A multivariable Chinese remainder theorem

Oliver Knill

January 27, 2005

Abstract

In this note we show a multivariable version of the Chinese remainder theorem: a system of linear modular equations $a_{i1}x_i + ... + a_{in}x_n = \vec{b}_i \mod \vec{m}_i, i = 1, ..., n$ has solutions if $m_i > 1$ are pairwise relatively prime and in each row, at least one matrix element a_{ij} is relatively prime to m_i . The solution \vec{x} can be found in a parallelepiped of volume $M = m_1 m_2 \cdots m_n$. The Chinese remainder theorem is the special case, where A has only one column and the parallelepiped has dimension $1 \times 1 \times ... \times 1 \times M$.

1 Introduction

The Chinese remainder theorem (CRT) is one of the oldest theorems in mathematics. It was used to calculate calendars as early as the first century AD [2, 7]. The mathematician Sun-Tsu, in the Chinese work 'Suan Ching' considered the problem to find the number x which satisfies

$$x = 2 \mod 3$$
$$x = 3 \mod 5$$
$$x = 2 \mod 7$$

The example with solution x = 23 appeared also in a textbook of Nicomachus of Gerasa in the first century. Linear congruences of more unknowns seem have appeared much later. Dickson [2] gives as the first reference Schönemann, who considered in the year 1839 equations of the type $a_1x_1 + ... + a_nx_n = 0 \mod p$ where pis a prime. It was probably Gauss, who first looked at systems of n linear equations of n unknowns with respect to different moduli ([2]).

George Mathews noted in his two volume book [5] on number theory that a system of linear equations $A\vec{x} = \vec{b} \mod \vec{m}$ can be reduced to a system $B\vec{x} = \vec{a} \mod m$, where $m = \operatorname{lcm}(m_1, ..., m_n)$. For example, the system

$$\begin{array}{rcl} x+y &=& 1 \mod 3 \\ x-y &=& 2 \mod 5 \end{array}$$

which has solution x = 3, y = 1 is equivalent to

$$5x + 5y = 5 \mod 15$$

$$3x - 3y = 6 \mod 15$$

However, since many results and methods developed for a single moduli do not work - like row reduction, inversion by Cramer's formula - there is not much gained with such a reduction. Gauss treated in his

disquisitiones arithmetica (1801) systems of linear congruences and considered also the system

$$3x + 5y + z = 4 \mod 12$$

$$2x + 3y + 2z = 7 \mod 12$$

$$5x + y + 3z = 6 \mod 12$$

which has the four solutions (2, 11, 3), (5, 11, 6), (8, 11, 9), (11, 11, 0) in \mathbf{Z}_{12}^3 . The discrete parallelepiped spanned by (3, 0, 3), (12, 0, 0), (0, 12, 0) is mapped by the linear map A bijectively to a proper subset of \mathbb{Z}_{12}^3 . Indeed, the matrix A over the ring \mathbb{Z}_{12} is not invertible because $\det(A) = 4$ is not invertible in \mathbb{Z}_{12} .



Figure 1. Gauss example. There is a parallelepiped in \mathbb{Z}_{12}^3 which is mapped onto a proper subset of \mathbb{Z}_{12}^3 by the transformation $A\vec{x} \mod 12$. For the same matrix A, only one forth of all vectors \vec{b} in \mathbb{Z}_{12}^3 allow that $A\vec{x} = \vec{b} \mod 12$ can be solved. In that case, there are four solutions.

The system of Gauss can be solved by Gaussian elimination: subtracting the last row from the sum of the first two gives $7y = 5 \mod 12$ or y = 11. We end up with the system

$$3x + z = 9 \mod 12$$

$$5x + 3z = 7 \mod 12$$

Eliminating x gives $4z = 0 \mod 12$ or $z = 0 \mod 3$ which leads to the 4 solutions z = 0, 3, 6, 9. In each case, the solution x is determined. H.J.S. Smith noted in 1859 that if all moduli are the same m and det(A) is relatively prime to m, then $A\vec{x} = \vec{b} \mod m$ has a unique solution in the module \mathbb{Z}_m^n over the ring \mathbb{Z}_m . Indeed, Cramers rule gives the explicit solution $\vec{x}_i = \det(A_{\vec{b},i})\det(A)^{-1}$ in which the determinant det(A) is inverted in \mathbb{Z}_m and $A_{\vec{b},i}$ is the matrix in which the *i*'th column had been replaced by \vec{b} .

Systems of linear modular equations had been treated in the 18'th century, but mainly in the case when all moduli m_i are equal. The general case can be reduced to the case when the moduli are all powers of prime numbers with the equivalence of each equation $a_1x_1 + \ldots + a_nx_n = b \mod q_1^{k_1} \cdots q_l^{k_l}$ to

$$a_1x_1 + \dots + a_nx_n = b \mod q_1^{k_1}$$
$$\dots$$
$$a_1x_1 + \dots + a_nx_n = b \mod q_l^{k_l}.$$

The general case can also be reduced to the case when all moduli are equal but most results known in the equal moduli case do not catch after the reduction. For example, in that case, the determinant of the new matrix is zero in \mathbb{Z}_m . As in the CRT, we can not do row-reduction with different moduli in general.

Beside the aim to find the structure of the solutions of a system of modular linear equations, there is also the computational task, which asks to find solutions and a minimal parallelepiped in \mathbb{Z}_M^n on which A is injective as a map to $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$. There is the problem of complexity: how many computation steps are needed to decide whether a system has a solution and how many steps are required to find it? The earliest and only reference we were able to find which addresses the question is [3], where the problem is dealt with the method of quantifier elimination in discretely valued fields.

Our approach here is elementary and generalizes the approach to the CRT, in which solutions can be found in $\{0, ..., M-1\}$, which can also be interpreted as a parallelepiped of length $M = m_1 m_2 \cdots m_n$ and width dimensions of length 1.

Despite the elementary nature of the problem, there are questions which need to be studied more. There is the computational problem to find the kernel effectively and the general complexity problem to decide effectively, when a general system $A\vec{x} = \vec{b} \mod \vec{m}$ has a solution and when not. The efficiency part is especially relevant in cryptological context like in lattice attacks [4], where one tries to reconstruct the keys from several messages.

2 A multivariable Chinese Remainder Theorem

We consider linear systems of equations $A\vec{x} = \vec{b} \mod \vec{m}$, where A is an integer $n \times n$ matrix and \vec{b}, \vec{m} are integer vectors with coefficients $m_i > 1$. Written out, the system of equations is

$$a_{11}x_1 + \dots + a_{1n}x_n = b_1 \mod m_1$$
$$\dots$$
$$a_{n1}x_1 + \dots + a_{nn}x_n = b_n \mod m_n$$

The problem is to find a maximal lattice L_A in \mathbb{Z}^n , which is the kernel of the group homomorphism $\vec{x} \mapsto A\vec{x}$ from \mathbb{Z}^n to the module $\mathcal{Y} = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ so that its fundamental region \mathcal{X} is mapped bijectively onto $A\mathcal{X} \subset \mathcal{Y}$, then to decide whether \vec{b} is in $A\mathcal{X}$ and if affirmative, to construct $\vec{x} \in \mathcal{X}$ which satisfies $A\vec{x} = \vec{b} \mod \vec{m}$. There are cases, where one can give the answer quickly:

1) If all moduli m_i are equal to a prime m = p, the problem can be solved using linear algebra over the finite field F_p . As noted first 150 years ago, if m is not prime, but the determinant of the matrix A is invertible in the ring \mathbb{Z}_m , then the problem can be solved for all \vec{b} .

2) If A has only one nonzero column, the problem is the Chinese remainder theorem (CRT). It is one of the first topics which appear in any introduction to number theory.

For which A and \vec{m} are there solutions to the general linear system for all \vec{b} ? The following result is a generalization of the CRT:

Theorem 2.1 (Multivariable CRT) If $m_i > 1$ are pairwise relatively prime and in each row, at least one matrix element is relatively prime to m_i , then $A\vec{x} = \vec{b} \mod \vec{m}$ has solutions for all \vec{b} . In that case, the solution \vec{x} can be found in an n-dimensional parallelepiped $\mathcal{X} = \mathbb{Z}_M^n / L$ of volume $M = m_1 \cdots m_n$, where L is a lattice in \mathbb{Z}_M^n .

Remarks:

1) The lattice L is not unique in general. For example, if the lattice spanned by $\vec{v}_1, ..., \vec{v}_n$, then it is also spanned by $\vec{v}_1 + \vec{v}_2, \vec{v}_2, ..., \vec{v}_n$ and the volume is the same.

2) The two conditions for solvability are necessary in general, as examples below show.

3) The parallelepiped can be very long. An extreme case is the CRT situation, where it has length $M = m_1 m_2 \cdots m_n$ and all other widths are 1.

4) It would be useful to have criteria which assure that the parallelepiped has a small diameter. If A is unimodular, the eigenvalues of A are relevant.

5) A modern formulation of the CRT is that for pairwise coprime elements $m_1, ..., m_n$ in a principal ideal domain R (or Euclidean domain), the map $x \mod M \to (x \mod m_1, ..., x \mod m_n)$ is an isomorphism between the rings $R/(m_1R) \times R/(m_nR)$ and R/(MR). Using the same language, the multivariable CRT can be restarted that if R is a principal ideal domain and a ring homomorphism $A : R^n \to R^n$, for which the *i'th* row of A is not zero in $R/(q_iR)$ with factors $q_i > 1$ of m_i , there is a lattice L in R^n such that A is a ring isomorphism between R^n/L and $R/(m_1R) \times \cdots \times R/(m_nR)$. When seen in such an algebraic frame work, the result is quite transparent and might be "well known". The multivariable CRT could well have entered as a homework in an algebra text book, but we were unable to locate such a place yet. Also a search through number theory text books could not reveal the statement of the multivariable CRT.

6) While the problem of **systems** of linear modular equations $A\vec{x} = \vec{b} \mod \vec{m}$ with different moduli m_i certainly is elementary, the lack of linear algebra and group theory could explain why it had not been studied 2000 years ago by Chinese or Greek mathematicians. The problem has the CRT as a special case and can be understood and solved without linear algebra. Indeed, one of the proofs of the CRT essentially goes over to the multivariable CRT. But the constructive aspect of finding L and effectively inverting ϕ is interesting and much more difficult than in the special case of the CRT.

7) There is unique solution to systems of modular equations if and only if there is a line $A(t\vec{v}) \mod \vec{m}$ which covers the entire torus $\mathcal{Y} = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$. If \vec{v} is known, then it reduces the multivariable CRT problem to a CRT problem.



Figure 2. With a curve $\vec{r}(t) = t\vec{v}$ such that $A\vec{r}(t) \mod \vec{m}$ covers the entire discrete torus \mathcal{Y} , the multivariable CRT is reduced to the CRT. Most vectors \vec{v} will work, if there is exactly one solution. The reason is that most vectors $\vec{w} = A\vec{v} \mod \vec{m}$ have the property that the curve $t\vec{w}$ covers the entire torus.

3 Examples

Let us look at the equations $A\vec{x} = \vec{b} \mod \vec{m}$ in some examples, where n = 2 and $\vec{m} = (p, q)$ has the property that p, q are relatively prime. Unlike in the situation $\vec{m} = (p, p)$ with prime p, where the solution can be found in the fixed algebra over the finite field \mathbb{Z}_p , it does now not matter in general, how singular the matrix A is. But the decision known from linear algebra about solvability, unique solvability or non-solvability has still to be made.

Systems of modular equations have either a unique solution, no solution or finitely many solutions. In the third case, the number of solutions is a factor of $M = m_1 \cdots m_n$.

$$\begin{array}{rcl} x+y &=& 1 \mod 3 \\ x-y &=& 2 \mod 5 \end{array}$$

To a given solution like $\vec{x} = (3, 1)$, we can add solutions of the homogeneous equation $A\vec{x}_0 = \vec{0}$ like (2,7), (3,3), (-1,4), (1,11). This is an example, where solutions exist for all vectors \vec{b} . The curve $\vec{x}(t) = (3t, t) \mod p$ reduces the problem to the CRT case

$$4t = 1 \mod 3$$
$$2t = 2 \mod 5$$

which can be solved for t.

Example 2:

$$2x + 3y = 6 \mod 7$$
$$-3x - 9y = 3 \mod 12$$

This is an example, where the existence of integer solution (x, y) depends on the vector \vec{b} . The above example has a solution. The system

$$2x + 3y = 1 \mod 7$$
$$-3x - 9y = 1 \mod 12$$

has no solution. In the set $\mathbb{Z}_7 \times \mathbb{Z}_{12}$ with 84 elements, we count 28 vectors \vec{b} for which there is a solution and 56 elements, for which there is no solution.

Example 3:

$$6x - 4y = 7 \mod 7$$
$$10x - 5y = 1 \mod 5$$

There is no solution because the second equation reads 0 = 1 modulo 5. However, for a different \vec{b} like

$$6x - 4y = 2 \mod 7$$
$$10x - 5y = 5 \mod 5$$

we have a solution $\vec{x} = (1, 1)$. In the set $\mathbb{Z}_7 \times \mathbb{Z}_5$ with 35 elements, only 7 vectors \vec{b} give a system with a solution.

Example 4:

 $\begin{array}{rcl} x+y &=& 1 \bmod 3 \\ x+y &=& 2 \bmod 5 \end{array}$

This system can be reduced to a case of the CRT case:

 $z = 1 \mod 3$ $z = 2 \mod 5.$

and is solved for z = 7. In the set $\mathbb{Z}_3 \times \mathbb{Z}_5$ with 15 elements, every vector \vec{b} has a unique solution z. The original system has now solutions like $\vec{x} = (1, 6)$ or $\vec{x} = (2, 5)$.

Example 5: The size of the lattice L in \mathbb{Z}_M^n can vary when \vec{m} is fixed. Here is a case with a relatively narrow lattice spanned by the vectors (1, -3), (43, 14):

 $6x - 2y = 0 \mod 11$ $11x - 5y = 0 \mod 13$

The extreme case is the CRT case, where the lattice has dimensions 143×1 :

$$6x - 3y = 0 \mod 11$$

$$12x - 6y = 0 \mod 13$$

Next, we look now at examples of general cases, where the moduli m_i are not necessarily pairwise prime:

a) A case for linear algebra.

If $\vec{m} = (m_1, ..., m_n) = (p, ..., p)$, where p is a prime number, we have a linear system of equations over the finite field F_p . This is a problem of linear algebra, where solutions can be found by Gaussian elimination or by inverting the matrix. If the determinant of A is nonzero in the field \mathbb{Z}_p , then A^{-1} exists and $x = A^{-1}y$. For example, with p = 11, solving $A\vec{x} = \vec{b} \mod \vec{m}$:

$$\begin{bmatrix} 2 & 1 & 2 \\ 1 & 2 & 9 \\ 1 & 2 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \mod{11}$$

is done in the same way as over the field of real numbers. The determinant is 5 modulo p = 11 so that the matrix is invertible over F_p . The inverse of A in F_p is $A^{-1} = \begin{bmatrix} 8 & 6 & 1 \\ 7 & 9 & 10 \\ 0 & 6 & 5 \end{bmatrix}$ and $A^{-1}\vec{b} = \begin{bmatrix} 1 \\ 0 \\ 5 \end{bmatrix}$. Indeed

 $\vec{x} = \begin{bmatrix} 1\\0\\5 \end{bmatrix}$ solves the original system of equations.

b) The case of the Chinese reminder theorem.

If the matrix A has only one nonzero column, we are in the CRT situation. This problem was considered 2000 years ago and was given its final form by Euler. For example,

$$\begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 5 \\ 8 \\ 11 \\ 9 \end{bmatrix} \mod \begin{bmatrix} 3 \\ 11 \\ 7 \\ 13 \end{bmatrix}$$

is equivalent to

$$2x = 5 \mod 3$$

$$3x = 8 \mod 11$$

$$x = 11 \mod 7$$

$$9x = 9 \mod 13$$
.

Let us describe, how the CRT problem $a_i x = b_i \mod m_i$ is solved in a geometric language: with an integer "time" parameter t and the "velocity" $\vec{v} = (v_1, ..., v_n)$, the parameterized curve $\vec{r}(t) = t\vec{v} \mod \vec{m}$ is a line on the "discrete torus" $\mathcal{Y} = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$. It covers the entire torus if the integers m_i are pairwise relatively prime and $a_i \neq 0 \mod m_i$. One can solve the task of hitting a specific point \vec{b} on the torus by solving the first equation $v_1x_1 = b_1 \mod m_1$, then consider the curve $v_1(x_1 + m_1t)$, reducing the problem to a similar problem in one dimension less. Proceeding like this leads to the solution.

The solution for the CRT was easy to find, because the group was Abelian. The strategy to retreat in larger and larger centralizer subgroups is also the key to navigate around in non-Abelian finite groups like the "Rubik cube", where one first fixes a part of the cube and then tries to construct words in the finitely presented group which fixe that subgroup. It is a natural idea which puzzle-solvers without mathematical training come up with. By the way, also the Gaussian elimination process is an incarnation of this principle.



Figure 3. Solving problems in nonlinear groups use the evolved ideas from the Abelian case. In the CRT, the Abelian group \mathbb{Z}^n acts on the finite group $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$. In the Rubik cube, the free group F_6 acts on a finite group. In both cases, the problem can be solved effectively by finding actions which fix a smaller subgroup, then solve the problem in the smaller subgroup. A popular solution to the Rubik cube first fixes the top layer of the cube, then uses moves in the centralizer group which fixes the top layer to fix the second layer, finally uses word combinations which fix the top two layers.

c) The case of independent equations.

If A is a diagonal matrix we have n independent equations of the form $a_i x_i = b_i \mod m_i$. Solutions exist if $gcd(a_i, m_i) = 1$ for all i. If gcd(a, m) > 1 like a = 3, p = 6, there are no solutions of $3x = 2 \mod 6$ as can be seen by inspecting the equation modulo 3. Example:

$$A\vec{x} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 5 \\ 8 \\ 11 \\ 9 \end{bmatrix} \mod \begin{bmatrix} 3 \\ 11 \\ 7 \\ 13 \end{bmatrix} = \vec{b} \mod \vec{m} .$$

d) A case, where row reduction works.

If A is upper triangular or lower triangular matrix, the system can be solved by successively solving systems $a_i x = b_i \mod m_i$. Again, we have solutions if $gcd(a_i, m_i) = 1$ for all *i*.

$$A\vec{x} = \begin{bmatrix} 2 & 1 & 1 & 0 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 7 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 5 \\ 8 \\ 11 \\ 9 \end{bmatrix} \mod \begin{bmatrix} 3 \\ 11 \\ 7 \\ 13 \end{bmatrix} = \vec{b} \mod \vec{m} .$$

e) The case when A is modular.

If A^{-1} has only integer entries, solutions can be obtained directly with the formula $x = A^{-1}\vec{b}$ in \mathbb{Z}^n . This works if A is modular that is if A has determinant 1 or -1.

Example:

$$A\vec{x} = \begin{bmatrix} 5 & 3 & 4 \\ 1 & 4 & 1 \\ 5 & 2 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \mod \begin{bmatrix} 5 \\ 7 \\ 11 \end{bmatrix} = \vec{b} \mod \vec{m} .$$

We get $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = A^{-1} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 14 & -4 & -13 \\ 1 & 0 & -1 \\ -18 & 5 & 17 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} -33 \\ -2 \\ 43 \end{bmatrix}.$

¹As a graduate student, I had participated in a contest in the Swiss town of Bern. A "Rubik cube" type puzzle, the "master ball" had to be solved competitively in front of a larger audience. The task had been to race doing a specific transposition in that group. Having been trained at ETH in algebra and theoretical computer science also been a course assistant in a course using computer algebra, I had used the computer algebra system Cayley (now Magma) to find a solution and assigned a Sun workstation to tackle the problem. After a few hours, it came up with a solution which consisted of several dozen moves. I brought this solution to the competition: after all the contestants had been introduced, we went on to race who would solve the puzzle first. The fastest solver was a farmer and cheese-maker from Emmental. Without computers and without any knowledge in group theory, he had the best understanding to walk around in that non-Abelian group. This event happened before the movie "Good Will Hunting" appeared and is no fiction.

4 Proof of the multivariable CRT

Note that in general, row operations as used in Gaussian elimination are not permitted to solve the problem $A\vec{x} = \vec{b} \mod \vec{m}$ because each row is an equation in a different ring of integers. But the geometric solution of the CRT can be generalized to solve the general case as well as to locate **small** solution vectors.

Let us prove the multivariable CRT: Assume $gcd(m_i, m_j) = 1$ for all $i \neq j$ and if for all i = 1, ..., n, there exists j such that $gcd(a_{ij}, m_i) = 1$. We show that there is a solution \vec{x} to the linear system $A\vec{x} = \vec{b} \mod \vec{m}$ for all \vec{b} . The solution \vec{x} is unique in a parallelepiped spanned by n vectors. This parallelepiped contains $M = m_1 m_2 \cdots m_n$ lattice points.

I. Existence.

The map $\phi: x \to Ax \mod \vec{m}$ is a group homomorphism from $X = \mathbb{Z}^n$ to the finite group $\mathcal{Y} = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n} = Y/L$, where $L = (m_1\mathbb{Z}) \times \ldots \times (m_n\mathbb{Z})$ is a subgroup of Y. We think of \mathcal{Y} as a discrete torus with $M = m_1 \cdot \ldots \cdot m_n$ lattice points. We can think of the order M of the group also as the "volume" of the torus \mathcal{Y} .

The kernel of ϕ is a subgroup L_A of X and $\mathcal{X} = X/L_A$. The image of ϕ is a subgroup of \mathcal{Y} . By the first isomorphism theorem in group theory, the quotient group \mathcal{X} and the image are isomorphic.

The kernel L_A is a lattice in X spanned by n vectors $\vec{k}_1, \ldots, \vec{k}_n$. We think of the quotient $\mathcal{X} = X/L_A$ as a "discrete torus" with "volume" $|\mathcal{X}|$.

By definition, ϕ is injective on \mathcal{X} . By Lagranges theorem in group theory, there exist finitely many vectors $\vec{y}_i \in Y$ such that $\bigcup_{i=1}^{d(A)} A(\mathcal{X}) + \vec{y}_i = \mathcal{Y}$ and $d(A)\operatorname{vol}(\mathcal{X}) = \operatorname{vol}(\mathcal{Y})$. The problem is solvable for all \vec{b} if and only if d(A) = 1. In that case, for every \vec{b} , there exists a unique integer vector \vec{x} in \mathcal{X} such that $A\vec{x} = \vec{b} \mod \vec{m}$. we will solve $A\vec{x} = \vec{b} \mod \vec{m}$ constructively.



Figure 4. The map ϕ is a bijection between the two finite sets $(X) = \mathbb{Z}^n/L$ and $\mathcal{Y} = \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$. The picture visualizes the linear system

$$4x + 17y = 2 \mod 5$$

$$11x + 13y = 1 \mod 19$$

which has the solution (x, y) = (8, 5). The vectors (11-, 2), (-2, 9) span the lattice of the kernel.

II. Construction In order to construct a solution of $A\vec{x} = \vec{b} \mod \vec{m}$. we have to find both the lattice L_A

and a particular solution \vec{x} of the equation $A\vec{x} = \vec{b} \mod \vec{m}$, then reduce $x \mod t$ has the lattice to make it small.

i) Finding a particular solution

To find the particular solution, we pick Pivot elements $a_{ij(k)}$ in the matrix A: these are entries in the *i*'th row which are relatively prime to m_i . Let \vec{e}_j denote the standard basis in n-dimensional space.

Consider a line $\vec{x}(t) = t\vec{e}_{j(1)}$ in X, where t is an integer. Using the assumption on the rows, we see that there exists an integer t_1 so that $\vec{x}(t)$ solves the first equation.

Now take the line $\vec{x}(t) = t_1 \vec{e}_{j(1)} + tm_1 \vec{e}_{j(2)}$. There is an integer t_2 so that $\vec{x}(t)$ solves the second equation. We use the fact that m_1 is relatively prime to m_2 . Note that $\vec{x}(t)$ solves the first equation for all t.

Now continue in the same way until we find the final solution $\vec{x}(t) = \sum t_i(m_1...m_i)\vec{e}_{ij(i)}$.

Remark: Because \mathcal{X} and \mathcal{Y} are isomorphic groups, there is a one-dimensional line $\vec{r}(t) = t\vec{v}$ such that $\vec{r}(t)/L_A$ covers \mathcal{Y} . We could find a special solution by searching on that line, which is a problem of the CRT. We have the problem to find a vector \vec{v} such that $A\vec{r}(t) = A(t\vec{v}) = t\vec{w}$ covers the entire set \mathcal{Y} .

Example:

$$4x + 17y = 2 \mod 5$$

$$11x + 13y = 1 \mod 19$$

Because all moduli are prime, any nonzero matrix element is a Pivot element in this example. Lets pick j(1) = 1, j(2) = 2. We first look at the line $\vec{x}(t) = t\vec{e_1} = \begin{bmatrix} t \\ 0 \end{bmatrix}$. We look for t_1 such that the first equation is solved. This means $4x = 2 \mod 5$ which gives x = 3.

Now consider the line $\vec{x}(t) = 3\vec{e_1} + 5t\vec{e_2} = \begin{bmatrix} 3\\5t \end{bmatrix}$. For every t, the first equation is solved. The second

equation gives $33 + 65t = 1 \mod 19$. which is solved by t = 15. So, $\vec{x}(1) = \begin{bmatrix} 3 \\ 75 \end{bmatrix}$ solves the system.

We could have solved the system also by taking the parametrized line $\vec{r}(t) = (x(t), y(t) = (t, t))$ which is mapped by A to the line $(A\vec{r}(t)) = (11t, 25t) = (t, 5t)$ on the discrete torus. It leads to the CRT problem

$$\begin{array}{rcl}t&=&2 \bmod 5\\5t&=&1 \bmod 19\end{array}$$

which is solved for t = 42 so that we get the particular solution $(x, y) = \vec{r}(42) = (42, 210)$.

ii) Finding the kernel.

On every line $\vec{r}(t) = (0, ..., t, ...0)$, there is a point \vec{x} which solves $A\vec{x} = \vec{0} \mod \vec{m}$. By the pigeon hole principle, the set $\{A\vec{x} \mod \vec{m} \mid t \in [0, M]\}$ must hit some point in the image twice. But then $A(\vec{x} - \vec{y}) = \vec{0} \mod \vec{m}$.

If we take n + 1 equations $A\vec{x}^{(i)} = y^{(i)} \mod \vec{m}$, then the collection of vectors $y^{(i)}$ is linearly dependent. Therefore, there exist rational numbers c_i such that $\sum_j c_j y^{(j)} = \vec{0} \mod \vec{m}$ so that $\sum_j c_j \vec{x}^{(j)} = \vec{0}$ is in the kernel. After multiplying with a common multiple of the denominators of the rational numbers c_j , we can assume c_j to be integers.

We first look for *n* linearly independent vectors $\vec{k_i}$ solving $A\vec{k_i} = \vec{0} \mod \vec{m}$. Define *K* to be a matrix which contains the vectors $\vec{k_i}$ as row vectors.

We use the LLL algorithm ([1] section 2.6) to reduce the lattice to a small lattice. It turns out that this is often not good enough. The lattice has a size which is a multiple of p. In order to find the lattice L_A of the kernel, we need

$$\det(K) = M = m_1 m_2 \cdots m_n \; .$$

Let $k = \det(A)/p$ and let $k = q_1...q_l$ be the prime factorization of k. We can now look whether $\vec{y}^{(i)}/q_j$ are integer vectors in the kernel for each i = 1, ..., n and j = 1, ..., l and if yes replace the basis vectors. Successive reduction of the lattice can lead us to the kernel for which $\det(K) = p$. If not, we start all over and construct a new lattice.

5 Related topics and open questions

a) Iteration of modular linear maps.

The map $T(\vec{x}) = A\vec{x} \mod \vec{m}$ defines a dynamical system on the finite group $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$. Since the discrete torus \mathcal{Y} does not match with the torus \mathcal{X} , orbits on this finite set behave rather irregular. The system can be extended to the real torus $\mathbb{R}/(m_1\mathbb{Z}) \times \mathbb{R}/(m_n\mathbb{Z})$, where it is in general a hyperbolic map. The orbits behave differently, if A is very singular, for example if A has only one column.

Example: The map

$$T\left[\begin{array}{c}x\\y\end{array}\right] = \left[\begin{array}{c}31x + 34y\\3x + 38y\end{array}\right] \mod \left[\begin{array}{c}7\\17\end{array}\right]$$

has 6 different orbits on \mathcal{Y} with a maximal orbit length of 49. It seems difficult to find ergodic examples with different moduli where ergodic means that there is only one orbit besides the trivial orbit of $\vec{0} = (0,0)$ a case which appears for example in

$$T\left[\begin{array}{c}x\\y\end{array}\right] = \left[\begin{array}{c}18x+5y\\7x+14y\end{array}\right] \mod \left[\begin{array}{c}37\\37\end{array}\right]$$

b) Systems of modular polynomial equations

The algorithm to solve systems of linear modular equations extends also to solve systems of polynomial equations $\vec{P}(\vec{x}) = \vec{b} \mod \vec{m}$

$$P_1(x_1, ..., x_n) = b_1 \mod m_1$$

$$P_2(x_1, ..., x_n) = b_2 \mod m_2$$
...
$$P_n(x_1, ..., x_n) = b_n \mod m_n$$

too, but in general, we do not have criteria which assure that such a system has solution. Start solving the first equation. Using $\vec{x} = (a_{11}t, ..., a_{1n}t)$ we have to solve a problem $q_1(t) = 0 \mod m_1$, where q_1 is a polynomial. If we find a solution t_1 , try to solve the second equation for t when using $\vec{x} = (m_1a_{21}t, ..., m_na_{2n}t) + (a_{11}t_1, ..., a_{1n}t_1)$. which solve the first equation etc.

For example, consider the system of nonlinear modular equations

$$x^{2} + y^{3} + z^{2} = 1 \mod 5$$

$$x^{3} + 2y^{4} - z^{2} = 1 \mod 7$$

$$3x - 2y^{3} + 5z^{4} = 7 \mod 11$$

Start with the "Ansatz" (x, y, z) = (t, t, t). The first equation is $t^2(2+t) = 1 \mod 5$ which has the solution t = 2. Now put $(x, y, z) = (2, 2, 2) + t \cdot 5(1, 1, 1)$ which solves the first equation and plug it into the second equation. This is $(2+5t)^2(2+3t+t^2) = 1 \mod 7$ and solved for t = 0. The point (2, 2, 2) + t(5, 5, 5) = (2, 2, 2) solves also the second equation. Now plug-in $(2, 2, 2) + 5 \times 7(0, 2t, t)$, which solves the first two equations for all t, into the third equation which requires to solve $6 + 5(2+35t)^4 - 2(2+70t)^3 = 7 \mod 11$ which is equivalent to $4 + 4t + 2t^2 + 5t^3 + 3t^4 = 7 \mod 11$ and solved for t = 1. So, the final solution found is

 $(2,2,2) + 5 \cdot 7(0,2,1) = (2,72,37)$. This method does not necessarily find small solutions like (2,6,4).

Nonlinear systems of modular equations with different moduli but with one variable can be treated with the CRT. Ore [6]) illustrates it with the example

$$x^3 - 2x + 3 = 0 \mod 7$$

 $2x^2 = 3 \mod 15$

Because the first equation has solutions $x = 2 \mod 7$ and the second has solutions $x = \pm 3 \mod 15$, we are in the case of the CRT. In general, for systems of polynomial equations in one variable, we are lead to many cases of CRT problems.

c) Finding the kernel efficiently

To find the kernel of the group homomorphism $T(\vec{x}) = A\vec{x} \mod \vec{m}$, we produce a large set of solutions of $T(\vec{x}) = 0$ and then reduce this to a small lattice using the LLL algorithm. Let H be the matrix which contains the reduced kernel vectors as columns. Then $AH = \vec{0} \mod \vec{m}$. In general, $\det(H) \neq M$, but we know that there exists a kernel for which $\det(H) = M$. How do we find such a matrix H directly?

d) The decision problem.

To decide whether $A\vec{x} = \vec{b} \mod \vec{m}$ has a solution or not is addressed in [3]. The multivariable CRT gives a criterion for the existence of solutions. One can often detect, whether one of the equations has no solution. This happens for example, if $a_{i1}, ..., a_{in}, m_i$ have a common denominator which is not shared by the denominators of b_i . If all m_i are equal to some number m with distinct prime factors can make a fast decision: by the CRT, a solution exists if and only if a solution exists modulo each prime factor of m and the later decisions can be done by computing determinants in finite fields.

References

- [1] H. Cohen. A course in computational algebraic number theory. Graduate Texts in Mathematics. Springer, fourth printing edition, 2000.
- [2] L.E. Dickson. History of the theory of numbers. Vol. II: Diophantine analysis. Chelsea Publishing Co., New York, 1966.
- [3] A. Dolzmann and T. Sturm. Parametric systems of linear congruences. In Computer algebra in scientific computing (Konstanz, 2001), pages 149–166. Springer, Berlin, 2001.
- [4] N.A. Howgrave-Graham and N.P. Smart. Lattice attacks on digital signature schemes. Designs, Codes and Cryptography, 23.
- [5] G.B. Mathews. Theory of Numbers. Cambridge, Deighton, Bell and Co.; London, G. Bell and Sons, 1892.
- [6] O. Ore. Number Theory and its History. Mc Graw-Hill Book Company, New York, Toronto, London, 1948.
- [7] Kang Sheng Shen. Historical development of the Chinese remainder theorem. Arch. Hist. Exact Sci., 38(4):285-305, 1988.