# Week 1 Summary

## Lecture 1

Number Theory is concerned mainly with properties of integers. In particular, *divisibility* and *factorization* of integers are basic concepts.
If $a$ is any integer and $b$ a positive integer then there are integers $q$ and $r$ such that $0 \leq r < b$ and $a = qb + r$. We call $r$ *the remainder when $a$ is divided by $b$.*
Definitions of the terms *divisor* (or *factor*), *multiple* and *prime number.*
Notation: "$a|b$" (where $a$ and $b$ are integers) means "$a$ divides $b$"—that is, $b = ka$ for some integer $k$.
The so-called Fundamental Theorem of Arithmetic asserts that every integer can be factorized as a product of prime numbers in an essentially unique way. We omit the proof of this.
Definition of the *greatest common divisor* (gcd) of two integers $a$ and $b$. Determination of $\gcd(a, b)$ if the prime factorizations of $a$ and $b$ are known.
Trial and error method for factorizing positive integers: if $a$ is not prime then it has a factor less than or equal to $\sqrt{a}$—try them all! This is obviously very time consuming if $a$ is large.

## Lecture 2

Definition: Integers $a$ and $b$ are said to be *congruent modulo $n$*, written $a \equiv b \pmod{n}$, if and only if $n|(a - b)$.
Students should be able to prove that congruence modulo $n$ is an equivalence relation.
Definition: The *mod $n$ congruence class of $a$* is the set of all integers that are congruent to $a$ mod $n$.
Definition: The *ring of integers modulo $n$*, denoted by $\mathbb{Z}_n$, is a number system created from the ordinary integers by identifying integers that are congruent mod $n$. To say that $a = b$ in $\mathbb{Z}_n$ is the same as saying that $a \equiv b \pmod{n}$. Thus, for example, $\cdots = -7 = -2 = 3 = 8 = 13 = 18 = 23 = \cdots$ in $\mathbb{Z}_5$. That is, $-7$, $-2$, 3, 8 etc. are **different names for the same element** of $\mathbb{Z}_5$.
We say that $b = a^{-1}$ in $\mathbb{Z}_n$ if $ab = 1$ in $\mathbb{Z}_n$. This is the same as saying that $ab \equiv 1 \pmod{n}$.
Proposition (proof examinable): If $a \equiv b \pmod{n}$ then $\gcd(a, n) = \gcd(b, n)$.
This proposition is the basis of the *Euclidean Algorithm* for determining the gcd of two integers $r_0$ and $r_1$ (where, without loss of generality, we assume that $r_0 \geq r_1 \geq 0$). Ir $r_1 > 0$, divide $r_1$ into $r_0$, and let $a_1$ be the quotient and $r_2$ the remainder. That is, $r_0 = a_1 r_1 + r_2$, with $0 \leq r_2 < r_1$. Then $r_2 \equiv r_0 \pmod{r_1}$. So $\gcd(r_0, r_1) = \gcd(r_2, r_1)$. We now have a smaller pair of numbers with the same gcd as the two we started with, and so we have simplified the problem of finding the gcd. Repeat this until one of the numbers is becomes 0. The gcd is then equal to the other number (since $\gcd(a, 0) = a$, if $a \neq 0$).