Notes on algorithms : 4

Version 1 at 14 February 2019

0 Contents

1 Introduction

This note is about an algorithm associated with the Chinese Remainder Theorem.

The Theorem is as follows :
Take a collection of divisors. For any number calculate the remainders on dividing the number by each divisor. Provided the divisors are pairwise co-prime, that is have a Highest Common Factor of 1, then each number in the range *0 ≤ number < the product of all the divisors* results in a different pattern of remainders.

The Theorem applies to both the Natural Numbers, (0, 1, 2, 3, …), and to the Integers (…, -3, -2, -1, 0, 1, 2, 3, …). The Theorem uses the division operator that returns a quotient and remainder where *0 ≤ remainder < the absolute value of the divisor*. Quotients are ignored; only the remainders are relevant.

The Theorem gives rise to two problems. The first problem is : given a number, what are the remainders? This is simple arithmetic and needs no further discussion.

The second problem is : given a pattern of remainders, what was the number (in the range described above). One way to solve the problem is to find the pattern of remainders for each possible number until finding the one that matches the given pattern. This is slow. It is also impractical if the product of the divisors is very large.

This note discusses a fast solution to the second problem, a solution that always performs the same fixed number of arithmetic operations whatever the original number.

One practical application of the algorithm arises when using a Fire code for error correction.

Notes on algorithms : 4

2 Example

Before giving the general algorithm, derive the solution in the particular case of three divisors named *a*, *b*, and *c*. The number to be found is *x*.

We have the results of three division operations :

$$x = q_a.a + r_a$$
$$x = q_b.b + r_b$$
$$x = q_c.c + r_c$$

where the quotients, q_a, q_b, q_c, are unknown, and will be eliminated.

Multiply the *a* line by *b.c*, the *b* line by *a.c*, and the *c* line by *a.b* giving

$$x.b.c = q_a.a.b.c + b.c.r_a$$
$$x.a.c = q_b.a.b.c + a.c.r_b$$
$$x.a.b = q_c.a.b.c + a.b.r_c$$

Then add them together :

$$x.(b.c + a.c + a.b) = (q_a + q_b + q_c).a.b.c + (r_a.b.c + r_b.a.c + r_c.a.b)$$

Define *P*, *T*, and *S* as

$$P = a.b.c$$
$$T = (b.c + a.c + a.b)$$
$$S = (r_a.b.c + r_b.a.c + r_c.a.b)$$

These can also be written as

$$P = a.b.c$$
$$T = (P/a + P/b + P/c)$$
$$S = (r_a.P/a + r_b.P/b + r_c.P/c)$$

which might be simpler to calculate and is easier to extend to other numbers of divisors. Note that the division symbol, /, has been used here only where the divisor is a factor of the dividend.

The equation for *x* can now be written as

$$x.T = (q_a + q_b + q_c).P + S$$

Assume that there is a number, named T^{-1}, with $0 \leq T^{-1} < a.b.c$ such that

$$T.T^{-1} = Q.P + 1$$

for some value of *Q*. (Proof that there is such a number and that it is unique is left until later).

Multiply the equation for *x* by T^{-1} :

$$x.T.T^{-1} = (q_a + q_b + q_c).T^{-1}.P + S.T^{-1}$$

Substituting for $T.T^{-1}$ gives

$$x.(Q.P + 1) = (q_a + q_b + q_c).T^{-1}.P + S.T^{-1}$$

Expanding this

$$x.Q.P + x = (q_a + q_b + q_c).T^{-1}.P + S.T^{-1}$$

Do **modulo** *a.b.c*, producing the remainder on division by *P*, to both sides of the equation :

$$(x.Q.P)\ \mathbf{mod}\ P + x\ \mathbf{mod}\ P = ((q_a + q_b + q_c).T^{-1}.P)\ \mathbf{mod}\ P + (S.T^{-1})\ \mathbf{mod}\ P$$

As (*any multiple of P* **mod** *P*) = 0 this simplifies to

$$x\ \mathbf{mod}\ P = (S.T^{-1})\ \mathbf{mod}\ P$$

Therefore, given the three equations and the values of a, b, c, r_a, r_b, r_c, the desired solution with $0 \le x < a.b.c$ is :

$$x = (S.T^{-1})\ \mathbf{mod}\ P.$$

QED

Notes on algorithms : 4

3 General case

Now consider the general case where there is some family, D, of divisors indexed by the set I so

$$D = (D_i \mid i \in I)$$

The Problem

There is a number, x, which we do not know, but we do know the remainders on division of x by each of the divisors in D. What is the lowest possible value of x?

The question assumes that all numbers in the problem and its solution are Natural Numbers (0, 1, 2, 3, …). The text also applies to Integers, (…, -2, -1, 0, 1, 2, …), if “lowest” is replaced by “lowest non-negative”.

The Solution

There are three cases to consider.

Case A
D contains no divisors. We are given no remainders.

In this case there is no problem to be solved.

Alternatively, there is no information about x so the problem cannot be solved.

Case B
D contains only one divisor.

In this case we are given one remainder so we have the one equation

$$x = q\mathbf{.}a + r \quad \text{for some } q$$

where a is the only divisor, $D_{i\in I}$. The solution for least x seems obvious, but we must allow for us being given a too-large remainder. The solution for least x is therefore

$$x = r'$$

where

$$r = q'\mathbf{.}a + r' \quad \text{for some } q' \quad \text{and} \quad 0 \le r' < a$$

In other words,

$$x = r \mathbf{\ mod\ } a$$

Notes on algorithms : 4

Case C

D contains more than one divisor, but the number of divisors is finite.

In this case for each *i* : *I* we are given the remainder r_i so we have the equation

$$x = q_i.D_i + r_i \text{ for some } q_i$$

(q_i will be eliminated later on)

Define the number *P* that is the product of all the divisors :

$$P = \prod_{i \in I} (D_i)$$

For each *i* : *I* multiply both sides of its equation by (P/D_i). The equation becomes

$$x.(P/D_i) = q_i.D_i.(P/D_i) + r_i.(P/D_i) \text{ for some } q_i$$

Note that the division symbol, /, has been used here only where the divisor is a factor of the number being divided.

Now add all the equations together to give one equation :

$$x.\sum_{i \in I} (P/D_i) = P.\sum_{i \in I} (q_i) + \sum_{i \in I} r_i.(P/D_i)$$

Define the numbers *T* and *S* to simplify the description :

$$T = \sum_{i \in I} (P/D_i)$$

$$S = \sum_{i \in I} r_i.(P/D_i)$$

so the equation can be written as

$$x.T = P.\sum_{i \in I} (q_i) + S$$

Assume that there is a number, named T^{-1}, with $0 \leq T^{-1} < P$ such that

$$T.T^{-1} = Q_t .P + 1 \text{ for some } Q_t$$

(Q_t will be eliminated later on)

It is proved in Section 4 that whenever some reasonable pre-conditions are true there is such a number and it is unique.

Multiply both sides of the equation by T^{-1}; the equation becomes

$$x.T.T^{-1} = P.T^{-1}.\sum_{i \in I} (q_i) + S.T^{-1}$$

and substituting for the assumed $T.T^{-1}$ gives

$$x.(Q_t .P + 1) = P.T^{-1}.\sum_{i \in I} (q_i) + S.T^{-1}$$

Take the modulus of both sides with respect to P :

Notes on algorithms : 4

$[x.Q_t\,.P + x]$ **mod** $P = [P.T^{-1}.\sum_{i\in I}(q_i) + S.T^{-1}]$ **mod** P

which is

x **mod** $P = [S.T^{-1})]$ **mod** P

as (*anything*.*P*) **mod** $P = 0$.

Now we can state the solution to the problem with the pre-conditions derived in Section 4 :

Preconditions

Pre 1 **Is_finite**(*I*) **and Number_of_members**(*I*) ≥ 2

Pre 2 **For each** $i \in I$, $D_i \geq 2$

Pre 3 **For each** $i, j \in I$, if $i \neq j$ **then hcf**(D_i, D_j) = 1

Solution

$x = [S.T^{-1}]$ **mod** P for $0 \leq x < P$

where P, T^{-1}, and S are as defined above.

QED

Case D

D contains an infinite number of divisors.

A practical algorithm cannot process an unlimited number of remainders, nor can it return a result of unlimited size. Any solution must restrict the number of remainders inspected and restrict the size of the product of those remainders. In other words, the problem must be converted to Case C for it to be practical.

Notes on algorithms : 4

4 On the existence of an inverse

Sections 2 and 3 assumed that a number named T^{-1} exists and is unique. This section determines the conditions under which it does exist.

Notes on algorithms : 1 discusses modulo inverses in general and proves the pre-conditions for them to exist and for their uniqueness. *Note 1* includes an algorithm for calculating inverses both for Natural Numbers and for Integers. *Note 1* can be found at

<https://www.jghnorth.org.uk/>

To summarise the Note :
Given numbers a and B, then there exists a unique number a^{-1} such that

$$a \times a^{-1} = q \times B + 1 \quad \text{for some number } q$$

provided

Inv Pre 1 $B > 1$
Inv Pre 2 $a \neq q' \times B + 0$ for any number q'
Inv Pre 3 $\mathbf{hcf}(a, B) = 1$

To repeat the definitions in Section 3 of this Note :

Definition : D is a family of divisors, indexed by the set I.

$$D = (D_i \mid i \in I)$$

Definition : P is the product of all the divisors.

$$P = \prod_{i \in I} D_i$$

Definition : T is a sum of products, where each product is the product of all the divisors except one of them, a different one in each product, as in $(b.c + c.a + a.b)$.

$$T = \sum_{i \in I} \left(\prod_{j \in I,\ j \neq i} D_j \right)$$

Requirement :
We want T^{-1} to be the inverse of T with respect to P. That is, we want to have

$$T.T^{-1} = Q_t .P + 1 \quad \text{for some } Q_t$$

Pre-conditions :
First, what are the restrictions on the number of divisors? If the number is zero then P, the product of no divisors, is not defined. If the number is one then T, the sum of a product of no divisors, is not defined. If the number of divisors is infinite then, again, P is not defined. The values are defined for any other number of divisors. Therefore, require :

Pre 1 **Is_finite**(I) **and Number_of_members**(I) ≥ 2

Remember that Case B in Section 3 gives the solution to the problem when there is only one divisor. That solution does not use an inverse.

Notes on algorithms : 4

Next, what are the restrictions on the values of divisors? If a divisor is 0 then division by that divisor is not defined. If a divisor is 1 then the divisor contributes nothing to the solution. When a divisor is 2 the remainder indicates whether *x* is odd or even, but when it is 1 it indicates no more than that *x* is a number, which we already know.

To show this in more detail, take the example in Section 2 where there are three divisors, *a, b,* and *c*. We have

$$P_3 = a.b.c$$
$$T_3 = (b.c + a.c + a.b)$$
$$S_3 = (r_a.b.c + r_b.a.c + r_c.a.b)$$

and the beginnings of the solution

$$[\ x.T_3.T_3^{-1}\ ]\ \mathbf{mod}\ P_3 = [\ (q_a + q_b + q_c).T_3^{-1}.P_3\ +\ S_3.T_3^{-1}\ ]\ \mathbf{mod}\ P_3$$

Suppose $a = 1$. Then P_3, T_3, and S_3 are

$$P_3 = 1.b.c = b.c$$
$$T_3 = (b.c + 1.c + 1.b) = (P_3 + c + b)$$
$$S_3 = (r_a.b.c + r_b.1.c + r_c.1.b) = (r_a.P_3 + r_b.c + r_c.b)$$

The solution equation becomes

$$[\ x.(P_3 + c + b).T_3^{-1}\ ]\ \mathbf{mod}\ P_3$$
$$= [\ (q_a + q_b + q_c).T_3^{-1}.P_3\ +\ (r_a.P_3 + r_b.c + r_c.b).T_3^{-1}\ ]\ \mathbf{mod}\ P_3$$

It was proved in *Notes on algorithms : 1* that a modulo operation acting on a sum or product can be done in stages. The equation can therefore be written as

$$[\ x.([\ P_3\ \mathbf{mod}\ P_3\ ] + c + b).T_3^{-1}\ ]\ \mathbf{mod}\ P_3$$
$$= (q_a + q_b + q_c).T_3^{-1}.\mathbf{[}\ P_3\ \mathbf{mod}\ P_3\ ]\ + [\ (r_a.\ [P_3\ \mathbf{mod}\ P_3\ ] + r_b.c + r_c.b).T_3^{-1}\ ]\ \mathbf{mod}\ P_3$$

As $[\ P_3\ \mathbf{mod}\ P_3\ ] = 0$ this is

$$[\ x.(c + b).T_3^{-1}\ ]\ \mathbf{mod}\ P_3 = (r_b.c + r_c.b).T_3^{-1}\ ]\ \mathbf{mod}\ P_3$$

The requirement for T_3^{-1} becomes

$$(b.c + c + b).T_3^{\ -1} = Q_3.b.c + 1 \quad \text{for some } Q_3$$

The divisor *a* has completely disappeared in these two equations! *a* does not contribute to the solution at all. The same analysis can be applied to the general case. Therefore, require :

Pre 2 For each $i \in I$, $D_i \geq 2$

Next, returning to the general case, what restrictions on *P* and *T* will ensure that the inverse, $T^{\ -1}$, exists? **Pre 1** and **2** ensure that *P* is a multiple of at least two numbers greater than 1. *P* will therefore be greater than 1 so it already obeys **Inv Pre 1**.

What will ensure that **Inv Pre 3**, which requires **hcf**$(P, T) = 1$, will be true? Consider any prime factor, *p*, of one of the divisors, D_k , $k \in I$. D_k is at least 2 so it does have a prime factor. (As usual, 1 is not a *prime* factor even though it is a factor). T is a sum of products. D_k appears in all but one of those products. To repeat, T is

$$T = \sum_{i\in I} \left(\prod_{j\in I,\ j\neq i} D_j\right)$$

Separating the terms containing D_k from the term that does not contain D_k gives

$$T = n_a.D_k + \left(\prod_{j\in I,\ j\neq k} D_j\right) \text{ for some number } n_a$$

As p is a factor of D_k this can also be written as

$$T = n_b.p + \left(\prod_{j\in I,\ j\neq k} D_j\right) \text{ for some number } n_b$$

Suppose p is a factor of some other divisor as well as D_k. Then p is also a factor of the second product in the equation above and so

$$T = p.\ n_b + p.n_c \text{ for some number } n_c$$

That is, p is a factor of T. Being a factor of a divisor, p must also be a factor of P. But p is a *prime* factor, hence greater than 1. Therefore

If p is a prime factor of 2 or more divisors **then hcf**$(P, T) \geq 2$

On the other hand, if p is *not* a factor of any other divisor then it is a factor of P but not of T. This result applies to all prime factors of the divisors. To ensure that **hcf**$(P, T) = 1$ no prime factor can belong to more than one divisor. The only common factor allowed is 1. Therefore, require

Pre 3 **For each** $i, j \in I$, if $i \neq j$ **then hcf**$(D_i, D_j) = 1$

By **Pre 1** there are at least two divisors so the pre-condition is not vacuous.

Next, the pre-conditions **Pre 1, 2, 3** ensure that **Inv Pre 1** and **3** are true. What about **Inv Pre 2**? It requires that $T \neq q' \times P + 0$ for any number q'.

Pre 1 and **2** ensure that P is the product of numbers greater than 1 and T is the sum of at least one number greater than 1. P will therefore be greater than 1 and T will be greater than 0. If T were an exact non-zero multiple of P then **hcf**(P, T) would be P and so the **hcf** would be greater than 1. **Pre 3** precludes this so **Pre 1**, **2**, **3** ensure that **Inv Pre 2** is true.

In total, if **Pre 1**, **2**, **3** are true then **Inv Pre 1, 2, 3** are true, substituting $a = T$ and $B = P$, therefore :

Conclusion

The inverse, T^{-1}, of T modulo P exists and is unique provided :

Pre 1 **Is_finite**(I) **and Number_of_members**(I) ≥ 2

Pre 2 **For each** $i \in I$, $D_i \geq 2$

Pre 3 **For each** $i, j \in I$, if $i \neq j$ **then hcf**(D_i, D_j) = 1

QED

5 Implementation

There are some choices available for an algorithm to solve the problem given in Section 3.

One way to organise the solution is to use all the remainders in one calculation, as described in Section 3. The algorithm then uses one inverse, T^{-1}, one product of all the divisors, P, and the results of dividing P by each divisor. These can be pre-calculated and built in to the algorithm in applications where the divisors do not change; the divisors are not needed in this case.

Another way to organise the solution is to take the remainders one at a time. For instance, suppose two of the divisors are a and b and their remainders are r_a and r_b. Solve for these two to give a virtual divisor of $a.b$ and virtual remainder r_{ab} where $0 \leq r_{ab} < a.b$. Suppose another divisor is c and its remainder is r_c. Now solve for $a.b$ with r_{ab} and c with r_c, to give a virtual divisor of $a.b.c$ and virtual remainder of r_{abc}. Continue taking one divisor and its remainder at a time until all have been used. The last one produces the final result.

The algorithm then uses several inverses, T_i^{-1}, several products of an increasing number of divisors, P_i, and all the divisors themselves. These can be pre-calculated and built in to the algorithm in applications where the divisors do not change.

In both cases the preconditions do not allow divisors to have a value of 1. This can be relaxed if convenient. Such divisors and their remainders can simply be ignored as they contribute nothing to the solution of the problem.