Number Theory

It is the goal of this work to give the reader a greater grasp of elementary number theory by presenting it in the context of the broader field of abstract algebra. Therefore, before entering into what you might conventionally consider to be elementary number theory, we will examine some of the basic properties of the number systems that we use. Between the comments and the excercises, it is expected that the reader will develop most pertinent results in elementary number theory. However, to make the excercises more challenging and to prevent redundancy, many results will only be seen indirectly, as intermediate results in proving a more difficult theorem, or as "obvious" consequences of some other statement proven. This does not, however, mean that they are not just as important as the other results.

1 Integers

I will assume that you are already sufficiently familiar with what integers are that I do not need to rigorously define them, and instead I will present you with a set of axioms:

Let $\mathbb{Z}$ be the set of integers, and let $+$ and $*$ be two operations taking a pair of integers to an integer. Then:

1. If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$.
2. There exists a unique element 0 such that $a + 0 = a$ for all $a \in \mathbb{Z}$.
3. For each $a \in \mathbb{Z}$, there exists a unique element $(-a) \in \mathbb{Z}$ such that $a + (-a) = 0$.
4. $a + b = b + a$
5. $a + (b + c) = (a + b) + c$
6. If $a, b \in \mathbb{Z}$, then $a * b \in \mathbb{Z}$.
7. There exists a unique element 1 such that $a * 1 = a$ for all $a \in \mathbb{Z}$.
8. $a * b = b * a$
9. $a * (b * c) = (a * b) * c$
10. $a * (b + c) = a * b + a * c$
11. $1 \neq 0$ (this eliminates the case that $\mathbb{Z} = \{0\}$).

Additionally, we assume a few axioms of equality:

1. $a = a$
2. If $a = b$, then $b = a$.
3. If $a = b$, and $b = c$, then $a = c$.
4. If $a = b$, then $a + c = b + c$ and $a * c = b * c$.

It should be noted that these axioms do not uniquely define the integers (the reals immediately come to mind as another set satisfying these axioms). As an excercise, come up with a finite set $S \neq \mathbb{Z}$ satisfying the same axioms.

It is worth pondering what extra condition the integers satisfy that allows us to uniquely define them. We will come back to this later, but first you should prove some of the basic things that we tend to assume about integers, using only the axioms above.

1. $a * 0 = 0$
2. $(-1) * a = -a$
3. $-a * -b = ab$ and $-a * b = -(ab)$
4. $a + b = a + c$ implies that $b = c$
5. Show that, at this point, it is impossible to show that if $ab = 0$, then $a = 0$ or $b = 0$. The easiest way to do this is to give an example of set satisfying the same axioms as those already given for $\mathbb{Z}$, in which $ab = 0$ but $a \neq 0$ and $b \neq 0$. Considering why we can't do this will help explain why we would want to construct the rational numbers, as well as give a better idea of what exactly is missing in our definition of the integers.
6. Prove that a sum/product is equivalent no matter how it is parenthesized (that is, for example, $a + b + c + d = (a + b) + c + d = a + b + (c + d) = (a + b) + (c + d) = (a + b + c) + d = a + (b + c + d) = ((a + b) + c) + d = (a + (b + c)) + d = \ldots$), and additionally that it is equivalent no matter how it is ordered ($a + b + c + d = b + a + c + d = a + c + b + d = c + a + b + d = \ldots$).

The most straightforward way to fix our current conundrum with the integers is to introduce a concept so seemingly obvious as to be often taken for granted: that is, that the integers are ordered. To be more precise, there exists an operator $<$ such that:

1. Exactly one of the following three statements is true: $a < b$,$a = b$,$b < a$.
2. If $a < b$ and $b < c$, then $a < c$.
3. If $a < b$, then $a + c < b + c$.
4. If $a > 0$ and $b > 0$, then $ab > 0$.

From this we should be able to get a bit further. Namely, you should now show, as an excercise, that:

1. $1 + 1 + 1 + \ldots \neq 0$ for any positive number of 1s. While this may seem obvious, it is in fact key, and is not true in the case of the sets you used as counterexamples in earlier excercises.
2. If $a > 0$ and $b < 0$, then $ab < 0$.
3. If $ab = 0$, then either $a = 0$ or $b = 0$.
4. Show that if $a \neq 0$, and $ab = ac$, then $b = c$ (be careful!).
5. $1 > 0$

6. If $a > 0$, and $b > c$, then $ab > ac$.

7. If $a < 0$, then $b > c$, then $ab < ac$.

8. If $a > 0$, then $(-a) < 0$.

Now that we've spent so much time juggling these definitions around, we might as well give a name to what we've been talking about. In fact, any set satisfying the axioms not having to do with ordering is known as a *commutative ring*. Hopefully by now you have constructed some more examples of commutative rings. Commutative rings that are also ordered are known as *totally ordered commutative rings*. Actually, it should be warned that we still have not fully defined the integers, as the reals would just as easily fit all of the above axioms. The final axiom (which will finally uniquely define the integers), is the **well-ordered principle**, which states that any subset of the positive integers has a smallest element (this seems obvious but is impossible to prove from the above axioms, as once again the reals satisfy the above axioms and are certainly not well-ordered). Use this fact to prove that 1 is the smallest positive integer.

As a note, for the rest of this work we will drop the adjective commutative and simply assume that all rings we are working with are commutative unless explicitly stated otherwise.
Many times, we like to work in commutative rings that are either simpler or more complicated than the integers, whatever that is supposed to mean. However, by doing this, we also lose something: namely, in more complicated rings, we tend to lose the condition that our ring is well-ordered. In simpler rings, we tend to lose the condition that our ring is totally ordered. To be a bit more precise about what we mean by complexity, the *characteristic* of a ring is the smallest number such that $1 + 1 + \ldots + 1 = 0$ in that ring (or the characteristic is said to be 0 if this is never true). You will now, as excercises, prove several key facts about rings:

1. Find rings with characteristic 2, 3, 4, and 5.

2. If a ring has a finite number of elements, then its characteristic is not 0

3. For a ring with characteristic $n \neq 0$, under what condition on a can we assert that $b = c$ if $ab = ac$? Show that this equivalently to saying that there exists an element a^{-1} such that $aa^{-1} = 1$. Elements with a multiplicative inverse are called *units*.

4. What are the units for the integers?

5. Prove that the Gaussian integers (all number of the form $a + bi$, where a and b are normal integers) form a ring (you may assume that the integers form a ring, even though we haven't actually proved this yet). Find the units in the Gaussian integers.

6. Show that the product of two units is also a unit.

The reader will be gratified to know that, having spent so much time talking about rings, we will finally actually give a concrete example of a ring (though you should already have at least 4 such examples). In fact, we shall give an infinite class of examples of finite rings: we use the notation $a \equiv b \pmod{n}$ to denote that $n|a - b$. Here $|$ means divides, or more precisely, that there exists c such that $c(a - b) = n$, $c \in \mathbb{Z}$. We can form a ring (called $\mathbb{Z}_n$) by taking all distinct sets of integers such that in each of the sets S, if $a, b \in S$, then $a \equiv b \pmod{n}$. These are called equivalence

classes, and it is important to prove a few things to establish that they are actually equivalence classes (i.e., they satisfy the axioms of equality):

1. $a \equiv a \pmod{n}$
2. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$
3. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

Next you should establish that $\mathbb{Z}_n$ is a ring with characteristic n. You may once again assume that the integers form a ring.

2 Primes

We can extend divisibility a bit further. In an arbitrary ring, $a|b$ means that there exists a c in that ring such that $ac = b$. A *prime* p is a number such that $a|p$ implies that a is a unit or is p times a unit. A *prime factorization* of a number is an expression of a number in the form

$$n = p_1^{e_1} p_2^{e_2} \dots$$

where $p_1, p_2, \dots$ are primes, $e_1, e_2, \dots$ are integers (this is true in an arbitrary ring), and $a^b = a(a^{b-1})$. You are probably already aware that prime factorization is unique down to units in the integers. In fact, this extends to any ring in which **division** holds. Division is the following property:

For any a, p (p need not be prime), there exists unique q and r such that

$$a = pq + r$$

and

$$0 \leq r < p$$

Verify, as an excercise, that the integers have this property.

2.1 Proof of Unique Factorization

3 Fields

We will now diverge from our discussion of rings for a bit in order to visit another set of numbers: the rationals, denoted by $\mathbb{Q}$. They are a commutative ring with one additional axiom: for every $a \in \mathbb{Q}$, except for 0, there exists an element $a^{-1} \in \mathbb{Q}$, with $a^{-1}a = 1$. Additionally, they are totally ordered, and no proper subset of the rationals satisfies the same axioms as the rationals under the same definition of multiplication and addition. This last property is not important for now, but just keep in mind that this is what separates the rationals from the real numbers and complex numbers. Thus, the rationals are almost equivalent to the integers, except that they are not well-ordered, and every rational is a unit. Therefore, anything proven about the integers that does not use well-ordering is also true about the rationals. Additionally, we can offer some new proofs of old results. For these results, you may not use the fact that the rationals are totally ordered:

1. If $ab = 0$, then either $a = 0$ or $b = 0$.

2. Show that if $a \neq 0$, and $ab = ac$, then $b = c$.

Note: We generally denote ab^{-1} by $\frac{a}{b}$.

As you may have guessed from the title of this section, the rationals are a part of a much broader class known as *fields*. A field is a commutative ring in which every non-zero element has a multiplicative inverse. The characteristic of a field is defined identically to that of a ring. Show that:

1. $\mathbb{Z}_p$ is a field for every prime p.

2. If F is a field, then its characteristic is either 0 or prime.

4 Modular Arithmetic

So far, this discussion has been mostly very abstract. The point is to show you that there are many sets with similar algebraic structure to the integers and rationals. For the remainder of this discussion, we will mostly limit our attention to a somewhat limited number of such sets. Aside from the standard sets that we are used to, they are $\mathbb{Z}_n$ and $\mathbb{Z}_p$. Since these are both embedded in the integers (as well as some other sets, as we shall soon see), we can talk about them not only in terms of their own algebraic properties, but in terms of their relation to the sets within which they are embedded. Before going further, however, it will behoove us to list all of the results major that we have proven in general about rings and fields:
Rings:

1. $a * 0 = 0$

2. $(-1) * a = -a$

3. $-a * -b = ab$ and $-a * b = -(ab)$

4. $a + b = a + c$ implies that $b = c$

Fields:

1. If $ab = 0$, then $a = 0$ or $b = 0$.

2. If $ab = ac$, then $a = 0$ or $b = c$.

Thus in particular, in any field an nth degree polynomial will have at most n roots, and they can be found by factoring the polynomial as normal. Additionally, in any mod, it follows from the fact that mods are an equivalence class for a ring that $a \equiv b \implies P(a) \equiv P(b)$ for any polynomial. We can also divide numbers as we please, provided that we are dividing by a unit (which in this case will be numbers relatively prime to the mod). The main caveat is in exponentiating, because $b \equiv c$ does not imply that $a^b \equiv a^c$. To see this break down, note that in mod 5, $2^1 = 2$, and $2^6 = 64 \equiv 4$, but $2 \not\equiv 4$. We can, however, say something about exponentiation in the context of a function known as *Euler's totient function*, sometimes called the phi function because it is denoted by $\phi(n)$. $\phi(n)$ is equal to the number of natural numbers relatively prime to and less than n. The theorem, known as **Euler's totient theorem**, is that for all units a,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

I will also take this opportunity to state another theorem, which is somewhat out of place, but for some reason always appears next to Fermat's theorem (you will see why a bit later). It is known as Wilson's theorem and states that, for all primes p,

$$(p-1)! \equiv -1 \pmod{p}$$

As I said earlier, there is a deep relationship between $\mathbb{Z}_n$ and other rings, as well as $\mathbb{Z}_p$ and other fields. In particular, $\mathbb{Z}_n$ looks somewhat similar to the integers, and $\mathbb{Z}_p$ as well as the set of units in $\mathbb{Z}_p$ (coupled with zero) in general. We generally denote the units of a ring as $U(R)$, R^*, or R^x. To save typing, such notation will implicitly mean that we are also including zero (though I'll let you know right now that this goes against the convention of most math texts). So, in particular, since $\frac{a}{b}$ is well-defined in $\mathbb{Z}_p$, so long as p does not divide b, we can map not only the integers, but the rationals as well, to $\mathbb{Z}_p$. Additionally, we can sometimes even get away with the reals, if we can show that every real we care about is also rational. As an example, here is a theorem that says that A is invertible in $\mathbb{Z}_n$ iff $\det(A)$ is a unit in $\mathbb{Z}_n$. Furthermore, if A is invertible then its inverse is unique (here ι indicates the identity matrix).

We first prove the uniqueness of A^{-1}. Suppose that $AB \equiv \iota$ and $AC \equiv \iota$. Then $AB \equiv AC$, so $BAB \equiv BAC$, so $\iota B \equiv \iota C$, or $B \equiv C$.

We next show that the matrix will be invertible if the determinant is relatively prime to n. We will leave A as it is, and temporarily switch to the reals. In the reals, we can easily invert a matrix provided that its determinant is non-zero (which must be true, since we are assuming that the determinant is non-zero mod n), and each entry will be of the form $\frac{C_{ji}}{\det(A)}$, where C_{ji} is the appropriate cofactor. Observe that C_{ji} will be plus or minus the determinant of some matrix whose elements are all *integers*, and thus will itself be an integer. Similarly, the determinant of A will have as its value some integer that is not divisible by p by assumption. Thus, each element of A^{-1} will be *rational*, and will be of the form $\frac{a}{b}$, where b is relatively prime to n. We now move back to mod n, where $\frac{a}{b}$ has a well-defined counterpart with identical algebraic properties: ab^{-1}. We have thus shown, by example, that matrices with determinants that are invertible in $\mathbb{Z}_n$ will themselves be invertible in $\mathbb{Z}_n$.

Finally, we will show that a matrix with a non-unitary determinant cannot be invertible. This is due to the property that $\det(A)\det(B) = \det(AB)$, which is true in the reals and so must certainly be true in $\mathbb{Z}_n$. If $\det(A) \equiv 0$, and assuming for the sake of contradiction that there exists B such that $AB \equiv \iota$, then $\det(A)\det(B) \equiv \det(\iota)$, but $\det(\iota) \equiv 1$, which implies that $\det(A)$ has a multiplicative inverse (contradicting the fact that $\det(A)$ is not a unit).

For the sake of brevity, I have assumed that the reader is familiar with a bit of linear algebra. The bulk of what is needed can be found here: http://en.wikipedia.org/wiki/Matrix_inversion#Analytic_solution.

5 Finally, some practice problems!

Phew! Now we have finally gotten to something of interest. As such, I will feel justified in giving you some practice problems that stretch your creativity in applying the concepts we have just discussed, rather than deriving new (or not so new) results.

1. $(x+y)^p \equiv x^p + y^p \pmod{p}$
2. If $n = p_1^{e_1} p_2^{e_2} \ldots$, then $\phi(n) = (p_1 - 1)p_1^{e_1 - 1} \ldots$.
3. If p and q are relatively prime, then $\phi(pq) = \phi(p)\phi(q)$.
4. Find the smallest integer, greater than 1, such that $2|n-1$, $3|n-1$, $4|n-1$, $5|n-1$, $6|n-1$, and $7|n-1$.
5. If $n \equiv 2 \pmod{3}$, and $n \equiv 4 \pmod{7}$, then what is the only possible value of n in $\mathbb{Z}_{21}$?
6. Generalize your result to show that if p and q are relatively prime, then if $n \equiv n_1 \pmod{p}$ and $n \equiv n_2 \pmod{q}$, then there is a unique value of n in $\mathbb{Z}_{pq}$ satisfying both equations. This result is known as the **Chinese Remainder Theorem**.
7. Show that there are infinitely many primes (hint: you will want to assume the contrary, then find a number that is relatively prime to every other prime).
8. Show that if $p|n^2+1$, and n is even, then p is 1 more than a multiple of 4, and that, conversely, if p is 1 more than a multiple of 4, then there exists n such that $p|n^2+1$.
9. (USAMO 1998) The sets $\{a_1, a_2, \ldots, a_{999}\}$ and $\{b_1, b_2, \ldots, b_{999}\}$ together contain all the integers from 1 to 1998. For each i, $|a_i - b_i| \in \{1, 6\}$. Show that the last digit of $\sum_{i=1}^{999} |a_i - b_i|$ is a 9.
10. (USAMO 2005) Prove that the system

$$x^6 + x^3 + x^3 y + y = 147^{157}$$
$$x^3 + x^3 y + y^2 + y + z^9 = 157^{147}$$

has no solutions in integers x, y, and z.

11. (USAMO 2006) Let p be a prime number and let s be an integer with $0 < s < p$. Prove that there exist integers m and n with $0 < m < n < p$ and

$$\left\{\frac{sm}{p}\right\} < \left\{\frac{sn}{p}\right\} < \frac{s}{p}$$

if and only if s is not a divisor of $p-1$. (For x a real number, let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x, and let $\{x\} = x - \lfloor x \rfloor$ denote the fractional part of x.)