

Math 100 Spring 2005

1 Some number theory

1.1 Some notation:

$\mathbb{N} = 0, 1, 2, 3, \dots$ (The **natural numbers**)

$\mathbb{Z} = 0, \pm 1, \pm 2, \pm 3, \dots$ (The **integers**)

$\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ (The **rational numbers**)

\mathbb{R} =the **real numbers**

$\mathbb{Z}^+ = \pm 1, \pm 2, \pm 3, \dots$ (The *positive* integers, or **whole numbers**) (also \mathbb{N}^+)

$\mathbb{Q}^+ = \{r \in \mathbb{Q} : r > 0\}$ (The *positive* rational numbers)

$\mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}$ (The *positive* real numbers)

A bit more notation (useful shorthand):

\forall means “for all” or “for every”

\forall is never used in isolation, but together with a *variable*, i.e. $\forall x$ or $\forall n$

\exists means “there exists” or “there is at least one”; also not used alone

Examples:

$\forall x(x = x)$

“For every x , $x = x$ ” (In other words, every number equals itself.)

$\exists n \in \mathbb{Z}(n + 1 = 0)$

“For some integer n , $n + 1 = 0$ ”... but note that it is *not* true that $\exists n \in \mathbb{N}(n + 1 = 0)$

$\forall x \exists y(x < y)$

“For every x there is at least one larger y .”
Note true for $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, etc.

$\exists x \forall y(x < y)$

“There exists an x such that for every y , $y > x$.” This is always false, since no x is bigger than itself.

2 Divisibility and prime numbers

God may not play dice with the universe,
but something strange is going on with the
prime numbers. (Paul Erdős)

For $a, b \in \mathbb{Z}$, say that a *divides* b , or b is *divisible*
by a , if $b = an$ for some $n \in \mathbb{Z}$.

Notation: Write $a|b$ if a divides b

We sometimes say that b is a *multiple* of a , or a
is a *divisor* of b

In the above shorthand:

$$\forall a, b \in \mathbb{Z} (a|b \text{ if and only if } \exists n \in \mathbb{Z} (an = b))$$

Convention: 0 is divisible by everything, but does
not divide anything: $\forall a \ a|0$ but $\forall a \ 0 \nmid a$

Examples: $3|27$, $4 \nmid 10$, $2|$ any even number

1 has only one divisor, 2 has two divisors (1 and
2), 20 has 6 divisors $\{1, 2, 4, 5, 10, 20\}$, 0 has
infinitely many divisors.

Definition 2.1 A natural number $p > 1$ is a prime number provided it is only divisible by itself and 1

In other words,

$$p > 1 \text{ is prime} \iff \forall n(n|p \implies n = 1 \text{ or } n = p)$$

Equivalently, a prime is a natural number with exactly two divisors.

A natural number > 1 which is not prime is called *composite* (or simply *nonprime*).

Examples: 2, 3, 5, 7, 11, 13, 17 are all prime. So is $2^{24036583} - 1$ (this has 7235733 digits, and is a *Mersenne* prime).

Convention 0 and 1 are not prime numbers, but we usually don't call them composite numbers either.

Some important facts about primes:

Euclid's theorem There are infinitely many primes.
(Book IX, Proposition 20)

Fundamental Theorem of Arithmetic Every natural number greater than 1 can be written as the product of primes numbers; moreover, this *prime representation* is unique in

the sense that any other such representation is just obtained by writing the same primes in a different order.

Prime Number Theorem The number of primes between 2 and N is “asymptotically”

$$\frac{N}{\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots + \frac{1}{N}}$$

Equivalently, if P_N is the N^{th} prime, then P_N is asymptotically approximately

$$N \times \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots + \frac{1}{N} \right)$$

Division Algorithm: Suppose a and d are positive integers; then there is a unique $k \in \mathbb{N}$ such that $a = kd + r$ and $0 \leq r < d$.

(a is the *dividend*, d the *divisor*, k the *quotient* of a by d , and r the *remainder*)

Euclidean Algorithm: Later (needs more terminology!)

Some things to look up on your own: Illegal primes, Sieve of Eratosthenes, Primality test, Prime Number Bear