Things to Know from Proofs (and Number Theory)

Charles F. Rocca Jr.

Western Connecticut State University

Outline

- Divisibility (proofs by definition and specification)
- Greatest Common Divisors
- Primes and More Divisibility
- Relations
- Miscellaneous Proofs

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that a *divides* b and write $a|b$ if and only if ...

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that a *divides* b and write $a|b$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that *a divides b* and write $a|b$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Lemma 2 (Linear Combinations)

Given $a, b, c \in \mathbb{Z}$, $c|a$ *and* $c|b$, *if and only if* $\forall x, y \in \mathbb{Z}$ ...

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that *a divides b* and write $a|b$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Lemma 2 (Linear Combinations)

Given $a, b, c \in \mathbb{Z}$, $c|a$ *and* $c|b$, *if and only if* $\forall x, y \in \mathbb{Z}$ $\; c|(ax + by)$.

Proof of Lemma 2

($\Longrightarrow$) If $c|a$ and $c|b$, then $\forall\ x, y,\ \ c|(ax + by)$.

Proof by Definition.

By definition $a = cq_a$ and $b = cq_b$ for some unique q_a and q_b in $\mathbb{Z}$. Therefore,

$$ax + by = cq_a x + cq_b y \tag{1}$$
$$= c(q_a x + q_b y) \tag{2}$$

and by definition of divisibility $\forall\ x, y :\ \ c|(ax + by)$. $\square$

Proof of Lemma 2

($\Longleftarrow$) If $\forall\ x, y,\ c|(ax + by)$, then $c|a$ and $c|b$.

Proof by Specification.

If $x = 1$ and $y = 0$, then $c|a$, and if $x = 0$ and $y = 1$, then $c|b$. $\square$

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that *a divides b* and write $a|b$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Lemma 2 (Linear Combinations)

Given $a, b, c \in \mathbb{Z}$, $c|a$ *and* $c|b$, *if and only if* $\forall x, y \in \mathbb{Z}$ $c|(ax + by)$.

Theorem 3 (Division Algorithm)

Given $a, b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$, *unique, such that* ... *and* ...

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that *a divides b* and write $a|b$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Lemma 2 (Linear Combinations)

Given $a, b, c \in \mathbb{Z}$, $c|a$ *and* $c|b$, *if and only if* $\forall x, y \in \mathbb{Z}$ $c|(ax + by)$.

Theorem 3 (Division Algorithm)

Given $a, b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$, *unique, such that* $a = qb + r$ *and* $0 \leq r < |b|$.

Outline

- Divisibility
- Greatest Common Divisors (proof by Well Ordering Principle)
- Primes and More Divisibility
- Relations
- Miscellaneous Proofs

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The *greatest common divisor of* $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the ...

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The *greatest common divisor of* $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The *greatest common divisor of* $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Axiom 1 (Well Ordering Principle)

In any non-empty set of positive integers . . . .

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The *greatest common divisor of* $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Axiom 1 (Well Ordering Principle)

In any non-empty set of positive integers there exists a least element.

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The *greatest common divisor of* $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Axiom 1 (Well Ordering Principle)

In any non-empty set of positive integers there exists a least element.

Theorem 5 (Bezout's Lemma)

Given $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $d = (a, b)$ *if and only if* ...

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The *greatest common divisor of* $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Axiom 1 (Well Ordering Principle)

In any non-empty set of positive integers there exists a least element.

Theorem 5 (Bezout's Lemma)

Given $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $d = (a, b)$ *if and only if* $\exists x, y \in \mathbb{Z}$ *such that* $d = ax + by$ *and it is the least such positive linear combination.*

Proof of Theorem 5

Proof using the W.O.P. (Part 1).

Let $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $d = (a, b)$, and

$$S = \{ax + by | ax + by > 0 \text{ and } x, y \in \mathbb{Z}\}.$$

Since at least one of a, b, $-a$, or $-b$ must be in S, by the *W.O.P.* we can let c be the least element in S. By the definition of S,

$$\exists\ x, y : \ c = ax + by.$$

Lemma 2 guarantees that $d|c$ and so $d \leq c$. □

Proof of Theorem 5

Proof using the W.O.P. (Part 2).

By theorem 3 we know $a = qc + r$ with $0 \leq r < c$. Now

$$\begin{aligned} r &= a - qc && (3)\\ &= a - q(ax + by) && (4)\\ &= a(1 - qx) + b(-qy). && (5) \end{aligned}$$

If $r \neq 0$, then $r \in S$ and this contradicts the assumption that c was the least element, therefore $r = 0$ and $c|a$. By similar proof, $c|b$.
Since $c|a$ and $c|b$, it is a common divisor so $c \leq d$, and we conclude $c = d$. That is the greatest common divisor is the least positive linear combination. □

Outline

- Divisibility
- Greatest Common Divisors
- Primes and More Divisibility (proof by theorem and of an "or" conclusion)
- Relations
- Miscellaneous Proofs

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if ...

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if p has exactly two divisors, 1 and p.

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if p has exactly two divisors, 1 and p.

Definition 7 (Relatively Prime)

Two integers a, b are *relatively prime* if . . .

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if p has exactly two divisors, 1 and p.

Definition 7 (Relatively Prime)

Two integers a, b are *relatively prime* if $(a, b) = 1$.

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if p has exactly two divisors, 1 and p.

Definition 7 (Relatively Prime)

Two integers a, b are *relatively prime* if $(a, b) = 1$.

Lemma 8 (Products and Divisibility)

If $a, b, c \in \mathbb{Z}$, $c|ab$, *and* $(a, c) = 1$, *then* ...

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if p has exactly two divisors, 1 and p.

Definition 7 (Relatively Prime)

Two integers a, b are *relatively prime* if $(a, b) = 1$.

Lemma 8 (Products and Divisibility)

If $a, b, c \in \mathbb{Z}$, $c|ab$, *and* $(a, c) = 1$, *then* $c|b$.

Proof of Lemma 8

Proof by Theorem.

Assume $c|ab$ and $(a, c) = 1$. By theorem 5,

$$\exists\, x, y : \; 1 = ax + cy,$$

multiplying by b we get

$$b = abx + cby.$$

Since, $c|ab$ and $c|c$ we can write

$$b = c(qx + by),$$

for some unique q. And, so, by definition $c|b$. $\square$

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if p has exactly two divisors, 1 and p.

Definition 7 (Relatively Prime)

Two integers a, b are *relatively prime* if $(a, b) = 1$.

Lemma 8 (Products and Divisibility)

If $a, b, c \in \mathbb{Z}$, $c|ab$, *and* $(a, c) = 1$, *then* $c|b$.

Lemma 9 (Products and Primes)

If $a, b, p \in \mathbb{Z}$, $p|ab$, *and* p *is prime, then* ...

Primes and More Divisibility

Definition 6 (Prime Number)

A natural number p is *prime* if p has exactly two divisors, 1 and p.

Definition 7 (Relatively Prime)

Two integers a, b are *relatively prime* if $(a, b) = 1$.

Lemma 8 (Products and Divisibility)

If $a, b, c \in \mathbb{Z}$, $c|ab$, *and* $(a, c) = 1$, *then* $c|b$.

Lemma 9 (Products and Primes)

If $a, b, p \in \mathbb{Z}$, $p|ab$, *and* p *is prime, then* $p|a$ *or* $p|b$.

Proof of Lemma 9

Proof of an *"or"* conclusion.

Assume that $p|ab$ and p is a prime number.
If $p|a$, then we are done.
If $p \not| a$, then, because p is prime and only has two divisors, $(a, p) = 1$. By lemma 8, we can conclude $p|b$. □

Fundamental Theorem of Arthimetic

Theorem 10 (Fundamental Theorem of Arithmetic)

If $n \in \mathbb{N}$, then n may be written ...

Fundamental Theorem of Arthimetic

Theorem 10 (Fundamental Theorem of Arithmetic)

If $n \in \mathbb{N}$, then n may be written as a product of prime numbers,

$$n = p_1 p_2 p_3 \cdots p_n,$$

which is unique up to order.

Outline

- Divisibility
- Greatest Common Divisors
- Primes and More Divisibility
- Relations (proof satisfying a definition)
- Miscellaneous Proofs

Relations

Definition 11 (Relation)

A *relation* between two sets R and S is a ...

Relations

Definition 11 (Relation)

A *relation* between two sets R and S is a subset of the Cartesian product $R \times S$.

Relations

Definition 11 (Relation)

A *relation* between two sets R and S is a subset of the Cartesian product $R \times S$.

Definition 12 (Equivalence Relation)

A relation between a set R and its self is an *equivalence relation* if ...

Relations

Definition 11 (Relation)

A *relation* between two sets R and S is a subset of the Cartesian product $R \times S$.

Definition 12 (Equivalence Relation)

A relation between a set R and its self is an *equivalence relation* if it is reflexive, $a \sim a$, symmetric, $a \sim b \Rightarrow b \sim a$, and transitive, $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Relations

Definition 11 (Relation)

A *relation* between two sets R and S is a subset of the Cartesian product $R \times S$.

Definition 12 (Equivalence Relation)

A relation between a set R and its self is an *equivalence relation* if it is reflexive, $a \sim a$, symmetric, $a \sim b \Rightarrow b \sim a$, and transitive, $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Definition 13 (Equivalence Classes)

Given an equivalence relation on a set R the *equivalence class of a in R* is the set of ...

Relations

Definition 11 (Relation)

A *relation* between two sets R and S is a subset of the Cartesian product $R \times S$.

Definition 12 (Equivalence Relation)

A relation between a set R and its self is an *equivalence relation* if it is reflexive, $a \sim a$, symmetric, $a \sim b \Rightarrow b \sim a$, and transitive, $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Definition 13 (Equivalence Classes)

Given an equivalence relation on a set R the *equivalence class of a in R* is the set of all elements of R which are equivalent to a.

Modular Relations

Definition 14 (Modular Equivalnce)

Two integers a, b are *equivalent modulo* $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if

...

Modular Relations

Definition 14 (Modular Equivalnce)

Two integers a, b are *equivalent modulo* $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a-b)$.

Modular Relations

Definition 14 (Modular Equivalnce)

Two integers a, b are *equivalent modulo* $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a-b)$.

Theorem 15

Modular equivalence is an ...

Modular Relations

Definition 14 (Modular Equivalnce)

Two integers a, b are *equivalent modulo* $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a-b)$.

Theorem 15

Modular equivalence is an equivalence relation.

Proof of Theorem 15

Proof of Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.

Proof of Theorem 15

Proof of Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
Since $a - a = 0$ and $n|0$, $a \equiv a \pmod{n}$ and modular equivalence is reflexive.

Proof of Theorem 15

Proof of Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
If $a \equiv b \pmod{n}$, by definition $n|(a-b)$, and there exists q such that $(a-b) = qn$. Then, $(b-a) = -qn$, $n|(b-a)$, and $b \equiv a \pmod{n}$. Thus modular equivalence is symmetric.

Proof of Theorem 15

Proof of Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $n|(a-b)$ and $n|(b-c)$.
Hence, $(a-b) = q_0 n$, $(b-c) = q_1 n$, and

$$(a-c) = (a-b+b-c) = (q_0 - q_1)n,$$

i.e. $a \equiv c \pmod{n}$ and modular equivalence is transitive.

Proof of Theorem 15

Proof of Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
Since we have shown that modular equivalence is reflexive, symmetric, and transitive, we may conclude that it is an equivalence relation. □

Modular Relations

Definition 14 (Modular Equivalnce)

Two integers a, b are *equivalent modulo* $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a-b)$.

Theorem 15

Modular equivalence is an equivalence relation.

Theorem 16 (Modular Arithmetic)

Given $a, b, c, d, n \in \mathbb{Z}$ *with* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, ...

Modular Relations

Definition 14 (Modular Equivalnce)

Two integers a, b are *equivalent modulo* $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a-b)$.

Theorem 15

Modular equivalence is an equivalence relation.

Theorem 16 (Modular Arithmetic)

Given $a, b, c, d, n \in \mathbb{Z}$ *with* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$,

$$a \pm c \equiv b \pm d \pmod{n} \text{ and } ac \equiv bd \pmod{n}.$$

Outline

- Divisibility
- Greatest Common Divisors
- Primes and More Divisibility
- Relations
- Miscellaneous Proofs (proof by induction, counter claim, and counter example)

Miscellaneous Proofs

Claim (A False Conjecture)

There exist infinitely many $n \in \mathbb{N}$ such that $n^2 + 4n - 5$ is prime.

Miscellaneous Proofs

Claim (A False Conjecture)

There exist infinitely many $n \in \mathbb{N}$ such that $n^2 + 4n - 5$ is prime.

Counter Claim.

Note that $n^2 + 4n - 5 = (n+5)(n-1)$, if $n = 1$ this is 0, if $n = 2$ this is 7 (which is prime), and if $n > 2$ this is composite. So,

$$\forall n \in \mathbb{N}, \text{ if } n > 2, \text{then } n^2 + 4n - 5 = (n+5)(n-1) \text{ is composite.}$$

Miscellaneous Proofs

Definition 17 (Lots of Ones Sequence)

For $n = 0$ let $a_0 = 12$, and for $n > 0$ let $a_n = 10 \cdot a_{n-1} + 1$, so that

$$a_0 = 12,\ a_1 = 121,\ a_2 = 1211,\ a_3 = 12111,\ \ldots$$

Miscellaneous Proofs

Definition 17 (Lots of Ones Sequence)

For $n = 0$ let $a_0 = 12$, and for $n > 0$ let $a_n = 10 \cdot a_{n-1} + 1$, so that

$$a_0 = 12,\ a_1 = 121,\ a_2 = 1211,\ a_3 = 12111,\ \ldots$$

Theorem 18

For all n the term a_{3n} is divisible by 3.

Miscellaneous Proofs

Proof by Induction.

If $n = 0$, then $a_{3n} = 12 = 3 \cdot 4$, and so by definition $3|a_{3n}$.
Suppose that $3|a_{3n}$ for some n and consider $a_{3(n+1)}$. By the definition of the sequence

$$a_{3(n+1)} = 10^3 \cdot a_{3n} + 111.$$

Note that $111 = 3 \cdot 37$ and by the induction assumption $a_{3n} = 3 \cdot m$ for some m. Therefore

$$a_{3(n+1)} = 10^3 \cdot 3 \cdot m + 3 \cdot 37 = 3 \cdot (10^3 \cdot m + 37),$$

which means that, by the definition of divisibility, $3|a_{3(n+1)}$.
Thus, by the principle of mathematical induction $3|a_{3n}$ for all n. □

Miscellaneous Proofs

Definition 17 (Lots of Ones Sequence)

For $n = 0$ let $a_0 = 12$, and for $n > 0$ let $a_n = 10 \cdot a_{n-1} + 1$, so that

$$a_0 = 12,\ a_1 = 121,\ a_2 = 1211,\ a_3 = 12111,\ \ldots$$

Claim (Another False Conjecture)

For all values of n, a_n as defined in definition 17 are composite.

Miscellaneous Proofs

Claim (Another False Conjecture)

For all values of n, a_n as defined in definition 17 is composite.

Counter Example.

Running the code:

```
[> a=12
[> for n in range(200):
       if is_prime(a):
           print "a_",n,"is prime"
       a=10*a+1
```

we get the output `a_136 is prime` and `a_184 is prime`.