

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 4.

Please attend the section you enrolled in - the earlier section had too many students attending last week.

The Well Ordering Principle states that every non-empty subset of \mathbb{N}^+ contains a smallest element.

In general, we can use the well ordering principle instead of induction.

We proved the **Division Theorem**: Given two integers a and b with $b \neq 0$, there exists unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

(We say that q is the quotient and r is the remainder when a is divided by b .)

We basically used the proof in the book, except we broke it down by first proving the case $b = 1$ (this case is obvious). Then we proved the case $b > 1$ using the book's approach. Now

$$\begin{aligned} a &= (-b)(-q) + r, & 0 \leq r < |b| \\ \Leftrightarrow a &= bq + r, & 0 \leq r < |b|, \end{aligned}$$

so if b is negative and q, r are the quotient and remainder when a is divided by $-b$, then $-q, r$ give a quotient and remainder when a is divided by b . Moreover this quotient and remainder must be unique, since if we get two (quotient, remainder) pairs for a divided by b , we get two for a divided by $-b$.

We showed that every positive integer a can uniquely be represented in base ten in the form

$$a = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0.$$

We showed that 2 divides $n^2 - n$ for every n .

We showed (again) that every number is a product of prime numbers.

We found the primes up to 60 by using the the sieve of Eratosthenes.

Lemma. *A number p is prime if and only if it is not divisible by any primes q with $1 < q \leq \sqrt{p}$.*

We will prove this by showing that every composite integer $n > 1$ has a prime factor $q \leq \sqrt{n}$. Since n is composite $n = ab$ for some integers a, b with $a, b > 1$. But then one of a and b is less than or equal to \sqrt{n} since otherwise both are greater than \sqrt{n} which implies $ab > n$, and this can't hold since $ab = n$. We can assume $a < \sqrt{n}$. But a has some prime factor q (every number is prime or a product of primes, so certainly has a prime factor). Then $q \leq a \leq \sqrt{n}$ and q divides n .