Number Theory Lecture, Feb. 1: Congruence equations

Larry Rolen

Polynomial equations

- In number theory, we often study solutions to polynomial equations $f(x) = 0$ for a polynomial $f(x)$.

Polynomial equations

- In number theory, we often study solutions to polynomial equations $f(x) = 0$ for a polynomial $f(x)$.
- Calculus gives easier ways to find real numbers x solving polynomial equations; for example the Mean Value Theorem.

Polynomial equations

- In number theory, we often study solutions to polynomial equations $f(x) = 0$ for a polynomial $f(x)$.
- Calculus gives easier ways to find real numbers x solving polynomial equations; for example the Mean Value Theorem.
- In number theory, we often want to find roots of polynomials in $\mathbb{Q}$, which is harder than $\mathbb{R}$, or $\mathbb{Z}$, which is even harder, or which are primes, which is even harder still.

Polynomial equations

- In number theory, we often study solutions to polynomial equations $f(x) = 0$ for a polynomial $f(x)$.
- Calculus gives easier ways to find real numbers x solving polynomial equations; for example the Mean Value Theorem.
- In number theory, we often want to find roots of polynomials in $\mathbb{Q}$, which is harder than $\mathbb{R}$, or $\mathbb{Z}$, which is even harder, or which are primes, which is even harder still.
- If a polynomial equation has an integral solution, it has a solution modulo m for all $m \geq 2$. For instance, we saw that the equation $x^2 + y^2 = n$ has no integral solutions x, y whenever $n \equiv 3 \pmod 4$, as squares are always 0 or 1 (mod 4).

Congruence equations

- In general, if we have a polynomial congruence equation $a_n x^n + \ldots + a_0 \equiv 0 \pmod{m}$, then we can write this as an equation in $\mathbb{Z}$ in two variables, namely, $a_n x^n + \ldots + a_0 = my$ for $x, y \in \mathbb{Z}$.

Congruence equations

- In general, if we have a polynomial congruence equation $a_n x^n + \ldots + a_0 \equiv 0 \pmod{m}$, then we can write this as an equation in $\mathbb{Z}$ in two variables, namely, $a_n x^n + \ldots + a_0 = my$ for $x, y \in \mathbb{Z}$.
- We will solve increasingly complicated equations of this shape. First, we'll start with degree 1 polynomials.

Congruence equations

- In general, if we have a polynomial congruence equation $a_n x^n + \ldots + a_0 \equiv 0 \pmod{m}$, then we can write this as an equation in $\mathbb{Z}$ in two variables, namely, $a_n x^n + \ldots + a_0 = my$ for $x, y \in \mathbb{Z}$.
- We will solve increasingly complicated equations of this shape. First, we'll start with degree 1 polynomials.
- A **linear congruence equation** is one of the form $ax \equiv b \pmod{m}$.

Congruence equations

- In general, if we have a polynomial congruence equation $a_n x^n + \ldots + a_0 \equiv 0 \pmod{m}$, then we can write this as an equation in $\mathbb{Z}$ in two variables, namely, $a_n x^n + \ldots + a_0 = my$ for $x, y \in \mathbb{Z}$.
- We will solve increasingly complicated equations of this shape. First, we'll start with degree 1 polynomials.
- A **linear congruence equation** is one of the form $ax \equiv b \pmod{m}$.
- First, we need a few facts about division modulo m.

Division modulo m

- To solve $ax = b$ over $\mathbb{R}$, as long as $a \neq 0$, we simply divide by a to obtain $x = b/a$.

Division modulo m

- To solve $ax = b$ over $\mathbb{R}$, as long as $a \neq 0$, we simply divide by a to obtain $x = b/a$.
- Similarly, we frequently use the cancellation law $ax = bx \implies a = b (x \neq 0)$ and the fact that if $xy = 0$, then x or y is 0.

Division modulo m

- To solve $ax = b$ over $\mathbb{R}$, as long as $a \neq 0$, we simply divide by a to obtain $x = b/a$.
- Similarly, we frequently use the cancellation law $ax = bx \implies a = b (x \neq 0)$ and the fact that if $xy = 0$, then x or y is 0.
- These rules don't work in $\mathbb{Z}/m\mathbb{Z}$.

Division modulo m

- To solve $ax = b$ over $\mathbb{R}$, as long as $a \neq 0$, we simply divide by a to obtain $x = b/a$.
- Similarly, we frequently use the cancellation law $ax = bx \implies a = b (x \neq 0)$ and the fact that if $xy = 0$, then x or y is 0.
- These rules don't work in $\mathbb{Z}/m\mathbb{Z}$.
- For instance, $2 \cdot 3 \equiv 0 \pmod 6$, but $2, 3 \neq 0 \pmod 6$.

Division modulo m

- To solve $ax = b$ over $\mathbb{R}$, as long as $a \neq 0$, we simply divide by a to obtain $x = b/a$.
- Similarly, we frequently use the cancellation law $ax = bx \implies a = b (x \neq 0)$ and the fact that if $xy = 0$, then x or y is 0.
- These rules don't work in $\mathbb{Z}/m\mathbb{Z}$.
- For instance, $2 \cdot 3 \equiv 0 \pmod 6$, but $2, 3 \neq 0 \pmod 6$. We also have $3 \cdot 2 \equiv 3 \cdot 4 \pmod 6$, but $2 \not\equiv 4 \pmod 6$.

Division modulo m

- To solve $ax = b$ over $\mathbb{R}$, as long as $a \neq 0$, we simply divide by a to obtain $x = b/a$.
- Similarly, we frequently use the cancellation law $ax = bx \implies a = b (x \neq 0)$ and the fact that if $xy = 0$, then x or y is 0.
- These rules don't work in $\mathbb{Z}/m\mathbb{Z}$.
- For instance, $2 \cdot 3 \equiv 0 \pmod 6$, but $2, 3 \neq 0 \pmod 6$. We also have $3 \cdot 2 \equiv 3 \cdot 4 \pmod 6$, but $2 \not\equiv 4 \pmod 6$.
- However, there is a replacement for the cancellation law mod m. It is just that we lose information.

Cancellation law modulo m

Proposition

We have $ca \equiv cb \pmod{m} \iff a \equiv b \pmod{m/d}$, *where* $d := (c, m)$.

Cancellation law modulo m

Proposition

We have $ca \equiv cb \pmod{m} \iff a \equiv b \pmod{m/d}$, *where* $d := (c, m)$.

Proof.

$\Longrightarrow$: We have $m|(ca - cb) \implies m|c(a-b) \implies \frac{m}{d}|\frac{c}{d}(a-b)$.

Cancellation law modulo m

Proposition

We have $ca \equiv cb \pmod{m} \iff a \equiv b \pmod{m/d}$, *where* $d := (c, m)$.

Proof.

$\implies$: We have $m|(ca - cb) \implies m|c(a-b) \implies \frac{m}{d}|\frac{c}{d}(a-b)$. By an earlier result, $(\frac{m}{d}, \frac{c}{d}) = 1$, and thus (think about prime factorizations for instance), $\frac{m}{d}|(a-d) \implies a \equiv b \pmod{m/d}$.

Cancellation law modulo m

Proposition

We have $ca \equiv cb \pmod{m} \iff a \equiv b \pmod{m/d}$, *where* $d := (c, m)$.

Proof.

$\implies$: We have $m|(ca - cb) \implies m|c(a-b) \implies \frac{m}{d}|\frac{c}{d}(a-b)$. By an earlier result, $(\frac{m}{d}, \frac{c}{d}) = 1$, and thus (think about prime factorizations for instance), $\frac{m}{d}|(a-d) \implies a \equiv b \pmod{m/d}$.
$\impliedby$: We have $a \equiv b \pmod{m/d} \implies \frac{m}{d}|(a-b) \implies m|(da - db) \implies m|\frac{c}{d}(da-db) \implies m|(ca-cb) \implies ca \equiv cb \pmod{m}$. □

Example

- We saw above that $3 \cdot 2 \equiv 3 \cdot 4 \pmod{6}$.

Example

- We saw above that $3 \cdot 2 \equiv 3 \cdot 4 \pmod{6}$.
- The proposition gives that we cancel the 3's, but we have to divide the modulus by $(3, 6) = 3$, giving $2 \equiv 4 \pmod{2}$.

Example

- We saw above that $3 \cdot 2 \equiv 3 \cdot 4 \pmod{6}$.
- The proposition gives that we cancel the 3's, but we have to divide the modulus by $(3, 6) = 3$, giving $2 \equiv 4 \pmod{2}$.
- This is true, but we only get information about a congruence modulo 2, which is less information than a congruence modulo 6.

Linear Diophantine Equations

Theorem

Suppose we want to solve $ax \equiv b \pmod{m}$. *Set* $d = (a, m)$.

1. *If* $d \nmid b$, *then there are no solutions.*

Linear Diophantine Equations

Theorem

Suppose we want to solve $ax \equiv b \pmod{m}$. *Set* $d = (a, m)$.

1. *If* $d \nmid b$, *then there are no solutions.*
2. *If* $d|b$, *then there are precisely* d *distinct congruence classes of solutions modulo* m.

Linear Diophantine Equations

Theorem

Suppose we want to solve $ax \equiv b \pmod{m}$. *Set* $d = (a, m)$.

1. *If* $d \nmid b$, *then there are no solutions.*
2. *If* $d|b$, *then there are precisely* d *distinct congruence classes of solutions modulo* m.

Proof.

First, we observe that $ax \equiv b \pmod{m} \iff ax - b = my$ has a solution in $\mathbb{Z} \iff ax - my = b$.

Linear Diophantine Equations

Theorem

Suppose we want to solve $ax \equiv b \pmod{m}$. *Set* $d = (a, m)$.

1. *If* $d \nmid b$, *then there are no solutions.*
2. *If* $d|b$, *then there are precisely* d *distinct congruence classes of solutions modulo* m.

Proof.

First, we observe that $ax \equiv b \pmod{m} \iff ax - b = my$ has a solution in $\mathbb{Z} \iff ax - my = b$. But
$d|a, m \implies d|(ax - my)$

Linear Diophantine Equations

Theorem

Suppose we want to solve $ax \equiv b \pmod{m}$. *Set* $d = (a, m)$.

1. *If* $d \nmid b$, *then there are no solutions.*
2. *If* $d|b$, *then there are precisely* d *distinct congruence classes of solutions modulo* m.

Proof.

First, we observe that $ax \equiv b \pmod{m} \iff ax - b = my$ has a solution in $\mathbb{Z} \iff ax - my = b$. But
$d|a, m \implies d|(ax - my) \implies d|b$.

Linear Diophantine Equations

Theorem

Suppose we want to solve $ax \equiv b \pmod{m}$. *Set* $d = (a, m)$.

1. *If* $d \nmid b$, *then there are no solutions.*
2. *If* $d|b$, *then there are precisely* d *distinct congruence classes of solutions modulo* m.

Proof.

First, we observe that $ax \equiv b \pmod{m} \iff ax - b = my$ has a solution in $\mathbb{Z} \iff ax - my = b$. But $d|a, m \implies d|(ax - my) \implies d|b$. This proves part 1). □

Proof (cont.)

- Now suppose $d|b$.

Proof (cont.)

- Now suppose $d|b$.
- By Bezout, there are $r, s \in \mathbb{Z}$ such that $d = ar + ms$.

Proof (cont.)

- Now suppose $d|b$.
- By Bezout, there are $r, s \in \mathbb{Z}$ such that $d = ar + ms$.
- As $d|b$, we have $b = de$ for some e.

Proof (cont.)

- Now suppose $d|b$.
- By Bezout, there are $r, s \in \mathbb{Z}$ such that $d = ar + ms$.
- As $d|b$, we have $b = de$ for some e.
- Thus, we have $b = a(er) + m(se)$.

Proof (cont.)

- Now suppose $d|b$.
- By Bezout, there are $r, s \in \mathbb{Z}$ such that $d = ar + ms$.
- As $d|b$, we have $b = de$ for some e.
- Thus, we have $b = a(er) + m(se)$. Thus, $x = re$, $y = -se$ solves the desired equation, and a solution exists.

Proof (cont.)

- Now suppose $d|b$.
- By Bezout, there are $r, s \in \mathbb{Z}$ such that $d = ar + ms$.
- As $d|b$, we have $b = de$ for some e.
- Thus, we have $b = a(er) + m(se)$. Thus, $x = re$, $y = -se$ solves the desired equation, and a solution exists.
- Two numbers x and x_0 are both solutions iff $b \equiv ax \equiv ax_0 \pmod{m} \iff x \equiv x_0 \pmod{m}/d$, by the Prop.

Proof (cont.)

- Now suppose $d|b$.
- By Bezout, there are $r, s \in \mathbb{Z}$ such that $d = ar + ms$.
- As $d|b$, we have $b = de$ for some e.
- Thus, we have $b = a(er) + m(se)$. Thus, $x = re$, $y = -se$ solves the desired equation, and a solution exists.
- Two numbers x and x_0 are both solutions iff $b \equiv ax \equiv ax_0 \pmod{m} \iff x \equiv x_0 \pmod{m}/d$, by the Prop.
- Thus, the solutions are given by the d many congruence classes $x \equiv x_0 + k(\frac{m}{d})$, $k = 0, \ldots, d-1$, where x_0 is a "particular solution."

Splitting of congruence classes

- An intuitive way of describing the final step is that the congruence class mod m/d "splits up" into d congruences mod m.

Splitting of congruence classes

- An intuitive way of describing the final step is that the congruence class mod m/d "splits up" into d congruences mod m.
- For instance, if $n \equiv 3 \pmod 6$, then it splits into two congruence classes modulo 12, n$\equiv 3, 9 \pmod{12}$.

Solve $56x \equiv 1 \pmod{93}$

- We first check that $d = (56, 93) = 1$ divides $b = 1$, and so there exists 1 solution mod 93.

Solve $56x \equiv 1 \pmod{93}$

- We first check that $d = (56, 93) = 1$ divides $b = 1$, and so there exists 1 solution mod 93.
- To find it, we solve $56x = 1 + 93y \iff 56x - 93y = 1$.

Solve $56x \equiv 1 \pmod{93}$

- We first check that $d = (56, 93) = 1$ divides $b = 1$, and so there exists 1 solution mod 93.
- To find it, we solve $56x = 1 + 93y \iff 56x - 93y = 1$.
- We perform the Euclidean algorithm:

$$93 = 56 \cdot 1 + 37,$$

$$56 = 37 \cdot 1 + 19,$$

$$37 = 19 \cdot 1 + 18,$$

$$19 = 18 \cdot 1 + 1.$$

Solve $56x \equiv 1 \pmod{93}$

- We first check that $d = (56, 93) = 1$ divides $b = 1$, and so there exists 1 solution mod 93.
- To find it, we solve $56x = 1 + 93y \iff 56x - 93y = 1$.
- We perform the Euclidean algorithm:

$$93 = 56 \cdot 1 + 37,$$

$$56 = 37 \cdot 1 + 19,$$

$$37 = 19 \cdot 1 + 18,$$

$$19 = 18 \cdot 1 + 1.$$

- Back substituting, we find:
  $1 = 19 - 18 = 19 - (37 - 19) = 2 \cdot 19 - 37$

Solve $56x \equiv 1 \pmod{93}$

- We first check that $d = (56, 93) = 1$ divides $b = 1$, and so there exists 1 solution mod 93.
- To find it, we solve $56x = 1 + 93y \iff 56x - 93y = 1$.
- We perform the Euclidean algorithm:

$$93 = 56 \cdot 1 + 37,$$

$$56 = 37 \cdot 1 + 19,$$

$$37 = 19 \cdot 1 + 18,$$

$$19 = 18 \cdot 1 + 1.$$

- Back substituting, we find:
$1 = 19 - 18 = 19 - (37 - 19) = 2 \cdot 19 - 37 = 2 \cdot (56 - 37) - 37 = 2 \cdot 56 - 3 \cdot 37$

Solve $56x \equiv 1 \pmod{93}$

- We first check that $d = (56, 93) = 1$ divides $b = 1$, and so there exists 1 solution mod 93.
- To find it, we solve $56x = 1 + 93y \iff 56x - 93y = 1$.
- We perform the Euclidean algorithm:

$$93 = 56 \cdot 1 + 37,$$

$$56 = 37 \cdot 1 + 19,$$

$$37 = 19 \cdot 1 + 18,$$

$$19 = 18 \cdot 1 + 1.$$

- Back substituting, we find:
$1 = 19 - 18 = 19 - (37 - 19) = 2 \cdot 19 - 37 = 2 \cdot (56 - 37) - 37 =$
$2 \cdot 56 - 3 \cdot 37 = 2 \cdot 56 - 3 \cdot (93 - 56) = (-3) \cdot 93 + 5 \cdot 56.$

Solve $56x \equiv 1 \pmod{93}$

- We first check that $d = (56, 93) = 1$ divides $b = 1$, and so there exists 1 solution mod 93.
- To find it, we solve $56x = 1 + 93y \iff 56x - 93y = 1$.
- We perform the Euclidean algorithm:

$$93 = 56 \cdot 1 + 37,$$

$$56 = 37 \cdot 1 + 19,$$

$$37 = 19 \cdot 1 + 18,$$

$$19 = 18 \cdot 1 + 1.$$

- Back substituting, we find:
  $1 = 19 - 18 = 19 - (37 - 19) = 2 \cdot 19 - 37 = 2 \cdot (56 - 37) - 37 = 2 \cdot 56 - 3 \cdot 37 = 2 \cdot 56 - 3 \cdot (93 - 56) = (-3) \cdot 93 + 5 \cdot 56.$
- Thus, the solution is $x \equiv 5 \pmod{93}$.

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.
- We find a particular solution by turning the congruence into an equation in two variables
  $15x = 12 + 57y \iff 15x - 57y = 12$. We divide through by the gcd to get $5x - 19y = 4$, and now note that $(5, 19) = 1$.

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.
- We find a particular solution by turning the congruence into an equation in two variables $15x = 12 + 57y \iff 15x - 57y = 12$. We divide through by the gcd to get $5x - 19y = 4$, and now note that $(5, 19) = 1$.
- We do the Euclidean algorithm to get $19 = 3 \cdot 5 + 4$ and $5 = 4 + 1$, and then plug in to get

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.
- We find a particular solution by turning the congruence into an equation in two variables
  $15x = 12 + 57y \iff 15x - 57y = 12$. We divide through by the gcd to get $5x - 19y = 4$, and now note that $(5, 19) = 1$.
- We do the Euclidean algorithm to get $19 = 3 \cdot 5 + 4$ and $5 = 4 + 1$, and then plug in to get
  $1 = 5 - 4 = 5 - (19 - 3 \cdot 5) = 4 \cdot 5 - 1 \cdot 19$.

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.
- We find a particular solution by turning the congruence into an equation in two variables
  $15x = 12 + 57y \iff 15x - 57y = 12$. We divide through by the gcd to get $5x - 19y = 4$, and now note that $(5, 19) = 1$.
- We do the Euclidean algorithm to get $19 = 3 \cdot 5 + 4$ and $5 = 4 + 1$, and then plug in to get
  $1 = 5 - 4 = 5 - (19 - 3 \cdot 5) = 4 \cdot 5 - 1 \cdot 19$.
- Thus, $3 = 4 \cdot 15 - 1 \cdot 57$. Now $b = 12 = 4 \cdot 3$, and so

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.
- We find a particular solution by turning the congruence into an equation in two variables
  $15x = 12 + 57y \iff 15x - 57y = 12$. We divide through by the gcd to get $5x - 19y = 4$, and now note that $(5, 19) = 1$.
- We do the Euclidean algorithm to get $19 = 3 \cdot 5 + 4$ and $5 = 4 + 1$, and then plug in to get
  $1 = 5 - 4 = 5 - (19 - 3 \cdot 5) = 4 \cdot 5 - 1 \cdot 19$.
- Thus, $3 = 4 \cdot 15 - 1 \cdot 57$. Now $b = 12 = 4 \cdot 3$, and so
  $4 \cdot 3 = b = 16 \cdot 15 - 4 \cdot 57$.

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.
- We find a particular solution by turning the congruence into an equation in two variables $15x = 12 + 57y \iff 15x - 57y = 12$. We divide through by the gcd to get $5x - 19y = 4$, and now note that $(5, 19) = 1$.
- We do the Euclidean algorithm to get $19 = 3 \cdot 5 + 4$ and $5 = 4 + 1$, and then plug in to get $1 = 5 - 4 = 5 - (19 - 3 \cdot 5) = 4 \cdot 5 - 1 \cdot 19$.
- Thus, $3 = 4 \cdot 15 - 1 \cdot 57$. Now $b = 12 = 4 \cdot 3$, and so $4 \cdot 3 = b = 16 \cdot 15 - 4 \cdot 57$.
- Thus, a particular solution is $x_0 = 16$.

Solve $15x \equiv 12 \pmod{57}$

- We first check that $(15, 57) = 3|12$. Thus, there are 3 solutions mod 57.
- We find a particular solution by turning the congruence into an equation in two variables $15x = 12 + 57y \iff 15x - 57y = 12$. We divide through by the gcd to get $5x - 19y = 4$, and now note that $(5, 19) = 1$.
- We do the Euclidean algorithm to get $19 = 3 \cdot 5 + 4$ and $5 = 4 + 1$, and then plug in to get $1 = 5 - 4 = 5 - (19 - 3 \cdot 5) = 4 \cdot 5 - 1 \cdot 19$.
- Thus, $3 = 4 \cdot 15 - 1 \cdot 57$. Now $b = 12 = 4 \cdot 3$, and so $4 \cdot 3 = b = 16 \cdot 15 - 4 \cdot 57$.
- Thus, a particular solution is $x_0 = 16$. All solutions are shifts by $57/3 = 19$ mod 57. That is, they are $x \equiv 16, 35, 54 \pmod{57}$.

Special case: inverses

- When $b = 1$, the equation is $ax \equiv 1 \pmod{m}$. In this situation, we say that x is an **inverse** of $a \pmod{m}$, and write $x = \overline{a}$.

Special case: inverses

- When $b = 1$, the equation is $ax \equiv 1 \pmod{m}$. In this situation, we say that x is an **inverse** of $a \pmod{m}$, and write $x = \overline{a}$.
- Note that $(a, m)|1 \iff (a, m) = 1$.

Special case: inverses

- When $b = 1$, the equation is $ax \equiv 1 \pmod{m}$. In this situation, we say that x is an **inverse** of $a \pmod{m}$, and write $x = \overline{a}$.
- Note that $(a, m)|1 \iff (a, m) = 1$. Thus, a is invertible modulo m, i.e., has an inverse, if and only if its coprime to m.

Special case: inverses

- When $b = 1$, the equation is $ax \equiv 1 \pmod{m}$. In this situation, we say that x is an **inverse** of $a \pmod{m}$, and write $x = \overline{a}$.
- Note that $(a, m)|1 \iff (a, m) = 1$. Thus, a is invertible modulo m, i.e., has an inverse, if and only if its coprime to m.
- Moreover, our theorem shows that when an inverse does exist, the inverse is unique modulo m, and as expected, the unique solution to the equation $ax \equiv b \pmod{m}$ for any b is $x \equiv \overline{a}b \pmod{m}$.

Special case: inverses

- When $b = 1$, the equation is $ax \equiv 1 \pmod{m}$. In this situation, we say that x is an **inverse** of $a \pmod{m}$, and write $x = \overline{a}$.
- Note that $(a, m)|1 \iff (a, m) = 1$. Thus, a is invertible modulo m, i.e., has an inverse, if and only if its coprime to m.
- Moreover, our theorem shows that when an inverse does exist, the inverse is unique modulo m, and as expected, the unique solution to the equation $ax \equiv b \pmod{m}$ for any b is $x \equiv \overline{a}b \pmod{m}$.
- In the special case when p is a prime, then *every* non-zero congruence class mod p has an inverse. This is encapsulated in the fancy, but important, fact that $\mathbb{Z}/p\mathbb{Z}$ is a **field**, which is like a ring, but inverses of non-zero elements exist.

Example: Find $\overline{56} \pmod{93}$

- We want to solve $56x \equiv 1 \pmod{93}$.

Example: Find $\overline{56} \pmod{93}$

- We want to solve $56x \equiv 1 \pmod{93}$.
- We write this as $56x - 93y = 1$.

Example: Find $\overline{56} \pmod{93}$

- We want to solve $56x \equiv 1 \pmod{93}$.
- We write this as $56x - 93y = 1$.
- From before, we have $1 = (-3) \cdot 93 + 5 \cdot 56$.

Example: Find $\overline{56} \pmod{93}$

- We want to solve $56x \equiv 1 \pmod{93}$.
- We write this as $56x - 93y = 1$.
- From before, we have $1 = (-3) \cdot 93 + 5 \cdot 56$.
- Thus, the inverse is $\overline{56} = 5$.

Example: Find $\overline{56} \pmod{93}$

- We want to solve $56x \equiv 1 \pmod{93}$.
- We write this as $56x - 93y = 1$.
- From before, we have $1 = (-3) \cdot 93 + 5 \cdot 56$.
- Thus, the inverse is $\overline{56} = 5$.
- As a sanity check, we have $56 \cdot 5 = 280 = 93 \cdot 3 + 1 \equiv 1 \pmod{93}$.

Example: Find $\overline{56} \pmod{93}$

- We want to solve $56x \equiv 1 \pmod{93}$.
- We write this as $56x - 93y = 1$.
- From before, we have $1 = (-3) \cdot 93 + 5 \cdot 56$.
- Thus, the inverse is $\overline{56} = 5$.
- As a sanity check, we have $56 \cdot 5 = 280 = 93 \cdot 3 + 1 \equiv 1 \pmod{93}$.
- Now, to solve an equation like $56x \equiv 5 \pmod{93}$, we can multiply by the inverse to find $x \equiv \overline{56} \cdot 5 \equiv 5 \cdot 5 \equiv 5 \pmod{93}$.

Generalizations

- Systems of equations (shortly, we'll cover the **Chinese Remainder Theorem** (CRT))

Generalizations

- Systems of equations (shortly, we'll cover the **Chinese Remainder Theorem** (CRT))
- Higher degree polynomials.

Generalizations

- Systems of equations (shortly, we'll cover the **Chinese Remainder Theorem** (CRT))
- Higher degree polynomials. The CRT implies that solving $f(x) \equiv 0 \pmod{n}$ for a polynomial $f(x)$ is equivalent to solving $f(x) \equiv 0 \pmod{p_i^{e_i}}$, where $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$.

Generalizations

- Systems of equations (shortly, we'll cover the **Chinese Remainder Theorem** (CRT))
- Higher degree polynomials. The CRT implies that solving $f(x) \equiv 0 \pmod{n}$ for a polynomial $f(x)$ is equivalent to solving $f(x) \equiv 0 \pmod{p_i^{e_i}}$, where $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$.
- Thus, solving all polynomial equations mod m is equivalent to solving them mod prime powers.

Generalizations

- Systems of equations (shortly, we'll cover the **Chinese Remainder Theorem** (CRT))
- Higher degree polynomials. The CRT implies that solving $f(x) \equiv 0 \pmod{n}$ for a polynomial $f(x)$ is equivalent to solving $f(x) \equiv 0 \pmod{p_i^{e_i}}$, where $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$.
- Thus, solving all polynomial equations mod m is equivalent to solving them mod prime powers.
- **Hensel's Lemma** (to be covered soon) gives conditions on when solutions to $f(x) \equiv 0 \pmod{p^a}$ **lift** to solutions to $f(x) \equiv 0 \pmod{p^{a+1}}$.

Generalizations

- Systems of equations (shortly, we'll cover the **Chinese Remainder Theorem** (CRT))
- Higher degree polynomials. The CRT implies that solving $f(x) \equiv 0 \pmod{n}$ for a polynomial $f(x)$ is equivalent to solving $f(x) \equiv 0 \pmod{p_i^{e_i}}$, where $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$.
- Thus, solving all polynomial equations mod m is equivalent to solving them mod prime powers.
- **Hensel's Lemma** (to be covered soon) gives conditions on when solutions to $f(x) \equiv 0 \pmod{p^a}$ **lift** to solutions to $f(x) \equiv 0 \pmod{p^{a+1}}$.
- Thus, its often enough to study $f(x) \equiv 0 \pmod{p}$ just for primes p.

A useful result

Theorem

If $f(x)$ is a polynomial with integer coefficients of degree d, and p doesn't divide every coefficient, then $f(x) \equiv 0 \pmod{p}$ has **at most** *d solutions.*

A useful result

Theorem

If $f(x)$ is a polynomial with integer coefficients of degree d, and p doesn't divide every coefficient, then $f(x) \equiv 0 \pmod{p}$ has **at most** *d solutions.*

- Why?

A useful result

Theorem

If $f(x)$ is a polynomial with integer coefficients of degree d, and p doesn't divide every coefficient, then $f(x) \equiv 0 \pmod{p}$ has **at most** *d solutions.*

- Why?
- There is a Euclidean *division algorithm!*

A useful result

Theorem

If $f(x)$ is a polynomial with integer coefficients of degree d, and p doesn't divide every coefficient, then $f(x) \equiv 0 \pmod{p}$ has **at most** *d solutions.*

- Why?
- There is a Euclidean *division algorithm!* Basically, because $\mathbb{Z}/p\mathbb{Z}$ is a *field*, polynomial long division with remainder is a Euclidean division algorithm (if inverses don't exist, you can't perform polynomial long division).

A useful result

Theorem

If $f(x)$ is a polynomial with integer coefficients of degree d, and p doesn't divide every coefficient, then $f(x) \equiv 0 \pmod{p}$ has **at most** *d solutions.*

- Why?
- There is a Euclidean *division algorithm!* Basically, because $\mathbb{Z}/p\mathbb{Z}$ is a *field*, polynomial long division with remainder is a Euclidean division algorithm (if inverses don't exist, you can't perform polynomial long division).
- Then its just like this fact over the real numbers. One checks that $f(a) \equiv 0 \pmod{p}$ iff $f(x) \equiv (x-a)g(x) \pmod{p}$ for some polynomial $g(x)$, and keep splitting off linear factors!