Congruences with a Prime-Power Modulus

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

09:00, Tuesday 06th December 2011
09:00, Tuesday 10th January 2012

Outline

University of Bedfordshire

Outline

University of Bedfordshire

- $ax \equiv b \bmod (n)$ has unique solution $\bmod(n)$ if $gcd(a, n) = 1$.
- If n is a prime, p, then $gcd(a, p)$ is either 1 or p.
  1. $gcd(a, p) = 1$ has a unique solution $\bmod(p)$
  2. $gcd(a, p) = p$
     - if $p \mid b$ every x is a solution.
     - if $p \nmid b$ no x is a solution.

If the polynomial $ax - b$ has degree $d = 1$ over $\mathbb{Z}_p$ (that is, if $a \not\equiv 0 \bmod (p)$), then it has at most one root in $\mathbb{Z}_p$.

In algebra we learn that a polynomial of degree d has at most d distinct roots.

Is this also true for number systems $\mathbb{Z}_p$ (we have just seen it is true for $d = 1$)?

University of Bedfordshire

Lagrange's Theorem

Theorem

Let p be prime, and let $f(x) = a_d x^d + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, where $a_i \not\equiv 0 \bmod (p)$ for some i. Then the congruence $f(x) \equiv 0 \bmod (p)$ is satisfied by at most d congruence classes $[x] \in \mathbb{Z}_p$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.

University of Bedfordshire

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.
$p = 3$; there are no classes in $\mathbb{Z}_3$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.
$p = 3$; there are no classes in $\mathbb{Z}_3$.
$p = 5$; there are two classes, $\pm[2]$ in $\mathbb{Z}_5$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.
$p = 3$; there are no classes in $\mathbb{Z}_3$.
$p = 5$; there are two classes, $\pm[2]$ in $\mathbb{Z}_5$.
$p = 7$; there are no classes in $\mathbb{Z}_7$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.
$p = 3$; there are no classes in $\mathbb{Z}_3$.
$p = 5$; there are two classes, $\pm[2]$ in $\mathbb{Z}_5$.
$p = 7$; there are no classes in $\mathbb{Z}_7$.
$p = 11$; there are no classes in $\mathbb{Z}_{11}$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.
$p = 3$; there are no classes in $\mathbb{Z}_3$.
$p = 5$; there are two classes, $\pm[2]$ in $\mathbb{Z}_5$.
$p = 7$; there are no classes in $\mathbb{Z}_7$.
$p = 11$; there are no classes in $\mathbb{Z}_{11}$.
$p = 13$; there are two classes, $\pm[5]$ in $\mathbb{Z}_{13}$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.
$p = 3$; there are no classes in $\mathbb{Z}_3$.
$p = 5$; there are two classes, $\pm[2]$ in $\mathbb{Z}_5$.
$p = 7$; there are no classes in $\mathbb{Z}_7$.
$p = 11$; there are no classes in $\mathbb{Z}_{11}$.
$p = 13$; there are two classes, $\pm[5]$ in $\mathbb{Z}_{13}$.
$p = 17$; there are two classes, $\pm[4]$ in $\mathbb{Z}_{17}$.

Example - Roots of $f(x) = x^2 + 1$ in $\mathbb{Z}_p$

As an example, we consider the polynomial $f(x) = x^2 + 1$ and find the roots in $\mathbb{Z}_p$.
Let us consider the primes $p \leq 17$.
$p = 2$; there is one class, $[1]$ in $\mathbb{Z}_2$.
$p = 3$; there are no classes in $\mathbb{Z}_3$.
$p = 5$; there are two classes, $\pm[2]$ in $\mathbb{Z}_5$.
$p = 7$; there are no classes in $\mathbb{Z}_7$.
$p = 11$; there are no classes in $\mathbb{Z}_{11}$.
$p = 13$; there are two classes, $\pm[5]$ in $\mathbb{Z}_{13}$.
$p = 17$; there are two classes, $\pm[4]$ in $\mathbb{Z}_{17}$.
There are two roots if $p \equiv 1 \bmod (4)$, none if $p \equiv 3 \bmod (4)$, and one if $p = 2$.

Fermat's Little Theorem

- If p is prime, the classes $[a] \neq [0]$ in $\mathbb{Z}_p$ are closed under taking products and inverses,

University of Bedfordshire

Fermat's Little Theorem

- If p is prime, the classes $[a] \neq [0]$ in $\mathbb{Z}_p$ are closed under taking products and inverses,
- so they form a group under multiplication, with identity $[1]$.

Fermat's Little Theorem

- If p is prime, the classes $[a] \neq [0]$ in $\mathbb{Z}_p$ are closed under taking products and inverses,
- so they form a group under multiplication, with identity $[1]$.
- If $[a] \neq [0]$ then the congruence $ax \equiv 1 \bmod (p)$ has unique solution $[x] \neq [0]$ in $(\mathbb{Z})_p$.

Fermat's Little Theorem

- If p is prime, the classes $[a] \neq [0]$ in $\mathbb{Z}_p$ are closed under taking products and inverses,
- so they form a group under multiplication, with identity $[1]$.
- If $[a] \neq [0]$ then the congruence $ax \equiv 1 \bmod (p)$ has unique solution $[x] \neq [0]$ in $(\mathbb{Z})_p$.
- This class is the inverse of $[a]$.

Fermat's Little Theorem

- If p is prime, the classes $[a] \neq [0]$ in $\mathbb{Z}_p$ are closed under taking products and inverses,
- so they form a group under multiplication, with identity [1].
- If $[a] \neq [0]$ then the congruence $ax \equiv 1 \bmod (p)$ has unique solution $[x] \neq [0]$ in $(\mathbb{Z})_p$.
- This class is the inverse of $[a]$.
- This group of non-zero classes has order $p - 1$ (it contains $p - 1$ elements).

FERMAT'S LITTLE THEOREM

- If p is prime, the classes $[a] \neq [0]$ in $\mathbb{Z}_p$ are closed under taking products and inverses,
- so they form a group under multiplication, with identity $[1]$.
- If $[a] \neq [0]$ then the congruence $ax \equiv 1 \bmod (p)$ has unique solution $[x] \neq [0]$ in $(\mathbb{Z})_p$.
- This class is the inverse of $[a]$.
- This group of non-zero classes has order $p - 1$ (it contains $p - 1$ elements).
- If g is any element of a group of finite order n, then g^n is the identity element in that group.

Fermat's Little Theorem

- If p is prime, the classes $[a] \neq [0]$ in $\mathbb{Z}_p$ are closed under taking products and inverses,
- so they form a group under multiplication, with identity $[1]$.
- If $[a] \neq [0]$ then the congruence $ax \equiv 1 \bmod (p)$ has unique solution $[x] \neq [0]$ in $(\mathbb{Z})_p$.
- This class is the inverse of $[a]$.
- This group of non-zero classes has order $p - 1$ (it contains $p - 1$ elements).
- If g is any element of a group of finite order n, then g^n is the identity element in that group.
- Therefore, each class $[a] \neq [0]$ satisfies $[a]^{p-1} = [1]$, so $a^{p-1} \equiv 1$.

Fermat's Little Theorem

Theorem

If p is prime and $a \not\equiv 0 \mod (p)$, then $a^{p-1} \equiv 1 \mod (p)$

Fermat's Little Theorem

If $a \not\equiv 0$ then Fermat's Little Theorem gives $a^{p-1} \equiv 1$, multiplying both sides by a gives the following corollary.

Corollary

If p is prime then $a^p \equiv a \bmod (p)$ for every integer a.

Example

Let us find the least non-negative reside of $2^{68} \bmod (19)$.

EXAMPLE

Let us find the least non-negative reside of 2^{68} mod (19). Since 19 is prime and 2 is not divisible by 19, we can apply Fermat's little theorem with $p = 19$ and $a = 2$, so that $2^{18} \equiv 1$ mod (19).

Example

Let us find the least non-negative reside of 2^{68} mod (19). Since 19 is prime and 2 is not divisible by 19, we can apply Fermat's little theorem with $p = 19$ and $a = 2$, so that $2^{18} \equiv 1 \bmod (19)$.

$$2^{68} = (2^{18})^3 \times 2^{14} \equiv 1^3 \times 2^{14} \equiv 2^{14} \bmod (19)$$

EXAMPLE

Let us find the least non-negative reside of 2^{68} mod (19). Since 19 is prime and 2 is not divisible by 19, we can apply Fermat's little theorem with $p = 19$ and $a = 2$, so that $2^{18} \equiv 1 \bmod (19)$.

$$2^{68} = (2^{18})^3 \times 2^{14} \equiv 1^3 \times 2^{14} \equiv 2^{14} \bmod (19)$$

Since $2^4 = 16 \equiv -3 \bmod (19)$, we can write $14 = 4 \times 3 + 2$

Example

Let us find the least non-negative reside of 2^{68} mod (19). Since 19 is prime and 2 is not divisible by 19, we can apply Fermat's little theorem with $p = 19$ and $a = 2$, so that $2^{18} \equiv 1$ mod (19).

$$2^{68} = (2^{18})^3 \times 2^{14} \equiv 1^3 \times 2^{14} \equiv 2^{14} \text{ mod } (19)$$

Since $2^4 = 16 \equiv -3$ mod (19), we can write $14 = 4 \times 3 + 2$ and deduce that

$$2^{14} = (2^4)^3 \times 2^2 \equiv (-3)^3 \times 2^2 \equiv -27 \times 4 \equiv -8 \times 4 \equiv -32$$

so that $2^{68} \equiv 6$ mod (19)

Example

Let us find all the roots of the congruence

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \bmod (5)$$

Example

Let us find all the roots of the congruence

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \bmod (5)$$

Here, $p = 5$

EXAMPLE

Let us find all the roots of the congruence

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \bmod (5)$$

Here, $p = 5$ so replacing x^5 with x we can replace $x^{17} = (x^5)^3x^2$

EXAMPLE

Let us find all the roots of the congruence

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \text{ mod } (5)$$

Here, $p = 5$ so replacing x^5 with x we can replace $x^{17} = (x^5)^3x^2$ with $x^3x^2 = x^5$ and hence with x.

Example

Let us find all the roots of the congruence

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \bmod (5)$$

Here, $p = 5$ so replacing x^5 with x we can replace $x^{17} = (x^5)^3x^2$ with $x^3x^2 = x^5$ and hence with x. Similarly we can replace x^{14} with x^2 and x^5 with x.

Example

Let us find all the roots of the congruence

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \bmod (5)$$

Here, $p = 5$ so replacing x^5 with x we can replace $x^{17} = (x^5)^3x^2$ with $x^3x^2 = x^5$ and hence with x. Similarly we can replace x^{14} with x^2 and x^5 with x. This gives the polynomial $6x^2 + 3x + 1$, which is a mush simpler congruence to deal with.

University of Bedfordshire

Wilson's theorem

Theorem

An integer n is prime if and only if $(n-1)! \equiv -1 \text{ mod } (n)$

ANOTHER THEOREM...

THEOREM

Let p be an odd prime. Then the quadratic congruence $x^2 + 1 \equiv 0 \bmod (p)$ *has a solution if and only if* $p \equiv 1 \bmod (4)$

Outline

- If we are given an integer n to test for primality, we chose an integer a and compute a^n mod (n).

- If we are given an integer n to test for primality, we chose an integer a and compute $a^n \bmod (n)$.
- n passes *the base a test* if $a^n \equiv a \bmod (n)$.

- If we are given an integer n to test for primality, we chose an integer a and compute $a^n \bmod (n)$.
- n passes *the base a test* if $a^n \equiv a \bmod (n)$.
- n fails *the base a test* if $a^n \not\equiv a \bmod (n)$, if n fails the test for any a then n must be composite (i.e. not prime).

- If we are given an integer n to test for primality, we chose an integer a and compute $a^n \bmod (n)$.
- n passes *the base a test* if $a^n \equiv a \bmod (n)$.
- n fails *the base a test* if $a^n \not\equiv a \bmod (n)$, if n fails the test for any a then n must be composite (i.e. not prime).
- If n passes the base 2 test, and n is not prime, n is called **pseudoprime**

Example - pseudoprime

$n = 341$. By noting $2^{10} = 1024 \equiv 1 \bmod (341)$, so

$$2^{314} = (2^{10})^{34} \times 2 \equiv 2 \bmod (341)$$

and 341 has passed the test. However $341 = 11 \times 13$, so it is not prime but a pseudoprime. 341 is in fact the smallest pseudoprime. Although pseudoprimes are quite rare, we theorise that there are infinitely many pseudoprimes.

Example - simplification of powers

- Let $n = 91$. This is odd, so $a^{91} = (a^{45})^2 a = g(a^{45})$.

Example - simplification of powers

- Let $n = 91$. This is odd, so $a^{91} = (a^{45})^2 a = g(a^{45})$.
- Similarly, 45 is odd, so $a^{45} = g(a^{22})$.

University of Bedfordshire

Example - simplification of powers

- Let $n = 91$. This is odd, so $a^{91} = (a^{45})^2 a = g(a^{45})$.
- Similarly, 45 is odd, so $a^{45} = g(a^{22})$.
- This gives $a^{91} = g(g(a^{22})) = (g \circ g)(a^{22})$.

University of Bedfordshire

Example - simplification of powers

- Let $n = 91$. This is odd, so $a^{91} = (a^{45})^2 a = g(a^{45})$.
- Similarly, 45 is odd, so $a^{45} = g(a^{22})$.
- This gives $a^{91} = g(g(a^{22})) = (g \circ g)(a^{22})$.
- Since 22 is even $a^{22} = (a^{11})^2 = f(a^{11})$.

Example - simplification of powers

- Let $n = 91$. This is odd, so $a^{91} = (a^{45})^2 a = g(a^{45})$.
- Similarly, 45 is odd, so $a^{45} = g(a^{22})$.
- This gives $a^{91} = g(g(a^{22})) = (g \circ g)(a^{22})$.
- Since 22 is even $a^{22} = (a^{11})^2 = f(a^{11})$.
- This gives $a^{91} = g(g(f(a^{11}))) = (g \circ g \circ f)(a^{11})$.

Example - simplification of powers

- Let $n = 91$. This is odd, so $a^{91} = (a^{45})^2 a = g(a^{45})$.
- Similarly, 45 is odd, so $a^{45} = g(a^{22})$.
- This gives $a^{91} = g(g(a^{22})) = (g \circ g)(a^{22})$.
- Since 22 is even $a^{22} = (a^{11})^2 = f(a^{11})$.
- This gives $a^{91} = g(g(f(a^{11}))) = (g \circ g \circ f)(a^{11})$.
- Continuing this we find $a^{91} = (g \circ g \circ f \circ g \circ g \circ f \circ g)(a^0)$.

Example - simplification of powers

- Let $n = 91$. This is odd, so $a^{91} = (a^{45})^2 a = g(a^{45})$.
- Similarly, 45 is odd, so $a^{45} = g(a^{22})$.
- This gives $a^{91} = g(g(a^{22})) = (g \circ g)(a^{22})$.
- Since 22 is even $a^{22} = (a^{11})^2 = f(a^{11})$.
- This gives $a^{91} = g(g(f(a^{11}))) = (g \circ g \circ f)(a^{11})$.
- Continuing this we find $a^{91} = (g \circ g \circ f \circ g \circ g \circ f \circ g)(a^0)$.

f involves one multiplication, and g involves two, so the total number of multiplications required is 12 (we can halt the iteration a step earlier and reduce the number to 10). Since each multiplication is performed in $\mathbb{Z}_{91}$, the number involved never becomes excessively large.

Example - simplification of powers

- Any integer n can easily be represented in binary.

Example - simplification of powers

- Any integer n can easily be represented in binary.
- We can apply f or g whenever we have 0 or 1, respectively.

Example - simplification of powers

- Any integer n can easily be represented in binary.
- We can apply f or g whenever we have 0 or 1, respectively.
- $91 = 1011011$, since we write functions from left to write, we reverse the order

University of Bedfordshire

Example - simplification of powers

- Any integer n can easily be represented in binary.
- We can apply f or g whenever we have 0 or 1, respectively.
- $91 = 1011011$, since we write functions from left to write, we reverse the order
- $1011011 \to g \circ g \circ f \circ g \circ g \circ f \circ g$

Example - simplification of powers

- Any integer n can easily be represented in binary.
- We can apply f or g whenever we have 0 or 1, respectively.
- $91 = 1011011$, since we write functions from left to write, we reverse the order
- $1011011 \rightarrow g \circ g \circ f \circ g \circ g \circ f \circ g$

Theorem

This argument implies that, for any n, the number of multiplications required to compute a^n is at most twice the number of digits in the binary expansion of n, that is, at most $2(1 + \lfloor lgn \rfloor)$

Carmichael Numbers

Definition

Carmicheal numbers are composite integers n with the property that $a^n \equiv a \bmod (n)$ for all integers a

- The smallest Carmicheal number is $561 = 3 \times 11 \times 17$.
- However, $a^{561} \equiv a \bmod (561)$ for all integers a.
- The next few Carmicheal numbers are 1105, 1729, 2465.

Lemma

If n is square-free (a product of distinct primes) and if $p - 1$ divides $n - 1$ for each prime p dividing n, then n is either a prime or a Carmichael number.

Carmichael Numbers

Outline

Definition

Definition

A multiplicative inverse for a class $[a] \in \mathbb{Z}_n$ is a class $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$. A class $[a] \in \mathbb{Z}_n$ is a **unit** if it has a multiplicative inverse in $\mathbb{Z}_n$.

Lemma

$[a]$ ia a unit in $\mathbb{Z}_n$ if and only if $gcd(a, n) = 1$.

Example

The units of $\mathbb{Z}_8$ are [1], [3], [5] and [7]: in fact $[1][1] = [3][3] = [5][5] = [7][7] = [1]$, so each of these units is its own multiplicative inverse. In $\mathbb{Z}_9$, the units are [1], [2], [4], [5], [7] and [8]: for instance $[2][5] = [1]$, so [2] and [5] are inverses of each other.

The Set of Units

We let U_n denote the set of units in $\mathbb{Z}_n$. Thus $U_8 = \{[1], [3], [5], [7]\}$ and $U_9 = \{[1], [2], [4], [5], [7], [8]\}$.

Theorem

For each integer $n \geq 1$, the set U_n forms a group under multiplication $\bmod(n)$, with identity element $[1]$.

University of Bedfordshire

The Set of Units

We let U_n denote the set of units in $\mathbb{Z}_n$. Thus
$U_8 = \{[1], [3], [5], [7]\}$ and $U_9 = \{[1], [2], [4], [5], [7], [8]\}$.

Theorem

For each integer $n \geq 1$, the set U_n forms a group under multiplication $\bmod(n)$, with identity element $[1]$.

Example (U_n is Abelian)

$[a][b] = [ab]$ and $[b][a] = [ba]$; since $ab = ba$ for all $a, b \in \mathbb{Z}$, we have $[a][b] = [b][a]$ for all $[a], [b] \in \mathbb{Z}_n$.

Proof U_n is a Group

The axioms that set out the constraints of a group are:

- Closure
- Associativity
- Identity
- Inverses

Closure of U_n

If $[a]$ and $[b]$ are units, they have inverse $[u]$ and $[v]$ such that $[a][u] = [au] = [1]$ and $[b][v] = [bv] = [1]$; then $[ab][uv] = [abuv] = [aubv] = [au][bv] = [1]^2 = [1]$, so $[ab]$ has inverse $[uv]$, and is therfore a unit. This proves closure.

University of Bedfordshire

Associativity of U_n

Associativity asserts that $[a]([b][c]) = ([a][b])[c]$ for all $[a]$, $[b]$ and $[c]$; the left and right classes are $[a(bc)]$ and $[(ab)c]$ so this follows from the associativity property $a(bc) = (ab)c$ in $\mathbb{Z}$.

Identity of U_n

The identity element of U_n is $[1]$, since $[a][1] = [a] = [1][a]$ for all $[a] \in U_n$.

Inverses of U_n

If $[a] \in U_n$ then by definition there exists $[u] \in \mathbb{Z}_n$ such that $[a][u] = [1]$; now $[u] \in U_n$ because $[a]$ satisfies $[u][a] = [1]$, so $[u]$ is the inverse of $[a]$ in U_n.

Outline

Definition

Definition

We define $\phi(n) = |U_n|$, the number of units in $\mathbb{Z}_n$; the number of integers $a = 1, 2, \ldots, n$ such that $gcd(a, n) = 1$. The function ϕ is called **Euler's function** (or Euler's totient function). For small n, its values are as follows:

$$n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$$
$$\phi(n) = 1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, \ldots$$

We define a subset R of $\mathbb{Z}$ to be a **reduced set of residues** mod(n) if it contains one element from each of the $\phi(n)$ congruence classes in U_n. For instance, $\{1, 3, 5, 7\}$ and $\{\pm 1, \pm 3\}$ are both reduced sets of residues mod(8).

Euler's Theorem - A Generalisation of Fermat's Little Theorem

Theorem

If $gcd(a, n) = 1$ *then* $a^{\phi(n)} \equiv 1 \bmod (n)$

A General Formula for $\phi(n)$

Lemma

$$\phi(n) = p^e - p^{e-1} = p^{e-1}(p-1) = n\left(1 - \frac{1}{p}\right)$$

University of Bedfordshire

Outline

Lemma

U_n is an abelian group under multiplication $\mod(n)$.

Lemma

If l and m are coprime positive integers, then $2^l - 1$ and $2^m - 1$ are coprime.

Mersenne numbers

Definition

Integers in the form $2^p - 1$, where p is prime, are called Mersenne numbers.

Corollary

Distinct Mersenne numbers are coprime.

Outline

Example

Find the last two decimal digits of 3^{1492}

Example

Find the last two decimal digits of 3^{1492}

- Equivalent to finding the least non-negative residue of 3^{1492} mod (100).

Example

Find the last two decimal digits of 3^{1492}

- Equivalent to finding the least non-negative residue of $3^{1492} \bmod (100)$.
- 3 is coprime to 100 so we can use $a^{\phi(n)} \equiv 1 \bmod (n)$ where $gcd(a, n) = 1$.

Example

Find the last two decimal digits of 3^{1492}

- Equivalent to finding the least non-negative residue of $3^{1492} \bmod (100)$.
- 3 is coprime to 100 so we can use $a^{\phi(n)} \equiv 1 \bmod (n)$ where $gcd(a, n) = 1$.
- gives $3^{\phi(100)} \equiv 1 \bmod (100)$, where the primes dividing 100 are 2 and 5.

EXAMPLE

Find the last two decimal digits of 3^{1492}

- Equivalent to finding the least non-negative residue of 3^{1492} mod (100).
- 3 is coprime to 100 so we can use $a^{\phi(n)} \equiv 1 \bmod (n)$ where $gcd(a, n) = 1$.
- gives $3^{\phi(100)} \equiv 1 \bmod (100)$, where the primes dividing 100 are 2 and 5.
- $\phi(100) = 100 \times (1/2) \times (4/5) = 40$, so $3^{40} \equiv 1 \bmod (100)$.

Example

Find the last two decimal digits of 3^{1492}

- Equivalent to finding the least non-negative residue of 3^{1492} mod (100).
- 3 is coprime to 100 so we can use $a^{\phi(n)} \equiv 1$ mod (n) where $gcd(a, n) = 1$.
- gives $3^{\phi(100)} \equiv 1$ mod (100), where the primes dividing 100 are 2 and 5.
- $\phi(100) = 100 \times (1/2) \times (4/5) = 40$, so $3^{40} \equiv 1$ mod (100).
- $1492 \equiv 12$ mod (40), so $3^{1492} \equiv 3^{12}$ mod (100).

University of Bedfordshire

Example

Find the last two decimal digits of 3^{1492}

- Equivalent to finding the least non-negative residue of $3^{1492} \bmod (100)$.
- 3 is coprime to 100 so we can use $a^{\phi(n)} \equiv 1 \bmod (n)$ where $gcd(a, n) = 1$.
- gives $3^{\phi(100)} \equiv 1 \bmod (100)$, where the primes dividing 100 are 2 and 5.
- $\phi(100) = 100 \times (1/2) \times (4/5) = 40$, so $3^{40} \equiv 1 \bmod (100)$.
- $1492 \equiv 12 \bmod (40)$, so $3^{1492} \equiv 3^{12} \bmod (100)$.
- $3^4 = 81 \equiv -19 \bmod (100)$ so $3^8 \equiv (-19)^2 = 361 \equiv -39$.

Example

Find the last two decimal digits of 3^{1492}

- Equivalent to finding the least non-negative residue of 3^{1492} mod (100).
- 3 is coprime to 100 so we can use $a^{\phi(n)} \equiv 1$ mod (n) where $gcd(a, n) = 1$.
- gives $3^{\phi(100)} \equiv 1$ mod (100), where the primes dividing 100 are 2 and 5.
- $\phi(100) = 100 \times (1/2) \times (4/5) = 40$, so $3^{40} \equiv 1$ mod (100).
- $1492 \equiv 12$ mod (40), so $3^{1492} \equiv 3^{12}$ mod (100).
- $3^4 = 81 \equiv -19$ mod (100) so $3^8 \equiv (-19)^2 = 361 \equiv -39$.
- therefore $3^{12} \equiv -19 \times -39 = 741 \equiv 41$. The last two digits are therefore 41.

Example

Using a similar method, check the consistancy of the above calculation by finding only the last digit of 3^{1492}.

Number theory and cryptography

If we represent letters as integers, say $A = 0, B = 1, \ldots, Z = 25$, and then add 1 to each. To encode Z as A, we must add mod (26), so that $25 + 1 \equiv 0$. Similar codes are obtained by adding some fixed integer k. To decode we subtract k mod (26). These codes are easy to break: we could try all possible values of k, or compare the most frequent letters (E and then T in English).

Example

Which mathematician is encoded in the above way as $LBSLY$, and what is the value of k?

NUMBER THEORY AND CRYPTOGRAPHY

A more secure class of codes uses transformations in the form $x \to ax + b \bmod (26)$, for various integers a and b. To decode, we need to find x from $ax + b$; this is possible if and only if a is a unit mod(26). It turns out there are $\phi(26) \times 26 = 12 \times 26 = 312$ such codes.

EXAMPLE

If the encoding transformation is $x \to 7x + 3 \bmod (26)$, encode *GAUSS* and decode *MFSJDG*.

Number theory and cryptography

We can do better with codes based on Fermat's Little Theorem. Choose a large prime p, and an integer e coprime to $p-1$. For encoding we use the transformation $\mathbb{Z}_p \to \mathbb{Z}_p$ given by $x \to x^e \bmod (p)$. If $0 < x < p$ then x is coprime to p, so $x^{p-1} \equiv 1 \bmod (p)$. To decode, we first find the multiplicative inverse f of $e \bmod (p-1)$, i.e. we solve the congruence $ef \equiv 1 \bmod (p-1)$. Then $ef = (p-1)k + 1$ for some integer k, so $(x^e)^f = x^{(p-1)k+1} = (x^{p-1})^k.x \equiv x \bmod (p)$, thus we find x and the message cane be decoded.

Example

Suppose $p = 29$, we choose e coprime to 28, and then find f such that $ef \equiv 1 \bmod (28)$. If we choose $e = 5$, the encoding would be $x \to x^5 \bmod (29)$, then $f = 17$ and decoding is given by $x \to x^{17} \bmod (29)$. Encode 9 and decode 11 in this example coding.