Factorization and Primality Testing Chapter 4 Primitive Roots and RSA

Robert C. Vaughan

September 13, 2024

Primitive Roots

- We have seen that on the residue classes modulo m we can perform many of the standard operations of arithmetic.

Primitive Roots

- We have seen that on the residue classes modulo m we can perform many of the standard operations of arithmetic.
- Such an object is called a ring. In this case it is usually denoted by $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}_m$.

Primitive Roots

- We have seen that on the residue classes modulo m we can perform many of the standard operations of arithmetic.
- Such an object is called a ring. In this case it is usually denoted by $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}_m$.
- In this chapter we will look at its multiplicative structure.

Primitive Roots

- We have seen that on the residue classes modulo m we can perform many of the standard operations of arithmetic.
- Such an object is called a ring. In this case it is usually denoted by $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}_m$.
- In this chapter we will look at its multiplicative structure.
- In particular we will consider the reduced residue classes modulo m.

- An obvious question is what happens if we take powers of a fixed residue a?

Definition 1

Given $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ we define the order $\mathrm{ord}_m(a)$ of a modulo m to be the smallest positive integer t such that

$$a^t \equiv 1 \pmod{m}.$$

We may express this by saying that a belongs to the exponent t modulo m, or that t is the order of a modulo m.

- An obvious question is what happens if we take powers of a fixed residue a?

Definition 1

Given $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ we define the order $\mathrm{ord}_m(a)$ of a modulo m to be the smallest positive integer t such that

$$a^t \equiv 1 \pmod{m}.$$

We may express this by saying that a belongs to the exponent t modulo m, or that t is the order of a modulo m.

- Note that by Euler's theorem, $a^{\phi(m)} \equiv 1 \pmod{m}$, so that $\mathrm{ord}_m(a)$ exists.

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ *and* $n \in \mathbb{N}$ *is such that* $a^n \equiv 1 \pmod{m}$. *Then* $\operatorname{ord}_m(a) | n$. *In particular* $\operatorname{ord}_m(a) | \phi(m)$.

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ and $n \in \mathbb{N}$ is such that $a^n \equiv 1 \pmod{m}$. Then $\operatorname{ord}_m(a) | n$. In particular $\operatorname{ord}_m(a) | \phi(m)$.

- **Proof.** For concision let $t = \operatorname{ord}_m(a)$.

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ *and* $n \in \mathbb{N}$ *is such that* $a^n \equiv 1 \pmod{m}$. *Then* $\mathrm{ord}_m(a) | n$. *In particular* $\mathrm{ord}_m(a) | \phi(m)$.

- **Proof.** For concision let $t = \mathrm{ord}_m(a)$.
- Since t is minimal we have $t \le n$.

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ and $n \in \mathbb{N}$ is such that $a^n \equiv 1 \pmod{m}$. Then $\text{ord}_m(a)|n$. In particular $\text{ord}_m(a)|\phi(m)$.

- **Proof.** For concision let $t = \text{ord}_m(a)$.
- Since t is minimal we have $t \le n$.
- Thus by the division algorithm there are q and r with $0 \le r < t$ such that $n = tq + r$.

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ and $n \in \mathbb{N}$ is such that $a^n \equiv 1 \pmod{m}$. Then $\operatorname{ord}_m(a) | n$. In particular $\operatorname{ord}_m(a) | \phi(m)$.

- **Proof.** For concision let $t = \operatorname{ord}_m(a)$.
- Since t is minimal we have $t \le n$.
- Thus by the division algorithm there are q and r with $0 \le r < t$ such that $n = tq + r$.
- Hence

$$a^r \equiv (a^t)^q a^r = a^{qt+r} = a^n \equiv 1 \pmod{m}.$$

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ and $n \in \mathbb{N}$ is such that $a^n \equiv 1 \pmod{m}$. Then $\mathrm{ord}_m(a)|n$. In particular $\mathrm{ord}_m(a)|\phi(m)$.

- **Proof.** For concision let $t = \mathrm{ord}_m(a)$.
- Since t is minimal we have $t \le n$.
- Thus by the division algorithm there are q and r with $0 \le r < t$ such that $n = tq + r$.
- Hence

$$a^r \equiv (a^t)^q a^r = a^{qt+r} = a^n \equiv 1 \pmod{m}.$$

- But $0 \le r < t$.

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ and $n \in \mathbb{N}$ is such that $a^n \equiv 1 \pmod{m}$. Then $\mathrm{ord}_m(a)|n$. In particular $\mathrm{ord}_m(a)|\phi(m)$.

- **Proof.** For concision let $t = \mathrm{ord}_m(a)$.
- Since t is minimal we have $t \le n$.
- Thus by the division algorithm there are q and r with $0 \le r < t$ such that $n = tq + r$.
- Hence

$$a^r \equiv (a^t)^q a^r = a^{qt+r} = a^n \equiv 1 \pmod{m}.$$

- But $0 \le r < t$.
- If we would have $r > 0$, then we would contradict the minimality of t.

- We can do better than that.

Theorem 2

Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ and $n \in \mathbb{N}$ is such that $a^n \equiv 1 \pmod{m}$. Then $\text{ord}_m(a)|n$. In particular $\text{ord}_m(a)|\phi(m)$.

- **Proof.** For concision let $t = \text{ord}_m(a)$.
- Since t is minimal we have $t \le n$.
- Thus by the division algorithm there are q and r with $0 \le r < t$ such that $n = tq + r$.
- Hence

$$a^r \equiv (a^t)^q a^r = a^{qt+r} = a^n \equiv 1 \pmod{m}.$$

- But $0 \le r < t$.
- If we would have $r > 0$, then we would contradict the minimality of t.
- Hence $r = 0$.

- Here is an application we will make use of later.

Theorem 3

Suppose that $d|p-1$. Then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

- Here is an application we will make use of later.

Theorem 3

Suppose that $d|p-1$. Then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

- **Proof.** We have

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{d-p-2d} + \cdots + x^d + 1).$$

- Here is an application we will make use of later.

Theorem 3

Suppose that $d|p-1$. Then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

- **Proof.** We have

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{d-p-2d} + \cdots + x^d + 1).$$

- To see this just multiply out the right hand side and observe that the terms telescope.

- Here is an application we will make use of later.

Theorem 3

Suppose that $d|p-1$. Then the congruence $x^d \equiv 1 \pmod p$ has exactly d solutions.

- **Proof.** We have

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{d-p-2d} + \cdots + x^d + 1).$$

- To see this just multiply out the right hand side and observe that the terms telescope.
- We know from Euler's theorem that there are exactly $p-1$ incongruent roots to the left hand side modulo p.

- Here is an application we will make use of later.

Theorem 3

Suppose that $d|p-1$. Then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

- **Proof.** We have

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{d-p-2d} + \cdots + x^d + 1).$$

- To see this just multiply out the right hand side and observe that the terms telescope.
- We know from Euler's theorem that there are exactly $p-1$ incongruent roots to the left hand side modulo p.
- On the other hand, by Lagrange's theorem, the second factor has at most $p-1-d$ such roots, so the first factor must account for at least d of them.

- Here is an application we will make use of later.

Theorem 3

Suppose that $d|p-1$. Then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

- **Proof.** We have

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{d-p-2d} + \cdots + x^d + 1).$$

- To see this just multiply out the right hand side and observe that the terms telescope.
- We know from Euler's theorem that there are exactly $p-1$ incongruent roots to the left hand side modulo p.
- On the other hand, by Lagrange's theorem, the second factor has at most $p-1-d$ such roots, so the first factor must account for at least d of them.
- On the other hand, again by Lagrange's theorem, it has at most d roots modulo p.

- We have already seen that, when $(a, m) = 1$, a has order modulo m which divides $\phi(m)$.

- We have already seen that, when $(a, m) = 1$, a has order modulo m which divides $\phi(m)$.
- One question one can ask is, given any $d|\phi(m)$, are there elements of order d?

- We have already seen that, when $(a, m) = 1$, a has order modulo m which divides $\phi(m)$.
- One question one can ask is, given any $d|\phi(m)$, are there elements of order d?
- In the special case $d = \phi(m)$ this would mean that

$$a, a^2, \ldots, a^{\phi(m)}$$

are distinct modulo m,

- We have already seen that, when $(a, m) = 1$, a has order modulo m which divides $\phi(m)$.
- One question one can ask is, given any $d|\phi(m)$, are there elements of order d?
- In the special case $d = \phi(m)$ this would mean that

$$a, a^2, \ldots, a^{\phi(m)}$$

are distinct modulo m,

- because otherwise we would have

$$a^u \equiv a^v \pmod{m}$$

with $1 \le u < v \le \phi(m)$,

- We have already seen that, when $(a, m) = 1$, a has order modulo m which divides $\phi(m)$.
- One question one can ask is, given any $d|\phi(m)$, are there elements of order d?
- In the special case $d = \phi(m)$ this would mean that

$$a, a^2, \ldots, a^{\phi(m)}$$

  are distinct modulo m,
- because otherwise we would have

$$a^u \equiv a^v \pmod{m}$$

  with $1 \le u < v \le \phi(m)$,
- and then

$$a^{v-u} \equiv 1 \pmod{m}$$

  and $1 \le v - u < \phi(m)$ contradicting the assumption that $\mathrm{ord}_m(a) = \phi(m)$.

- Consider

Example 4

$m = 7$.

- Consider

Example 4

$m = 7$.

- $a = 1$, $\mathrm{ord}_7(1) = 1$.

- Consider

Example 4

$m = 7.$

- $a = 1$, $\mathrm{ord}_7(1) = 1.$
- $a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\mathrm{ord}_7(2) = 3.$

- Consider

Example 4

$m = 7$.

- $a = 1$, $\mathrm{ord}_7(1) = 1$.
- $a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\mathrm{ord}_7(2) = 3$.
- $a = 3$, $3^2 = 9 \equiv 2$, $3^3 = 27 \equiv 6$, $3^4 \equiv 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 1$, $\mathrm{ord}_7(3) = 6$.

- Consider

Example 4

$m = 7$.

- $a = 1$, $\mathrm{ord}_7(1) = 1$.
- $a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\mathrm{ord}_7(2) = 3$.
- $a = 3$, $3^2 = 9 \equiv 2$, $3^3 = 27 \equiv 6$, $3^4 \equiv 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 1$, $\mathrm{ord}_7(3) = 6$.
- $a = 4$, $4^2 \equiv 2$, $4^3 \equiv 2^6 \equiv 1$, $\mathrm{ord}_7(4) = 3$.

- Consider

Example 4

$m = 7$.

- $a = 1$, $\mathrm{ord}_7(1) = 1$.
- $a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\mathrm{ord}_7(2) = 3$.
- $a = 3$, $3^2 = 9 \equiv 2$, $3^3 = 27 \equiv 6$, $3^4 \equiv 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 1$, $\mathrm{ord}_7(3) = 6$.
- $a = 4$, $4^2 \equiv 2$, $4^3 \equiv 2^6 \equiv 1$, $\mathrm{ord}_7(4) = 3$.
- $a = 5$, $5^2 = 25 \equiv 4$, $5^3 \equiv 20 \equiv 6$, $5^4 \equiv 30 \equiv 2$, $5^5 \equiv 10 \equiv 3$, $5^6 \equiv 1$, $\mathrm{ord}_7(5) = 6$.

- Consider

Example 4

$m = 7$.

- $a = 1$, $\mathrm{ord}_7(1) = 1$.
- $a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\mathrm{ord}_7(2) = 3$.
- $a = 3$, $3^2 = 9 \equiv 2$, $3^3 = 27 \equiv 6$, $3^4 \equiv 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 1$, $\mathrm{ord}_7(3) = 6$.
- $a = 4$, $4^2 \equiv 2$, $4^3 \equiv 2^6 \equiv 1$, $\mathrm{ord}_7(4) = 3$.
- $a = 5$, $5^2 = 25 \equiv 4$, $5^3 \equiv 20 \equiv 6$, $5^4 \equiv 30 \equiv 2$, $5^5 \equiv 10 \equiv 3$, $5^6 \equiv 1$, $\mathrm{ord}_7(5) = 6$.
- $a = 6$, $6^2 = 36 \equiv 1$, $\mathrm{ord}_7(6) = 2$.

- Consider

Example 4

$m = 7$.

- $a = 1$, $\text{ord}_7(1) = 1$.
- $a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\text{ord}_7(2) = 3$.
- $a = 3$, $3^2 = 9 \equiv 2$, $3^3 = 27 \equiv 6$, $3^4 \equiv 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 1$, $\text{ord}_7(3) = 6$.
- $a = 4$, $4^2 \equiv 2$, $4^3 \equiv 2^6 \equiv 1$, $\text{ord}_7(4) = 3$.
- $a = 5$, $5^2 = 25 \equiv 4$, $5^3 \equiv 20 \equiv 6$, $5^4 \equiv 30 \equiv 2$, $5^5 \equiv 10 \equiv 3$, $5^6 \equiv 1$, $\text{ord}_7(5) = 6$.
- $a = 6$, $6^2 = 36 \equiv 1$, $\text{ord}_7(6) = 2$.
- Thus there is one element of order 1, one element of order 2, two of order 3 and two of order 6.

- Consider

Example 4

$m = 7$.

- $a = 1$, $\text{ord}_7(1) = 1$.
- $a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\text{ord}_7(2) = 3$.
- $a = 3$, $3^2 = 9 \equiv 2$, $3^3 = 27 \equiv 6$, $3^4 \equiv 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 1$, $\text{ord}_7(3) = 6$.
- $a = 4$, $4^2 \equiv 2$, $4^3 \equiv 2^6 \equiv 1$, $\text{ord}_7(4) = 3$.
- $a = 5$, $5^2 = 25 \equiv 4$, $5^3 \equiv 20 \equiv 6$, $5^4 \equiv 30 \equiv 2$, $5^5 \equiv 10 \equiv 3$, $5^6 \equiv 1$, $\text{ord}_7(5) = 6$.
- $a = 6$, $6^2 = 36 \equiv 1$, $\text{ord}_7(6) = 2$.
- Thus there is one element of order 1, one element of order 2, two of order 3 and two of order 6.
- Is it a fluke that for each $d|6 = \phi(7)$ the number of elements of order d is $\phi(d)$?

- We now come to an important concept

Definition 5

Suppose that $m \in \mathbb{N}$ and $(a, m) = 1$. If $\operatorname{ord}_m(a) = \phi(m)$ then we say that a is a primitive root modulo m.

- We now come to an important concept

Definition 5

Suppose that $m \in \mathbb{N}$ and $(a, m) = 1$. If $\text{ord}_m(a) = \phi(m)$ then we say that a is a primitive root modulo m.

- We know that we do not always have primitive roots.

- We now come to an important concept

Definition 5

Suppose that $m \in \mathbb{N}$ and $(a, m) = 1$. If $\text{ord}_m(a) = \phi(m)$ then we say that a is a primitive root modulo m.

- We know that we do not always have primitive roots.
- For example, any number a with $(a, 8) = 1$ is odd and so $a^2 \equiv 1 \mod 8$, whereas $\phi(8) = 4$.

- We now come to an important concept

Definition 5

Suppose that $m \in \mathbb{N}$ and $(a, m) = 1$. If $\text{ord}_m(a) = \phi(m)$ then we say that a is a primitive root modulo m.

- We know that we do not always have primitive roots.
- For example, any number a with $(a, 8) = 1$ is odd and so $a^2 \equiv 1 \mod 8$, whereas $\phi(8) = 4$.
- There are primitive roots to some moduli. For example, modulo 7 the powers of 3 are successively $3, 2, 6, 4, 5, 1$.

- We now come to an important concept

Definition 5

Suppose that $m \in \mathbb{N}$ and $(a, m) = 1$. If $\mathrm{ord}_m(a) = \phi(m)$ then we say that a is a primitive root modulo m.

- We know that we do not always have primitive roots.
- For example, any number a with $(a, 8) = 1$ is odd and so $a^2 \equiv 1 \mod 8$, whereas $\phi(8) = 4$.
- There are primitive roots to some moduli. For example, modulo 7 the powers of 3 are successively $3, 2, 6, 4, 5, 1$.
- Gauss determined precisely which moduli possess primitive roots. The first step is the case of prime modulus.

Theorem 6 (Gauss)

Suppose that p is a prime number. Let $d|p-1$ then there are $\phi(d)$ residue classes a with $\mathrm{ord}_p(a) = d$. In particular there are $\phi(p-1) = \phi(\phi(p))$ primitive roots modulo p.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.
- The congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.
- The congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
- Thus every solution has order dividing d.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.
- The congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
- Thus every solution has order dividing d.
- Also each residue with order dividing d is a solution.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.
- The congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
- Thus every solution has order dividing d.
- Also each residue with order dividing d is a solution.
- Thus for each $d|p-1$ we have $\displaystyle\sum_{r|d} \psi(r) = d$.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.
- The congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
- Thus every solution has order dividing d.
- Also each residue with order dividing d is a solution.
- Thus for each $d|p-1$ we have $\sum_{r|d} \psi(r) = d$.
- This is reminiscent of an earlier formula $\sum_{r|d} \phi(r) = d$.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.
- The congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
- Thus every solution has order dividing d.
- Also each residue with order dividing d is a solution.
- Thus for each $d|p-1$ we have $\displaystyle\sum_{r|d} \psi(r) = d$.
- This is reminiscent of an earlier formula $\displaystyle\sum_{r|d} \phi(r) = d$.
- Let $1 = d_1 < d_2 < \ldots < d_k = p-1$ be the divisors of $p-1$ in order.

- **Proof of Gauss' Theorem** We have seen that the order of every reduced residue class modulo p divides $p-1$.
- For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p.
- The congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
- Thus every solution has order dividing d.
- Also each residue with order dividing d is a solution.
- Thus for each $d|p-1$ we have $\displaystyle\sum_{r|d} \psi(r) = d$.
- This is reminiscent of an earlier formula $\displaystyle\sum_{r|d} \phi(r) = d$.
- Let $1 = d_1 < d_2 < \ldots < d_k = p-1$ be the divisors of $p-1$ in order.
- We have a relationship $\displaystyle\sum_{r|d_j} \psi(r) = d_j$ for each $j = 1, 2, \ldots$ and, of course, the sum is over a subset of the divisors of $p-1$. I claim that this determines $\psi(d_j)$ uniquely.

- We have a relationship

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ where the sum is over the divisors of d_j and so is over a subset of the divisors of $p - 1$.

- We have a relationship

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ where the sum is over the divisors of d_j and so is over a subset of the divisors of $p - 1$.

- I claim that these relationships determines $\psi(d_j)$ uniquely.

- We have a relationship

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ where the sum is over the divisors of d_j and so is over a subset of the divisors of $p-1$.

- I claim that these relationships determines $\psi(d_j)$ uniquely.
- We can prove this by observing that if N is the number of positive divisors of $p-1$, then we have N linear equations in the N unknowns $\psi(r)$ and we can we can write this in matrix notation

$$\boldsymbol{\psi}\mathcal{U} = \mathbf{d}.$$

- We have a relationship

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \dots$ where the sum is over the divisors of d_j and so is over a subset of the divisors of $p-1$.
- I claim that these relationships determines $\psi(d_j)$ uniquely.
- We can prove this by observing that if N is the number of positive divisors of $p-1$, then we have N linear equations in the N unknowns $\psi(r)$ and we can we can write this in matrix notation

$$\boldsymbol{\psi}\mathcal{U} = \mathbf{d}.$$

- Moreover $\mathcal{U}$ is an upper triangular matrix with non-zero entries on the diagonal and so is invertible.

- We have a relationship

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ where the sum is over the divisors of d_j and so is over a subset of the divisors of $p-1$.

- I claim that these relationships determines $\psi(d_j)$ uniquely.
- We can prove this by observing that if N is the number of positive divisors of $p-1$, then we have N linear equations in the N unknowns $\psi(r)$ and we can we can write this in matrix notation

$$\boldsymbol{\psi}\mathcal{U} = \mathbf{d}.$$

- Moreover $\mathcal{U}$ is an upper triangular matrix with non-zero entries on the diagonal and so is invertible.
- Hence the $\psi(d_j)$ are uniquely determined.

- We have a relationship

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ where the sum is over the divisors of d_j and so is over a subset of the divisors of $p - 1$.

- I claim that these relationships determines $\psi(d_j)$ uniquely.
- We can prove this by observing that if N is the number of positive divisors of $p - 1$, then we have N linear equations in the N unknowns $\psi(r)$ and we can we can write this in matrix notation

$$\boldsymbol{\psi}\mathcal{U} = \mathbf{d}.$$

- Moreover $\mathcal{U}$ is an upper triangular matrix with non-zero entries on the diagonal and so is invertible.
- Hence the $\psi(d_j)$ are uniquely determined.
- But we already know a solution, namely $\psi = \phi$.

- If we wish to avoid the linear algebra, starting from

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ we can prove uniqueness by induction.

- If we wish to avoid the linear algebra, starting from

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ we can prove uniqueness by induction.
- For the base case we have $\psi(1) = 1$.

- If we wish to avoid the linear algebra, starting from

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ we can prove uniqueness by induction.
- For the base case we have $\psi(1) = 1$.
- Then suppose that $\psi(d_1), \ldots, \psi(d_j)$ are determined.

- If we wish to avoid the linear algebra, starting from

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ we can prove uniqueness by induction.
- For the base case we have $\psi(1) = 1$.
- Then suppose that $\psi(d_1), \ldots, \psi(d_j)$ are determined.
- Then we have

$$\sum_{r|d_{j+1}} \psi(r) = d_{j+1}.$$

- If we wish to avoid the linear algebra, starting from

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ we can prove uniqueness by induction.
- For the base case we have $\psi(1) = 1$.
- Then suppose that $\psi(d_1), \ldots, \psi(d_j)$ are determined.
- Then we have

$$\sum_{r|d_{j+1}} \psi(r) = d_{j+1}.$$

- Hence

$$\psi(d_{j+1}) = d_{j+1} - \sum_{\substack{r|d_{j+1} \\ r<d_{j+1}}} \psi(r)$$

and every term on the right hand side is already determined.

- If we wish to avoid the linear algebra, starting from

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ we can prove uniqueness by induction.

- For the base case we have $\psi(1) = 1$.
- Then suppose that $\psi(d_1), \ldots, \psi(d_j)$ are determined.
- Then we have

$$\sum_{r|d_{j+1}} \psi(r) = d_{j+1}.$$

- Hence

$$\psi(d_{j+1}) = d_{j+1} - \sum_{\substack{r|d_{j+1}\\ r<d_{j+1}}} \psi(r)$$

and every term on the right hand side is already determined.

- Thus we can conclude there is only one solution to our system of equations.

- If we wish to avoid the linear algebra, starting from

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ we can prove uniqueness by induction.
- For the base case we have $\psi(1) = 1$.
- Then suppose that $\psi(d_1), \ldots, \psi(d_j)$ are determined.
- Then we have

$$\sum_{r|d_{j+1}} \psi(r) = d_{j+1}.$$

- Hence

$$\psi(d_{j+1}) = d_{j+1} - \sum_{\substack{r|d_{j+1}\\ r<d_{j+1}}} \psi(r)$$

and every term on the right hand side is already determined.
- Thus we can conclude there is only one solution to our system of equations.
- But we already know one solution, namely $\psi(r) = \phi(r)$.

- To get a better insight here is the proof in the special case $p = 13$

Example 7

Here is the proof when $p = 13$, so we are concerned with the divisors of 12.

$$\big(\psi(1), \psi(2), \psi(3), \psi(4), \psi(6), \psi(12)\big) \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (1, 2, 3, 4, 6, 12)$$

- How about higher powers of odd primes?

Theorem 8 (Gauss)

We have primitive roots modulo m when $m = 2$, $m = 4$, $m = p^k$ and $m = 2p^k$ with p an odd prime and in no other cases.

- How about higher powers of odd primes?

Theorem 8 (Gauss)

We have primitive roots modulo m *when* $m = 2$, $m = 4$, $m = p^k$ *and* $m = 2p^k$ *with* p *an odd prime and in no other cases.*

- In applications one can usually reduce via the Chinese Remainder Theorem to powers of primes.

- How about higher powers of odd primes?

Theorem 8 (Gauss)

We have primitive roots modulo m when $m = 2$, $m = 4$, $m = p^k$ and $m = 2p^k$ with p an odd prime and in no other cases.

- In applications one can usually reduce via the Chinese Remainder Theorem to powers of primes.
- Thus the lack of primitive roots for higher powers of 2 us a nuisance.

- How about higher powers of odd primes?

Theorem 8 (Gauss)

We have primitive roots modulo m when $m = 2$, $m = 4$, $m = p^k$ and $m = 2p^k$ with p an odd prime and in no other cases.

- In applications one can usually reduce via the Chinese Remainder Theorem to powers of primes.
- Thus the lack of primitive roots for higher powers of 2 us a nuisance.
- Nevertheless Gauss did prove something.

Theorem 9 (Gauss)

Suppose that $k \geq 3$. Then the numbers $(-1)^u 5^v$ with $u = 0, 1$ and $0 \leq v < 2^{k-2}$ form a set of reduced residues modulo 2^k

- How about higher powers of odd primes?

Theorem 8 (Gauss)

We have primitive roots modulo m when $m = 2$, $m = 4$, $m = p^k$ and $m = 2p^k$ with p an odd prime and in no other cases.

- In applications one can usually reduce via the Chinese Remainder Theorem to powers of primes.
- Thus the lack of primitive roots for higher powers of 2 us a nuisance.
- Nevertheless Gauss did prove something.

Theorem 9 (Gauss)

Suppose that $k \geq 3$. Then the numbers $(-1)^u 5^v$ with $u = 0, 1$ and $0 \leq v < 2^{k-2}$ form a set of reduced residues modulo 2^k

- We will not need these results but I will include the proofs in the class text for anyone interested.

Binomial Congruences

- As an application of primitive roots we can say something when p is odd about the solution of congruences of the form
$$x^k \equiv a \pmod{p}.$$

Binomial Congruences

- As an application of primitive roots we can say something when p is odd about the solution of congruences of the form
$$x^k \equiv a \pmod{p}.$$
- The case $a = 0$ is easy.

Binomial Congruences

- As an application of primitive roots we can say something when p is odd about the solution of congruences of the form
$$x^k \equiv a \pmod{p}.$$
- The case $a = 0$ is easy.
- The only solution is $x \equiv 0 \pmod{p}$.

Binomial Congruences

- As an application of primitive roots we can say something when p is odd about the solution of congruences of the form
$$x^k \equiv a \pmod{p}.$$
- The case $a = 0$ is easy.
- The only solution is $x \equiv 0 \pmod{p}$.
- Suppose $a \not\equiv 0 \pmod{p}$. Then pick a primitive root g modulo p, and a c so that $g^c \equiv a \pmod{p}$.

Binomial Congruences

- As an application of primitive roots we can say something when p is odd about the solution of congruences of the form
$$x^k \equiv a \pmod{p}.$$
- The case $a = 0$ is easy.
- The only solution is $x \equiv 0 \pmod{p}$.
- Suppose $a \not\equiv 0 \pmod{p}$. Then pick a primitive root g modulo p, and a c so that $g^c \equiv a \pmod{p}$.
- Also, since any solution x will have $p \nmid x$ we can define y so that $g^y \equiv x \pmod{p}$.

Binomial Congruences

- As an application of primitive roots we can say something when p is odd about the solution of congruences of the form
$$x^k \equiv a \pmod{p}.$$
- The case $a = 0$ is easy.
- The only solution is $x \equiv 0 \pmod{p}$.
- Suppose $a \not\equiv 0 \pmod{p}$. Then pick a primitive root g modulo p, and a c so that $g^c \equiv a \pmod{p}$.
- Also, since any solution x will have $p \nmid x$ we can define y so that $g^y \equiv x \pmod{p}$.
- Thus our congruence becomes
$$g^{ky} \equiv g^c \pmod{p}.$$

Binomial Congruences

- As an application of primitive roots we can say something when p is odd about the solution of congruences of the form
$$x^k \equiv a \pmod{p}.$$
- The case $a = 0$ is easy.
- The only solution is $x \equiv 0 \pmod{p}$.
- Suppose $a \not\equiv 0 \pmod{p}$. Then pick a primitive root g modulo p, and a c so that $g^c \equiv a \pmod{p}$.
- Also, since any solution x will have $p \nmid x$ we can define y so that $g^y \equiv x \pmod{p}$.
- Thus our congruence becomes
$$g^{ky} \equiv g^c \pmod{p}.$$
- Hence it follows that
$$ky \equiv c \pmod{p-1}.$$

- We have turned a polynomial congruence into a linear one.

- We have turned a polynomial congruence into a linear one.
- This is a bit like using logarithms on real numbers.

$$x^k \equiv a \pmod p,\ g^{ky} \equiv g^c \pmod p,$$

$$ky \equiv c \pmod{p-1}.$$

- We have turned a polynomial congruence into a linear one.
- This is a bit like using logarithms on real numbers.

$$x^k \equiv a \pmod{p},\ g^{ky} \equiv g^c \pmod{p},$$

$$ky \equiv c \pmod{p-1}.$$

- Sometimes the exponents c and y are referred to as the discrete logarithms modulo p to the base g.

- We have turned a polynomial congruence into a linear one.
- This is a bit like using logarithms on real numbers.

$$x^k \equiv a \pmod{p},\ g^{ky} \equiv g^c \pmod{p},$$

$$ky \equiv c \pmod{p-1}.$$

- Sometimes the exponents c and y are referred to as the discrete logarithms modulo p to the base g.
- Computing them numerically is hard and there is a protocol (Diffie-Hellman) which uses them to exchange secure keys and passwords.

- We have turned a polynomial congruence into a linear one.
- This is a bit like using logarithms on real numbers.

$$x^k \equiv a \pmod{p},\ g^{ky} \equiv g^c \pmod{p},$$

$$ky \equiv c \pmod{p-1}.$$

- Sometimes the exponents c and y are referred to as the discrete logarithms modulo p to the base g.
- Computing them numerically is hard and there is a protocol (Diffie-Hellman) which uses them to exchange secure keys and passwords.
- Our new congruence is soluble if and only if $(k, p-1)|c$, and when this holds the y which satisfy it lie in a residue class modulo $\frac{p-1}{(k,p-1)}$, i.e. $(k, p-1)$ different residue classes modulo $p-1$.

- We have turned a polynomial congruence into a linear one.
- This is a bit like using logarithms on real numbers.

$$x^k \equiv a \pmod{p},\ g^{ky} \equiv g^c \pmod{p},$$

$$ky \equiv c \pmod{p-1}.$$

- Sometimes the exponents c and y are referred to as the discrete logarithms modulo p to the base g.
- Computing them numerically is hard and there is a protocol (Diffie-Hellman) which uses them to exchange secure keys and passwords.
- Our new congruence is soluble if and only if $(k, p-1)|c$, and when this holds the y which satisfy it lie in a residue class modulo $\frac{p-1}{(k,p-1)}$, i.e. $(k, p-1)$ different residue classes modulo $p-1$.
- Thus, when $a \not\equiv 0 \pmod{p}$ the original congruence is either insoluble or has $(k, p-1)$ solutions.

- We have turned a polynomial congruence into a linear one.
- This is a bit like using logarithms on real numbers.

$$x^k \equiv a \pmod p,\ g^{ky} \equiv g^c \pmod p,$$

$$ky \equiv c \pmod{p-1}.$$

- Sometimes the exponents c and y are referred to as the discrete logarithms modulo p to the base g.
- Computing them numerically is hard and there is a protocol (Diffie-Hellman) which uses them to exchange secure keys and passwords.
- Our new congruence is soluble if and only if $(k, p-1)|c$, and when this holds the y which satisfy it lie in a residue class modulo $\frac{p-1}{(k,p-1)}$, i.e. $(k, p-1)$ different residue classes modulo $p-1$.
- Thus, when $a \not\equiv 0 \pmod p$ the original congruence is either insoluble or has $(k, p-1)$ solutions.

- We have turned a polynomial congruence into a linear one.
- This is a bit like using logarithms on real numbers.

$$x^k \equiv a \pmod p,\ g^{ky} \equiv g^c \pmod p,$$

$$ky \equiv c \pmod{p-1}.$$

- Sometimes the exponents c and y are referred to as the discrete logarithms modulo p to the base g.
- Computing them numerically is hard and there is a protocol (Diffie-Hellman) which uses them to exchange secure keys and passwords.
- Our new congruence is soluble if and only if $(k, p-1)|c$, and when this holds the y which satisfy it lie in a residue class modulo $\frac{p-1}{(k,p-1)}$, i.e. $(k, p-1)$ different residue classes modulo $p-1$.
- Thus, when $a \not\equiv 0 \pmod p$ the original congruence is either insoluble or has $(k, p-1)$ solutions.
- Thus we just proved a theorem.

Discrete Logarithms

- Thus we just proved a theorem.

Theorem 10

Suppose p is an odd prime. When $p \nmid a$ the congruence $x^k \equiv a \pmod{p}$ has 0 or $(k, p-1)$ solutions, and the number of reduced residues a modulo p for which it is soluble is $\frac{p-1}{(k,p-1)}$.

Discrete Logarithms

- Thus we just proved a theorem.

Theorem 10

Suppose p is an odd prime. When $p \nmid a$ the congruence $x^k \equiv a \pmod{p}$ has 0 or $(k, p-1)$ solutions, and the number of reduced residues a modulo p for which it is soluble is $\frac{p-1}{(k,p-1)}$.

- The above theorem suggests the following.

Definition 11

Given a primitive root g and a reduced residue class a modulo m we define the discrete logarithm $\text{dlog}_g(a)$, or index $\text{ind}_g(a)$ to be that unique residue class l modulo $\phi(m)$ such that $g^l \equiv a \pmod{m}$

Discrete Logarithms

- Thus we just proved a theorem.

Theorem 10

Suppose p is an odd prime. When $p \nmid a$ the congruence $x^k \equiv a \pmod{p}$ has 0 or $(k, p-1)$ solutions, and the number of reduced residues a modulo p for which it is soluble is $\frac{p-1}{(k,p-1)}$.

- The above theorem suggests the following.

Definition 11

Given a primitive root g and a reduced residue class a modulo m we define the discrete logarithm $\mathrm{dlog}_g(a)$, or index $\mathrm{ind}_g(a)$ to be that unique residue class l modulo $\phi(m)$ such that $g^l \equiv a \pmod{m}$

- The notation $\mathrm{ind}_g(x)$ is more commonly used, but $\mathrm{dlog}_g(x)$ seems more natural.

- It is useful to work through a detailed example.

Example 12

Find a primitive root modulo 11 and construct a table of discrete logarithms.

- It is useful to work through a detailed example.

Example 12

Find a primitive root modulo 11 and construct a table of discrete logarithms.

- First we try 2. The divisors of $11 - 1 = 10$ are 1, 2, 5, 10 and $2^1 = 2 \not\equiv 1 \pmod{11}$, $2^2 = 4 \not\equiv 1 \pmod{11}$, $2^5 = 32 \equiv 10 \not\equiv 1 \pmod{11}$, so 2 is a primitive root.

- It is useful to work through a detailed example.

Example 12

Find a primitive root modulo 11 and construct a table of discrete logarithms.

- First we try 2. The divisors of $11 - 1 = 10$ are 1, 2, 5, 10 and $2^1 = 2 \not\equiv 1 \pmod{11}$, $2^2 = 4 \not\equiv 1 \pmod{11}$, $2^5 = 32 \equiv 10 \not\equiv 1 \pmod{11}$, so 2 is a primitive root.
- Now we construct a table of powers of 2 modulo 11

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

- It is useful to work through a detailed example.

Example 12

Find a primitive root modulo 11 and construct a table of discrete logarithms.

- First we try 2. The divisors of $11-1=10$ are 1, 2, 5, 10 and $2^1=2\not\equiv 1 \pmod{11}$, $2^2=4\not\equiv 1 \pmod{11}$, $2^5=32\equiv 10\not\equiv 1 \pmod{11}$, so 2 is a primitive root.
- Now we construct a table of powers of 2 modulo 11

y	1	2	3	4	5	6	7	8	9	10
$x\equiv 2^y$	2	4	8	5	10	9	7	3	6	1

- Then we construct the "inverse" table

x	1	2	3	4	5	6	7	8	9	10
$y=\mathrm{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- It is useful to work through a detailed example.

Example 12

Find a primitive root modulo 11 and construct a table of discrete logarithms.

- First we try 2. The divisors of $11-1=10$ are 1, 2, 5, 10 and $2^1=2\not\equiv 1 \pmod{11}$, $2^2=4\not\equiv 1 \pmod{11}$, $2^5=32\equiv 10\not\equiv 1 \pmod{11}$, so 2 is a primitive root.
- Now we construct a table of powers of 2 modulo 11

y	1	2	3	4	5	6	7	8	9	10
$x\equiv 2^y$	2	4	8	5	10	9	7	3	6	1

- Then we construct the "inverse" table

x	1	2	3	4	5	6	7	8	9	10
$y=\mathrm{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- Note that while x is a residue modulo p (here $p=11$), the y are residues modulo $p-1$ (here 10).

- It is useful to work through a detailed example.

Example 12

Find a primitive root modulo 11 and construct a table of discrete logarithms.

- First we try 2. The divisors of $11 - 1 = 10$ are 1, 2, 5, 10 and $2^1 = 2 \not\equiv 1 \pmod{11}$, $2^2 = 4 \not\equiv 1 \pmod{11}$, $2^5 = 32 \equiv 10 \not\equiv 1 \pmod{11}$, so 2 is a primitive root.
- Now we construct a table of powers of 2 modulo 11

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

- Then we construct the "inverse" table

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- Note that while x is a residue modulo p (here $p = 11$), the y are residues modulo $p - 1$ (here 10).
- y is the order, or exponent, to which 2 has to be raised to give x modulo p. In other words $x \equiv g^{\text{dlog}_g(x)} \pmod{p}$.

- It is useful to work through a detailed example.

Example 12

Find a primitive root modulo 11 and construct a table of discrete logarithms.

- First we try 2. The divisors of $11-1=10$ are 1, 2, 5, 10 and $2^1=2\not\equiv 1 \pmod{11}$, $2^2=4\not\equiv 1 \pmod{11}$, $2^5=32\equiv 10\not\equiv 1 \pmod{11}$, so 2 is a primitive root.
- Now we construct a table of powers of 2 modulo 11

y	1	2	3	4	5	6	7	8	9	10
$x\equiv 2^y$	2	4	8	5	10	9	7	3	6	1

- Then we construct the “inverse” table

x	1	2	3	4	5	6	7	8	9	10
$y=\mathrm{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- Note that while x is a residue modulo p (here $p=11$), the y are residues modulo $p-1$ (here 10).
- y is the order, or exponent, to which 2 has to be raised to give x modulo p. In other words $x\equiv g^{\mathrm{dlog}_g(x)} \pmod{p}$.
- We can use this to solve congruences.

-

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

-

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- We can use this to solve,

Example 13

if possible, the congruences,

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- We can use this to solve,

Example 13

if possible, the congruences,

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- In the first put $x \equiv 2^y \pmod{11}$, so that $x^3 = 2^{3y}$ and we see from the second table that $6 \equiv 2^9 \pmod{11}$.

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- We can use this to solve,

Example 13

if possible, the congruences,

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- In the first put $x \equiv 2^y \pmod{11}$, so that $x^3 = 2^{3y}$ and we see from the second table that $6 \equiv 2^9 \pmod{11}$.

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- We can use this to solve,

Example 13

if possible, the congruences,

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- In the first put $x \equiv 2^y \pmod{11}$, so that $x^3 = 2^{3y}$ and we see from the second table that $6 \equiv 2^9 \pmod{11}$.
- We need $3y \equiv 9 \pmod{10}$.

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- We can use this to solve,

Example 13

if possible, the congruences,

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- In the first put $x \equiv 2^y \pmod{11}$, so that $x^3 = 2^{3y}$ and we see from the second table that $6 \equiv 2^9 \pmod{11}$.
- We need $3y \equiv 9 \pmod{10}$.
- This has the unique solution $y \equiv 3 \pmod{10}$.

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

- We can use this to solve,

Example 13

if possible, the congruences,

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- In the first put $x \equiv 2^y \pmod{11}$, so that $x^3 = 2^{3y}$ and we see from the second table that $6 \equiv 2^9 \pmod{11}$.
- We need $3y \equiv 9 \pmod{10}$.
- This has the unique solution $y \equiv 3 \pmod{10}$.
- Going to the first table we find that $x \equiv 8 \pmod{11}$.

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- For the second congruence we find that $5y \equiv 6 \pmod{10}$ and now we see that this has no solutions because $(5, 10) = 5 \nmid 6$.

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- For the second congruence we find that $5y \equiv 6 \pmod{10}$ and now we see that this has no solutions because $(5, 10) = 5 \nmid 6$.
- In the third case we have $65y \equiv 5 \pmod{10}$ and this is equivalent to $13y \equiv 1 \pmod{2}$ and this has one solution modulo $y \equiv 1 \pmod{2}$, and so 5 solutions modulo 10 given by $y \equiv 1$, 3, 5, 7 or 9 modulo 10.

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

x	1	2	3	4	5	6	7	8	9	10
$y = \text{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

- For the second congruence we find that $5y \equiv 6 \pmod{10}$ and now we see that this has no solutions because $(5, 10) = 5 \nmid 6$.
- In the third case we have $65y \equiv 5 \pmod{10}$ and this is equivalent to $13y \equiv 1 \pmod{2}$ and this has one solution modulo $y \equiv 1 \pmod{2}$, and so 5 solutions modulo 10 given by $y \equiv 1$, 3, 5, 7 or 9 modulo 10.
- Hence the original congruence has five solutions given by

$$x \equiv 2, 8, 10, 7, 6 \pmod{11}$$

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,
- compute $E \equiv M^e \pmod{n}$ and transmit E.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,
- compute $E \equiv M^e \pmod{n}$ and transmit E.
- The recipient then computes $E^d \pmod{n}$.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,
- compute $E \equiv M^e \pmod{n}$ and transmit E.
- The recipient then computes $E^d \pmod{n}$.
- Then $E^d \equiv (M^e)^d = M^{de} \equiv M \pmod{n}$, since $\phi(n)|de - 1$, and the recipient recovers the message.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,
- compute $E \equiv M^e \pmod{n}$ and transmit E.
- The recipient then computes $E^d \pmod{n}$.
- Then $E^d \equiv (M^e)^d = M^{de} \equiv M \pmod{n}$, since $\phi(n)|de - 1$, and the recipient recovers the message.
- The sender has to know only n and e.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,
- compute $E \equiv M^e \pmod{n}$ and transmit E.
- The recipient then computes $E^d \pmod{n}$.
- Then $E^d \equiv (M^e)^d = M^{de} \equiv M \pmod{n}$, since $\phi(n) | de - 1$, and the recipient recovers the message.
- The sender has to know only n and e.
- The recipient only has to know n and d.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,
- compute $E \equiv M^e \pmod{n}$ and transmit E.
- The recipient then computes $E^d \pmod{n}$.
- Then $E^d \equiv (M^e)^d = M^{de} \equiv M \pmod{n}$, since $\phi(n)|de - 1$, and the recipient recovers the message.
- The sender has to know only n and e.
- The recipient only has to know n and d.
- The level of security depends only on the ease with which one can find d knowing n and e.

RSA

- Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA.
- This is sometimes described as a way of sharing information by public key encryption.
- The principle of the method is as follows.
- Let $n, d, e \in \mathbb{N}$ be such that $de \equiv 1 \pmod{\phi(n)}$.
- Given a message M encoded as a number with $M < n$,
- compute $E \equiv M^e \pmod{n}$ and transmit E.
- The recipient then computes $E^d \pmod{n}$.
- Then $E^d \equiv (M^e)^d = M^{de} \equiv M \pmod{n}$, since $\phi(n) | de - 1$, and the recipient recovers the message.
- The sender has to know only n and e.
- The recipient only has to know n and d.
- The level of security depends only on the ease with which one can find d knowing n and e.
- The numbers n and e can be in the public domain.

- The crucial question is, given n and d, the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$.

- The crucial question is, given n and d, the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$.
- Suppose that n is the product of two primes

$$n = pq.$$

- The crucial question is, given n and d, the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$.

- Suppose that n is the product of two primes

$$n = pq.$$

- If n can be factored then we have $\phi(n) = (p-1)(q-1)$.

- The crucial question is, given n and d, the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$.

- Suppose that n is the product of two primes

$$n = pq.$$

- If n can be factored then we have $\phi(n) = (p-1)(q-1)$.
- But this factorization is a known hard problem, especially when the primes are roughly of the same size.

- The crucial question is, given n and d, the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$.
- Suppose that n is the product of two primes

$$n = pq.$$

- If n can be factored then we have $\phi(n) = (p-1)(q-1)$.
- But this factorization is a known hard problem, especially when the primes are roughly of the same size.
- Of course if the value of $\phi(n)$ can be discovered not only is the message easily broken,

- The crucial question is, given n and d, the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$.

- Suppose that n is the product of two primes

$$n = pq.$$

- If n can be factored then we have $\phi(n) = (p-1)(q-1)$.
- But this factorization is a known hard problem, especially when the primes are roughly of the same size.
- Of course if the value of $\phi(n)$ can be discovered not only is the message easily broken,
- but n is easily factored since one has

$$p + q = pq + 1 - \phi(n) = n + 1 - \phi(n),$$

$$pq = n$$

and once can substitute for q and then solve the quadratic equation in p.

- The crucial question is, given n and d, the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$.
- Suppose that n is the product of two primes

$$n = pq.$$

- If n can be factored then we have $\phi(n) = (p-1)(q-1)$.
- But this factorization is a known hard problem, especially when the primes are roughly of the same size.
- Of course if the value of $\phi(n)$ can be discovered not only is the message easily broken,
- but n is easily factored since one has

$$p + q = pq + 1 - \phi(n) = n + 1 - \phi(n),$$

$$pq = n$$

and once can substitute for q and then solve the quadratic equation in p.
- In other words, knowing $\phi(n)$ is equivalent to factoring n.