Chinese Remainder Theorem and Powers of an Element

9 The Chinese Remainder Theorem

Let

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

define mapping

$$cr : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

$$cr(a) = (a \bmod n_1, \dots, a \bmod n_k)$$

We (and only we) call $cr(a)$ the *chinese remainder representation* of a

Lemma 25. *Mapping cr is bijective.*

9 The Chinese Remainder Theorem

Let

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \to gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

define mapping

$$cr : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

$$cr(a) = (a \text{ mod } n_1, \dots, a \text{ mod } n_k)$$

We (and only we) call $cr(a)$ the *chinese remainder representation* of a

Lemma 25. *Mapping cr is bijective.*

Proof.

- by construction of inverse function. Given

  $$(a_1, \dots, a_k) \in \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

  define

  $$m_i = n/n_i \text{ for } i = 1, \dots, k$$

  $$m_i = n_1 \dots n_{i-1} n_{i+1} \dots n_k$$

9 The Chinese Remainder Theorem

Let

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

define mapping

$$cr : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

$$cr(a) = (a \bmod n_1, \dots, a \bmod n_k)$$

We (and only we) call $cr(a)$ the *chinese remainder representation* of a

Lemma 25. *Mapping cr is bijective.*

Proof.

- by construction of inverse function. Given

$$(a_1, \dots, a_k) \in \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

define

$$m_i = n/n_i \text{ for } i = 1, \dots, k$$

$$m_i = n_1 \dots n_{i-1} n_{i+1} \dots n_k$$

- $gcd(n_i, m_i) = 1$ and lemma 24 $\rightarrow$

$$m_i x \equiv 1 \bmod n_i \text{ has unique solution } m_i^{-1}$$

$$c_i = m_i (m_i^{-1} \bmod n_i)$$

$$a \equiv (a_1 c_1 . + \dots + a_k c_k) \bmod n$$

9 The Chinese Remainder Theorem

Let

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

define mapping

$$cr : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

$$cr(a) = (a \bmod n_1, \dots, a \bmod n_k)$$

We (and only we) call $cr(a)$ the *chinese remainder representation* of a

Lemma 25. *Mapping cr is bijective.*

Proof.

- by construction of inverse function. Given

$$(a_1, \dots, a_k) \in \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

define

$$m_i = n/n_i \text{ for } i = 1, \dots, k$$

$$m_i = n_1 \dots n_{i-1} n_{i+1} \dots n_k$$

- $gcd(n_i, m_i) = 1$ and lemma 24 $\rightarrow$

$$m_i x \equiv 1 \bmod n_i \text{ has unique solution } m_i^{-1}$$

$$c_i = m_i(m_i^{-1} \bmod n_i)$$

$$a \equiv (a_1 c_1 . + \dots + a_k c_k) \bmod n$$

- claim: $a \equiv a_i \bmod n_i$ for all i.

$$i \neq j \rightarrow c_j = m_j(m_j^{-1} \bmod n_j) \equiv 0 \bmod n_i$$

$$c_i \equiv 1 \bmod n_i$$

Observe

$$cr(c_i) = (0, \dots, 0, 1, 0 \dots 0) \quad \text{with 1 at position } i$$

$$\begin{aligned} a &\equiv a_i c_i \bmod n_i \\ &\equiv a_i m_i (m_i^{-1} mod n_i) \bmod n_i \\ &\equiv a_i \bmod n_i \end{aligned}$$

9 The Chinese Remainder Theorem

Let

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \to gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

define mapping

$$cr : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

$$cr(a) = (a \bmod n_1, \dots, a \bmod n_k)$$

We (and only we) call $cr(a)$ the *chinese remainder representation* of a

Lemma 25. *Mapping cr is bijective.*

Chinese remainder theorem

Lemma 26. *Mapping cr is a ring* ~~*homo*~~iso*morphism, i.e.it is bijective and if*

$$\begin{aligned} cr(a) &= (a_1, \dots, a_k) \\ cr(b) &= (b_1, \dots, b_k) \end{aligned}$$

then

$$\begin{aligned} cr(a+b) &= (a_1 + b_1 \bmod n_1, \dots, a_k + b_k \bmod n_k) \\ cr(a-b) &= (a_1 - b_1 \bmod n_1, \dots, a_k - b_k \bmod n_k) \\ cr(ab) &= (a_1 b_1 \bmod n_1, \dots, a_k b_k \bmod n_k) \end{aligned}$$

Proof. known equations from I2CA

9 The Chinese Remainder Theorem

Let

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

define mapping

$$cr : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

$$cr(a) = (a \bmod n_1, \dots, a \bmod n_k)$$

We (and only we) call $cr(a)$ the *chinese remainder representation* of a

Lemma 25. *Mapping cr is bijective.*

Chinese remainder theorem

Lemma 26. *Mapping cr is a ring homomorphism, i.e.it is bijective and if*

$$\begin{aligned} cr(a) &= (a_1, \dots, a_k) \\ cr(b) &= (b_1, \dots, b_k) \end{aligned}$$

then

$$\begin{aligned} cr(a+b) &= (a_1 + b_1 \bmod n_1, \dots, a_k + b_k \bmod n_k) \\ cr(a-b) &= (a_1 - b_1 \bmod n_1, \dots, a_k - b_k \bmod n_k) \\ cr(ab) &= (a_1 b_1 \bmod n_1, \dots, a_k b_k \bmod n_k) \end{aligned}$$

Proof. known equations from I2CA

Lemma 27. *Let*

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

and

$$(a_1, \dots, a_k) \in \mathbb{N}^k$$

Then the set of equations

$$x \equiv a_i \bmod n_i \ , \ 1 \leq i \leq k$$

has a unique solution in Z_n

9 The Chinese Remainder Theorem

Let

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

define mapping

$$cr : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \dots \mathbb{Z}_{n_k}$$

$$cr(a) = (a \bmod n_1, \dots, a \bmod n_k)$$

We (and only we) call $cr(a)$ the *chinese remainder representation* of a

Lemma 25. *Mapping cr is bijective.*

Chinese remainder theorem

Lemma 26. *Mapping cr is a ring homomorphism, i.e.it is bijective and if*

$$\begin{aligned} cr(a) &= (a_1, \dots, a_k) \\ cr(b) &= (b_1, \dots, b_k) \end{aligned}$$

then

$$\begin{aligned} cr(a+b) &= (a_1 + b_1 \bmod n_1, \dots, a_k + b_k \bmod n_k) \\ cr(a-b) &= (a_1 - b_1 \bmod n_1, \dots, a_k - b_k \bmod n_k) \\ cr(ab) &= (a_1 b_1 \bmod n_1, \dots, a_k b_k \bmod n_k) \end{aligned}$$

Proof. known equations from I2CA

Lemma 27. *Let*

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

and

$$(a_1, \dots, a_k) \in \mathbb{N}^k$$

Then the set of equations

$$x \equiv a_i \bmod n_i \ , \ 1 \leq i \leq k$$

has a unique solution in Z_n

Lemma 28. *Let*

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

and

$$a, x \in \mathbb{Z}$$

then

$$x \equiv a \bmod n_i \text{ for all } i \in [1:k] \quad \leftrightarrow \quad x \equiv a \bmod n$$

9 The Chinese Remainder Theorem

example:

$$\begin{aligned} a &\equiv 2 \bmod 5 \\ a &\equiv 3 \bmod 13 \\ a \bmod 65 &= ? \end{aligned}$$

$$a_1 = 2\ ,\ n_1 = m_2 = 5$$

$$a_2 = 3\ ,\ n_2 = m_1 = 13$$

$$13^{-1} \equiv 2 \bmod 5\ ,5^{-1} \equiv 8 \bmod 13$$

$$\begin{aligned} c_1 &= 13(2 \bmod 5) = 26 \\ c_2 &= 5(8 \bmod 13) = 40 \end{aligned}$$

$$\begin{aligned} a &\equiv 2 \cdot 26 + 3 \cdot 40 \bmod 65 \\ &\equiv 52 + 120 \bmod 65 \\ &\equiv 42 \bmod 65 \end{aligned}$$

10 Powers of an element

Consider group

$$(Z_n^*, \cdot_n) \quad , \quad Z_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}$$

$$a^{(i)} = a^i \bmod n \quad , \quad \langle a \rangle = \{a^i \bmod n \ : \ i \in \mathbb{N}\} \quad , \quad ord(a) = |\langle a \rangle|$$

$i = 0$ **?**

$$e = 1 \ , \ \exists j : a \cdot_n a^j = e = 1 \text{ (group)}$$
$$a^{(0)} = a^{j+1} \bmod n = 1 \in \langle a \rangle$$

10 Powers of an element

Consider group

$$(Z_n^*, \cdot_n) \quad , \quad Z_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}$$

$$a^{(i)} = a^i \bmod n \quad , \quad \langle a \rangle = \{a^i \bmod n \ : \ i \in \mathbb{N}\} \quad , \quad ord(a) = |\langle a \rangle|$$

$i = 0$ **?**

$$e = 1 \ , \ \exists j : a \cdot_n a^j = e = 1 \ \text{(group)}$$
$$a^{(0)} = a^{j+1} \bmod n = 1 \in \langle a \rangle$$

examples:

i	0	1	2	3	4	5	6	7	8	...
3^i mod 7	1	3	2	6	4	5	1	3	2	...

Table 3: Illustration of $\langle 3 \rangle \subseteq \mathbb{Z}_7^*$

$$\langle 3 \rangle = \{1,2,3,4,5,6\} \quad , \quad ord(3) = 6$$

10 Powers of an element

Consider group

$$(Z_n^*, \cdot_n) \quad , \quad Z_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}$$

$$a^{(i)} = a^i \bmod n \quad , \quad \langle a \rangle = \{a^i \bmod n \ : \ i \in \mathbb{N}\} \quad , \quad ord(a) = |\langle a \rangle|$$

$i = 0$ **?**

$$e = 1 \ , \ \exists j : a \cdot_n a^j = e = 1 \text{ (group)}$$
$$a^{(0)} = a^{j+1} \bmod n = 1 \in \langle a \rangle$$

examples:

i	0	1	2	3	4	5	6	7	8	...
3^i mod 7	1	3	2	6	4	5	1	3	2	...

Table 3: Illustration of $\langle 3 \rangle \subseteq \mathbb{Z}_7^*$

$$\langle 3 \rangle = \{1,2,3,4,5,6\} \quad , \quad ord(3) = 6$$

i	0	1	2	3	4	5	6	7	8	...
2^i mod 7	1	2	4	1	2	4	1	2	4	...

Table 4: Illustration of $\langle 2 \rangle \subseteq \mathbb{Z}_7^*$

$$\langle 2 \rangle = \{1,2,4\} \quad , \quad ord(2) = 3$$

10 Powers of an element

Consider group

$$(Z_n^*, \cdot_n) \quad , \quad Z_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}$$

$$a^{(i)} = a^i \bmod n \quad , \quad \langle a \rangle = \{a^i \bmod n \ : \ i \in \mathbb{N}\} \quad , \quad ord(a) = |\langle a \rangle|$$

$i = 0$ **?**

$$e = 1 \ , \ \exists j : a \cdot_n a^j = e = 1 \text{ (group)}$$
$$a^{(0)} = a^{j+1} \bmod n = 1 \in \langle a \rangle$$

examples:

i	0	1	2	3	4	5	6	7	8	...
3^i mod 7	1	3	2	6	4	5	1	3	2	...

Table 3: Illustration of $\langle 3 \rangle \subseteq \mathbb{Z}_7^*$

$$\langle 3 \rangle = \{1,2,3,4,5,6\} \quad , \quad ord(3) = 6$$

i	0	1	2	3	4	5	6	7	8	...
2^i mod 7	1	2	4	1	2	4	1	2	4	...

Table 4: Illustration of $\langle 3 \rangle \subseteq \mathbb{Z}_7^*$

$$\langle 2 \rangle = \{1,2,4\} \quad , \quad ord(2) = 3$$

recall $|\mathbb{Z}_n^*| = \varphi(n)$ and lemma 17:

If $(S, \circ)$ is a finite group with identity e, then $a^{(|S|)} = e \quad$ for all $a \in S$.

Euler's theorem

Lemma 29.

$$a^{\varphi(n)} \equiv 1 \bmod n \quad \textit{for all } a \in \mathbb{Z}_n^*$$

10 Powers of an element

Consider group

$$(Z_n^*, \cdot_n) \quad , \quad Z_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}$$

$$a^{(i)} = a^i \bmod n \quad , \quad \langle a \rangle = \{a^i \bmod n \ : \ i \in \mathbb{N}\} \quad , \quad ord(a) = |\langle a \rangle|$$

$i = 0$ **?**

$$e = 1 \ , \ \exists j : a \cdot_n a^j = e = 1 \ \text{(group)}$$
$$a^{(0)} = a^{j+1} \bmod n = 1 \in \langle a \rangle$$

examples:

i	0	1	2	3	4	5	6	7	8	...
3^i mod 7	1	3	2	6	4	5	1	3	2	...

Table 3: Illustration of $\langle 3 \rangle \subseteq \mathbb{Z}_7^*$

$$\langle 3 \rangle = \{1,2,3,4,5,6\} \quad , \quad ord(3) = 6$$

i	0	1	2	3	4	5	6	7	8	...
2^i mod 7	1	2	4	1	2	4	1	2	4	...

Table 4: Illustration of $\langle 3 \rangle \subseteq \mathbb{Z}_7^*$

$$\langle 2 \rangle = \{1,2,4\} \quad , \quad ord(2) = 3$$

recall $|\mathbb{Z}_n^*| = \varphi(n)$ and lemma 17:

If $(S, \circ)$ is a finite group with identity e, then $a^{(|S|)} = e \quad$ for all $a \in S$.

Euler's theorem

Lemma 29.
$$a^{\varphi(n)} \equiv 1 \bmod n \quad \textit{for all } a \in \mathbb{Z}_n^*$$

Fermat's theorem

Lemma 30. *If p is prime, then*

$$a^{p-1} \equiv 1 \bmod p \quad \textit{for all } a \in \mathbb{Z}_p^*$$

Proof.

$$p \text{ prime} \quad \rightarrow \quad \varphi(p) = p - 1$$

10 Powers of an element

primitive roots, generators

If $g \in \mathbb{Z}_n^*$ and $ord(g) = |Z_n^*|$, then g is called a *primitive root* or *generator* of Z_n^*.

e.g. 3 is generator of $\mathbb{Z}_7^*$ and 2 is not.

$\mathbb{Z}_n^*$ is *cyclic* iff it has a generator.

Lemma 31. *The only values $n > 1$, for which $\mathbb{Z}_n^*$ is cyclic are*

$$2, 4, p^e, 2p^e \quad \textit{for } p \textit{ prime and } e \in \mathbb{N}$$

10 Powers of an element

primitive roots, generators

If $g \in \mathbb{Z}_n^*$ and $ord(g) = |Z_n^*|$, then g is called a *primitive root* or *generator* of Z_n^*.

e.g. 3 is generator of $\mathbb{Z}_7^*$ and 2 is not.

$\mathbb{Z}_n^*$ is *cyclic* iff it has a generator.

Lemma 31. *The only values $n > 1$, for which $\mathbb{Z}_n^*$ is cyclic are*

$$2, 4, p^e, 2p^e \quad \textit{for } p \textit{ prime and } e \in \mathbb{N}$$

Proof.

- in: Niven and Zuckermann: An Introduction to the Theory of Numbers, John Wiley & Sons, fourth edition 1980. Out of print. Used books are available but expensive.
- part of the proof in Kuldeep Singh: Number Theory step by step. Oxford University Press 2020. The remaining part is on 'the books web site':

  https://fdslive.oup.com/www.oup.com/booksites/uk/booksites/content/9780198846734/Section 6.5.pdf

$\square$

10 Powers of an element

primitive roots, generators

If $g \in \mathbb{Z}_n^*$ and $ord(g) = |Z_n^*|$, then g is called a *primitive root* or *generator* of Z_n^*.

e.g. 3 is generator of $\mathbb{Z}_7^*$ and 2 is not.

$\mathbb{Z}_n^*$ is *cyclic* iff it has a generator.

Lemma 31. *The only values $n > 1$, for which $\mathbb{Z}_n^*$ is cyclic are*

$$2, 4, p^e, 2p^e \quad \textit{for } p \textit{ prime and } e \in \mathbb{N}$$

Proof.

- in: Niven and Zuckermann: An Introduction to the Theory of Numbers, John Wiley & Sons, fourth edition 1980. Out of print. Used books are available but expensive.
- part of the proof in Kuldeep Singh: Number Theory step by step. Oxford University Press 2020. The remaining part is on 'the books web site':

  https://fdslive.oup.com/www.oup.com/booksites/uk/booksites/content/9780198846734/Section 6.5.pdf

□

Discrete logarithm theorem

Lemma 32. *Let g be primitive root of $\mathbb{Z}_n^*$, then*

$$g^x \equiv g^y \bmod n \quad \leftrightarrow \quad x \equiv y \bmod \varphi(n)$$

10 Powers of an element

primitive roots, generators

If $g \in \mathbb{Z}_n^*$ and $ord(g) = |Z_n^*|$, then g is called a *primitive root* or *generator* of Z_n^*.

e.g. 3 is generator of $\mathbb{Z}_7^*$ and 2 is not.

$\mathbb{Z}_n^*$ is *cyclic* iff it has a generator.

Lemma 31. *The only values $n > 1$, for which $\mathbb{Z}_n^*$ is cyclic are*

$$2, 4, p^e, 2p^e \quad \text{for } p \text{ prime and } e \in \mathbb{N}$$

Proof.

- in: Niven and Zuckermann: An Introduction to the Theory of Numbers, John Wiley & Sons, fourth edition 1980. Out of print. Used books are available but expensive.
- part of the proof in Kuldeep Singh: Number Theory step by step. Oxford University Press 2020. The remaining part is on 'the books web site':

  https://fdslive.oup.com/www.oup.com/booksites/uk/booksites/content/9780198846734/Section 6.5.pdf

□

Discrete logarithm theorem

Lemma 32. *Let g be primitive root of $\mathbb{Z}_n^*$, then*

$$g^x \equiv g^y \bmod n \quad \leftrightarrow \quad x \equiv y \bmod \varphi(n)$$

- assume $x \equiv y \bmod \varphi(n)$:

$$x = y + k\varphi(n) \text{ with } k \in \mathbb{Z}$$

$$\begin{aligned} g^x &\equiv g^{y+k\varphi(n)} \bmod n \\ &\equiv g^y \cdot (g^{\varphi(n)})^k \bmod n \\ &\equiv g^y \cdot 1^k \bmod n \quad \text{(Euler's theorem)} \\ &\equiv g^y \bmod n \end{aligned}$$

10 Powers of an element

primitive roots, generators

If $g \in \mathbb{Z}_n^*$ and $ord(g) = |Z_n^*|$, then g is called a *primitive root* or *generator* of Z_n^*.

e.g. 3 is generator of $\mathbb{Z}_7^*$ and 2 is not.

$\mathbb{Z}_n^*$ is *cyclic* iff it has a generator.

Lemma 31. *The only values $n > 1$, for which $\mathbb{Z}_n^*$ is cyclic are*

$$2, 4, p^e, 2p^e \quad \textit{for } p \textit{ prime and } e \in \mathbb{N}$$

Proof.

- in: Niven and Zuckermann: An Introduction to the Theory of Numbers, John Wiley & Sons, fourth edition 1980. Out of print. Used books are available but expensive.
- part of the proof in Kuldeep Singh: Number Theory step by step. Oxford University Press 2020. The remaining part is on 'the books web site':

  https://fdslive.oup.com/www.oup.com/booksites/uk/booksites/content/9780198846734/Section 6.5.pdf

$\square$

Discrete logarithm theorem

Lemma 32. *Let g be primitive root of $\mathbb{Z}_n^*$, then*

$$g^x \equiv g^y \bmod n \quad \leftrightarrow \quad x \equiv y \bmod \varphi(n)$$

- assume $x \equiv y \bmod \varphi(n)$:

$$x = y + k\varphi(n) \text{ with } k \in \mathbb{Z}$$

$$\begin{aligned} g^x &\equiv g^{y+k\varphi(n)} \bmod n \\ &\equiv g^y \cdot (g^{\varphi(n)})^k \bmod n \\ &\equiv g^y \cdot 1^k \bmod n \quad \text{(Euler's theorem)} \\ &\equiv g^y \bmod n \end{aligned}$$

- assume $g^x \equiv g^y \bmod n$

$$|\langle g \rangle| = |\mathbb{Z}_n^*| = \varphi(n)$$

recall lemma 16: with $|\langle a \rangle| = t$ sequence $a^{(0)}, a^{(1)}, \ldots$ is periodic with period t, i.e. for all i, j:

$$i \equiv j \bmod t \leftrightarrow a^{(i)} = a^{(j)}$$

Hence with $t = \varphi(n)$:

$$x \equiv y \bmod \varphi(n)$$

10 Powers of an element

square roots of 1 modulo n:

Lemma 33. *Let $p \neq 2$ be prime and $e \geq 1$. Then the only solutions of equation*

$$x^2 \equiv 1 \bmod p^e$$

are

$$x = 1 \;,\; x = -1$$

10 Powers of an element

square roots of 1 modulo n:

Lemma 33. *Let $p \neq 2$ be prime and $e \geq 1$. Then the only solutions of equation*

$$x^2 \equiv 1 \bmod p^e$$

are

$$x = 1 \; , \; x = -1$$

- $$x^2 \equiv 1 \bmod p^e \quad \leftrightarrow p^e \mid (x-1)(x+1)$$

  $$p > 2 \quad \rightarrow \quad \sim (p|(x-1) \wedge p|(x+1))$$

  i.e. p cannot divide both.

10 Powers of an element

square roots of 1 modulo n:

Lemma 33. *Let $p \neq 2$ be prime and $e \geq 1$. Then the only solutions of equation*

$$x^2 \equiv 1 \bmod p^e$$

are

$$x = 1 \ , \ x = -1$$

- $$x^2 \equiv 1 \bmod p^e \quad \leftrightarrow p^e \mid (x-1)(x+1)$$

  $$p > 2 \quad \rightarrow \quad \sim (p|(x-1) \wedge p|(x+1))$$

  i.e. p cannot divide both.

$$\left\{ \begin{array}{l} x-1 = kp \\ x+1 = sp \\ (s-k)p = 2 \\ s-k = \frac{2}{p} < 1 \end{array} \right.$$

contradiction

- $p \nmid (x-1)$

  $$gcd(p^e, (x-1)) = 1 \quad , \quad p^e \mid (x+1) \quad , \quad x \equiv -1 \bmod p^e$$

- $p \nmid (x+1)$

  $$gcd(p^e, (x+1)) = 1 \quad , \quad p^e \mid (x-1) \quad , \quad x \equiv 1 \bmod p^e$$

10 Powers of an element

square roots of 1 modulo n:

Lemma 33. *Let $p \neq 2$ be prime and $e \geq 1$. Then the only solutions of equation*

$$x^2 \equiv 1 \bmod p^e$$

are

$$x = 1 \ , \ x = -1$$

- $$x^2 \equiv 1 \bmod p^e \quad \leftrightarrow p^e \mid (x-1)(x+1)$$

  $$p > 2 \quad \rightarrow \quad \sim (p|(x-1) \wedge p|(x+1))$$

  i.e. p cannot divide both.

- $p^e \ \not| (x-1)$

  $$gcd(p^e,(x-1)) = 1 \quad , \quad p^e \mid (x+1) \quad , \quad x \equiv -1 \bmod p^e$$

- $p^e \ \not| (x+1)$

  $$gcd(p^e,(x+1)) = 1 \quad , \quad p^e \mid (x-1) \quad , \quad x \equiv 1 \bmod p^e$$

nontrivial square roots of 1 modulo n

x is a *nontrivial square root of 1* modulo n iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

e.g. 6 is nontrivial square root of 1 modulo 35.

10 Powers of an element

square roots of 1 modulo n:

Lemma 33. *Let $p \neq 2$ be prime and $e \geq 1$. Then the only solutions of equation*

$$x^2 \equiv 1 \bmod p^e$$

are

$$x = 1 \ , \ x = -1$$

- $$x^2 \equiv 1 \bmod p^e \quad \leftrightarrow p^e \mid (x-1)(x+1)$$

  $$p > 2 \quad \rightarrow \quad \sim (p|(x-1) \wedge p|(x+1))$$

  i.e. p cannot divide both.

- $p^e \nmid (x-1)$

  $$gcd(p^e, (x-1)) = 1 \quad , \quad p^e \mid (x+1) \quad , \quad x \equiv -1 \bmod p^e$$

- $p^e \nmid (x+1)$

  $$gcd(p^e, (x+1)) = 1 \quad , \quad p^e \mid (x-1) \quad , \quad x \equiv 1 \bmod p^e$$

nontrivial square roots of 1 modulo n

x is a *nontrivial square root of 1* modulo n iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

e.g. 6 is nontrivial square root of 1 modulo 35.

Lemma 34. *If there exists a nontrivial square root of $n > 1$, then n is composite.*

Proof. Lemma 33: $n \neq p^e$ with $p > 2$.

$$x^2 \equiv 1 \bmod 2 \quad \rightarrow \quad x \equiv 1 \bmod 2 \quad \text{(trivial square root)}$$

$n > 1$ is not prime, hence composite.

10 Powers of an element

square roots of 1 modulo n:

Lemma 33. *Let $p \neq 2$ be prime and $e \geq 1$. Then the only solutions of equation*

$$x^2 \equiv 1 \bmod p^e$$

are

$$x = 1 \ , \ x = -1$$

- $$x^2 \equiv 1 \bmod p^e \quad \leftrightarrow p^e \mid (x-1)(x+1)$$

$$p > 2 \quad \rightarrow \quad \sim (p|(x-1) \wedge p|(x+1))$$

i.e. p cannot divide both.

- $p^e \not| (x-1)$

$$gcd(p^e, (x-1)) = 1 \quad , \quad p^e \mid (x+1) \quad , \quad x \equiv -1 \bmod p^e$$

- $p^e \not| (x+1)$

$$gcd(p^e, (x+1)) = 1 \quad , \quad p^e \mid (x-1) \quad , \quad x \equiv 1 \bmod p^e$$

nontrivial square roots of 1 modulo n

x is a *nontrivial square root of 1* modulo n iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

e.g. 6 is nontrivial square root of 1 modulo 35.

Lemma 34. *If there exists a nontrivial square root of $n > 1$, then n is composite.*

Proof. Lemma 33: $n \neq p^e$ with $p > 2$.

$$x^2 \equiv 1 \bmod 2 \quad \rightarrow \quad x \equiv 1 \bmod 2 \quad \text{(trivial square root)}$$

$n > 1$ is not prime, hence composite.

nontrivial square root mod n proves that n is not a prime

11 Exponentiation by successive squaring (Horner rule)

goal: compute $a^c \bmod n$. Let

$$c \in [0 : 2^k - 1] \quad , \quad b = b[k-1:0] = bin_k(c) \quad \text{(binary representation of } c\text{)}$$

$$c = \sum_{i=0}^{k-1} b[i] 2^i$$

For $i \in [0 : k-1]$ the leading $i+1$ high order bits of b are $b[k-1 : k-1-i]$.

11 Exponentiation by successive squaring (Horner rule)

goal: compute $a^c \bmod n$. Let

$$c \in [0 : 2^k - 1] \quad , \quad b = b[k-1:0] = bin_k(c) \quad \text{(binary representation of } c\text{)}$$

$$c = \sum_{i=0}^{k-1} b[i] 2^i$$

For $i \in [0 : k-1]$ the leading $i+1$ high order bits of b are $b[k-1 : k-1-i]$.

computation:

For $i = 0$ to $k-1$ compute successively

$$C(i) = a^{\langle b[k-1:k-1-i] \rangle} \bmod n$$

11 Exponentiation by successive squaring (Horner rule)

goal: compute $a^c \bmod n$. Let

$$c \in [0 : 2^k - 1] \quad , \quad b = b[k-1:0] = bin_k(c) \quad \text{(binary representation of } c\text{)}$$

$$c = \sum_{i=0}^{k-1} b[i]2^i$$

For $i \in [0 : k-1]$ the leading $i+1$ high order bits of b are $b[k-1 : k-1-i]$.

computation:

For $i = 0$ to $k-1$ compute successively

$$C(i) = a^{\langle b[k-1:k-1-i]\rangle} \bmod n$$

- $i = 0$

$$\begin{aligned} C(0) &= a^{b[k-1]} \\ &= \begin{cases} a \bmod n & b[k-1] = 1 \\ 1 & b[k-1] = 0 \end{cases} \end{aligned}$$

11 Exponentiation by successive squaring (Horner rule)

goal: compute a^c mod n. Let

$$c \in [0:2^k-1] \quad , \quad b = b[k-1:0] = bin_k(c) \quad \text{(binary representation of } c\text{)}$$

$$c = \sum_{i=0}^{k-1} b[i]2^i$$

For $i \in [0:k-1]$ the leading $i+1$ high order bits of b are $b[k-1:k-1-i]$.

computation:

For $i = 0$ to $k-1$ compute successively

$$C(i) = a^{\langle b[k-1:k-1-i]\rangle} \bmod n$$

- $i = 0$

$$\begin{aligned} C(0) &= a^{b[k-1]} \\ &= \begin{cases} a \bmod n & b[k-1] = 1 \\ 1 & b[k-1] = 0 \end{cases} \end{aligned}$$

- $i-1 \to i$

$$\begin{aligned} C(i) &= a^{\langle b[k-1:k-1-i]\rangle} \bmod n \\ &= a^{2\langle b[k-1:k-1-(i-1)]\rangle + b[k-1-i]} \bmod n \\ &= C(i-1)^2 \cdot a^{b[k-1-i]} \bmod n \\ &= \begin{cases} C(i-1)^2 \cdot a \bmod n & b[k-1-i] = 1 \\ C(i-1)^2 \bmod n & b[k-1-i] = 0 \end{cases} \end{aligned}$$

11 Exponentiation by successive squaring (Horner rule)

goal: compute $a^c \bmod n$. Let

$$c \in [0 : 2^k - 1] \quad , \quad b = b[k-1:0] = bin_k(c) \quad \text{(binary representation of } c\text{)}$$

$$c = \sum_{i=0}^{k-1} b[i] 2^i$$

For $i \in [0 : k-1]$ the leading $i+1$ high order bits of b are $b[k-1 : k-1-i]$.

computation:

For $i = 0$ to $k-1$ compute successively

$$C(i) = a^{\langle b[k-1:k-1-i] \rangle} \bmod n$$

- $i = 0$

$$\begin{aligned} C(0) &= a^{b[k-1]} \\ &= \begin{cases} a \bmod n & b[k-1] = 1 \\ 1 & b[k-1] = 0 \end{cases} \end{aligned}$$

- $i - 1 \to i$

$\langle 10011 \rangle = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$
$= 2(1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) + 1$
$= 2 \langle 1001 \rangle + 1$

for example.

$$\begin{aligned} C(i) &= a^{\langle b[k-1:k-1-i] \rangle} \bmod n \\ &= a^{2\langle b[k-1:k-1-(i-1)] \rangle + b[k-1-i]} \bmod n \\ &= C(i-1)^2 \cdot a^{b[k-1-i]} \bmod n \\ &= \begin{cases} C(i-1)^2 \cdot a \bmod n & b[k-1-i] = 1 \\ C(i-1)^2 \bmod n & b[k-1-i] = 0 \end{cases} \end{aligned}$$

complexity: $O(\log b)$ arithmetic operations mod n.