The Chinese remainder theorem

Andrei Paskevich (2007), Steffen Frerix (2018), Adrian De Lon (2021)

The Chinese remainder theorem is a number theoretical result about the solution of simultaneous congruences in the case of coprime modules. The earliest known formulation of the theorem dates back to the Chinese mathematician Sun-tzu in the third century. In the following we present a formalization of a generalization of the theorem in terms of ideals in an integral domain. Checking the formalization takes about 3 minutes on a modest laptop.

1 Integral domain axioms

We assume that our universe is a fixed integral domain. We call elements of our universe simply "elements". In particular, we have two special elements, 0 and 1. Moreover, there is a unary operation, $-$, and two binary operations, $+$ and $\cdot$.

[read `examples/lang/vocabulary.ftl.tex`]

Let $a, b, c, x, y, z, u, v, w$ denote elements.

Signature 1. 0 is an element.

Signature 2. 1 is an element.

Signature 3. $-x$ is an element.

Signature 4. $x + y$ is an element.

Signature 5. $x \cdot y$ is an element.

Let x is nonzero stand for $x \neq 0$. Let $x - y$ stand for $x + (-y)$.

To ensure that our operations form a commutative ring we have to state the appropriate axioms. First we make sure that the addition yields an abelian group.

Axiom 6. $x + y = y + x$.

Axiom 7. $(x + y) + z = x + (y + z)$.

Axiom 8. $x + (y + z) = y + (x + z)$.

Axiom 9. $x + 0 = x = 0 + x$.

Axiom 10. $x + (-x) = 0 = -x + x$.

In fact axiom *AddBubble* is redundant. We can easily prove it from *AddComm* and *AddAsso*:

$$x + (y + z) \overset{AddComm}{=} (y + z) + x \overset{AddAsso}{=} y + (z + x) \overset{AddComm}{=} y + (x + z).$$

Let us continue with the axioms that ensure that the multiplication yields a commutative monoid.

Axiom 11. $x \cdot y = y \cdot x$.

Axiom 12. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Axiom 13. $x \cdot (y \cdot z) = y \cdot (x \cdot z)$.

Axiom 14. $x \cdot 1 = x = 1 \cdot x$.

As above we can prove *MulBubble* from *MulComm* and *MulAsso*. Now we ensure that the distribution laws hold.

Axiom 15. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Axiom 16. $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$.

The next two statements are some simple computation rules. The first one concerning multiplication with -1 can be derived from our previous laws together with *MulZero*, even if we state it as an axiom here. We leave the proof of this claim as an exercise for the reader.

Axiom 17. $(-1) \cdot x = -x = x \cdot (-1)$.

Lemma 18. $x \cdot 0 = 0 = 0 \cdot x$.

Proof. Let us show that $x \cdot 0 = 0$. $x \cdot 0. = x \cdot (0 + 0)$ (by AddZero) $. = (x \cdot 0) + (x \cdot 0)$ (by AMDistr1). End.

Let us show that $0 \cdot x = 0$. $0 \cdot x. = (0+0) \cdot x$ (by AddZero) $. = (0 \cdot x) + (0 \cdot x)$ (by AMDistr2). End. □

There are two axioms remaining to ensure that our universe is not just a commutative ring but an integral domain: There must be no non-trivial zero-divisors and our ring must not be trivial.

Axiom 19. $x \neq 0 \wedge y \neq 0 \implies x \cdot y \neq 0$.

Axiom 20. $1 \neq 0$.

2 Sets

Next we consider subsets of our universe. To keep our notion of sets as easy as possible we state that *every* set is a subset of our universe.

Let X, Y, Z, U, V, W denote sets.

Axiom 21. Every element of X is an object.

Let x belongs to W denote x is an element of W.

Axiom 22. If every element of X belongs to Y and every element of Y belongs to X then $X = Y$.

Definition 23. $X \oplus Y$ is a set such that for every element z ($z \in X \oplus Y$) iff there exist $x \in X, y \in Y$ such that $z = x + y$.

Definition 24. $X \cap Y$ is a set such that for every element z ($z \in X \cap Y$) iff $z \in X$ and $z \in Y$.

3 Ideals and the Chinese Remainder Theorem

Now we can define ideals as sets which are closed under certain operations.

Let $a, b, c, x, y, z, u, v, w$ denote elements.

Definition 25. An ideal is a set X such that for every $x \in X$ we have $\forall y \in X(x + y \in X)$ and $\forall z(z \cdot x \in X)$.

Let I, J denote ideals.

We can show that the sum and the intersection of two ideals is again an ideal.

Lemma 26. $I \oplus J$ is an ideal.

Proof. Let x belong to $(I \oplus J)$.

$\forall y \in (I \oplus J)(x + y) \in (I \oplus J)$.

Proof. Let $y \in (I \oplus J)$. (1) Take $k \in I$ and $l \in J$ such that $x = k + l$. (2) Take $m \in I$ and $n \in J$ such that $y = m + n$. $k + m$ belongs to I and $l + n$ belongs to J. $x + y. = (k + m) + (l + n)$ (by 1, 2, AddComm,AddAsso,AddBubble). Therefore the thesis. □

For every element z $(z \cdot x) \in (I \oplus J)$.

Proof. Let z be an element. (1) Take $k \in I$ and $l \in J$ such that $x = k + l$. $z \cdot k$ belongs to I and $z \cdot l$ belongs to J. $z \cdot x. = (z \cdot k) + (z \cdot l)$ (by AMDistr1, 1). Therefore the thesis. □

□

Lemma 27. $I \cap J$ is an ideal (by DefIdeal).

Proof. Let x belong to $I \cap J$. $\forall y \in (I \cap J)(x + y) \in (I \cap J)$. For every element z $(z \cdot x) \in (I \cap J)$. □

Now we can state the Chinese remainder theorem in terms of congruence modulo some ideal.

Definition 28. $x = y \pmod I$ iff $x - y \in I$.

Theorem 29. Suppose that every element belongs to $I \oplus J$. Let x, y be elements. There exists an element w such that $w = x \pmod I$ and $w = y \pmod J$.

Proof. Take $a \in I$ and $b \in J$ such that $a + b = 1$ (by DefSum). (1) Take $w = (y \cdot a) + (x \cdot b)$.

Let us show that $w = x \pmod I$ and $w = y \pmod J$.

$w - x$ belongs to I.

Proof. $w{-}x = (y{\cdot}a){+}((x{\cdot}b){-}x)$. $x{\cdot}(b{-}1)$ belongs to I. $x{\cdot}(b{-}1) = (x{\cdot}b){-}x$. □

$w - y$ belongs to J.

Proof. $w{-}y = (x{\cdot}b){+}((y{\cdot}a){-}y)$. $y{\cdot}(a{-}1)$ belongs to J. $y{\cdot}(a{-}1) = (y{\cdot}a){-}y$. □

End. □

4 Greatest common divisors and principal ideals

In this section we extend our integral domain to a Euclidean domain. To be able to do this we first have to establish a notion of natural numbers.

Let $a, b, c, x, y, z, u, v, w$ denote elements.

Signature 30. A natural number is an object.

Now we can equip our domain with a Euclidean function $|\cdot|$.

Signature 31. Let x be a nonzero element. $|x|$ is a natural number.

Axiom 32. Let x, y be elements and $y \neq 0$. There exist elements q, r such that $x = (q \cdot y) + r$ and $(r \neq 0 \implies |r| \prec |y|)$.

The *Division* axiom makes use of ℕaproche's built-in induction scheme: For any statement $\varphi(x)$ (with one free variable x) and any element r the following is true:

$$(\forall r'(|r'| \prec |r| \to \varphi(r'))) \to \varphi(r)$$

This allows us to prove certain statements about r by induction on $|r|$.

Next let us have a look at the notion of *divisors* and, in particular, *greatest common divisors* (*gcd*s).

Definition 33. x divides y iff for some z $(x \cdot z = y)$.

Let $x \mid y$ stand for x divides y. Let x is divided by y stand for $y \mid x$.

Definition 34. A divisor of x is an element that divides x.

Definition 35. A gcd of x and y is a common divisor c of x and y such that any common divisor of x and y divides c.

Definition 36. x, y are relatively prime iff 1 is a gcd of x and y.

If we have two elements, say a and b, we will see that the ideal *generated* by a and b also contains the gcd of a and b (as long as a or b is non-zero). An ideal which is generated by a single element, a so-called *principal ideal*, is defined as follows.

Definition 37. $\langle c \rangle$ is a set such that for every z z is an element of $\langle c \rangle$ iff there exists an element x such that $z = c \cdot x$.

Lemma 38. $\langle c \rangle$ is an ideal.

Proof. Let x belong to $\langle c \rangle$.

$\forall y \in \langle c \rangle x + y \in \langle c \rangle$.

Proof. Let $y \in \langle c \rangle$. (1) Take an element u such that $c \cdot u = x$. (2) Take an element v such that $c \cdot v = y$. $x + y. = c \cdot (u + v)$ (by 1, 2, AMDistr1). Therefore the thesis. □

$\forall z z \cdot x \in \langle c \rangle$.

Proof. Let z be an element. (1) Take an element u such that $c \cdot u = x$. $z \cdot x. = c \cdot (u \cdot z)$ (by 1, MulComm, MulAsso, MulBubble). Therefore the thesis. □

□

The notion of a principal ideal allows us write the ideal which is generated by two elements a and b as $\langle a \rangle \oplus \langle b \rangle$. As mentioned before if not both a and b are zero, $\langle a \rangle \oplus \langle b \rangle$ contains the gcd of a and b. That means that if c is the gcd of a and b then c is of the form $x \cdot a + y \cdot b$ for certain elements x and y. For example if we take $\mathbb{Z}$ as our Euclidean domain we get *Bézout's identity*: For two integers n, m with a gcd d there exist integers x, y such that $d = x \cdot n + y \cdot m$. For instance

$$\gcd(8, 14) = 2 = 2 \cdot 8 + (-1) \cdot 14$$

and

$$\gcd(9, 25) = 1 = -11 \cdot 9 + 4 \cdot 25.$$

Theorem 39. Let a, b be elements. Assume that a is nonzero or b is nonzero. Let c be a gcd of a and b. Then c belongs to $\langle a \rangle \oplus \langle b \rangle$.

Proof. Take an ideal I equal to $\langle a \rangle \oplus \langle b \rangle$. We have $0, a \in \langle a \rangle$ and $0, b \in \langle b \rangle$ (by MulZero, MulUnit). Hence there exists a nonzero element of $\langle a \rangle \oplus \langle b \rangle$. Indeed $a \in \langle a \rangle \oplus \langle b \rangle$ and $b \in \langle a \rangle \oplus \langle b \rangle$ (by AddZero).

Take a nonzero $u \in I$ such that for no nonzero $v \in I$ ($|v| \prec |u|$). Indeed we can show by induction on $|w|$ that for every nonzero $w \in I$ there exists nonzero $u \in I$ such that for no nonzero $v \in I$ ($|v| \prec |u|$). Obvious.

u is a common divisor of a and b.

Proof by contradiction. Assume the contrary.

For some elements x, y $u = (a \cdot x) + (b \cdot y)$.

Proof. Take $k \in \langle a \rangle$ and $l \in \langle b \rangle$ such that $u = k + l$. Take elements x, y such that ($k = a \cdot x$ and $l = b \cdot y$). Hence the thesis. □

Case u does not divide a. Take elements q, r such that $a = (q \cdot u) + r$ and ($r = 0 \vee |r| \prec |u|$) (by Division). r is nonzero. $-(q \cdot u)$ belongs to I. a belongs to I (by AddZero). $r = -(q \cdot u) + a$. Hence r belongs to I (by DefIdeal). End.

Case u does not divide b. Take elements q, r such that $b = (q \cdot u) + r$ and ($r = 0 \vee |r| \prec |u|$) (by Division). r is nonzero. $-(q \cdot u)$ belongs to I. b belongs to I (by AddZero). $r = -(q \cdot u) + b$. Hence r belongs to I (by DefIdeal). End. □

Hence u divides c.

Hence the thesis.

Proof. Take an element z such that $c = z \cdot u$. Then $c \in I$ (by DefIdeal). □

□

Bézout's identity ensures that for any two coprime integers n, m we have $n\mathbb{Z} \oplus m\mathbb{Z} = \mathbb{Z}$. Because we can take integers x, y such that $x \cdot n + y \cdot m = 1$ and thus for every integer z we have $zx \cdot n + zy \cdot m = z$, hence $z \in n\mathbb{Z} \oplus m\mathbb{Z}$. So as a special case of the Chinese remainder theorem if n and m are coprime then for all integers x, y the simultaneous congruence

$$w = x \pmod{n}$$

$$w = y \pmod{m}$$

has a solution.