Divisibility

Rosen's "Discrete Mathematics and its Applications"'s chapter 4 along with Gallian's "Contemporary Abstract Algebra" chapter 0 make great references for this material.

An $a \neq 0 \in \mathbb{Z}$ is called a **divisor** of a $b \in \mathbb{Z}$ if there is a $c \in \mathbb{Z}$, such that $b = ac$. We write $a|b$, "a divides b". We also commonly say that "b is a multiple of a".

Note that this working definition means that $a|b$ is an integer. So for example, $3 \not| 7$ since $7/3 \notin \mathbb{Z}$ but $3|12$ since $12/3 \in \mathbb{Z}$.

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 integer $k > 0$. 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, not exceeding n, is $\lfloor n/d \rfloor$.

3.1.1 Properties of Divisibility of Integers

1. If $a|b$ and $a|c$, then $a|(b + c)$ and $a|(b - c)$.
2. If $a|b$, then $a|bc$ for all $c \in \mathbb{Z}$.
3. If $a|b$ and $b|c$, then $a|c$ (transitivity).

To prove the first statement, use the fact that $a|b$ means that $b = as$, $a|c$ means that $c = at$, and $b+c = a(s+t)$. Hence $a|(b+c)$. (Closure under addition of integers.) Since the integers form a ring, $b - c = a(s - t)$, where $s - t \in \mathbb{Z}$.

To prove the second statement, use the fact that $a|b$ means $b = as$, so $b \times c = as \times c$. (Closure under multiplication of integers.)

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

Corollary: If $a.b, c \in \mathbb{Z}$, where $a \neq 0$,and $a|b$ 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.

3.1.2 Division Algorithm

- If $a = bq + r$ where $0 \leq r < b$ and $b > 0$

- $q = a \text{ div } b = \lfloor a/b \rfloor$ (quotient)
- $r = a \pmod b = a - bq$ (remainder)

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

$$101 = 11 \cdot 9 + 2$$

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

$$-11 = 3 \cdot -4 + 1$$

Note how we are multiplying $3 \cdot -4$. This is so that our remainder, r, mets the criteria of $0 \leq r < b$.

In Gallian's "Contemporary Abstract Algebra", the division algorithm is stated as follows: let a and b be integers with $b > 0$. Then there exists unique integers q and r with the propperty that $a = bq + r$ and $0 \leq r < b$.

The proof begins with the existence portion of the theorem where it considers a set $S = \{a - bk : k \in \mathbb{Z}, a - bk \geq 0\}$.

If $0 \in S$, then b divides a $(b|a)$, and so $q = a/b$ and $r = 0$.

If we assume $0 \notin S$ $(b \not| a)$, then we will also need to investigate whether S is empty or not. But we can quickly come up with a cases to see that $S \neq \emptyset$ if we assume $0 \notin S$:

1. $a > 0$: if $k = 0$, $a - bk = a \geq 0$.
2. $a < 0$: if $k = 2a$, then $a - bk = a - b(2a) \geq 0$.
3. $a = 0$: here technically we could have some $k < 0$ so that $a - bk = -b(-|k|) \geq 0$. However, in the context of $\lfloor a/b \rfloor$, which is the operation we want to evaluate, this gives us a very trivial case $\lfloor a/b \rfloor = 0$ and it reduce our initial problem to $r = bk$ (except we still haven't introduced r), which is our initial definition of divisibility.

Going through all the possible cases leads us to believe that $S \not\emptyset$ so we can apply the **well ordering principle** which states that every non-empty set of positive integers contains a smallest members. We will call this smallest member of S $r = a - bq$ $(a = bp + r)$. This construction of r also tells us that $0 \leq r$, so now we need to prove that $r < b$ and the uniqueness of r and q (we just proved their existence).

To prove that $b < r$, let's try a proof by contradiction. Assume $r \geq b$, we already know that $a - bq \in S$ is supposed to be the smallest positive integer of our set, so let's look at the next one which is $a - b(q+1) = a - bq - b = r - b \geq 0$ (we used our assumption of $r \geq b$ in the last step). However, $a - b(q+1) < a - bq$, wich leads us to a contradiciton, so we need $r < b$ to have a consistent convention. Let's finally move to proving the uniqueness of q and r.

Let's do another proof by contradition. Let's say we have $a = bq + r$, where $0 \leq r < b$ and $a = bq' + r'$, where $0 \leq r' < b$. For convenience, suppose $r' \geq r$. Then $bq + r = bq' + r'$ and $b(q - q') = r' - r$. The last expression meands that b divides $r' - r$ $(b|r' - r)$, then $r' - r = bu$ for some $u \in \mathbb{Z}$. Also, since $r' \geq r$, then $0 \leq r' - r < r \leq r' < b$. To reach the conclusion we need to look back: if $r' - r$ were a non-zero positive integer, then it would mean that $q - q'$ is also a non-zero integer, so that $bq \neq bq'$, and thus either r or r' would not be the smallest member of S. But if $r' - r = 0$, then we achieve consistency all around.

3.2 Congruences

If a and b are congruent modulo m $(a, b \in \mathbb{Z}, m > 0)$, $a \equiv b \pmod{m}$, if m divides $a - b$ (written another way, $m|a - b$).

The above does not yet tell is much, there is another theorem we need: let $a, b, m \in \mathbb{Z}$ and $m \geq 0$. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$ (**if the remainders are equal!**).

Another way of seeing it is that a and b have the same remainder when divided by m, goes as follows: If m divides $a-b$, then $a-b = mc$ for some $c \in \mathbb{Z}$. If both a and b have the same remainders when divided by m, then $r = a - mq$ and $r = b - mp$. In turn $a-b = (mq-r)-(mp-r) = mq-mp = m(q-p) = mc$ (we have consistency once again).

The above also means that

$$a \equiv b \pmod{m} \leftrightarrow a \bmod m = b \bmod m \leftrightarrow a = b + mc$$

The thing to keep in mind is that congruences are binary relations: is $17 \equiv 5 \pmod{6}$? yes, because $6|17 - 5$ $(17R5)$. Does $6|17 - 6$? No, so $17 \not\equiv 6 \pmod{6}$ $(17\not R6)$. Whereas the other two equivalences give us ways to compute and further understand the relation.

3.2.1 Modular Arithmetic

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \tag{3.1}$$

and

$$ac \equiv bd \pmod{m} \tag{3.2}$$

To prove these, you can use something like the following reasoning:
$a-b = mp$ and $c-d = mq$. Adding these two, we get $a+c-(b+d) = m(p+q)$.
For the second one, since $c = d + mq$

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

Corollary detailing more forms of addition and multiplication

$$(a+b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m \tag{3.3}$$

To show this, $a = mk + r = mk + (a \bmod m)$ hence $a \equiv (a \bmod m) \pmod m$ (a and $a \bmod m$ are congruent). Similarly, $b \equiv (b \bmod m) \pmod m$ (b and $b \bmod m$ are congruent) 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 $(a+b) \bmod = [(a \bmod m) + (b \bmod m)] \pmod m$.

$$ab \bmod m = [(a \bmod m)(b \bmod m)] \bmod m \tag{3.4}$$

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

3.2.2 Arithmetic Module m

The reason for the above complexities is because it just so happens that it is useful and informational to define arithmetic operations on the set of non-negative integers less than m because they form a **commutative ring** which we denote as $\mathbb{Z}_m$.

For example, addition in $\mathbb{Z}_m$, looks like

$$a + b = (a + b) \bmod m$$

And in the previous subsection we saw an algorithm to crank out the result.

Similarly, multiplication in $\mathbb{Z}_m$, looks like,

$$ab = (ab) \bmod m$$

Note: the reason we mentioned that $\mathbb{Z}_m$ is a commutative ring is to help you remember that multiplicative inverses don't always exist in $\mathbb{Z}_m$.

Also, note that these definitions of additiona and multiplication are equivalent to $a + b \equiv c + d \pmod m$ and $ac \equiv dc \pmod m$. For example, the multiplicative inverse can be written as $ab = ab \bmod m = 1$ or $ab \equiv 1 \pmod m$ and the additive inverse can be written as $a+b = (a+b) \bmod = 0$ or as $a+b \equiv 0 \pmod m$.

It is worth expanding on why we have a ring and why the multiplicative inverse may sometimes not exist in a ring based on modular arithmetic.

We are essentially looking for a number b such that when a given a is multiplied by it, the result will be one, $ab = ab \bmod m = 1$ or $ab \equiv 1 \pmod m$.

First, let's see a case where it does not exist, 2 mod 6:

- $2 \cdot 0 = 0 \bmod 6 = 0$
- $2 \cdot 1 = 2 \bmod 6 = 2$

- $2 \cdot 2 = 4 \bmod 6 = 4$
- $2 \cdot 3 = 6 \bmod 6 = 0$
- $2 \cdot 4 = 8 \bmod 6 = 2$
- $2 \cdot 5 = 10 \bmod 6 = 4$
- $2 \cdot 6 = 12 \bmod 6 = 0$

and so on. Maybe this gives you a rough idea of what the issue maybe. Let's look at our general formula $ab\text{mod} = 1$ once again. We know that this formula implies that $ab = mk + 1$ or $ab - mk = 1$. This last expression tells us that in order to get a multiplicative inverse we need to be able to add to Products of integers in such a way as to end up with a sum of one (hard to do that when you are dealing with 2 even numbers such as 2 and 6).

3.3 Primes and Greates Common Divisors

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

The proof is by contradiction: if n is composite, then $n = ab$. The negation of one prime divisior less than or equal to $\sqrt{n}$ means that all divisors are greater than $\sqrt{n}$, which means $n = ab > \sqrt{n}^2 = n$, leading to a contradition.

The prime number theorem the ratio fo the number of primes not exceeding x and $x/\ln(x)$ approaches 1 as x grows without bound.

The theorem was first proved by Jacques Hadamard and Charles-Jean-Gustave-Nicholas de la Valle-Poussin in 1986 using the theory of complex variables.

The odds of randonly selecting a positive integer less than n that is prime is approximately $(n/\ln(n))/n = 1/\ln(n)$.

The greatest commmon divisor let $a, b \in \mathbb{Z}$, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisior or a and b.

On the otherhand, the **least common multiple** is the smallest positive integer that is divisible by a and b ($a|lcm$ and $b|lcm$).

A simple way to compute these two values is by looking at the prime factorization of two numbers a and b,

$$a = p_1^{a_1} p_2^{a^2} p_3^{a_3} \dots p_n^{a_n}, \quad a = p_1^{b_1} p_2^{b^2} p_3^{b_3} \dots p_n^{b_n}$$

Then,

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

and,

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

From here we can also see that $ab = gcd(a, b) = lcm(a, b)$.

3.3.1 The Euclidean Algorithm

Let's look for more efficient ways to find a greatest commmon divisor. Let's say that we have an $a, b, d \in \mathbb{Z}$ and we want to find $d = \gcd(a, b)$.

So we first divide a by b

$$a = b \cdot q + r$$

Note that if we rewrite the above a tad, we get $r = a - bq$. By property (2), if $d|b$, then $d|bq$. Now the remainder is the difference of two integers whose divisor is d, this should make you think about propoerty (1) which says that if $d|(a - bq)$. In other words, **the d is also a divisor of the remainder r**.

Note: there is a very good argument describing this in chapter 3, section 7, starting on page 160 of Data Structures with C++ using STL second edition by William Ford and William Topp.

Now, let's say that we had another common divisor, this time let's call it e. If e were a common divisor or r and b, then e would be a common divisor of a as well - propoerty (1) and $a = bq + r$ together. This means that $d = e$ or $\gcd(a, b) = \gcd(r, b)$.

One thing to note here is that this process works great when $a > b$. In such a case, we keep replacing the largest of the two numbers by the remainder when dividing it by the other number. This process keeps going until we reach the operation $\gcd(s, 0)$. In such a case, we are looking for an integer x, such that $0 = xt_1$ and $s = xt_2$. Since the division algorithm requires $x > 0$, then $x = s$ is the largest number dividing 0 and s.

Finally, not that if $a = b$, then $\gcd(a, b) = \gcd(a, a) = \gcd(a, 0) = a$, since the remainder of a/a is zero. And if $a < b$, then the remainder $a\%b = a$, so we are back to the previous instance of $\gcd(a, b) = \gcd(a, a) = \gcd(a, 0) = a$

3.3.1.1 Runtime of the Euclidean Algorithm The following is an addendum to a discussion in Section 1.2 "Divisibility and Greatest Common Divisors" presented in "An introduction to mathematical Cryptography".

The claim presented is that the runtime of the Euclidean algorithm is $\log_2(b) + b$, where b is the smaller of the two integers in $\gcd(a, b)$.

We know that the r_i values are nondecreasing since the division algorithm guarantees us that $0 \leq r_{i+1} < r_i$. Then the claim we investigate is that after two iterations, the value of r_i is at least cut in half: $r_{i+2} \leq \frac{1}{2} r_i$.

Since our claim is about what happens every two iterations, we still want to investigate what happens every iteration, which leaves us with the two cases of $r_{i+1} \leq \frac{1}{2} r_i$ and $r_{i+1} > \frac{1}{2} r_i$. Both cases possible since we only have a guarantee that $0 \leq r_{i+1} < r_i$.

For the case of $r_{i+1} \leq \frac{1}{2}r_i$, we would have $0 \leq r_{i+1} \leq \frac{1}{2}r_i < r_i$, based on the division algorithmn and this specific case we are exploring. Then on the next iteration, we would have $0 \leq r_{i+2} < r_{i+1}$, and when we our case we get $0 \leq r_{i+2} \leq \frac{1}{2}r_{i+1} < r_{i+1} \leq \frac{1}{2}r_i < r_1$. Which simplifies to what the book says, $0 \leq r_{i+2} < r_{i+1} \leq \frac{1}{2}r_i$.

The argument for the second case is misleadingly clever. Since $r_{i+1} > \frac{1}{2}r_i$, then we can only divide r_i by r_{i+1} no more than once, that is, the quotien in $r_i = r_{i+1} \cdot q + r_{i+2}$ must be 2, otherwise $r_{i+2} > r_{i+2}$, contradicting the division algorithm's promise that $0 \leq r_{i+1} < r_i$.

4 Abstract Algebra

4.1 Preliminaries

4.1.1 Division Algorithm

UPC example: Correct code is $a_1a_2a_3a_4a_5$, incorrect code is $a_2a_1a_3a_4a_5$. So correct check digit is $(3a_1 + a_2 + 3a_3 + a_4 + 3a_5)$ mod 10. Incorrect check digit is $(3a_2 + a_1 + 3a_3 + a_4 + 3a_5)$ mod 10.

If x mod 10 and y mod 10 are equal, then $x \equiv y \pmod 1 0$, which implies that $x - y = 10k$.

Error won't be caught is $(3a_1+a_2+3a_3+a_4+3a_5)-(3a_2+a_1+3a_3+a_4+3a_5)$ is a multiple of 10. The above simplifies to $[3a_1 \bmod 10 + a_1 \bmod 10 + \cdots - 3a_2 \bmod 10 - a_1 \bmod 10 - \ldots]mod10$. Which can be simplified to $3a_1 \bmod 10 + a_1 \bmod 10 - 3a_2 \bmod 10 - a_1 \bmod 10] \bmod 10$. Or $(3a_1+a_2-3a_2-a_1) \bmod 10 = 0$. Which means $(2a_1 - 2a_2) \bmod 10 = 0$. No error caught if $a_1 - a_2$ is a multiple of $10/2 = 5$ same as writing $|a_1 - a_2| = 5$.

GCD is a linear combination

Since $S = am + bn : am + bn > 0$. Well ordering axiom says there must exist a d s.t. $d = as + bt$. Claim is that d is also $\gcd(a, b)$ meaning that $a = dq + r$ where $0 \leq r < d$. If $r = 0$: then r is not in S, and we have no member in S smaller than d. If $r > 0$: then any linear combination that was equal to r would have r in S and because $0 \leq r < d$, it would be smaller than d, leading to a contradiction.

Euclid's lemma

If p is a prime, and if p does not divide another integer a, then it means that $a \neq pu$ (no common factor). And since a prime only has 1 and itself as divisors (factors), then the only other possibility is 1. Hence p not dividing $a \geq \gcd(p, a) = 1$. if $p|ab$: $ab = pc$, for some integer c. Thus, $b = abs + ptp = pcs + ptb$.