THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF MATHEMATICS

CHINESE REMAINDER THEOREM

CHENG JIN
SPRING 2013

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees
in Mathematics and Economics
with honors in Mathematics

Reviewed and approved* by the following:

Karl Schwede
Assistant Professor
Thesis Supervisor

Sergei Tabachnikov
Professor
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

This paper studies the geometry of Chinese Remainder Theorem using Hilbert's Nullstellensatz. In the following, I will discuss the background of Chinese Remainder Theorem and give basic definitions for the terms in abstract algebra that we are going to use in this paper. Then, I will present the Chinese Remainder Theorem and its generalization in rings. In addition, I will present the Hilbert's Nullstellensatz and use that to interpret the Chinese Remainder Theorem. Finally, I will change some conditions in Chinese Remainder Theorem and discuss whether it still works.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I thank my parents for supporting me through college. This honors thesis serves as a testament to their love and the time and effort they put into my education.

I would like to thank Dr. Karl Schwede for leading me into the realm of abstract algebra and for supervising me on this thesis. Dr. Schwede showed great patience in helping me through this thesis. Even when he was travelling, he spent a great amount of time to read and comment on my writings. Without him, I could never have made it.

I thank Mr. Jim Ausherman for encouraging me to finish this thesis.

I want to thank Nate for showing me the beauty of mathematics, teaching me the language of mathematicians, recommending to further explore mathematics in the 2011 PMASS program, and guiding me in an honors independent study course on linear algebra. I thank Dr. Jenny Li for giving me advice on what classes I should take and for guiding me in a reading course on dynamic programming. I thank Dr. Svetlana Katok for teaching me in honors real analysis class in PMASS and showing me rigorous mathematical thinking. I also thank Dr. Sergei Tabachnikov for teaching me honors modern geometry class in PMASS, accepting me into Schreyer, and being my honors advisor.

Furthermore, I also want to thank Dr. John Fricks, Dr. Zhibiao Zhao, Dr. Svetlana Katok, Dr. Arkady Tempelman, Dr. Karl Schwede, Dr. Jonathan Eaton, Dr. Jenny Li and Nate for their recommendation letters. Without those letters, I could not have been accepted by Harvard, Stanford and Duke.

I thank Dr. Russell Chuderewicz for giving me so many opportunities: honors option in Econ351, REU, and conferences at Federal Reserve Banks. I thank Dr. Jonathan Eaton for letting me sit in his Honors Intermediate Microeconomics class and teaching me during one of my REU's. I also thank Dr. Charles Cao and Dr. Christoph Hinkelmann. I have always been interested in finance and wanted to take finance classes, but Smeal would not let non-finance majors schedule for finance classes. Dr. Charles Cao and Dr. Christoph Hinkelmann were kind enough to speak for me and help me register in their classes.

I also want to thank Dr. Neil Wallace, Dr. David Little, Dr. Jason Morton, Dr. Donald Richards, Dr. Aissa Wade, Dr. Steven Hair, Dr. Manfred Denker, Dr. Xiaozhe Hu, Dr. Debashis Ghosh, Dr. Murali Haran, Dr. Kalyan Chatterjee, Dr. Sung Jae Jun, Dr. Bee-Yan Roberts and Prof. Kazimierz Wiesak.

I thank Jun Ni and Xiaofei Zheng for their generous help in Math 501. I thank all my teachers, classmates, friends, all those who helped me, and all those who had belief in me.

I thank Dr. Arun Upneja for trusting me and Shreyer Honors College for giving me an extension. Most importantly, I would like to thank Penn State. Four years ago, I decided to come to Penn State. My life has changed ever since. During the past four years, what I experienced at Penn State had shaped my worldview and what I learned at Penn State had become a solid foundation for my graduate studies. After graduation, no matter where I will be, I will always remember that I have spent four wonderful years at Penn State. I am proud to be a Penn Stater!

Chapter 1

History and Background

The Chinese Remainder Theorem is a theorem about the solution of a system of congruence equations. It is used in number theory and has generalizations in abstract algebra. It is also a key point in RSA Cryptography. This theorem has a very long history.

1.1 The Ancient Chinese

The Chinese Remainder Theorem can be traced back to ancient China. In *Sun Tzu's Calculation Classic* (孙子算经) [1], there was the following problem:

> *There are a number of objects. If we divide them into groups of three, there will be two left. If we divide them into groups of five, there will be three left. If we divide them into groups of seven, there will be two left. How many objects are there?*

Sun Tzu's Calculation Classic was written sometime between 3 A.D. and 5 A.D. This problem is the following system of simultaneous congruence equations.

$$(*)\begin{cases} x = 2 \pmod 3 \\ x = 3 \pmod 5 \\ x = 2 \pmod 7 \end{cases}$$

In the 13th century A.D., Ch'in Chiu-Shao, a Chinese mathematician offered a solution to this problem[2].

He found a number 70, which is not only a common multiple of 5 and 7, but also congruent to 1 modulo 3. He also found 21, a common multiple of 3 and7 that is congruent to 1 modulo 5, and 15, a common multiple of 3 and 5 that is congruent to 1 modulo 7.

He then set

$$x = 70\times2+21\times3+15\times2=233$$

If we divide x by 3, 70×2 will give a remainder of 1×2=2, and 21×3+15×2 will give a remainder of 0. If we divide x by 5, 21×3 will give a remainder of 1×3=3, and 70×2+15×2 will give a remainder of 0. . If we divide x by 7, 15×2 will give a remainder of 1×2=2, and 70×2+21×3 will give a remainder of 0.

Therefore, x is congruent to 2 modulo 3, congruent to 3 modulo 5, and congruent to 2 modulo 7. So x satisfies the condition (*). While 233 is a number that satisfies (*), it is not the smallest positive integer that satisfies (*). The smallest such positive integer is 23.

But this is not a problem. We can always take this a step further by subtracting 233 by integer multiples of 105, the least common multiple of 3, 5, and 7. After two iterations, we have

$$233-2\times105=23$$

Although ancient Chinese mathematicians like Ch'in Chiu-Shao could solve Sun Tzu's problem, they did not realize that there is a theorem behind this intricate solution.

1.2 Later Discoveries

After ancient Chinese mathematicians, their Indian counterparts attempted to solve simultaneous congruence systems. According to legend, a mathematician named Aryabhata discovered a way to solve a system of simultaneous congruences equations[3].

Around 1000 A.D., Islamic scholar Ibn Al-Haitham collected the following remainder problem in his book [3].

$$X=1 \pmod 2=1 \pmod 3=1 \pmod 4=1 \pmod 5=1 \pmod 6=0 \pmod 7$$

His answer was 721. Just like Ch'in Chiu-Shao, Ibn Al-Haitham failed to provide the smallest positive integer answer.

Later, Euler, Lagrange, and Gauss generalized the solutions of systems of simultaneous congruence, and put forward theorems that lead to the Chinese Remainder Theorem [3].

1.3 Basics of Abstract Algebra

To understand the Chinese Remainder Theorem, we need tools in abstract algebra. In the following, I will explain some basic building blocks of abstract algebra.

1.3.1 Group

A group is a set, G, together with an operation • (the group operation) that is a function from G×G to G, which combines any two elements, a and b to form another element, denoted a • b or ab. To qualify as a group, the set and operation, (G, •), must satisfy the following four axioms:

1. For all a, b in G, the result of the operation, a • b, is also in G.

2. For all a, b and c in G, (a • b) • c = a • (b • c).

3. There exists an element e in G, such that for every element a in G, the equation e • a = a • e = a holds. Such an element is unique, and thus one speaks of the identity element.

4. For each a in G, there exists an element b in G such that a • b = b • a = e.

The notion of a group is the most basic element in abstract algebra. Examples of groups are abundant in mathematics. One of the most obvious is the set of integers, Z, under addition. If we add an integer to another integer, we still get an integer. Therefore, the Z is closed operation. Addition is associative. 0 is the additive identity. And finally, for all a in Z, -a is its inverse element.

Other examples of groups include the set of rational numbers under addition, the set of rational numbers except 0 under multiplication, and the set of positive real numbers under multiplication.

1.3.2 Normal Subgroup and Quotient Group

A subgroup is a group structure inside a group with the same operation. Concretely, a subgroup must contain the identity element and be closed under the group operation and inverse.

A coset is a definition relative to a subgroup. Given a subgroup H of G, a • H is a left coset of H, whereas H • a is a right coset of H.

If any left coset is a right coset, i.e. H • a = a • H, then the subgroup H is called normal.

For a normal subgroup H, we can define a quotient group G/H. The elements in the quotient group are cosets of H. The operation is defined as follows. aH • bH = (ab) • H.

1.3.3 Rings

A ring is a set R equipped with two binary operations + and • called addition and multiplication, that map every pair of elements of R to a unique element of R. These operations must satisfy the following properties called ring axioms (the symbol • is often omitted and multiplication is just denoted by juxtaposition.), which must be true for all a, b, c in R:

1. (a + b) + c = a + (b + c) (+ is associative)
2. There is an element 0 in R such that 0 + a = a (0 is the zero element)
3. a + b = b + a (+ is commutative)
4. For each a in R there exists −a in R such that a + (−a) = (−a) + a = 0 (−a is the inverse element of a)
5. (a • b) • c = a • (b • c)
6. a • (b + c) = (a • b) + (a • c)
7. (a + b) • c = (a • c) + (b • c).

In this paper, we are looking at rings with unity. In other words, we require the following.

8. There is an element 1 in R such that a • 1 = 1 • a = a

A ring is a more complex structure than a group. It is first of all an abelian group under addition. In addition, a ring has to be closed under multiplication. Moreover, addition and multiplication must satisfy the distributive properties.

For example, the set of integers, Z, under addition and multiplication is a ring. Also, the set of rational numbers, Q, the set of real numbers, R, and the set of complex

numbers, C, are all examples of rings under the usual addition and multiplication on numbers.

A ring is said to be commutative if the multiplication is commutative. That is to say for all a, b in R, $a \bullet b = b \bullet a$. In this paper, we shall only look at commutative rings in our analysis of the geometry of the Chinese Remainder Theorem.

There are some special cases of rings. If R is a commutative ring with identity, and for all nonzero a and b in R, $a \bullet b \neq 0$, then R is called an integral domain. One example of integral domain is the ring Z of all integers.

A commutative ring R is called a field if all nonzero elements of R have a multiplicative inverse. Equivalently, a field is a ring whose nonzero elements form an abelian group under multiplication. The set Q of rational numbers is one common example of field.

1.3.4 Ideals

Let R be a ring. An ideal of R is a subset I of R with the following property. For all a, b in R, and for all f, g in I, af+bg is in I. I is closed under linear combinations in R. Ideals are to rings as normal subgroups are to groups. The set of "cosets" of I form a ring with respect to the operation: $aI \bullet bI = (ab)\, I$.

There are two special cases of ideals that are especially interesting to us. They are prime ideals and maximal ideals. A prime ideal P of a commutative ring R has the following two properties:

1. If a and b are two elements of R such that their product ab is an element of P, then a is in P or b is in P,
2. P is not equal to the whole ring R.

m is a maximal ideal of a ring R if there are no proper ideal in R which contains m. Equivalently, the ideal m of ring R is a maximal ideal if there are no other ideals contained between m and R.

An ideal P of a commutative ring R is a prime ideal if R/P is an integral domain. This is true because of the following chain of logic:

R/P is an integral domain

R/P is a ring that has no zero divisors.

[a][b]=P implies [a] is P or [b] is P.

ab is in P implies a is in P or b is in P

P is a prime ideal.

Similarly, an ideal m of a commutative ring R (with unity) is maximal if R/m is a field. To prove this theorem, we follow the strategy of Wikiproof [4].

Since $J \subset R$, R/J is a commutative ring with unity. We now need to prove that every non-zero element of R/J has an inverse for multiplication in R/J. Let $x \in R$ such that $x+J \neq J$, i.e. $x \notin J$. Thus $x+J \in R/J$ is not the zero element of R/J. Take $K \subseteq R$ such that $K=\{j+r \bullet x : j \in J, r \in R\}$, that is, the subset of R which can be expressed as a sum of an

element of J and a product in R of x, i.e. the ideal in R generated by x. Now $0 \in K$ as $0 \in J$ and $0 \in R$, giving $0+0 \bullet x=0$. So, $K \neq \emptyset$. Take $g, f \in K$. Then there exist j, j' in J, a, b in R, such that $g=j+ax$, $f=j'+bx$. Then for all c, d in R, $cg+df=c(j+ax)+d(j'+bx)=(cj+dj')+(ac+bd)x \in K$. Therefore, K is closed under linear combination in R. So K is an ideal in R. It is obvious that $J \subseteq K$. The fact that J is a maximal ideal forces K to be the entire ring R. Since R has unity, there exist j'' in J and r in R, such that $1=j''+rx$. Consider $1+J$ in R/J. $1+J= (j''+rx)+J=rx+J$. But $(r+J)(x+J)= rx+J$. So, $(r+J)(x+J)=1+J$. Therefore, for every nonzero element $x+J$ in R/J, there exists $r+J$ in R/J which is the multiplicative inverse of $x+J$. Therefore, R/J is a field, which completes the proof.

Chapter 2

The Chinese Remainder Theorem

In this chapter, we will discuss the Chinese Remainder Theorem and its proof.

2.1 A Theorem from Abstract Algebra Class

The following theorem is from Math 435 Abstract Algebra class in spring 2012. Dr. Karl Schwede gave an exercise in worksheet #3[5], which is similar to this theorem. This theorem is basically the Chinese Remainder Theorem.

Theorem

If p and q are coprime, then the natural map

$Z \bmod pq \to Z \bmod p \times Z \bmod q$ *is bijective.*

Before we continue with the proof, let us consider the following facts.

Since p, q are coprime, there exist integers c and d, such that cp+dq=1. Given (a mod p, b mod q) in Z mod p ×Z mod q, let r=bcp+adq, then

r mod p= bcp+adq mod p= adq mod p= adq+acp mod p=a(cp+dq) mod p

= a×1 mod p= a mod p.

r mod q= bcp+adq mod q= bcp mod q= bcp+bdq mod q= b(cp+dq) mod q

=b×1 mod q = b mod q.

Proof

Consider the map Z mod p ×Z mod q→ Z mod pq. Φ: n mod pq → (n mod p, n mod q).

This map is injective. If n_1 mod pq = n_2 mod pq, then $n_1=n_2+xpq$ for some x in Z. Then n_1 mod p = n_2+xpq mod p= n_2 mod p. n_1 mod q = n_2+xpq mod q= n_2 mod q. That means for n_1 mod pq = n_2 mod pq, Φ (n_1 mod pq) = (n_1 mod p, n_1 mod q) = (n_2 mod p, n_2 mod q) = Φ (n_2 mod pq). Therefore, this map is injective.

This map is surjective since for all (a mod p, b mod q) in Z mod p ×Z mod q, we can find r=bcp+adq, such that f(a mod p, b mod q) = r mod pq. Therefore, f is bijective.

This bijection means a lot to us. It is the special case of the Chinese Remainder theorem, were we only have two congruence equations. The theorem basically says, under this situation, if we have

$$x \equiv b_1 (\text{mod } a_1)$$

$$x \equiv b_2 (\text{mod } a_2)$$

Then, we can always find a unique x modulo pq that satisfies this congruence system.

This theorem is a simplified version of the Chinese Remainder Theorem. If we add more details to it in a more general setting, we get the following theorem.

2.2 Chinese Remainder Theorem

In the following, I will present the statement and proof of the Chinese Remainder Theorem.

Theorem

Let $a_1,a_2,\ldots,a_n$ be positive integer such that for all $i\neq j$, $gcd\{a_i,a_j\}=1$.

Then the system of congruence equations

$x\equiv b_1 \pmod{a_1}$

$x\equiv b_2 \pmod{a_2}$

...

$x\equiv b_n \pmod{a_n}$

has a simultaneous solution which is unique modulo the product of a_i's

Before going into the proof, we should be clear that if a,b,c are pairwise coprime, then ab an c are coprime. This is easy to see so we will skip the proof.

Taking for granted the aforementioned fact, we will go right into the proof of the Chinese Remainder Theorem.

Proof

We will prove by induction on n.

(Base Case) See the theorem in Section 2.1

(Induction Step) Assume the system of congruence equations

$x \equiv b_1 \pmod{a_1}$

$x \equiv b_2 \pmod{a_2}$

…

$x \equiv b_r \pmod{a_r}$

has a simultaneous solution which is unique modulo the product of $a_1\, a_{2\ldots}\, a_r$. Let the solution be $y \bmod a_1\, a_{2\ldots}\, a_r$. We will show that the system of congruence equations

$x \equiv b_1 \pmod{a_1}$

$x \equiv b_2 \pmod{a_2}$

…

$x \equiv b_{r+1} \pmod{a_{r+1}}$

has a simultaneous solution which is unique modulo the product of $a_1\, a_{2\ldots}\, a_{r+1}$

But the system

$x \equiv b_1 \pmod{a_1}$

$x \equiv b_2 \pmod{a_2}$

…

$x \equiv b_{r+1} \pmod{a_{r+1}}$

is the same as the system

$x \equiv y \pmod{a_1\, a_{2\ldots}\, a_r}$

$x \equiv b_{r+1} (\text{mod } a_{r+1})$

By the base case, there exists a unique solution mod $a_1\ a_{2\ldots}\ a_{r+1}$.The proof is complete.

Chapter 3

Chinese Remainder Theorem for Rings

In this chapter, we will consider a more general case. We will not restrict ourselves to the ring of integers. We will consider the general case of commutative rings with unity. In other words, we will generalize the Chinese Remainder Theorem to commutative rings with unity.

3.1 First Isomorphism Theorem

A homomorphism is a map between algebraic structures, which preserves the algebraic structure. For example, consider the group Z mod 2={[1],[0]} under addition. Consider another group, A = {a,e}, where a^2=e, e^2=e, ae=ea=a. Then let f be a function from Z mod 2 to A, such that f([1])=a, f([0])=e. Then, f satisfies f(ab)=f(a)f(b) for all a, b in Z mod 2. The algebraic structure of Z mod 2 is preserved by the function f. Therefore, f is a homomorphism.

The First Isomorphism Theorem is widely used in the field of abstract algebra. The following is the First Isomorphism Theorem for Rings

Theorem

Let ϕ:R→S be a surjective ring homomorphism.

Let ker(ϕ) be the kernel of ϕ.

Then: $S \cong R/\ker(\phi)$

We will use this theorem in the proof of Chinese Remainder Theorem for Rings.

3.2 Chinese Remainder Theorem for Rings

Theorem

R is a commutative ring with unity. $I_1, I_2, \ldots I_n$ are ideals such that $I_i + I_j = R$ for $i \neq j$. Then:

1. *For all $a_1, a_2, \ldots, a_n \in R$, there exist $a \in R$ such that $a = a_i \bmod I_i$ for $i=1,2,\ldots,n$*
2. *There exists $b \in R$, such that $b = a_i \bmod I_i$ for $i=1,2,\ldots,n$*

   if and only if $b = a \bmod \cap i\ I_i$
3. *$R/\cap i\ I_i$ is isomorphic to $\prod i\ R/I_i$*

Proof:

1. Consider I_1 first. Since $I_1+I_j=R$, there exist $b_j \in I_1$ and $d_j \in I_j$ for all $j \neq 1$, such that $b_j + d_j = 1$ for all $j \neq 1$. Consider $\prod_{j\neq1} (b_j + d_j) \bmod I_1$. $\prod_{j\neq1} (b_j + d_j) = 1$ since $b_j + d_j = 1$ for all $j \neq 1$, $\prod_{j\neq1} (b_j + d_j) \bmod I_1 = 1 \bmod I_1$.

   $\prod_{j\neq1} (b_j + d_j) = (b_2 + d_2)(b_3 + d_3)(b_4 + d_4)\ldots (b_n + d_n)$

$= (\underline{b_2 b_3} + \underline{b_2 d_3} + \underline{b_3 d_2} + d_2 d_3)(b_4 + d_4)\ldots (b_n + d_n)$

The underscored part is in I_1. If we keep doing this multiplication, eventually, we will get $\prod_{j\neq 1}(b_j + d_j) = x + \prod j\, d_j$, where x is in I_1.Let $c_1 = \prod_{j\neq 1} d_j$. Then $c_1 = 1 \bmod I_1$, $c_1 = 0 \bmod I_j$ for all $j\neq 1$. In the same manner, we can find c_k's, such that $c_k = 1 \bmod I_k$, $c_k = 0 \bmod I_j$ for all $j\neq k$. Let $a=a_1c_1 + a_2c_2 + \dots + a_nc_n$. $a=a_i \bmod I_i$ for $i=1,2,\dots,n$.

2. $b = a_i \bmod I_i$ for all i $\leftrightarrow$ $b = a \bmod I_i$ for all i $\leftrightarrow$

   $b-a = 0 \bmod I_i$ for all I $\leftrightarrow$ $b-a \in I_i$ for all I $\leftrightarrow$ $b-a \in \cap i\ I_i$

   $\leftrightarrow$ $b=a \bmod \cap i\ I_i$

3. Consider $f: R\rightarrow \prod i\ R/I_i$

   Such that $f(a)=(a+I_1, a+I_2, a+I_3, \dots a+I_n)$. It is easy to check that f is a homomorphism.

   $f(a+b)=(a+b+I_1, a+b+I_2, a+b+I_3, \dots a+b+I_n)$

   $=(a+I_1, a+I_2, a+I_3, \dots a+I_n)+ (b+I_1, b+I_2, a+I_3, \dots b+I_n)$

   $=f(a)+f(b)$

   $f(ab)=(ab+I_1, ab+I_2, ab+I_3, \dots ab+I_n)$

   $=(a+I_1, a+I_2, a+I_3, \dots a+I_n)(b+I_1, b+I_2, a+I_3, \dots b+I_n)$

   $=f(a)f(b)$

   Therefore, f is a homomorphism. This map is also surjective by 1.

   The kernel of the map is $\{a \in R : (a+I_1, a+I_2, a+I_3, \dots a+I_n) = (I_1, I_2, I_3, \dots I_n)\}$

   So $a \in I_1$, $a \in I_2$, $a \in I_3$, … , $a \in I_n$. So $a \in \cap i\ I_i$. So Kernel of f is $\cap i\ I_i$.

   By the first homomorphism theorem, $R/\cap i\ I_i \rightarrow \prod i\ R/I_i$

Chapter 4

Nullstellensatz

In German, Nullstellensatz means zero-locus-theorem. In this chapter, I will discuss the Nullstellensatz and its proof.

4.1 Basic Definitions and Facts

I and J are ideals in R. Then I+J = {i+j: i ∈ I, j ∈ J}. I + J is an ideal of R.

If J is a prime ideal, then rad J = J.

A field is algebraically closed if every polynomial in one variable has a solution in the field.

The following are some definitions and facts and theorem taken from *Undergraduate Commutative Algebra*[8].

Let k be a field. J is an ideal of polynomial ring $k[x_1,x_2,\dots , x_n]$.

Then $V(J) :=\{a \text{ in } k^n : f(a)=0 \text{ for all } f \text{ in } J\}$ (Page 71)

$I(V(J)) := \{ f \text{ in } k[x_1,x_2,\dots , x_n] : f(a) = 0 \text{ for all } a \text{ in } V(J)\}$ (Page 72)

$\text{rad } J := \{f \text{ in } k[x_1,x_2,\dots , x_n] : f^m \text{ is in } J \text{ for some integer } m\}$(Page 29)

Every maximum ideal of $k[x_1,x_2,\dots , x_n]$ has the form $(x_1-a_1, x_2-a_2,\dots,x_n-a_n)$. (Page 70)

Maximal ideals in $k[x_1,x_2,\dots , x_n]$ containing J corresponds to the points in V(J). (Page 71)

4.2 Nullstellensatz

Theorem

Let k be an algebraically closed field.

(a) If V is a proper ideal of $k[x_1,x_2,\dots , x_n]$, then V(J) is non-empty

(b) I(V(J)) = rad J

Proof

(a) Since J is a proper ideal, it is contained in some maximum ideal of $k[x_1,x_2,\dots , x_n]$. So, J is contained in $(x_1-a_1, x_2-a_2,\dots,x_n-a_n)$. So, $(a_1, a_2,\dots, a_n)$ is in V(J). Therefore, V(J) is non-empty.

(b) Take f in I(V(J)). Consider J'= (J, fY-1), which is an ideal generated by J and fY-1, in the ring $k[x_1,x_2,\dots , x_n, Y]$. Then V(J') consist of points $(a_1, a_2,\dots, a_n, b)$, such that $(a_1, a_2,\dots, a_n)$ is in V(J), so $f(a_1, a_2,\dots, a_n)=0$; and $bf(a_1, a_2,\dots, a_n)=1$, so $f(a_1, a_2,\dots, a_n)\neq 0$. So V(J') is empty. By the contrapositive of (a), J' is not a proper ideal in $k[x_1,x_2,\dots , x_n, Y]$. Then J' is the entire ring $k[x_1,x_2,\dots , x_n, Y]$. Since 1 is in the ring, $1= \sum g_i h_i+g_0(fY-1)$. Multiplying f^m on both sides of the equation, we get $f^m = \sum G_i(X_1,..X_n,fY)h_i + G_0(X_1,..X_n,fY)(fY-1)$, where $G_i=g_i f^m$. Let fY=1.Then $f^m = \sum G_i(X_1,..X_n,fY)h_i$ is in J. Therefore, I(V(J)) = rad J

4.3 Nullstellensatz and the Chinese Remainder Theorem

In this section, we will discuss the connection between the Nullstellensatz and the Chinese Remainder Theorem.

Theorem

I an ideal in $k[x_1,x_2,\dots,x_n]$, such that I = rad I. x, r are in $k[x_1,x_2,\dots,x_n]$. x=r mod I if and only if x,r agree on V(I).

Proof

Let x=r mod I. Then, take an arbitrary a in V(I). Then (x-r)(a)=0. So x(a)-r(a)=0. So x(a) = r(a). Since a is arbitrary, x and r agree on all points in V(I).

Let x(a) = r(a) for all a in V(I). Then x(a)-r(a)=0. So (x-r)(a)=0 for all a in V(I). Then x-r is in I(V(I)). By (b) of Nullstellensatz, I(V(I)) = rad J. So I(V(I)) = I. Therefore x-r is in J as required, which completes the proof.

Note that for a prime ideal I, I = rad I. By the theorem, for x and r in I, x=r mod I if and only if x,r agree on V(I).

Theorem

I and J are ideals of $R = k[x_1, x_2, \ldots, x_n]$. $I + J = R$ *if and only if* $V(I) \cap V(J)$ *is empty.*

Proof

Let $I + J = R$. Suppose $V(I) \cap V(J)$ is non-empty. Then there exists an x in k^n, such that x is in both V(I) and V(J). Then f(x)=0 all f in R, since all f can be written as f_1+f_2, where f_1 is in I and f_2 is in V. But we know that the constant function 1 cannot be zero for any point in k. Therefore, it is a contradiction. So $V(I) \cap V(J)$ must be empty.

Let $V(I) \cap V(J)$ be empty. Suppose $I + J \neq R$ then $I+J = L$, where L is a proper ideal of R. By (a) of Nullstellensatz, V(L) is non-empty. Then V(L) is contained in V(I) And V(L) is contained in V(J). So V(L) is contained in $V(I) \cap V(J)$, which is empty. So V(L) must be empty. That is a contradiction. Therefore, $I + J = R$ must hold.

The previous two theorems give us a new perspective on the Chinese Remainder Theorem. Namely, given two ideals that are relatively prime, we can always find a function that agrees with an arbitrary function s on the vanishing set of one ideal, and agrees with function t on the vanishing set of another ideal. That is because by the theorem we just proved, the vanishing sets of the two ideals share no common points.

Chapter 5

More on the Chinese Remainder Theorem

In this Chapter, we will erase some conditions in the Chinese Remainder Theorem for Rings, and see if it is still true without these conditions.

5.1 Chinese Remainder "Theorem" for Abelian Groups

In the Chinese Remainder Theorem for Rings, we require that the algebraic structure be commutative rings. But does it have to be rings? If we change rings into abelian groups, do we have the following conjecture?

Conjecture

R is an abelian group. $I_1, I_2, \ldots I_n$ *are subgroups such that* $I_i+I_j = R$ *for* $i \neq j$. *Then for all* $a_1, a_2, \ldots, a_n \in R$, *there exist* $a \in R$ *such that* $a=a_i \bmod I_i$ *for* $i=1,2,\ldots,n$

First of all, in an abelian group, every subgroup is normal. That enables us to consider the factor groups R/I.

This theorem actually works for two abelian groups. Consider the following.

Theorem

R is an abelian group with unity. I_1, I_2 are subgroups such that $I_1+I_2= R$. Then for all a_1, $a_2 \in R$, there exist $a \in R$ such that $a=a_i \bmod I_i$ for i=1,2.

Proof

Since $I_1+I_2=R$, there exist x_1,x_2 in I_1, y_1, y_2 in I_2 such that $a_1=x_1+y_1$, $a_2=x_2+ y_2$. Then, let $a = x_2 +y_1$. $a – a_1 =(x_2 +y_1) – (x_1+y_1) = x_2 - x_1$, which is in I_1. $a – a_2 =(x_2 +y_1) – (x_2+y_2) = y_1 – y_2$, which is in I_2.

The theorem holds for two normal subgroups in an abelian group. But does the conjecture work in general cases where we have three normal subgoups? As it turned out, the ring structure is very important. The conjecture above does not work. The following is a counter example to the case of three ideals.

Consider the direct product of $Z \oplus Z \oplus Z$.

Let $I_1 = \langle(1,1,1)\rangle$, the ideal generated by (1,1,1), and $I_2 = \langle(1,0,0), (0,1,0)\rangle$, $I_3 = \langle(0,1,0), (0,0,1)\rangle$. Then, it is easy to check that $I_1+I_2 = R$, $I_2+I_3 = R$, and $I_3+I_1 = R$. Let $a_1 = (2,6,9)$, $a_2 = (5,7,10)$, $a_3 = (1,3,9)$. Suppose there exists an a in R such that $a=a_i \bmod I_i$ for i=1, 2, 3. Then, $a=a_2 \bmod I_2$ forces the last component of a to be 10. And $a=a_3 \bmod I_3$ forces the first component of a to be 1. Therefore, a=(1,x,10) for some x in Z. But a also has to satisfy $a=a_1 \bmod I_1$, which means there exists y in Z, such that (1,x,10) = y(1,1,1) +

(2,6,9). Since left hand side = right hand side, they must coincide in each component. Specifically, the differences between the first and third components should be equal. However, the difference on the left hand side is 10-1=9, but the difference on the right hand side is (y+9) – (y+2) = 7. $9 \neq 7$. That is a contradiction! Therefore, our original assumption must be wrong. Therefore, such an a that $a=a_i \bmod I_i$ for i=1, 2, 3 does not exist. Therefore, the three ideal case does not work, and the conjecture does not hold in general.

However, if we add more restrictions to a_1, a_2, a_3, the conjecture actually works. Then we have the following theorem.

5.2 Chinese Remainder "Theorem" for Ideals that are not Coprime

In the last section, we concluded that the ring structure is essential for the theorem. Now we move on to the next condition in the theorem: ideals that are pairwise coprime. We ask whether we have the following conjecture.

Conjecture

R is a ring with unity. $I_1, I_2, \ldots I_n$ are ideals of R. Then for all $a_1, a_2, \ldots, a_n \in R$, there exist $a \in R$ such that $a=a_i \bmod I_i$ for $i=1,2,\ldots,n$

It turns out that pairwise coprime is an essential condition as well. Without the pairwise coprime condition, the conjecture does not hold. The following is a counterexample.

Let R=k[x,y]. Ideals of R: I=(x), the ideal generated by x; J=(y), the ideal generated by y. Then I + J = (x, y). $V(I) \cap V(J) = V(I+J) = \{(0,0)\}$. Let $f_1 = 3x+y$, $f_2=1$. Suppose $a = f_1 \bmod I$ and $a = f_2 \bmod J$, then a and f_1 agree at every point of V(I). Also a and $f_2$agree at every point of V(J). Hence a and f_1 and f_2 agree on $V(I) \cap V(J) = V(I+J) = \{(0,0)\}$. But $f_1(0,0) = 0$, $f_2(0,0)=1$, so it is a contradiction.

However, in the case of two ideals, if we set some restrictions on f_1 and f_2, we have a theorem. Let's take a look at the following.

Theorem

I, J are ideals in R. If a= b mod I+J, then there is always a solution to the system

$x = a \bmod I$

$x = b \bmod J$

Proof

Since a= b mod I+J, let a= b+i+j for some $i \in I$, $j \in J$. Then let x=b+j. x mod I = b+j mod I = b+i+j mod I = a mod I. x mod J = b+j mod J = b mod I.

The theorem above says that if a and b agree on V(I + J) = V(I) intersect V(J), then there exists a global function x which agrees with a on V(I) and agrees b on V(J) respectively. But if we consider the case of three such ideals, the proof does not work anymore. That is to say, the following conjecture is false.

Conjecture

R is a ring with unity. I, J and K are ideals of R. Then for all $a_1, a_2, a_3 \in R$, *such that*

$a_1 = a_2 \bmod I+J$

$a_2 = a_3 \bmod J+K$

$a_1 = a_3 \bmod I+K$

then there exist $a \in R$ *such that* $a=a_i \bmod I_i$ *for* $i=1,2,3$.

The following is a counterexample. Let R=k[x,y]. Ideals of R: I=(x), the ideal generated by x; J=(y), the ideal generated by y; and K=(x+y), the ideal generated by (x+y). Let r=(x+1)y=xy+y; s=(y+1)x=xy+x; t=x-y. Since I + J = J + K = I + K = (x, y), r = s mod I + J, s = t mod J + K, r = t mod I + K.

Suppose there exist such an a, then in order to satisfy a = r mod I and a = s mod J, a = x+y+xyG(x,y). But if that were to be the case, a-t = 2y+xyG(x,y) must be in K. But there is a 2y in the equation, there must be a 2x in the term xyG(x,y), which cannot happen. Then, there exists no such a that a=r mod I; a=s mod J; and a=t mod K.

Every rule has an exception. If we restrict R=k[x, y, z], I=(x, y), J=(x, z), K=(y, z), we have the following theorem.

Theorem

Let R=k[x, y, z], I=(x, y), J=(x, z), K=(y, z). Then for every a, b, c such that

a=b mod I+J

a=c mod I+K

b=c mod J+K

there exists a d such that

d=a mod I

d=b mod J

d=c mod K

Proof

For f, g in R, f=g mod I if and only if f(0,0,z)=g(0,0,z), f=g mod I+J it's just if f(0,0,0)=g(0,0,0). Then d=a mod I, d=b mod J, d=c mod K forces a(0, 0, 0) = b(0, 0, 0) = c(0, 0, 0). Let d(x, y, z) = a(0, 0, z) + b(0, y, 0) + c(x, 0, 0) – 2a(0,0,0). Then d=a mod I since d(0, 0, z) = a(0, 0, z) + b(0, 0, 0) + c(0, 0, 0) – 2a(0 ,0 ,0) = a(0, 0, z) + [b(0, 0, 0) + c(0, 0, 0) – 2a(0 ,0 ,0)] = a(0, 0, z). d=b mod J since d(0, y, 0) = a(0, 0, 0) + b(0, y, 0) + c(0, 0, 0) – 2a(0 ,0 ,0) = b(0, y, 0). d=a mod I since d(x, 0, 0) = a(0, 0, 0) + b(0, 0, 0) + c(x, 0, 0) – 2a(0 ,0 ,0) = c(x, 0, 0). Hence d is the solution the system

d=a mod I

d=b mod J

d=c mod K.

REFERENCES

[1]Baidubaike, 孙子定理,
<http://baike.baidu.com/view/157384.htm?subLemmaId=157384&fromenter=%D6%D0%B9%FA%CA%A3%D3%E0%B6%A8%C0%ED>

[2]Wikipedia, 中国剩余定理, 9, March, 2013
<http://zh.wikipedia.org/wiki/%E4%B8%AD%E5%9B%BD%E5%89%A9%E4%BD%99%E5%AE%9A%E7%90%86 >

[3] Shen, Kangsheng (1987), Historical Development of the Chinese Remainder Theorem

[4] Wikiproof, Maximal Ideal iff Quotient Ring is Field,
<http://www.proofwiki.org/wiki/Maximal_Ideal_iff_Quotient_Ring_is_Field >

[5] Schwede, Karl (2012), Worksheet#3(RSA CRYPTOGRAPHY)

[6]Wikiproof, First Isomorphism Theorem,
< http://www.proofwiki.org/wiki/First_Isomorphism_Theorem>

[7] Frédérique Oggier, Ring Theory,

<http://www3.ntu.edu.sg/home/Frederique/chap2.pdf >

[8] Reid, Miles (1996). Undergraduate Commutative Algebra. Cambridge University Press. ISBN 0-521-45889-7.

ACADEMIC VITA

Cheng Jin

cwj5060@gmail.com

Education

B.S., Mathematics, Expected May 2013, the Pennsylvania State University, University Park, PA

B.S., Economics, Expected May 2013, the Pennsylvania State University, University Park, PA

Honors and Awards

- PMASS Scholarship
- Dean's List every semester

Association Memberships/Activities

Penn State Economics Association

2010 Conference on Real-Time Data Analysis, Methods, and Applications

2011 Economics Association Trip to the Federal Reserve

2013 Economics Association Trip to the Federal Reserve

Professional Experience

Penn State Economics Department, Fall 2011 and 2012, Spring 2013

Research Experience for Undergraduate

Penn State Learning Center, *Fall 2010-Spring 2013*

Peer tutor in mathematics and economics

Penn State Mathematics Department, Spring 2013

Grader for Differential Equations

Related Projects

Millionth Digit of Pi (Math 311W)

Supervisor: Dr. Nate Brown

Honors Real Analysis Fractal Dimension (Math 312H Honors)

Supervisor: Dr. Svetlana Katok

Geometry Schwarzian Derivative (Math 397B Honors)

Supervisor: Dr. Sergei Tabachnikov

Efficient Propagation of Shocks and the Optimal Return on Money (Econ 451H Honors)

Supervisor: Dr. Neil Wallace