Magma Assignment 03

Combinatorics and Cryptography

Chinese Remainder Theorem

During Lecture 8 we proved the following:

Theorem 1 (Chinese Remainder Theorem)**.** *Let $s, t \in \mathbb{N}$ be coprime. For each pair of integers a, b there exists a solution x to the system of equations*

$$\begin{cases} x = a \pmod{s} \\ x = b \pmod{t} \end{cases} . \tag{1}$$

The solution x is unique in $\mathbb{Z}_n$, where $n = st$.

Task

Implement a function called `CRTsolver` which takes as inputs

- a sequence `L` of positive integers (≥ 0) and
- a sequence `M` of *pairwise coprime*[1] natural numbers (> 0) such that `#L=#M=m`,

and returns a solution x to the system of equations

$$\begin{cases} x = L[1] \pmod{M[1]} \\ x = L[2] \pmod{M[2]} \\ \quad \vdots \\ x = L[m] \pmod{M[m]} \end{cases} .$$

Notice that x is unique in $\mathbb{Z}_n$, where $n = \prod_{i=1}^{m} M[i]$.

[1] the greatest common divisor of each pair of two distinct elements in the sequence is 1.

Requirements

- Let `CRTsolver` check if `#L eq #M`. If not, return an error string.
- Let `CRTsolver` double check if all the elements in `M` are pairwise coprime. If not, return an error string.
- Let `CRTsolver` return, if it exists, the unique solution x satisfying $0 \leq x \leq n-1$. When the solution exists, the output of the function must be only x.
- Any call at Magma inner functions for solving the same problem[2] is forbidden.

Points

Submitting a working solution will give you up to three points.

Hints

- You may want to implement an auxiliary function which takes as inputs $([a,b],[s,t])$ and returns the solution of the system in Eq. (1) (and any other information you may need).

Example

An example of a working program will produce:

```
> CRTsolver([3,61,73],[8,21,24]);
Error: modules are not pairwise coprime

> CRTsolver([3,61,73,1],[8,21,24]);
Error: incompatible lengths

> CRTsolver([3,61,73],[8,21,25]);
523
```

[2]`CRT` and `ChineseRemainderTheorem` or similar