Number theory

Hamad Khan

July 2020

1 Introduction

These are my number theory notes. I am studying from both the Silverman book and the Ireland, Kenneth and Ross book

2 Division rules and their proofs

1. $a \mid b \Rightarrow a \neq 0$
2. $a \mid b$ and $b \mid a \Rightarrow a = \pm b$
3. $a \mid b$ and $b \mid c \Rightarrow a \mid c$
4. $a \mid b$ and $a \mid c \Rightarrow a \mid (b + c)$

2.1 Result 1

Proof. Result 1 follows trivially from the fact that we exclude division by zero. If $a \mid a$ then that means that $a \neq 0$ by definition.

□

2.2 Result 2

Result 2 comes from the following.

Proof. Consider $a \mid b$. This simply means that $b = ac$ for some $c \in \mathbb{Z}$, likewise $b \mid a$ simply means that $a = bs$ for some $s \in \mathbb{Z}$

$b = ac$ and $a = bs \Rightarrow a = (ac)s \Rightarrow \frac{1}{c} = s = c^-1$
Then this implies $\frac{1}{sc} = 1$ since $cs = 1$
We multiply by c on both sides giving

$$\frac{c}{sc} = c \Rightarrow \frac{c}{s} = c \Rightarrow s \mid c \Rightarrow s = kc$$

for some $k \in \mathbb{Z}$
However since $s = c^{-1}$ we have

$$s = ks^{-1} \Rightarrow s^2 = k \Rightarrow s = \pm\sqrt{k}$$

But we know that

$$c = s^{-1} \Rightarrow c = \frac{1}{\pm\sqrt{k}}$$

And from $s = kc \Rightarrow \frac{s}{c} = k$ we have

$$\frac{\pm\sqrt{k}}{\pm\sqrt{k}} = \pm\sqrt{k} \Rightarrow k = 1$$

Finally, we get that $c = \pm 1 = s$ which gives us, after substitution into $b = ac$ and $a = bs$ that $a = \pm b$ $\square$

2.3 Result 3

Proof. We start by recognizing that $a \mid b \Rightarrow b = ac$ and $b \mid c \Rightarrow c = bk$ for some $b, k \in \mathbb{Z}$
Then

$$\frac{c}{k} = b \Rightarrow \frac{c}{k} = ac \Rightarrow c = a(ck)$$

Let $ck = d$
We have

$$c = ad$$

Which is precisely the definition of $a \mid c$ $\square$

2.4 Result 4

Proof. This proof is similar to the third result's proof.

Begin, again, by noting that $a \mid b \Rightarrow b = ac$ and $a \mid c \Rightarrow c = ak$

Again for some $c, k \in \mathbb{Z}$

By adding the two equations we have

$$b + c = ac + ak \Rightarrow b + c = a(c + k)$$

Letting $c + k = d$

We now have $b + c = ad$

Which, again, is precisely the definition of $a \mid (b + c)$

□

3 Factorization into primes

The proof of this fact consists of a few steps.

1) Proving that every integer can be written as a product of primes (use contradiction) - Smallest integer N. Two cases, it's prime or it isn't. Case 1 proves it trivially. Otherwise it is a product of 2 composite numbers m and n. M and n are smaller than N, so they're written as a product of primes. Hence N is a product of primes and is therefore a product of primes. Contradiction.

2) Proving that for $a, b \in \mathbb{Z}, b > 0 \implies \exists q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$

Proof. Consider all integers of the form $a - xb$. Let $r = a - qb$ be the smallest of these integers. If $0 \leq r < b$ does not hold, then by trichotomy, $r \geq b$ must hold.

$$r \geq b \implies a - qb \geq b \implies a \geq b + qb = b(q+1) \implies 0 \geq b(q+1) - a \implies 0 \leq a - b(q+1)$$

Since $b > 0$, we have $0 \leq r < q - b(q + 1)$

This contradicts the minimality of r. Hence $0 \leq r < b$ must hold.

□

3) If $a, b \in \mathbb{Z}$, $\exists d \in \mathbb{Z}$ such that $(a, b) = (d)$ where (x) denotes the ideal of x.

Proof. (We assume $a, b \neq 0$ otherwise this is trivial) Let d be the least element in (a,b). Intuitively, $(d) \subseteq (a, b)$. We now need to show that $(a, b) \subseteq (d)$ so that we can then claim $(a, b) = (d)$.

Consider $c \in (a, b)$. By (2) we know that c can be written as $c = qd + r$ for $b > 0$ and $q, r \in \mathbb{Z}$ under the condition $0 \leq r < d$

r is thus squeezed between 0 and 1. Hence by the inequality r = 0.

$c = qd \in (d)$ since $qd \in (d)$ (The definition of an ideal)

Since both of them are subsets of each other they must be equal. □

4) Given that (a,b) = (d), d is the greatest common divisor.

Proof. Notice that $a \in (d)$ and $b \in (d)$. Hence d is a divisor. Consider any other generic divisor k of (a,b).

$$k \mid (a, b) \implies k \mid ax_1 + bx_2 \implies k \mid (d)$$

$k \mid dx_3$ Let $x_3 = 1$

We have $k \mid d$. □

5) $a \mid bc$ and $(a, b) = d \implies a|dc$ For particular r and s $\in \mathbb{Z}$ we have $ra + sb = d$

Proof. Multiplying through by c gives us

$rac + sbc = dc$. We know that $a \mid bc$ so $a \mid sbc$. And $a \mid rac$ since it contains a. We know that if $a \mid b$ and $a \mid c$ then $a \mid b + c$. hence $a \mid rac + sbc = dc \implies a \mid dc$.

In particular when $d = 1$, we have $a \mid c$ □

6) If p is prime and $p \mid bc$ either $p \mid b$ or $p \mid c$.

Proof. We have two cases. Case 1 where $(p, b) = p$. This gives $p \mid b$. And case 2 where $(p, b) = 1$. In this case by (5) we have $p \mid c$ □

7) $ord_p(ab) = ord_p(a) + ord_p(b)$

Proof. $a = p^{\gamma}c$ and $p^{\alpha}d$

Multiplying the two we get $ab = p^{\gamma+\alpha}(dc)$

This gives $ord_p(ab) = \gamma + \alpha = ord_p(a) + ord_p(b)$ □

8) Now we just have to apply the previous theorems to the following expression.

$$n = (-1)^{\epsilon(n)} \prod_{p} p^{a(p)}$$

Taking the order base q of each side, and recognizing that the order function obeys the same laws as logarithms we get the following

$$ord_q(n) = \epsilon(n) ord_q(-1) + \sum_{p} a(p) ord_q(p)$$

$ord_q(-1) = 0$

Giving

$$ord_q(n) = \sum_{p} a(p) ord_q(p)$$

when $p \neq q$ we have $ord_q(p) = 0$ which means that when $p = q$ we get $ord_q(p) = 1$ since both p and q are primes. And then we're left with $a(q) = ord_q(n)$

Thus the proof of the fundamental theorem of arithmatic is complete.