

Chinese Remainder Theorem

John Leo

November 20, 2023

1 Instrumentation

1. Xiaoluo [small gong] (30 bar phrases)
2. Paigu [drums] (7 bar phrases)
3. Yanqin (5 bar phrase)
4. Plucked Strings (3 bar phrases)
 - (a) Zhongruan
 - (b) Pipa
5. Bowed Strings (2 bar phrases)
 - (a) Erhu
 - (b) Zhonghu

2 Musical Structure

- There are $2 \cdot 3 \cdot 5 \cdot 7 = 210$ bars of music.
- Tempo is 120 bpm. 4/4 time, so 840 beats and exactly 7 minutes of music. Divide into 7 one-minute sections of 30 bars of music.
- Key is G major.
- All instruments play only scale tones.
 - Yangqin plays the pentatonic scale omitting 4 and 7 (G, A, B, D, E). (Major Pentatonic: <https://ianring.com/musictheory/scales/661>)
 - All other strings play a hexatonic scale omitting only 4 (G, A, B, D, E, F#). (Raga Kumud: <https://ianring.com/musictheory/scales/2709>)

3 Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem). *Let I_1, \dots, I_N be pairwise comaximal ideals of commutative ring R ($I_i + I_j = R$ for all $i \neq j$). Then there is a ring isomorphism $R/(\cap_k I_k) \simeq \prod_k (R/I_k)$. In particular if $n_k \in \mathbb{Z}$ are pairwise coprime then $\mathbb{Z}/[(\prod_k n_k)\mathbb{Z}] \simeq \prod_k (\mathbb{Z}/n_k\mathbb{Z})$.*

Proof Outline. The primary source for the proof is Serge Lang, *Algebra, Revised Third Edition* (2002), pages 94-95.

1. Bézout's Lemma: Coprime implies comaximal. If $(m, n) = 1$, then $\exists a, b$ s.t. $1 = am + bn$.
2. Surjectivity. Base case $n = 2$. Given $(c, d) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, let $x = dam + cbn$.
3. Induction: For all k , $n_k\mathbb{Z}$ is comaximal to the product of the other $n_i\mathbb{Z}$: $n_k\mathbb{Z} + \prod_{i \neq k} n_i\mathbb{Z} = \mathbb{Z}$.
4. By the theorem with $n = 2$, for all k we can find y_k satisfying $y_k \equiv 1 \pmod{n_k}$, $y_k \equiv 0 \pmod{\prod_{i \neq k} n_i}$.
5. Then given $(x_1, \dots, x_N) \in \prod_k (\mathbb{Z}/n_k\mathbb{Z})$, $\sum_k x_k y_k$ maps to (x_1, \dots, x_N) .
6. Injectivity. The kernel of the homomorphism is $(\prod_k n_k)\mathbb{Z}$.
7. Todo

□

4 Musical Realization

Xiaoluo introduces each 30 bar section, counting the section number. Paigu plays patterns changing every 7 bars so that the full cycle is completed in 210 bars. Each section is described below.

1. Bézout's Lemma ([EuclideanDomain.gcd_eq_gcd_ab](#)) is illustrated by the special case $m = 2, n = 3$ following the extended Euclidean algorithm ([EuclideanDomain.xgcd](#)). Erhu/Zhonghu represent 2, Pipa/Zhongruan represent 3, and Yangqin does additional work. The sequence (following [EuclideanDomain.xgcdAux](#)) is:

- (a) $2 = 1 \cdot 2 + 0 \cdot 3$
- (b) $3 = 0 \cdot 2 + 1 \cdot 3$
- (c) $2 = 1 \cdot 2 + 0 \cdot 3$
- (d) $1 = (-1) \cdot 2 + 1 \cdot 3$

Each step takes 6 bars. The final 6 bars is devoted to a special case of the surjectivity base case: $2 = (-2) \cdot 2 + 2 \cdot 3$

2. Surjectivity. Base case $n = 2$. Again for $m = 2, n = 3$, five of the six cases (omitting only $(0, 0)$) are illustrated using different themes in this order:

- (a) $2 = 1 \cdot 2 + 0 \cdot 3$ [$2 \leftrightarrow (0, 2)$]
- (b) $4 = 2 \cdot 2 + 0 \cdot 3$ [$4 \leftrightarrow (0, 1)$]
- (c) $3 = 0 \cdot 2 + 1 \cdot 3$ [$3 \leftrightarrow (1, 0)$]
- (d) $5 = 1 \cdot 2 + 1 \cdot 3$ [$5 \leftrightarrow (1, 2)$]
- (e) $7 = 2 \cdot 2 + 1 \cdot 3$ [$1 \leftrightarrow (1, 1)$]

3. Illustration of the beginning of induction using 2, 3, 5: Each number is comaximal to the product of the other two.

(a) $1 = (-1) \cdot 5 + 1 \cdot 6$

(b) $1 = (-3) \cdot 3 + 1 \cdot 10$

(c) $1 = (-7) \cdot 2 + 1 \cdot 15$

The sections are 5, 10, 15 measures long respectively. The basic idea is that the “lone” instrument plays in opposition to the other two.

4. Inductive hypothesis with $n = 2$ illustrated for five of the thirty cases for $m = 5, n = 6$.

(a) $11 = 1 \cdot 5 + 1 \cdot 6$ [$11 \leftrightarrow (1, 5)$]

(b) $16 = 2 \cdot 5 + 1 \cdot 6$ [$16 \leftrightarrow (1, 4)$]

(c) $17 = 1 \cdot 5 + 2 \cdot 6$ [$17 \leftrightarrow (2, 5)$]

(d) $22 = 2 \cdot 5 + 2 \cdot 6$ [$22 \leftrightarrow (2, 4)$]

(e) $27 = 3 \cdot 5 + 2 \cdot 6$ [$27 \leftrightarrow (2, 3)$]

5. 5

6. 6

7. 7