BASIC NUMBER THEORY

Masum Billal

October 11, 2016

Preface (2016 Edition)

This is an edited version of a note I wrote in $2010-2011$ (approximately). The primary objective was not to write a note though. I used to write something everyday as a habit of practicing LaTeX, specially when I learned about a new feature. The end result was this note. For that reason, you can see that the original document structure (I lost the source file of that one, so I re-wrote it) is quite clumsy. Also, some topics seem random and not really connected to the main topic. I am keeping them here anyway since they may be useful after all.

The note was primarily intended for BdMO math campers. However, it may be useful for any newcomer looking for interesting problems and ideas to solve them. It should be mentioned that, this is not a textbook. And you should not use it as a reference for something rigorous such as definitions. The reason is that, I have focused more on making the sense rather than stating something rigorous that makes less sense. Moreover, I could not write too much at that time and even though I am writing it now, I hardly have the time to improve it or add more to it. You can see the references section for further reading.

I want to take this chance to clear something up. From my personal experience, I have seen most of the beginners try to learn lots of theorems in order to be able to solve problems. They do this mostly as a mean of shortcut. I have tried a lot to change that thinking among the students. But it has become a tradition to follow that one must know thousands of theorems so everyone calls you master of number theory. There are two things to mention here. One is that you can never become a master of number theory. Second is that, even though the word `theory` is juxtaposed with **Number Theory**, by no means it implies that you must know a lot of theorems.

With that said, after you are done with this book, you may think that I am being two faced here. Therefore, I will explain it more. At first I have tried to show why you should solve problems as if you know nothing. That means, you will solve everything right from the start without any heads up. Once you think that you are at the point where you can find theorems or lemmas associated with a problem to solve, you will know what I mean. After that, you are ready to read about any book in number theory (though it depends on the pre-requisite of that book). The point is that, you should realize, we use theorems just to speed up our thinking process and save the time of doing the same thing twice all over again. We should not use theorems to actually solve problems. That is the reason why there is no choice but to discuss theorems when we talking about number theory. But this does not imply in any way that theorem is the core of number theory. It only means that we will study how the numbers dance and develop interesting properties. Although this is my personal opinion, I have found it to be true practically that, if you use theorems as means of solving problems rather than spending the time to gain your

intuitive maturity, you can not solve problems beyond a certain level (roughly saying, I do not intend to argue about level of problems or anything). I hope you get my point. Even if you don't, it will not matter to me. But it will matter to me a lot if someone tries not to use theorems to make sense of something.

Since this note was not reviewed or edited by anyone else, it may contain errors. One may find the definitions or some proofs too informal, but that is precisely the reason of creating this document. So, please do not brag about formality in this regard. Making better sense of something is more important to me than stating something that does not make a whole lot sense.

Finally, I would like to mention that you can use or distribute it however you like as long as you don't use it for financial gain. Feel free to email me for making this better or if you want to be a contributor.

Masum Billal
October 10, 2016

1 Divisibility

Note the following division of 97 by 24.

$$97 = 4 \cdot 24 + 1$$

In this division, we call 4 the *quotient* (the result of the division) and 1 the *remainder* (the part which was left) of this division. For the division $96 = 244 + 0$ we have the remainder 0. In this case, we say that 96 is divisible by 24 (so by 4 as well).

Definition 1. Let a and b be two natural numbers such that b leaves remainder 0 upon division by a. Then b is said to be divisible by a. We denote it by $a|b$.

Sometimes, the notation $b \vdots a$ is also used. But in this note, we shall make use of the notation of $a|b$ mostly.

Here, a is called a *divisor* or *factor* of b and b is called a *multiple* of a. If b leaves a remainder other than 0, then b is not divisible by a and is denoted by $a \nmid b$. Moreover, unless stated explicitly, we usually assume the associated integers are positive integers.

Example. $7|343$, 565655 is a multiple of 5, 29 is a divisor of 841 and so on.

Try some more examples and make sure with the notations and definitions of divisibility. Because your further reading of this note requires this excellency.

Definition 2 (Prime and Composite)**.** A natural number n is *prime* if it has exactly 2 positive divisors. Any positive integer that has more than 2 positive divisors is a *composite number*.

You may notice that this definition is a bit different from what you know. But this definition clears up the ambiguity that keeps going around regarding 1: is 1 a prime or not?

Example. 2 is the only even prime. If an even number is greater than 2, then it must be divisible by 2. Thus, it can not be a prime. First 3 odd primes are $3, 5, 7$.

1.1 Parity

Definition 3. If a number leaves remainder 0 upon division by 2, then it is *even*. If it leaves the remainder 1, then it is *odd*. The property of a number being even or odd is called *parity*. Two numbers are of the same parity if they both are odd or both are even. Otherwise they are of opposite parity. In other words, if two numbers give same remainder upon division by 2, they are of the same parity, otherwise they are of opposite parity.

Example. 5 and 7 are of the same parity, whereas 4 and 3 are not.

Proposition 1. *The following statements are true.*

i. The sum and difference of two numbers of the same parity is even.

ii. The sum and difference of two numbers of different parity is odd.

iii. Increasing or decreasing a number by a multiple of 2 does not change the parity.

iv. Any odd multiple of a number has the same parity of the number, and for even multiple has a parity even.

v. The parity remains unchanged after raising to a power.

Problem 1. The difference of two odd numbers is divisible by 2 but not by 4. Prove that their sum is divisible by 4.

How do we proceed to solve this? Since this involves divisibility by 2, we should at least give parity a try. Here are two solutions.

Solution (1)**.** We have to take two odd number. So let us do the most obvious thing and assume that $2a+1$ and $2b+1$ are two odd numbers. From the condition, $2a+1-(2b+1) = 2(a-b)$ is not divisible by 4. This tells us that $a-b$ is odd. In that case, $a-b = 2x+1$ for some integer x. We are required to show that $a+b$ must be divisible by 4.

$$\begin{aligned} a+b &= 2a+1+2b+1 \\ &= 2(b+2x+1)+1+2b+1 \\ &= 4b+4x+4 \\ &= 4(b+x+1) \end{aligned}$$

This is certainly divisible by 4.

Solution (2)**.** What would be a good alternative approach to prove this claim? Since we need to prove some divisibility regarding 4, we should consider what happens when we divide odd numbers by 4. And not very surprisingly we find that an odd number is either of the form $4k+1$ or of the form $4l+3$. Therefore, we have three cases.

(a) Both odd numbers are of the form $4k+1$. However, this can not hold. The reason is that this would imply their difference is divisible by 4 since $4k+1-(4l+1) = 4(k-l)$.

(b) Both odd numbers are of the form $4k+3$. Same argument shows that this can not be true as well.

(c) We are only left with the option where one is of the form $4k+1$ and the other is of the form $4l+3$. This indeed complies with the condition of the statement since $4k+1-(4l+3) = 2(2k-2l+1)$ and $2k-2l+1$ is odd. And if we sum them now, $4k+1+4l+3 = 4(k+l+1)$ is found to be divisible by 4.

A clever reader would ask themselves, how do we jump to the third case without checking the first two manually? This kind of thinking can lead you to direct and better solutions, whereas others may find some tedious solutions.

Proposition 2. *Let a and b be two positive integers.*

i. *If $a|b$, then $\frac{b}{a}$ is an integer. So, there is an integer k such that $\frac{b}{a} = k$ or $b = ak$. Moreover, we can say that $k|b$.*

ii. *For any integer a, $a|a$ and $a|0$.*

iii. *If $0|a$ then a must be 0.*

iv. *If we assume that $a|b$ then $|b| \geq |a|$ where $|a|$ denotes the absolute value of integer b.*[1]

v. *The above claim is not entirely true. The only exception is that $b = 0$.*

vi. *Let c be an integer such that $a|c$. If $a|b$ holds true as well, $a|b \pm c$.*

vii. *The above proposition can be generalized. If $a|b$ and $a|c$ then for any two integers x, y we have $a|bx+cy$.*

Euclid's Lemma *If p is a prime and a, b are positive integers such that p divides ab, then at least one of $p|a$ or $p|b$ must be true.*

viii. *The least positive remainder in a division is unique.*

If $a|b$, then it must leave a remainder other than 0. Say, it is r. Then, $b-r$ would be divisible by a. Let

$$b - r = aq \iff b = aq + r$$

When we mention such a remainder r, we usually mean the least positive remainder. To explain this, take the example $23 = 5 \cdot 4 + 3 = 5 \cdot 3 + 8$. So technically both 3 and 8 are remainders. But 3 is the least positive remainder

[1] This claim has a flaw in it. Find it!

when 23 *is divided by* 5*. Moreover, notice that the least positive remainder is less than the dividing number.*

What the proposition says is that, for positive integer a, b *there are unique integer* q *and a unique positive integer* r *such that* $b = aq + r$ *and* $0 \leq r < a$*. We can prove this easily as well. And the uniqueness of* r *can prove the uniqueness of* q *as well (and vice versa). For the sake of contradiction, suppose that,*

$$b = aq_1 + r_1 = aq_2 + r_2$$

where both $0 \leq r_1, r_2 < a$*. From the latter, we get*

$$a(q_1 - q_2) = r_2 - r_1$$

This equation says that a *divides* $r_2 - r_1$*. Unless* $|r_2 - r_1| = 0$*, this can not be true (why?). The conclusion follows.*

ix. For all composite $n > 1$*,* n *has a prime divisor* p *such that*

$$p \leq \sqrt{n}$$

First you should think for yourself why this has to be true. Actually, no. First you should think if this is even true at all or I am playing with you. After you play around with some examples and convince yourself that this might actually be true, only then you can work on proving it. And this goes for all problems in general. Take $n = 12$ *and* $n = 35$*. They have prime divisors* 2 *and* 5*. Take some more and you should realize why this must be true.*

Assume that the smallest prime factor of n *is* p*. Then* $n = pk$ *for some* $k \geq p$*. If* $k < p$*, then* k *would have at least one prime factor less than* p*, but that is not possible. Therefore,* $k \geq p$*. Then*

$$\begin{aligned} n &= kp \\ &\geq p^2 \\ \iff p &\leq \sqrt{n} \end{aligned}$$

Using this property, we can determine whether a number is a prime or not. Though this is not an efficient approach at all, it is very useful for small numbers.

2 GCD-LCM

Take the numbers 18 and 12 and consider their divisors. The list of their divisors is

$$\{1,2,3,6,9,18\},\{1,2,3,4,6,12\}$$

Since 1 belongs to both list, we will have at least one element common. But is there any other common element? In this case we have $1,2,3,6$. The greatest one among these common divisors is 6. We call 6 the *greatest common divisor* of 12 and 18. We denote the greatest common divisor of a and b by $\gcd(a,b)$ or shortly (a,b). In this note, we shall use this notation for brevity. When $(a,b)=1$ that is two numbers do not have a common divisor other than 1, then a is called to be co-prime or relatively prime with b and is denoted by $a\perp b$.

Example. $(6,28)=2$, because 2 is the most common part among them. $56\perp 243$, since $56=2^3\cdot 7$ and $243=3^5$ do not share any common factor other than 1.

Can you prove that it must be unique for any two positive integer? *Least common multiple* follows from the idea of greatest common divisor. Both a and b have infinite multiples namely

$$a\cdot 1, a\cdot 2,\cdots$$
$$b\cdot 1, b\cdot 2,\cdots$$

For example, the multiples of 12 are $12,24,36,\ldots$ The multiples of 18 are $18,36,\ldots$. Now, an analogous question to greatest common divisor would be, is there a multiple of 12 that is a multiple of 18 as well? Well, the answer is simple. Yes, $12\cdot 18$. Ok, but this makes us ask something not so obvious. What is the smallest possible positive integer that is a multiple of both 12 and 18? We know that such a multiple exists but the product of those two positive integers may not be the one we are looking for. In this case, $12\cdot 18=216$ but as we can see, 36 is the number with the desired property. We call 36 the least common multiple of 12 and 18. It is denoted by $\operatorname{lcm}(a,b)$ or shortly $[a,b]$ sometimes.

Definition 4. $\gcd(a,b)$ is the greatest positive integer that divides both a and b. $\operatorname{lcm}(a,b)$ is the least positive integer that is divisible by both a and b.

References

[1] *Arthur Engel*, Problem-Solving Strategies (Chapter 6), 1998 Springer-Verlag New York, Inc.

[2] *Paul Zeitz*, The Art and Craft of Problem Solving (Chapter 7), John Wiley & Sons, Inc.