COMP170 Discrete Mathematical Tools for Computer Science

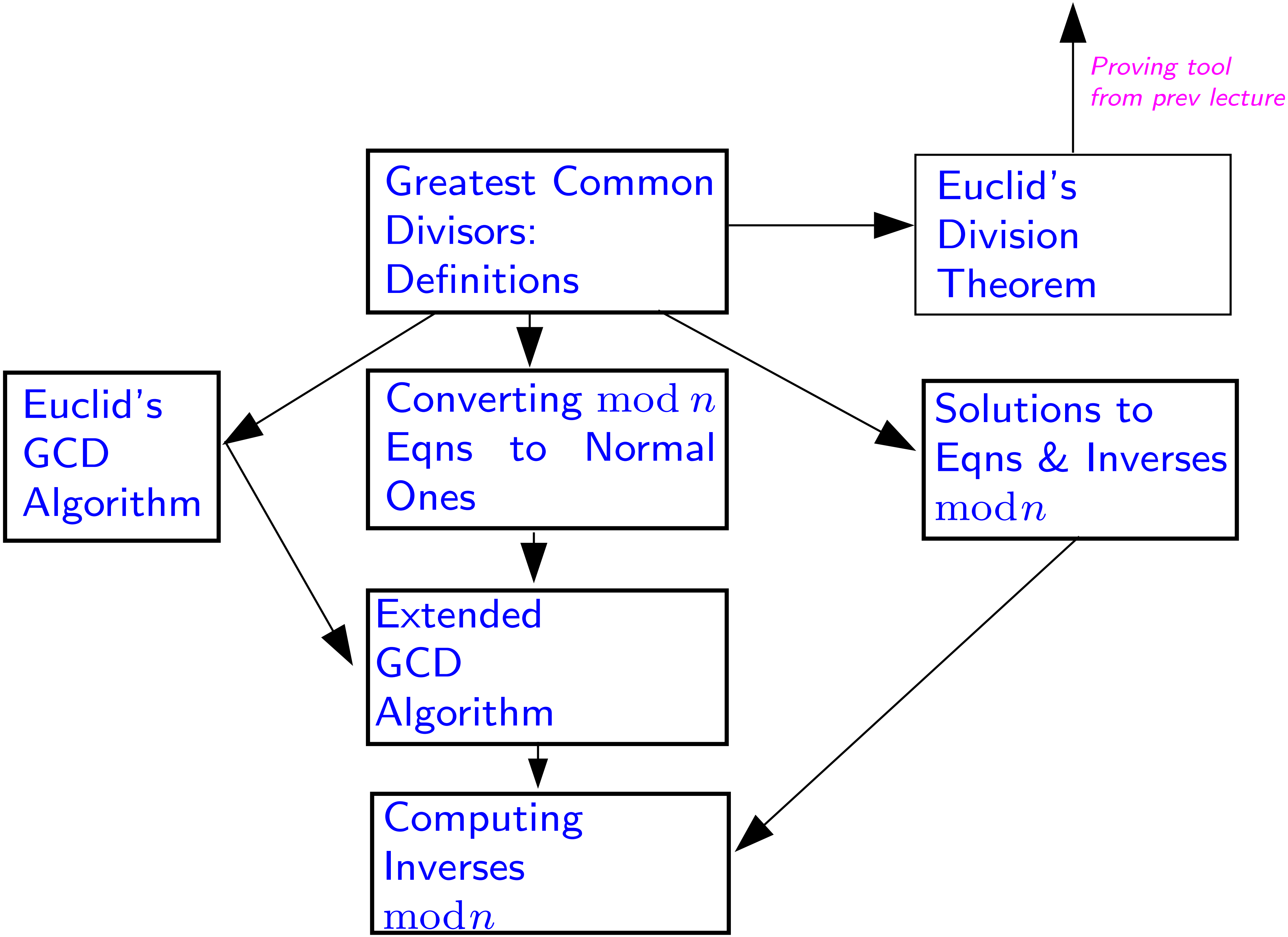
Lecture 5

Version 5: Last updated, Oct 3, 2005

Discrete Math for Computer Science
K. Bogart, C. Stein and R.L. Drysdale
Section 2.2, pp. 56-69

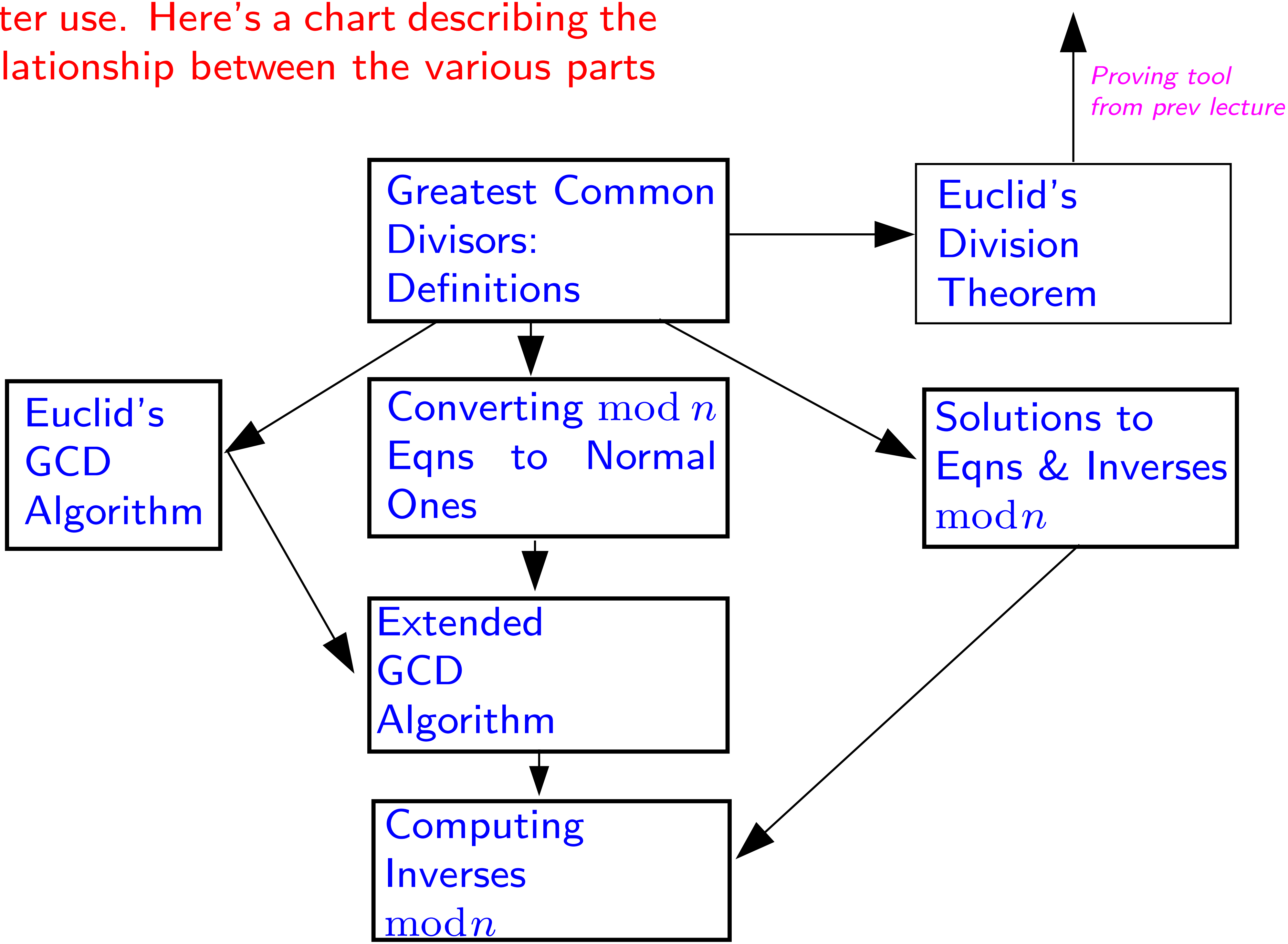
2.2 Inverses and Greatest Common Divisors

- Greatest Common Divisors
- Euclid's Division Theorem
- Euclid's GCD Algorithm
- Solutions to Equations and Inverses mod n
- Converting Modular Equations to Normal Equations
- Extended GCD Agorithm
- Computing Inverses

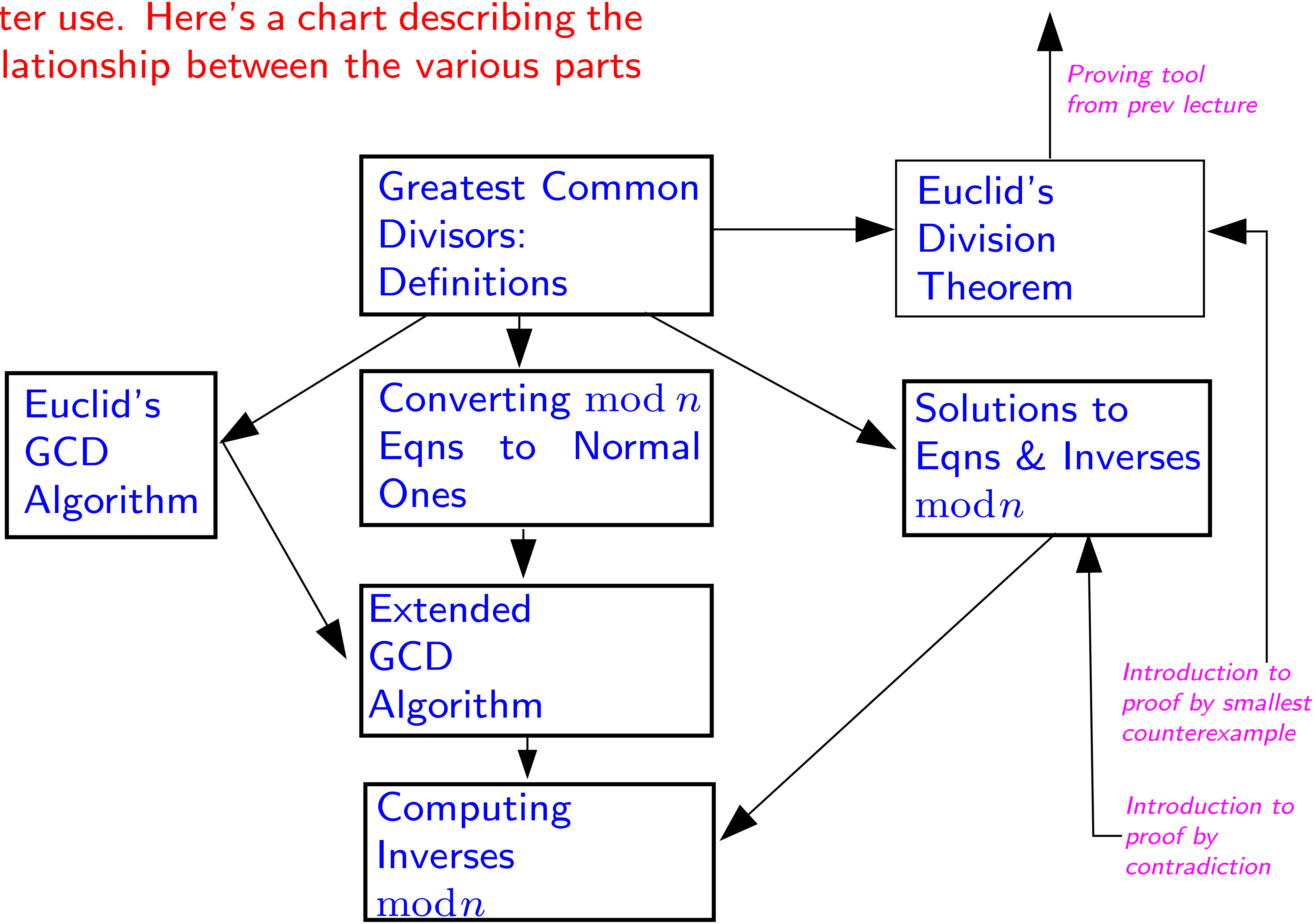


Proving tool
from prev lecture
Greatest Common Divisors: Definitions
Euclid's Division Theorem
Euclid's GCD Algorithm
Converting mod n Eqns to Normal Ones
Solutions to Eqns & Inverses mod n
Extended GCD Algorithm
Computing Inverses mod n

This lecture develops lots of tools for later use. Here's a chart describing the relationship between the various parts



This lecture develops lots of tools for later use. Here's a chart describing the relationship between the various parts



Definition:

- Positive integer m is a divisor of integer n
  if $n = mq$ for some integer q

- if m is a divisor of n we write $m|n$.
  (say) "m divides n"

- if m is a not a divisor of n we write $m \not| n$.
  (say) "m does not divide n"

Definition:

- Positive integer m is a divisor of integer n
  if $n = mq$ for some integer q

- if m is a divisor of n we write $m|n$.
  (say) "m divides n"

- if m is a not a divisor of n we write $m \not| n$.
  (say) "m does not divide n"

Examples:

- $1|30, \quad 5|30, \quad 5|35, \quad 5 \not| 31$

Definition:

- If p is a divisor of both m and n then
  p is a common divisor of m and n

- $gcd(m, n)$ denotes the greatest common divisor of m and n.
  1 is aways a common divisor of m and n

Definition:

- If p is a divisor of both m and n then
  p is a common divisor of m and n

- $gcd(m, n)$ denotes the greatest common divisor of m and n.
  1 is aways a common divisor of m and n

Examples:

- $\{1, 2, 3, 6\}$ are *all* of the common divisors of 24 and 30.

- $gcd(24, 30) = 6$

Definition:

- Positive integer $p > 1$ is prime if its only divisors are 1 and itself . If p is not prime, it is composite.
- m and n are relatively prime if they have no common divisor other than 1, i.e., $gcd(m, n) = 1$.

Definition:

- Positive integer $p > 1$ is prime if its only divisors are 1 and itself . If p is not prime, it is composite.
- m and n are relatively prime if they have no common divisor other than 1, i.e., $gcd(m, n) = 1$.

Examples:

- $2, 3, 5, 7, 11$ are prime.
  $33 = 3 \cdot 11$ is composite
- $gcd(77, 34) = 1$, so 77 and 34 are relatively prime
  $gcd(77, 33) = 11$, so 77 and 33 are *not* relatively prime

The main goal of this lecture is to prove the Theorem and Corollary below and also to show how to calculate the corresponding x and y and multiplicative inverses.

In order to get to that point we will have to develop a lot of auxillary machinery. We will see in the next lecture that this auxillary machinery will be useful for implementing RSA public-key cryptography.

Theorem 2.15: Two positive integers j, k are relatively prime, i.e., $gcd(i, j) = 1$, if and only if there are integers x and y such that $jx + ky = 1$.

Corollary 2.16: For any positive integer n, an element $a \in Z_n$ has a multiplicative inverse if and only if $gcd(a, n) = 1$.

2.2 Inverses and Greatest Common Divisors

- Greatest Common Divisors
- Euclid's Division Theorem
- Euclid's GCD Algorithm
- Solutions to Equations and Inverses mod n
- Converting Modular Equations to Normal Equations
- Extended GCD Agorithm
- Computing Inverses

Recall that in the last section we learnt about Euclid's division theorem and proved facts based upon it. In this subsection, we prove the correctness of Euclid's division theorem

Euclid's Division Theorem

Theorem 2.12 (Euclid's Division Theorem, Restricted Version): Let n be a positive integer. Then for every nonnegative integer m, there exist unique integers q, r such that $m = nq + r$ and $0 \leq r < n$.

Euclid's Division Theorem

Theorem 2.12 (Euclid's Division Theorem, Restricted Version): Let n be a positive integer. Then for every nonnegative integer m, there exist unique integers q, r such that $m = nq + r$ and $0 \leq r < n$.

Note 1: By definition, $r = m \bmod n$*.*

Euclid's Division Theorem

Theorem 2.12 (Euclid's Division Theorem, Restricted Version): Let n be a positive integer. Then for every nonnegative integer m, there exist unique integers q, r such that $m = nq + r$ and $0 \leq r < n$.

Note 1: By definition, $r = m \bmod n$.

Note 2: This is ***restricted*** *because we assume that* m *is positive. Book problem shows how to extend this to negative* m *as well.*

Theorem 2.12 (Euclid's Division Theorem, Restricted Version): Let n be a positive integer. Then for every nonnegative integer m, there exist unique integers q, r such that $m = nq + r$ and $0 \leq r < n$.

Proof:

(i) First, show that, for each m, there is at least one pair of integers q, r satisfying

(*) $m = qn + r$ with $0 \leq r < n$

(ii) Then show that this pair q, r is *unique*

Assume, (proof by contradiction), that there is a nonnegative integer m for which no such q and r exist.

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow$ $m = 0 \cdot n + m$ so
(*) is satisfied with $q = 0$, $r = m$
contradicting assumption.

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow$ $m = 0 \cdot n + m$ so
(*) is satisfied with $q = 0$, $r = m$
contradicting assumption.

$\Rightarrow$ $m \geq n$, so $m - n$ is a nonnegative integer

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow$ $m = 0 \cdot n + m$ so
(*) is satisfied with $q = 0$, $r = m$
contradicting assumption.

$\Rightarrow$ $m \geq n$, so $m - n$ is a nonnegative integer

Since $m - n$ *is smaller than* m, there exist integers q', r'
such that $m - n = nq' + r'$ with $0 \leq r' < n$.

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow m = 0 \cdot n + m$ so

(*) is satisfied with $q = 0$, $r = m$

contradicting assumption.

$\Rightarrow m \geq n$, so $m - n$ is a nonnegative integer

Since $m - n$ *is smaller than* m, there exist integers q', r'

such that $m - n = nq' + r'$ with $0 \leq r' < n$.

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow m = 0 \cdot n + m$ so
(*) is satisfied with $q = 0$, $r = m$
contradicting assumption.

$\Rightarrow m \geq n$, so $m - n$ is a nonnegative integer

Since $m - n$ *is smaller than* m, there exist integers q', r'
such that $m - n = nq' + r'$ with $0 \leq r' < n$.

Setting $q = q' + 1$ and $r = r'$, we obtain
(*) $m = qn + r$ with $0 \leq r < n$.

(*) $m = qn + r$ with $0 \le r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow m = 0 \cdot n + m$ so

(*) is satisfied with $q = 0$, $r = m$

contradicting assumption.

$\Rightarrow m \ge n$, so $m - n$ is a nonnegative integer

Since $m - n$ *is smaller than* m, there exist integers q', r' such that $m - n = nq' + r'$ with $0 \le r' < n$.

Setting $q = q' + 1$ and $r = r'$, we obtain

(*) $m = qn + r$ with $0 \le r < n$.

This contradicts choice of m

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow m = 0 \cdot n + m$ so

(*) is satisfied with $q = 0$, $r = m$

contradicting assumption.

$\Rightarrow m \geq n$, so $m - n$ is a nonnegative integer

Since $m - n$ *is smaller than* m, there exist integers q', r'

such that $m - n = nq' + r'$ with $0 \leq r' < n$.

Setting $q = q' + 1$ and $r = r'$, we obtain

(*) $m = qn + r$ with $0 \leq r < n$.

This contradicts choice of m

$\Rightarrow$ for all m there exist some q, r satisfying $(*)$

(*) $m = qn + r$ with $0 \leq r < n$

(i) Assume (proof by contradiction) that there is a nonnegative integer m for which no q, r satisfying (*) exists

Choose the **smallest** m for which q, r satisfying (*) does not exist.

If $m < n$, $\Rightarrow m = 0 \cdot n + m$ so
(*) is satisfied with $q = 0$, $r = m$
contradicting assumption.

$\Rightarrow m \geq n$, so $m - n$ is a nonnegative integer

Since $m - n$ *is smaller than* m, there exist integers q', r'
such that $m - n = nq' + r'$ with $0 \leq r' < n$.

Setting $q = q' + 1$ and $r = r'$, we obtain
(*) $m = qn + r$ with $0 \leq r < n$.

This $\boxed{\text{contradicts choice of } m}$ $\Rightarrow$ for all m there exist some q, r satisfying $(*)$

(*) $m = qn + r$ with $0 \leq r < n$

(ii) We just showed that, for every m, there *exists* some q, r satisfying m. We now show that these q, r are *unique*

(*) $m = qn + r$ with $0 \leq r < n$

(ii) We just showed that, for every m, there *exists* some q, r satisfying m. We now show that these q, r are *unique*

Suppose that $m = nq + r$ and $m = nq^* + r^*$ with $0 \leq r < n$ and $0 \leq r^* < n$.

(*) $m = qn + r$ with $0 \leq r < n$

(ii) We just showed that, for every m, there *exists* some q, r satisfying m. We now show that these q, r are *unique*

Suppose that $m = nq + r$ and $m = nq^* + r^*$ with $0 \leq r < n$ and $0 \leq r^* < n$.

$$0 = n(q - q^*) + r - r^* \quad \Rightarrow \quad n(q - q^*) = r^* - r.$$

(*) $m = qn + r$ with $0 \le r < n$

(ii) We just showed that, for every m, there *exists* some q, r satisfying m. We now show that these q, r are *unique*

Suppose that $m = nq + r$ and $m = nq^* + r^*$ with $0 \le r < n$ and $0 \le r^* < n$.

$$0 = n(q - q^*) + r - r^* \quad \Rightarrow \quad n(q - q^*) = r^* - r.$$

$$|r^* - r| < n \text{ (why)} \quad \Rightarrow \quad |n(q - q^*)| = |r^* - r| < n.$$

(*) $m = qn + r$ with $0 \le r < n$

(ii) We just showed that, for every m, there *exists* some q, r satisfying m. We now show that these q, r are *unique*

Suppose that $m = nq + r$ and $m = nq^* + r^*$ with $0 \le r < n$ and $0 \le r^* < n$.

$$0 = n(q - q^*) + r - r^* \quad \Rightarrow \quad n(q - q^*) = r^* - r.$$

$$|r^* - r| < n \text{ (why)} \quad \Rightarrow \quad |n(q - q^*)| = |r^* - r| < n.$$

Because n is a factor of the left side, the only way the inequality can hold is if $|n(q - q^*)| = |r^* - r| = 0$.

(*) $m = qn + r$ with $0 \leq r < n$

(ii) We just showed that, for every m, there *exists* some q, r satisfying m. We now show that these q, r are *unique*

Suppose that $m = nq + r$ and $m = nq^* + r^*$ with $0 \leq r < n$ and $0 \leq r^* < n$.

$$0 = n(q - q^*) + r - r^* \quad \Rightarrow \quad n(q - q^*) = r^* - r.$$

$$|r^* - r| < n \text{ (why)} \quad \Rightarrow \quad |n(q - q^*)| = |r^* - r| < n.$$

Because n is a factor of the left side, the only way the inequality can hold is if $|n(q - q^*)| = |r^* - r| = 0$.

Therefore, $q = q^*$ and $r = r^*$,
proving that q and r satisfying (*) are unique.

Here, we have used a special case of

proof by contradiction

that we call

proof by smallest counterexample.

In this method, we assume, as in all proofs by contradiction, that the theorem is false, which implies that there must be a **counterexample** that does not satisfy the theorem's conditions.

Here, we have used a special case of

proof by contradiction

that we call

proof by smallest counterexample.

In this method, we assume, as in all proofs by contradiction, that the theorem is false, which implies that there must be a **counterexample** that does not satisfy the theorem's conditions.

This method is closely related to a proof method called *proof by induction* *(to be seen later)*

Proof by smallest counterexample that
statement $P(n)$ is true for all $n = 0, 1, 2 \ldots$ works by

Proof by smallest counterexample that statement $P(n)$ is true for all $n = 0, 1, 2 \ldots$ works by

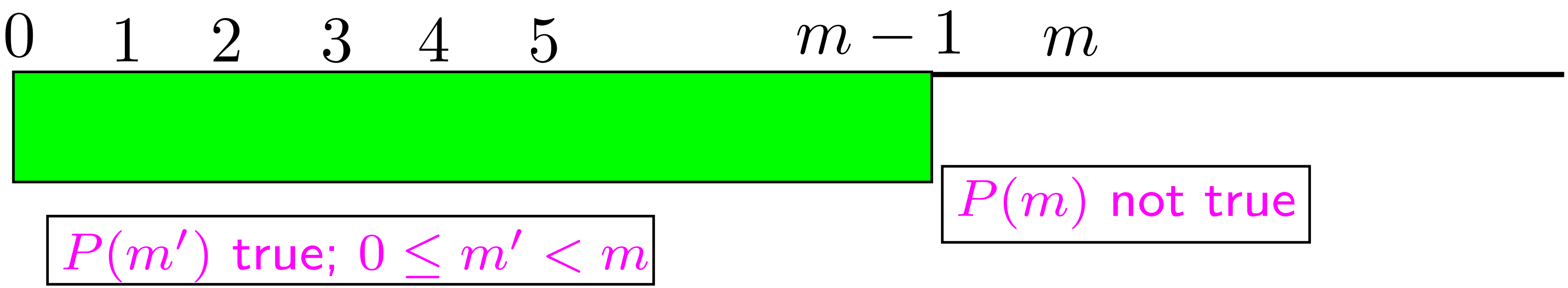
(i) Assuming that a non-zero counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is not true

$1 \quad 2 \quad 3 \quad 4 \quad 5$

Proof by smallest counterexample that statement $P(n)$ is true for all $n = 0, 1, 2 \ldots$ works by

(i) Assuming that a non-zero counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is not true

(ii) Letting $m > 0$ be *smallest* value for which $P(m)$ is not true

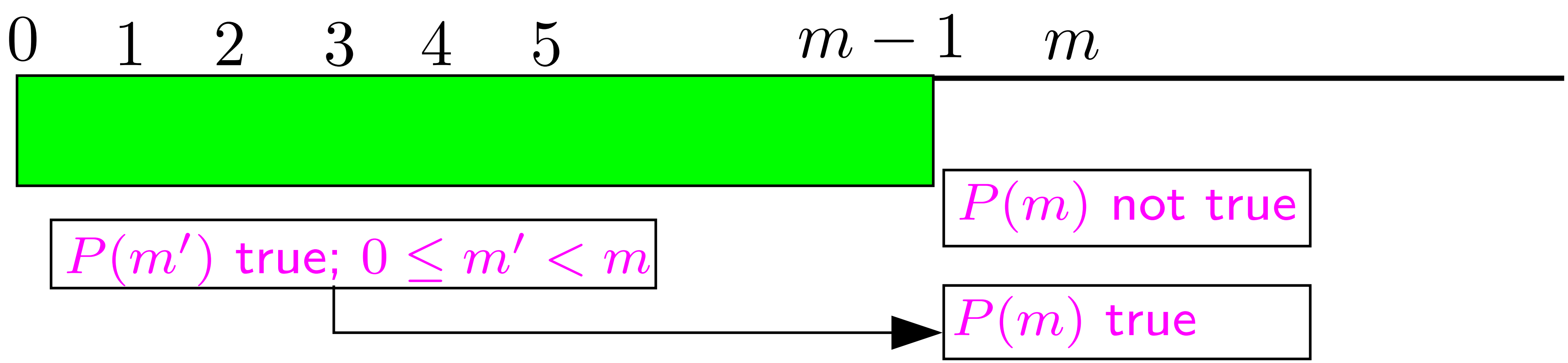


Proof by smallest counterexample that
statement $P(n)$ is true for all $n = 0, 1, 2 \ldots$ works by

(i) Assuming that a non-zero counterexample exists, i.e.,
There is some $n > 0$ for which $P(n)$ is not true

(ii) Letting $m > 0$ be *smallest* value for which $P(m)$ is not true

(iii) Then use fact that $P(m')$ is true for all $0 \leq m' < m$
to show that $P(m)$ is true,
contradicting original choice of m.
$\Rightarrow P(n)$ true for **all** $n = 0, 1, 2, \ldots$

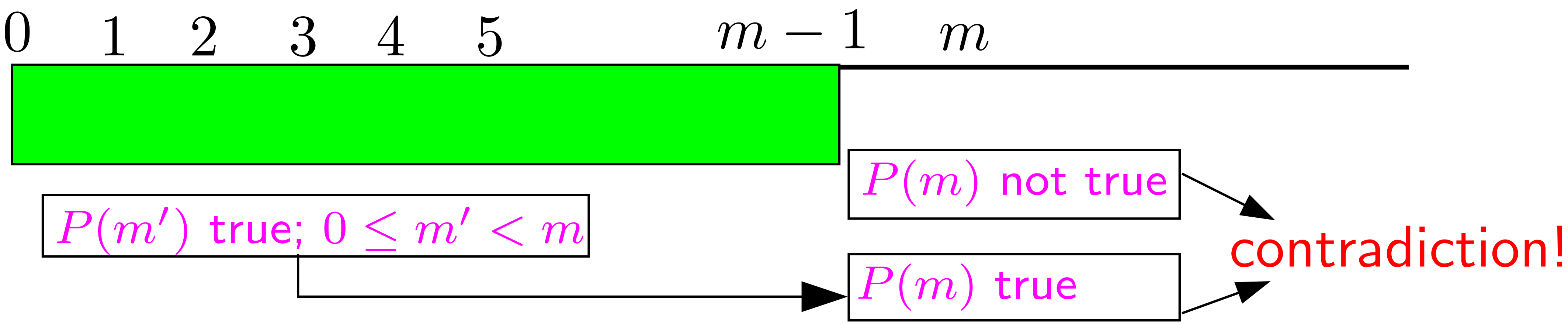


Proof by smallest counterexample that
statement $P(n)$ is true for all $n = 0, 1, 2 \ldots$ works by

(i) Assuming that a non-zero counterexample exists, i.e.,
There is some $n > 0$ for which $P(n)$ is not true

(ii) Letting $m > 0$ be *smallest* value for which $P(m)$ is not true

(iii) Then use fact that $P(m')$ is true for all $0 \le m' < m$
to show that $P(m)$ is true,
contradicting original choice of m.
$\Rightarrow P(n)$ true for **all** $n = 0, 1, 2, \ldots$



2.2 Inverses and Greatest Common Divisors

- Greatest Common Divisors
- Euclid's Division Theorem
- Euclid's GCD Algorithm
- Solutions to Equations and Inverses mod n
- Converting Modular Equations to Normal Equations
- Extended GCD Agorithm
- Computing Inverses

Before returning to multiplicative inverses, we first see how to calculate $gcd(j, k)$

Before returning to multiplicative inverses, we first see how to calculate $gcd(j,k)$

Suppose $k = jq + r$. Is there a relationship between $gcd(j,k)$ and $gcd(r,j)$?

Before returning to multiplicative inverses, we first see how to calculate $gcd(j,k)$

Suppose $k = jq + r$. Is there a relationship between $gcd(j,k)$ and $gcd(r,j)$?

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j,k) = gcd(r,j)$.

Before returning to multiplicative inverses, we first see how to calculate $gcd(j, k)$

Suppose $k = jq + r$. Is there a relationship between $gcd(j, k)$ and $gcd(r, j)$?

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

Proof:

(i) $r = 0$:
Then $gcd(r, j) = j$ since *every number* divides 0.

But $k = jq$ so $gcd(k, j) = j = gcd(j, r)$
and we are done.

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

Proof: (cont)
(ii) $r > 0$:

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

Proof: (cont)

(ii) $r > 0$:

Let d be a *common factor* of j, k

$\Rightarrow k = i_1 d$ and $j = i_2 d$ for some nonnegative i_1, i_2.

$\Rightarrow d$ is a *common factor* of $r = k - jq = (i_1 - i_2 q)d$

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

Proof: (cont)

(ii) $r > 0$:

Let d be a *common factor* of j, k

$\Rightarrow k = i_1 d$ and $j = i_2 d$ for some nonnegative i_1, i_2.

$\Rightarrow d$ is a *common factor* of $r = k - jq = (i_1 - i_2 q)d$

Let d be a *common factor* of j, r

$\Rightarrow j = i_2 d$ and $r = i_3 d$ for some nonnegative i_2, i_3.

$\Rightarrow d$ is a *common factor* of $k = jq + r = (i_2 q + i_3)d$

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

Proof: (cont)

(ii) $r > 0$:

Let d be a *common factor* of j, k

$\Rightarrow k = i_1 d$ and $j = i_2 d$ for some nonnegative i_1, i_2.

$\Rightarrow d$ is a *common factor* of $r = k - jq = (i_1 - i_2 q)d$

Let d be a *common factor* of j, r

$\Rightarrow j = i_2 d$ and $r = i_3 d$ for some nonnegative i_2, i_3.

$\Rightarrow d$ is a *common factor* of $k = jq + r = (i_2 q + i_3)d$

So d is a *common factor* of j, k iff d is a *common factor* of r, j

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

Proof: (cont)

(ii) $r > 0$:

Let d be a *common factor* of j, k

$\Rightarrow k = i_1 d$ and $j = i_2 d$ for some nonnegative i_1, i_2.

$\Rightarrow d$ is a *common factor* of $r = k - jq = (i_1 - i_2 q)d$

Let d be a *common factor* of j, r

$\Rightarrow j = i_2 d$ and $r = i_3 d$ for some nonnegative i_2, i_3.

$\Rightarrow d$ is a *common factor* of $k = jq + r = (i_2 q + i_3)d$

So d is a *common factor* of j, k iff d is a *common factor* of r, j

$$\Rightarrow \quad d = gcd(j, k) \text{ iff } d = gcd(r, j)$$

Euclid's GCD Algorithm

Euclid's GCD Algorithm

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

Euclid's GCD Algorithm

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

1) $GCD(k, j)$ where $0 \leq j < k$

Euclid's GCD Algorithm

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

Euclid's GCD Algorithm

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

1) $GCD(k, j)$ where $0 \leq j < k$
2) If $j = 0$ answer is k
3) Else
4) Write $k = jq + r$ where $r = k \bmod j$
5) Answer is $GCD(j, r)$

Euclid's GCD Algorithm

Lemma 2.13 If j, k, q, and r are nonnegative integers such that $k = jq + r$, then $gcd(j, k) = gcd(r, j)$.

1) $GCD(k, j)$ where $0 \leq j < k$
2) If $j = 0$ answer is k
3) Else
4) Write $k = jq + r$ where $r = k \bmod j$
5) Answer is $GCD(j, r)$

Note that r is nonegative, and every time line 4 is executed, $r < j$, so the value of r **decreases**. Therefore, in a finite number of steps, process reaches $j = 0$ and **terminates**

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

1) $GCD(k,j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j,r)$

Example: Find $gcd(102, 70)$

$k \quad = \quad j(q) \quad + \quad r$

k	j	r	q
102	70		

1) $GCD(k, j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

k	$=$	$j(q)$	$+$	r		k	j	r	q
102	$=$	$70(1)$	$+$	32		102	70		

1) $GCD(k, j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$k = j(q) + r$$

$$102 = 70(1) + 32$$

k	j	r	q
102	70	32	1

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

k	$=$	$j(q)$	$+$	r
102	$=$	$70(1)$	$+$	32

k	j	r	q
102	70	32	1
70	32		

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$
\begin{array}{rcccc}
k & = & j(q) & + & r \\
102 & = & 70(1) & + & 32 \\
70 & = & 32(2) & + & 6
\end{array}
$$

k	j	r	q
102	70	32	1
70	32		

1) $GCD(k,j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j,r)$

Example: Find $gcd(102, 70)$

$$
\begin{array}{ccccc}
k & = & j(q) & + & r \\
 & & & & \\
102 & = & 70(1) & + & 32 \\
70 & = & 32(2) & + & 6
\end{array}
$$

k	j	r	q
102	70	32	1
70	32	6	2

1) $GCD(k, j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$
\begin{array}{ccccc}
k & = & j(q) & + & r \\
 & & & & \\
102 & = & 70(1) & + & 32 \\
70 & = & 32(2) & + & 6
\end{array}
$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6		

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$\begin{array}{rcrcr} k & = & j(q) & + & r \\ 102 & = & 70(1) & + & 32 \\ 70 & = & 32(2) & + & 6 \\ 32 & = & 6(5) & + & 2 \end{array}$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6		

1) $GCD(k, j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$\begin{array}{ccccc} k & = & j(q) & + & r \\ 102 & = & 70(1) & + & 32 \\ 70 & = & 32(2) & + & 6 \\ 32 & = & 6(5) & + & 2 \end{array}$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6	2	5

1) $GCD(k, j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$\begin{array}{rcrcr} k & = & j(q) & + & r \\ 102 & = & 70(1) & + & 32 \\ 70 & = & 32(2) & + & 6 \\ 32 & = & 6(5) & + & 2 \end{array}$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6	2	5
6	2		

1) $GCD(k,j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j,r)$

Example: Find $gcd(102, 70)$

$$\begin{array}{rcrcr} k & = & j(q) & + & r \\ 102 & = & 70(1) & + & 32 \\ 70 & = & 32(2) & + & 6 \\ 32 & = & 6(5) & + & 2 \\ 6 & = & 2(3) & + & 0 \end{array}$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6	2	5
6	2		

1) $GCD(k,j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j,r)$

Example: Find $gcd(102, 70)$

$$\begin{array}{rcccr} k & = & j(q) & + & r \\ \\ 102 & = & 70(1) & + & 32 \\ 70 & = & 32(2) & + & 6 \\ 32 & = & 6(5) & + & 2 \\ 6 & = & 2(3) & + & 0 \end{array}$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6	2	5
6	2	0	3

1) $GCD(k,j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$\begin{array}{rcrcr} k & = & j(q) & + & r \\ \\ 102 & = & 70(1) & + & 32 \\ 70 & = & 32(2) & + & 6 \\ 32 & = & 6(5) & + & 2 \\ 6 & = & 2(3) & + & 0 \end{array}$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6	2	5
6	2	0	3
2	0		

$GCD(k, j)$ where $0 \leq j < k$

If $j = 0$ answer is k

Else

Write $k = jq + r$ where $r = k \bmod j$

Answer is $GCD(j, r)$

Example: Find $gcd(102, 70)$

$$
\begin{array}{rcrcr}
k & = & j(q) & + & r \\
\\
102 & = & 70(1) & + & 32 \\
70 & = & 32(2) & + & 6 \\
32 & = & 6(5) & + & 2 \\
6 & = & 2(3) & + & 0
\end{array}
$$

k	j	r	q
102	70	32	1
70	32	6	2
32	6	2	5
6	2	0	3
2	0		

$gcd(102, 70) = 2$

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(252, 189)$

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(252, 189)$

k	$=$	$j(q)$	$+$	r

k	j	r	q
252	189		

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(252, 189)$

k	$=$	$j(q)$	$+$	r		k	j	r	q
252	$=$	$189(1)$	$+$	63		252	189		

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(252, 189)$

$$k \quad = \quad j(q) \quad + \quad r$$

$$252 \quad = \quad 189(1) \quad + \quad 63$$

k	j	r	q
252	189	63	1

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(252, 189)$

k	$=$	$j(q)$	$+$	r
252	$=$	$189(1)$	$+$	63

k	j	r	q
252	189	63	1
189	63		

1) $GCD(k,j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j,r)$

Example: Find $gcd(252, 189)$

$$
\begin{array}{ccccc}
k & = & j(q) & + & r \\
252 & = & 189(1) & + & 63 \\
189 & = & 63(3) & + & 0
\end{array}
$$

k	j	r	q
252	189	63	1
189	63		

1) $GCD(k, j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j, r)$

Example: Find $gcd(252, 189)$

$$\begin{array}{ccccc} k & = & j(q) & + & r \\ 252 & = & 189(1) & + & 63 \\ 189 & = & 63(3) & + & 0 \end{array}$$

k	j	r	q
252	189	63	1
189	63	0	4

1) $GCD(k,j)$ where $0 \leq j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j,r)$

Example: Find $gcd(252, 189)$

$$\begin{array}{ccccc} k & = & j(q) & + & r \\ 252 & = & 189(1) & + & 63 \\ 189 & = & 63(3) & + & 0 \end{array}$$

k	j	r	q
252	189	63	1
189	63	0	4
63	0		

1) $GCD(k,j)$ where $0 \le j < k$

2) If $j = 0$ answer is k

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Answer is $GCD(j,r)$

Example: Find $gcd(252, 189)$

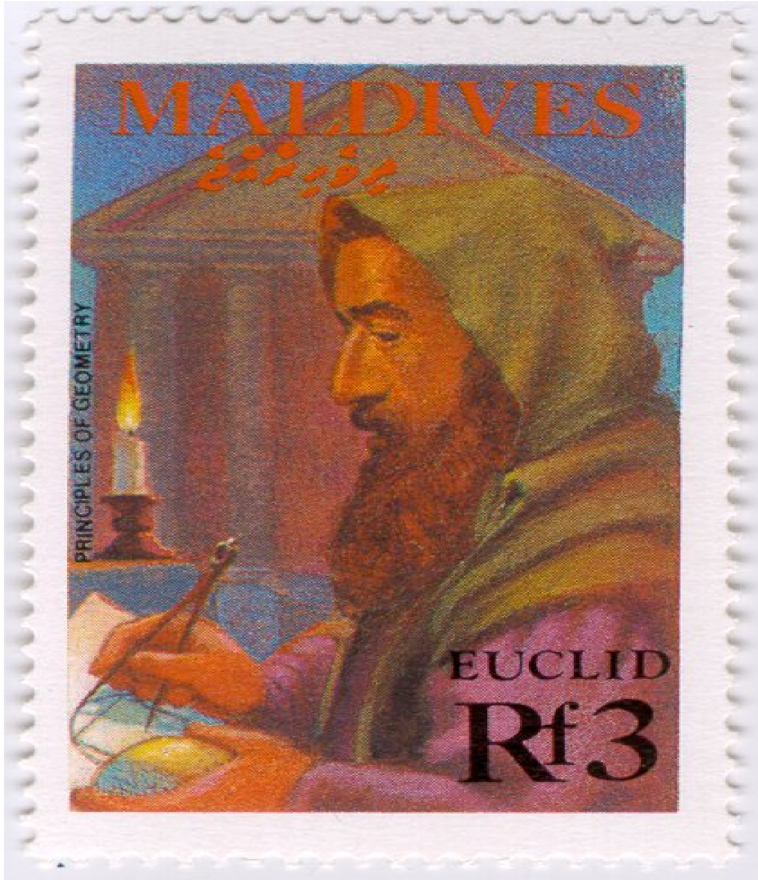
k	$=$	$j(q)$	$+$	r
252	$=$	$189(1)$	$+$	63
189	$=$	$63(3)$	$+$	0

k	j	r	q
252	189	63	1
189	63	0	4
63	0		

$$gcd(252, 189) = 63$$

Euclid of Alexandria

ca. 325BC – 265BC



If he existed, most probably a Greek Mathematician who taught at Alexandria (Egypt)

Most famous for his *Elements*, considered to be one of history's most successful textbooks.

The *Elements* contains 13 books. Book 7 is on number theory and contains the GCD algorithm

See *http://en.wikipedia.org/wiki/Euclid and http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Euclid.html*

2.2 Inverses and Greatest Common Divisors

- Greatest Common Divisors
- Euclid's Division Theorem
- Euclid's GCD Algorithm
- Solutions to Equations and Inverses mod n
- Converting Modular Equations to Normal Equations
- Extended GCD Agorithm
- Computing Inverses

Solutions to Equations and Inverses $\mathrm{mod}\, n$

Solutions to Equations and Inverses $\bmod n$

- Given a, to decide whether $a \cdot_n x = b$ has a *unique solution* in Z_n, it helps to know whether a has a **multiplicative inverse** in Z_n.

Solutions to Equations and Inverses $\bmod n$

- Given a, to decide whether $a \cdot_n x = b$ has a *unique solution* in Z_n, it helps to know whether a has a **multiplicative inverse** in Z_n.

- A **multiplicative inverse** is a' such that $a' \cdot_n a = 1$.

Solutions to Equations and Inverses $\bmod n$

- Given a, to decide whether $a \cdot_n x = b$ has a *unique solution* in Z_n, it helps to know whether a has a **multiplicative inverse** in Z_n.

- A **multiplicative inverse** is a' such that $a' \cdot_n a = 1$.

- Example: in Z_9
  $2 \cdot_9 5 = 1$ so the inverse of 2 is 5
  3 does not have an inverse because
  $3 \cdot_9 x = 1$ does not have a solution.
  This can be verified by checking the 9 possible values for x.

Lemma 2.5: If a has multiplicative inverse $a' \in Z_n$, then for any $b \in Z_n$, the equation $a \cdot_n x = b$ has the solution $x = a' \cdot_n b$, and this solution is unique.

Lemma 2.5: If a has multiplicative inverse $a' \in Z_n$, then for any $b \in Z_n$, the equation $a \cdot_n x = b$ has the solution $x = a' \cdot_n b$, and this solution is unique.

Proof:

If a has inverse $a' \in Z_n$ and (*) $a \cdot_n x = b$

Lemma 2.5: If a has multiplicative inverse $a' \in Z_n$, then for any $b \in Z_n$, the equation $a \cdot_n x = b$ has the solution $x = a' \cdot_n b$, and this solution is unique.

Proof:

If a has inverse $a' \in Z_n$ and (*) $a \cdot_n x = b$

i) $a' \cdot_n (a \cdot_n x) = a' \cdot_n b$ Multiply both sides by a'

Lemma 2.5: If a has multiplicative inverse $a' \in Z_n$, then for any $b \in Z_n$, the equation $a \cdot_n x = b$ has the solution $x = a' \cdot_n b$, and this solution is unique.

Proof:

If a has inverse $a' \in Z_n$ and (*) $a \cdot_n x = b$

i) $a' \cdot_n (a \cdot_n x) = a' \cdot_n b$ Multiply both sides by a'

ii) $(a' \cdot_n a) \cdot_n x = a' \cdot_n b$ By the associative law

Lemma 2.5: If a has multiplicative inverse $a' \in Z_n$, then for any $b \in Z_n$, the equation $a \cdot_n x = b$ has the solution $x = a' \cdot_n b$, and this solution is unique.

Proof:

If a has inverse $a' \in Z_n$ and (*) $a \cdot_n x = b$

i) $a' \cdot_n (a \cdot_n x) = a' \cdot_n b$ Multiply both sides by a'

ii) $(a' \cdot_n a) \cdot_n x = a' \cdot_n b$ By the associative law

iii) $x = a' \cdot_n b$ By definition of inverse

Lemma 2.5: If a has multiplicative inverse $a' \in Z_n$, then for any $b \in Z_n$, the equation $a \cdot_n x = b$ has the solution $x = a' \cdot_n b$, and this solution is unique.

Proof:

If a has inverse $a' \in Z_n$ and (*) $a \cdot_n x = b$

i) $a' \cdot_n (a \cdot_n x) = a' \cdot_n b$ Multiply both sides by a'

ii) $(a' \cdot_n a) \cdot_n x = a' \cdot_n b$ By the associative law

iii) $x = a' \cdot_n b$ By definition of inverse

Since this is valid for *any* x that satisfies (*), we conclude that *only* $x = a' \cdot_n b$ could satisfy (*).

Lemma 2.5: If a has multiplicative inverse $a' \in Z_n$, then for any $b \in Z_n$, the equation $a \cdot_n x = b$ has the solution $x = a' \cdot_n b$, and this solution is unique.

Proof:

If a has inverse $a' \in Z_n$ and (*) $a \cdot_n x = b$

i) $a' \cdot_n (a \cdot_n x) = a' \cdot_n b$ Multiply both sides by a'

ii) $(a' \cdot_n a) \cdot_n x = a' \cdot_n b$ By the associative law

iii) $x = a' \cdot_n b$ By definition of inverse

Since this is valid for *any* x that satisfies (*), we conclude that *only* $x = a' \cdot_n b$ could satisfy (*).

To see that $x = a' \cdot_n b$ satisfies (*) just multiply to find that

$$\boxed{a \cdot_n x = a \cdot_n (a' \cdot_n b) = b}$$

Theorem 2.7: If element of $a \in Z_n$ has a multiplicative inverse, then the inverse is unique

Theorem 2.7: If element of $a \in Z_n$ has a multiplicative inverse, then the inverse is unique

Proof:

Let a have some inverse $a' \in Z_n$.
Now apply the previous lemma with $b = 1$. It says that

$$\text{If } a \cdot_n x = 1 \quad \Rightarrow \quad x = a' \cdot_n 1 = a'.$$

This can be read as saying that,

"if a' is an inverse of a in Z_n
and x is also an inverse of a in Z_n
then $x = a'$",

so the inverse is unique.

For each for $n = 5, 6, 7, 8,$ and 9, determine which nonzero elements $a \in Z_n$ have mutiplicative inverses and, if they do, what the inverses are.

For each for $n = 5, 6, 7, 8$, and 9, determine which nonzero elements $a \in Z_n$ have mutiplicative inverses and, if they do, what the inverses are.

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

For each for $n = 5, 6, 7, 8,$ and 9, determine which nonzero elements $a \in Z_n$ have mutiplicative inverses and, if they do, what the inverses are.

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

For each for $n = 5, 6, 7, 8,$ and 9, determine which nonzero elements $a \in Z_n$ have mutiplicative inverses and, if they do, what the inverses are.

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

a	1	2	3	4
a'	1	3	2	4

For each for $n = 5, 6, 7, 8,$ and 9, determine which nonzero elements $a \in Z_n$ have mutiplicative inverses and, if they do, what the inverses are.

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\longrightarrow$

a	1	2	3	4
a'	1	3	2	4

Z_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

For each for $n = 5, 6, 7, 8,$ and 9, determine which nonzero elements $a \in Z_n$ have mutiplicative inverses and, if they do, what the inverses are.

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

a	1	2	3	4
a'	1	3	2	4

Z_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

a	1	2	3	4	5
a'	1	X	X	X	5

X denotes no inverse

Z_5:

a	1	2	3	4
a'	1	3	2	4

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_7:

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Z_8:

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

Z_9:

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

- We've just seen how to find inverses (or the lack of them) by scanning through the entire multiplication table. Is there a more efficient way?

- We've just seen how to find inverses (or the lack of them) by scanning through the entire multiplication table.
  Is there a more efficient way?

- We will now see a way of proving that an inverse does not exist,

- We've just seen how to find inverses (or the lack of them) by scanning through the entire multiplication table. Is there a more efficient way?

- We will now see a way of proving that an inverse does not exist,

- We will then develop an efficient way of calculating inverses when they do exist.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Proof (by contradiction!):

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Proof (by contradiction!):

i) Assume (*) $a \cdot_n x = b$ does not have a solution.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Proof (by contradiction!):

i) Assume (*) $a \cdot_n x = b$ does not have a solution.

ii) Suppose further that

(**) a does have a multiplicative inverse $a' \in Z_n$.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Proof (by contradiction!):

i) Assume (*) $a \cdot_n x = b$ does not have a solution.

ii) Suppose further that

(**) a does have a multiplicative inverse $a' \in Z_n$.

iii) Then by Lemma 2.5,

$x = a' \cdot_n b$ is a solution to $a \cdot_n x = b$.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Proof (by contradiction!):

i) Assume (*) $a \cdot_n x = b$ does not have a solution.

ii) Suppose further that

(**) a does have a multiplicative inverse $a' \in Z_n$.

iii) Then by Lemma 2.5,

$x = a' \cdot_n b$ is a solution to $a \cdot_n x = b$.

iv) This contradicts the hypothesis (*) that

$a \cdot_n x = b$ does not have a solution.

One of the assumptions —

(*) $a \cdot_n x = b$ does not have a solution.

– was the hypothesis given to us in the corollary's statement.

One of the assumptions —

(*) $a \cdot_n x = b$ does not have a solution.

– was the hypothesis given to us in the corollary's statement.

The only other assumption we made was

(**) a does have a multiplicative inverse $a' \in Z_n$.

One of the assumptions —

(*) $a \cdot_n x = b$ does not have a solution.

– was the hypothesis given to us in the corollary's statement.

The only other assumption we made was

(**) a does have a multiplicative inverse $a' \in Z_n$.

Assuming both (*) and (**) led to a contradiction. It must therefore be the case that, if (*) is true, then (**) can not be true.

One of the assumptions —

(*) $a \cdot_n x = b$ does not have a solution.

– was the hypothesis given to us in the corollary's statement.

The only other assumption we made was

(**) a does have a multiplicative inverse $a' \in Z_n$.

Assuming both (*) and (**) led to a contradiction. It must therefore be the case that, if (*) is true, then (**) can not be true.

Thus, if $a \cdot_n x = b$ does not have a solution, then a does not have a multiplicative inverse $a' \in Z_n$.

One of the assumptions —

(*) $a \cdot_n x = b$ does not have a solution.

– was the hypothesis given to us in the corollary's statement.

The only other assumption we made was

(**) a does have a multiplicative inverse $a' \in Z_n$.

Assuming both (*) and (**) led to a contradiction.
It must therefore be the case that, if (*) is true, then (**) can not be true.

Thus, if $a \cdot_n x = b$ does not have a solution, then a does not have a multiplicative inverse $a' \in Z_n$.

A classical example of **proof by contradiction**.

Principle 2.1 (Proof by Contradiction):
If, by assuming a statement we want to prove is false,
we are led to a contradiction,
then the statement we are trying to prove
must be true.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Now consider Z_6. The equation $2 \cdot_6 x = 3$ can not have a solution because $2x$ will always be even so $2x \bmod 6$ will always be even.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Now consider Z_6. The equation $2 \cdot_6 x = 3$ can not have a solution because $2x$ will always be even so $2x \bmod 6$ will always be even.

The corollary therefore tells us that 2 does not have a multiplicative inverse in Z_6. We originally discovered this by checking all of the possibilities, but now we don't have to.

Corollary 2.6: Suppose there is a $b \in Z_n$ such that $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Now consider Z_6. The equation $2 \cdot_6 x = 3$ can not have a solution because $2x$ will always be even so $2x \bmod 6$ will always be even.

The corollary therefore tells us that 2 does not have a multiplicative inverse in Z_6. We originally discovered this by checking all of the possibilities, but now we don't have to.

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_5:

a	1	2	3	4
a'	1	3	2	4

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_7:

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Z_8:

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

Z_9:

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

Z_5:

a	1	2	3	4
a'	1	3	2	4

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_7:

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Z_8:

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

Z_9:

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

Note that $5, 7$ are prime and all of the elements in Z_5, Z_7 have inverses.

For the non-prime $n \in 6, 8, 9$ the elements in Z_n that have inverses are exactly those elements that are relatively prime to n.

Z_5:

a	1	2	3	4
a'	1	3	2	4

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_7:

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Z_8:

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

Z_9:

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

Note that $5, 7$ are prime and all of the elements in Z_5, Z_7 have inverses.

For the non-prime $n \in 6, 8, 9$ the elements in Z_n that have inverses are exactly those elements that are relatively prime to n.

Nice pattern!
Is this aways true?
Yes!

2.2 Inverses and Greatest Common Divisors

- Greatest Common Divisors
- Euclid's Division Theorem
- Euclid's GCD Algorithm
- Solutions to Equations and Inverses mod n
- Converting Modular Equations to Normal Equations
- Extended GCD Agorithm
- Computing Inverses

Converting Modular Equations to Normal Equations

Lemma 2.8 The modular equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x, y such that (*) $ax + ny = 1$.

Converting Modular Equations to Normal Equations

Lemma 2.8 The modular equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x, y such that (*) $ax + ny = 1$.

Proof:

Rewrite $a \cdot_n x = 1$ as $ax \bmod n = 1$.

Converting Modular Equations to Normal Equations

Lemma 2.8 The modular equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x, y such that (*) $ax + ny = 1$.

Proof:

Rewrite $a \cdot_n x = 1$ as ax mod $n = 1$.

But $ax \bmod n$ is *defined* as remainder r that we get when we write $ax = qn + r$, with $0 \leq r < n$.

Converting Modular Equations to Normal Equations

Lemma 2.8 The modular equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x, y such that (*) $ax + ny = 1$.

Proof:

Rewrite $a \cdot_n x = 1$ as ax mod $n = 1$.

But $ax \bmod n$ is *defined* as remainder r that we get when we write $ax = qn + r$, with $0 \le r < n$.

So, $\boxed{\text{if } a \cdot_n x = 1}$ $\Rightarrow$ we can write $ax + (-q)n = 1$ in form (*).

Converting Modular Equations to Normal Equations

Lemma 2.8 The modular equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x, y such that (*) $ax + ny = 1$.

Proof:

Rewrite $a \cdot_n x = 1$ as ax mod $n = 1$.

But $ax \bmod n$ is *defined* as remainder r that we get when we write $ax = qn + r$, with $0 \leq r < n$.

So, $\boxed{\text{if } a \cdot_n x = 1}$ $\Rightarrow$ we can write $ax + (-q)n = 1$ in form (*).

$\boxed{\text{If (*) for some } y}$ then $ax = (-y)n + 1$ so
by definition of $\bmod$, $ax \bmod n = 1 \Rightarrow a \cdot_n x = 1$.

We just derived

Lemma 2.8 The modular equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x, y such that (*) $ax + ny = 1$.

We just derived

Lemma 2.8 The modular equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x, y such that (*) $ax + ny = 1.$

This can be restated as

Theorem 2.9: A number a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1.$

We just characterized the *existence* of a mutiplicative inverse by

Theorem 2.9: A number a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.

We just characterized the *existence* of a mutiplicative inverse by

Theorem 2.9: A number a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.

Can this Theorem help us *find* the inverse?

We just characterized the *existence* of a mutiplicative inverse by

Theorem 2.9: A number a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.

Can this Theorem help us *find* the inverse? **Yes!**

Corollary 2.10: If $a \in Z_n$ and x, y are integers such that $ax + ny = 1$, then the multiplicative inverse of a in Z_n is $x \bmod n$.

We just characterized the *existence* of a mutiplicative inverse by

Theorem 2.9: A number a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.

Can this Theorem help us *find* the inverse? **Yes!**

Corollary 2.10: If $a \in Z_n$ and x, y are integers such that $ax + ny = 1$, then the multiplicative inverse of a in Z_n is $x \bmod n$.

Proof: Since $n \cdot_n y = 0$,

$$a \cdot_n x \; = \; a \cdot_n x +_n n \cdot_n y \; = \; (ax + ny) \bmod n = 1$$

We just characterized the *existence* of a mutiplicative inverse by

Theorem 2.9: A number a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.

Can this Theorem help us *find* the inverse? **Yes!**

Corollary 2.10: If $a \in Z_n$ and x, y are integers such that $ax + ny = 1$, then the multiplicative inverse of a in Z_n is $x \bmod n$.

Proof: Since $n \cdot_n y = 0$,

$$a \cdot_n x \;=\; a \cdot_n x +_n n \cdot_n y \;=\; (ax + ny) \bmod n = 1$$

Multiple appl of Lemma 2.3

Suppose $ax + ny = 1$ for integers x, y.
Can a, n have any common divisors other than 1 and -1?

Suppose $ax + ny = 1$ for integers x, y.
Can a, n have any common divisors other than 1 and -1?

- If a, n have a common divisor k
  $\Rightarrow$ must exist integers s and q
  such that $a = sk$ and $n = qk$.

Suppose $ax + ny = 1$ for integers x, y.
Can a, n have any common divisors other than 1 and -1?

- If a, n have a common divisor k
  $\Rightarrow$ must exist integers s and q
  such that $a = sk$ and $n = qk$.

- Plugging into $ax + ny = 1$ gives

$$\begin{aligned} 1 &= ax + ny \\ &= skx + qky \\ &= k(sx + qy). \end{aligned}$$

Suppose $ax + ny = 1$ for integers x, y.
Can a, n have any common divisors other than 1 and -1?

- If a, n have a common divisor k
  $\Rightarrow$ must exist integers s and q
  such that $a = sk$ and $n = qk$.

- Plugging into $ax + ny = 1$ gives

$$\begin{aligned} 1 &= ax + ny \\ &= skx + qky \\ &= k(sx + qy). \end{aligned}$$

- But then k is a divisor of 1.
  Since *only* divisors of 1 are $1, -1 \Rightarrow k = 1$ or -1.

We just saw that, if $ax + ny = 1$ for integers x, y then the only common divisors of a, n are $1, -1$.

We just saw that, if $ax + ny = 1$ for integers x, y then the only common divisors of a, n are $1, -1$.

This can be restated as

We just saw that, if $ax + ny = 1$ for integers x, y then the only common divisors of a, n are $1, -1$.

This can be restated as

Lemma 2.11: Given a and n, if there exist integers x and y such that $ax + ny = 1$, then $\gcd(a, n) = 1$ — that is, a and n are relatively prime.

The Story So Far ....

- **Theorem 2.9**: a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.
- **Corollary 2.10**: If $a \in Z_n$ and x, y are integers s.t. $ax + ny = 1$, then the solution to $a \cdot_n \overline{x} = 1$ is $\overline{x} = x \bmod n$.
- **Lemma 2.11**: Given a, n, if there exist integers x, y such that $ax + ny = 1$, then $gcd(a, n) = 1$.

The Story So Far ....

- **Theorem 2.9**: a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.
- **Corollary 2.10**: If $a \in Z_n$ and x, y are integers s.t. $ax + ny = 1$, then the solution to $a \cdot_n \overline{x} = 1$ is $\overline{x} = x \bmod n$.
- **Lemma 2.11**: Given a, n, if there exist integers x, y such that $ax + ny = 1$, then $gcd(a, n) = 1$.

What's missing?

The Story So Far ....

- **Theorem 2.9**: a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.
- **Corollary 2.10**: If $a \in Z_n$ and x, y are integers s.t. $ax + ny = 1$, then the solution to $a \cdot_n \overline{x} = 1$ is $\overline{x} = x \bmod n$.
- **Lemma 2.11**: Given a, n, if there exist integers x, y such that $ax + ny = 1$, then $gcd(a, n) = 1$.

What's missing?

- If x, y exist, how do we find them
  (and via x, the mutiplicative inverses)?

The Story So Far ....

- **Theorem 2.9**: a has a multiplicative inverse in Z_n if and only if there are integers x, y such that $ax + ny = 1$.

- **Corollary 2.10**: If $a \in Z_n$ and x, y are integers s.t. $ax + ny = 1$, then the solution to $a \cdot_n \overline{x} = 1$ is $\overline{x} = x \bmod n$.

- **Lemma 2.11**: Given a, n, if there exist integers x, y such that $ax + ny = 1$, then $gcd(a, n) = 1$.

What's missing?

- If x, y exist, how do we find them
  (and via x, the mutiplicative inverses)?
- If $gcd(a, n) = 1$, do there aways exist x, y s.t. $ax + ny = 1$?

2.2 Inverses and Greatest Common Divisors

- Greatest Common Divisors
- Euclid's Division Theorem
- Euclid's GCD Algorithm
- Solutions to Equations and Inverses mod n
- Converting Modular Equations to Normal Equations
- Extended GCD Agorithm
- Computing Inverses

What's missing?

- If x, y exist, how do we find them (and via x, the muti-plicative inverses)?
- If $gcd(a, n) = 1$, do there aways exist x, y s.t. $ax + ny = 1$?

What's missing?

- If x, y exist, how do we find them (and via x, the mutiplicative inverses)?
- If $gcd(a, n) = 1$, do there aways exist x, y s.t. $ax + ny = 1$?

We will be able to find the x, y using the **Extended GCD Algorithm**.

As a side effect, it will also prove that, if $gcd(a, n) = 1$, there aways exists x, y s.t. $ax + ny = 1$.

Combining with Lemma 2.11 this will show that $gcd(a, n) = 1$ iff there exists x, y s.t. $ax + ny = 1$

Extended GCD Algorithm

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also
x, y such that $\text{gcd}(j, k) = jx + ky$.

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also x, y such that $\mathsf{gcd}(j, k) = jx + ky$.

(i) Base case: $k = jq$:
$gcd(j, k) = j$ with $x = 1$, $y = 0$.

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also
x, y such that $\mathsf{gcd}(j, k) = jx + ky$.

(i) Base case: $k = jq$:
$gcd(j, k) = j$ with $x = 1$, $y = 0$.

(ii) Nonbase case: $k \neq jq$ so $k = jq + r$ with $0 < r < j$

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also
x, y such that $\text{gcd}(j, k) = jx + ky$.

(i) Base case: $k = jq$:
$gcd(j, k) = j$ with $x = 1$, $y = 0$.

(ii) Nonbase case: $k \neq jq$ so $k = jq + r$ with $0 < r < j$
Recursively compute $gcd(r, j)$
and x', y' s.t. $gcd(r, j) = rx' + jy'$.

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also
x, y such that $\text{gcd}(j, k) = jx + ky$.

(i) Base case: $k = jq$:
$gcd(j, k) = j$ with $x = 1$, $y = 0$.

(ii) Nonbase case: $k \neq jq$ so $k = jq + r$ with $0 < r < j$
Recursively compute $\boxed{gcd(r, j)}$
and $\boxed{x', y'}$ s.t. $gcd(r, j) = rx' + jy'$.

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also
x, y such that $\text{gcd}(j, k) = jx + ky$.

(i) Base case: $k = jq$:
$gcd(j, k) = j$ with $x = 1$, $y = 0$.

(ii) Nonbase case: $k \neq jq$ so $k = jq + r$ with $0 < r < j$

Recursively compute $\boxed{gcd(r, j)}$
and $\boxed{x', y'}$ s.t. $gcd(r, j) = rx' + jy'$.

Because $r = k - jq$,
$gcd(r, j) = (k - jq)x' + jy' = kx' + j(y' - qx')$

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also
x, y such that $\text{gcd}(j, k) = jx + ky$.

(i) Base case: $k = jq$:
$gcd(j, k) = j$ with $x = 1$, $y = 0$.

(ii) Nonbase case: $k \neq jq$ so $k = jq + r$ with $0 < r < j$

Recursively compute $\boxed{gcd(r, j)}$
and $\boxed{x', y'}$ s.t. $gcd(r, j) = rx' + jy'$.

Because $r = k - jq$,
$gcd(r, j) = (k - jq)x' + jy' = kx' + j(y' - qx')$

so $gcd(k, j) = gcd(r, j) = jx + ky$
where $y = x'$ and $x = y' - qx'$.

Extended GCD Algorithm

Returns not only GCD, of j, k with $j < k$ but also x, y such that $\text{gcd}(j,k) = jx + ky$.

(i) Base case: $k = jq$:
$gcd(j,k) = j$ with $x = 1$, $y = 0$.

(ii) Nonbase case: $k \neq jq$ so $k = jq + r$ with $0 < r < j$

Recursively compute $\boxed{gcd(r,j)}$
and $\boxed{x', y'}$ s.t. $gcd(r,j) = rx' + jy'$.

Because $r = k - jq$,
$$gcd(r,j) = (k - jq)x' + jy' = kx' + j(y' - qx')$$

so $\boxed{gcd(k,j)} = gcd(r,j) = jx + ky$
where $\boxed{y = x'}$ and $\boxed{x = y' - qx'}$.

1) $GCD(k,j)$ where $0 \le j < k$

Returns $gcd(k,j)$ and

x, y s.t. $jx + ky = gcd(k,j)$

2) If $k = jq$, return $gcd(k,j) = j$, $x = 1$, $y = 0$

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Run $GCD(r,j)$ to find $gcd(r,j)$

and x', y' s.t. $gcd(r,j) = rx' + jy'$

6) Return $gcd(r,j)$, $x = y' - qx'$ and $y = x'$

1) $GCD(k,j)$ where $0 \le j < k$

Returns $gcd(k,j)$ and

x, y s.t. $jx + ky = gcd(k,j)$

2) If $k = jq$, return $gcd(k,j) = j$, $x = 1$, $y = 0$

3) Else

4) Write $k = jq + r$ where $r = k \bmod j$

5) Run $GCD(r,j)$ to find $gcd(r,j)$

and x', y' s.t. $gcd(r,j) = rx' + jy'$

6) Return $gcd(r,j)$, $x = y' - qx'$ and $y = x'$

Can implement this in two different ways

(i) Recursively (if you know about recursion already) or

(ii) Iteratively. First run the standard GCD algorithm "top-down", calculating all of the k, j, r, q.

Then run the extended part "bottom-up", calculating the values of the x, y.

We will now see an example of the iterative version.
We start at $i = 0$ with our original j, k and increase i each time we descend. This means that, given $j[i], k[i]$, we calculate

We will now see an example of the iterative version.
We start at $i = 0$ with our original j, k and increase i each time we descend. This means that, given $j[i], k[i]$, we calculate

$q[i], r[i]$ such that $k[i] = j[i]q[i] + r[i]$ where
$$r[i] = k[i] \bmod j[i]$$

and also $x[i], y[i]$ such that
$$j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$$

We will now see an example of the iterative version.
We start at $i = 0$ with our original j, k and increase i each time we descend. This means that, given $j[i], k[i]$, we calculate

$q[i], r[i]$ such that $k[i] = j[i]q[i] + r[i]$ where
$$r[i] = k[i] \bmod j[i]$$

and also $x[i], y[i]$ such that
$$j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$$

Note that, in this notation
$y[i-1] = x[i]$ and $x[i-1] = y[i] - q[i-1]x[i]$

Recall that (**) $y[i-1] = x[i]$ and (*) $x[i-1] = y[i] - q[i-1]x[i]$

and we want $j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$

Example: $k = 24, j = 14$

Recall that (**) $y[i-1] = x[i]$ and (*) $x[i-1] = y[i] - q[i-1]x[i]$

and we want $j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$

Example: $k = 24, j = 14$

i	$k[i]$	$=$	$j[i]q[i]$	$+$	$r[i]$	$k[i]$	$j[i]$	$r[i]$	$q[i]$
0	24	$=$	14(1)	$+$	10	24	14	10	1
1	14	$=$	10(1)	$+$	4	14	10	4	1
2	10	$=$	4(2)	$+$	2	10	4	2	2
3	4	$=$	2(2)	$+$	0	4	2	0	2

1) First run the regular GCD algorithm: get $gcd(24, 14) = 2$

Recall that (**) $y[i-1] = x[i]$ and (*) $x[i-1] = y[i] - q[i-1]x[i]$

and we want $j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$

Example: $k = 24, j = 14$

i	$k[i]$	$=$	$j[i]q[i]$	$+$	$r[i]$	$k[i]$	$j[i]$	$r[i]$	$q[i]$	$y[i]$	$x[i]$
0	24	$=$	14(1)	$+$	10	24	14	10	1		
1	14	$=$	10(1)	$+$	4	14	10	4	1		
2	10	$=$	4(2)	$+$	2	10	4	2	2		
3	4	$=$	2(2)	$+$	0	4	2	0	2	0	1

1) First run the regular GCD algorithm: get $gcd(24, 14) = 2$

2) Then calculate $y[3] = 0, x[3] = 1$

Recall that (**) $y[i-1] = x[i]$ and (*) $x[i-1] = y[i] - q[i-1]x[i]$

and we want $j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$

Example: $k = 24, j = 14$

i	$k[i]$	$=$	$j[i]q[i]$	$+$	$r[i]$	$k[i]$	$j[i]$	$r[i]$	$q[i]$	$y[i]$	$x[i]$
0	24	$=$	14(1)	$+$	10	24	14	10	1		
1	14	$=$	10(1)	$+$	4	14	10	4	1		
2	10	$=$	4(2)	$+$	2	10	4	2	2	1	-2
3	4	$=$	2(2)	$+$	0	4	2	0	2	0	1

1) First run the regular GCD algorithm: get $gcd(24, 14) = 2$

2) Then calculate $y[3] = 0, x[3] = 1$

3) Continue bottom-up, calculating the $x[i], y[i]$ from (*) and (**)

Recall that (**) $y[i-1] = x[i]$ and (*) $x[i-1] = y[i] - q[i-1]x[i]$

and we want $j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$

Example: $k = 24, j = 14$

i	$k[i]$	$=$	$j[i]q[i]$	$+$	$r[i]$	$k[i]$	$j[i]$	$r[i]$	$q[i]$	$y[i]$	$x[i]$
0	24	$=$	14(1)	$+$	10	24	14	10	1		
1	14	$=$	10(1)	$+$	4	14	10	4	1	-2	3
2	10	$=$	4(2)	$+$	2	10	4	2	2	1	-2
3	4	$=$	2(2)	$+$	0	4	2	0	2	0	1

1) First run the regular GCD algorithm: get $gcd(24, 14) = 2$

2) Then calculate $y[3] = 0, x[3] = 1$

3) Continue bottom-up, calculating the $x[i], y[i]$ from (*) and (**)

Recall that (**) $y[i-1] = x[i]$ and (*) $x[i-1] = y[i] - q[i-1]x[i]$

and we want $j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$

Example: $k = 24, j = 14$

i	$k[i]$	$=$	$j[i]q[i]$	$+$	$r[i]$	$k[i]$	$j[i]$	$r[i]$	$q[i]$	$y[i]$	$x[i]$
0	24	=	14(1)	+	10	24	14	10	1	3	-5
1	14	=	10(1)	+	4	14	10	4	1	-2	3
2	10	=	4(2)	+	2	10	4	2	2	1	-2
3	4	=	2(2)	+	0	4	2	0	2	0	1

1) First run the regular GCD algorithm: get $gcd(24, 14) = 2$

2) Then calculate $y[3] = 0, x[3] = 1$

3) Continue bottom-up, calculating the $x[i], y[i]$ from (*) and (**)

Recall that (**) $y[i-1] = x[i]$ and (*) $x[i-1] = y[i] - q[i-1]x[i]$

and we want $j[i]x[i] + k[i]y[i] = gcd(k[i], j[i])$

Example: $k = 24, j = 14$

i	$k[i]$	$=$	$j[i]q[i]$	$+$	$r[i]$	$k[i]$	$j[i]$	$r[i]$	$q[i]$	$y[i]$	$x[i]$
0	24	=	14(1)	+	10	24	14	10	1	3	-5
1	14	=	10(1)	+	4	14	10	4	1	-2	3
2	10	=	4(2)	+	2	10	4	2	2	1	-2
3	4	=	2(2)	+	0	4	2	0	2	0	1

1) First run the regular GCD algorithm: get $gcd(24, 14) = 2$

2) Then calculate $y[3] = 0, x[3] = 1$

3) Continue bottom-up, calculating the $x[i], y[i]$ from (*) and (**)

4) We are done! Note that $24(3) + 14(-5) = 2 = gcd(24, 14)$.

Euclid's extended GCD algorithm then gives

Euclid's extended GCD algorithm then gives

Theorem 2.14: Given two integers j, k, Euclid's extended GCD algorithm computes $gcd(j, k)$ and two integers x, y such that $gcd(j, k) = jx + ky$.

Euclid's extended GCD algorithm then gives

Theorem 2.14: Given two integers j, k, Euclid's extended GCD algorithm computes $gcd(j, k)$ and two integers x, y such that $gcd(j, k) = jx + ky$.

We can now extend Lemma 2.11 to

Euclid's extended GCD algorithm then gives

Theorem 2.14: Given two integers j, k, Euclid's extended GCD algorithm computes $gcd(j, k)$ and two integers x, y such that $gcd(j, k) = jx + ky$.

We can now extend Lemma 2.11 to

Theorem 2.15: Two positive integers j, k have $gcd(j, k) = 1$ (and thus are relatively prime) if and only if there are integers x, y such that $jx + ky = 1$.

Euclid's extended GCD algorithm then gives

Theorem 2.14: Given two integers j, k, Euclid's extended GCD algorithm computes $gcd(j, k)$ and two integers x, y such that $gcd(j, k) = jx + ky$.

We can now extend Lemma 2.11 to

Theorem 2.15: Two positive integers j, k have $gcd(j, k) = 1$ (and thus are relatively prime) if and only if there are integers x, y such that $jx + ky = 1$.

Proof: *"if"* comes from Lemma 2.11
"only if" comes from Theorem 2.14

Recall

Lemma 2.8 The equation $a \cdot_n x = 1$ has a solution in Z_n iff there exist integers x, y such that $ax + ny = 1$.

Recall

Lemma 2.8 The equation $a \cdot_n x = 1$ has a solution in Z_n iff there exist integers x, y such that $ax + ny = 1$.

Combining this and Theorem 2.15 gives

Corollary 2.16: For any positive integer n, $a \in Z_n$ has a multiplicative inverse iff $gcd(a, n) = 1$.

Recall

Lemma 2.8 The equation $a \cdot_n x = 1$ has a solution in Z_n iff there exist integers x, y such that $ax + ny = 1$.

Combining this and Theorem 2.15 gives

Corollary 2.16: For any positive integer n, $a \in Z_n$ has a multiplicative inverse iff $gcd(a, n) = 1$.

Using the fact that if n is prime, $gcd(a, n) = 1$ for all nonzero $a \in Z_n$, we obtain

Recall

Lemma 2.8 The equation $a \cdot_n x = 1$ has a solution in Z_n iff there exist integers x, y such that $ax + ny = 1$.

Combining this and Theorem 2.15 gives

Corollary 2.16: For any positive integer n, $a \in Z_n$ has a multiplicative inverse iff $gcd(a, n) = 1$.

Using the fact that if n is prime, $gcd(a, n) = 1$ for all nonzero $a \in Z_n$, we obtain

Corollary 2.17: For any prime p, every nonzero $a \in Z_p$ has a mutiplicative inverse.

Z_5:

a	1	2	3	4
a'	1	3	2	4

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_7:

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Z_8:

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

Z_9:

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

We noted that $5, 7$ are prime and all of the elements in Z_5, Z_7 have inverses.

For the non-prime $n \in 6, 8, 9$ the elements in Z_9 that have inverses are exactly those elements that are relatively prime to n.

Nice pattern!!
We now know that it's aways true

2.2 Inverses and Greatest Common Divisors

- Greatest Common Divisors
- Euclid's Division Theorem
- Euclid's GCD Algorithm
- Solutions to Equations and Inverses mod n
- Converting Modular Equations to Normal Equations
- Extended GCD Agorithm
- Computing Inverses

Computing Inverses

Computing Inverses

Corollary 2.18: If an element $a \in Z_n$ has an inverse, we can compute it by running Euclid's extended GCD algorithm to determine integers x, y so that $ax + ny = 1$. The inverse of $a \in Z_n$ is $x \bmod n$.

Computing Inverses

Corollary 2.18: If an element $a \in Z_n$ has an inverse, we can compute it by running Euclid's extended GCD algorithm to determine integers x, y so that $ax + ny = 1$. The inverse of $a \in Z_n$ is $x \bmod n$.

Example: Given $a = 27$, $n = 58$ we can use the Extended GCD algorithm to find that

$$27(-15) + 58(7) = 1.$$

Thus the multiplicative inverse of 27 in Z_{58} is

$$-15 \bmod 58 = 43.$$

Computing Inverses

Corollary 2.18: If an element $a \in Z_n$ has an inverse, we can compute it by running Euclid's extended GCD algorithm to determine integers x, y so that $ax + ny = 1$. The inverse of $a \in Z_n$ is $x \bmod n$.

Example: Given $a = 27$, $n = 58$ we can use the Extended GCD algorithm to find that

$$27(-15) + 58(7) = 1.$$

Thus the multiplicative inverse of 27 in Z_{58} is

$$-15 \bmod 58 = 43.$$

Reality check: $27 \cdot 43 = 1161 = 20 \cdot 58 + 1$

We now know how to *efficiently* find inverses $\bmod n$.

We are almost ready to learn the RSA public-key algorithm.