RATIONAL REPRESENTATION OF MODULAR NUMBERS

Peter Hintenaus **Vilmar Trevisan***

Abstract

We find conditions, restricting the size of the fractions, and present algorithms to obtain a rational number from a set of residues modulo relatively prime integers. We also discuss the nature and the number of solutions for the rational representation, introducing conditions for the existence and for the uniqueness.

Resumo

Restringindo o tamanho das frações, condições são estabelecidas e algoritmos são apresentados para que um número racional seja obtido a partir de um conjunto de resíduos módulo inteiros que são primos entre si. Também são discutidos a natureza e o número de soluções para a representação racional, estabelecendo condições para a existência e unicidade.

1. Introduction

In Symbolic and Algebraic Computation, a wide range of problems have been solved very efficiently via a *modular approach*. Many problems over the integers are mapped onto a prime field and once the image of the solution is known, it is recovered to a true solution for the original problem, by means of the chinese remainder or Hensel p-adic lifting algorithm. Representative examples of this approach include polynomial factorization algorithms (see, for example, [3]), polynomial GCD computations (see, for instance, [3]) and Gröbner basis computation algorithms [8].

Some of these problems would be more efficiently solved over the rationals, and other problems arise more naturally in this field. Can we design an efficient

*Partially supported by CAPES, Brazil, under grant 0744/96-04

modular method for the rationals? Given a rational number $r = u/v$ and a positive integer a relatively prime to v, it is easy to find an integer $-a/2 \leq k \leq a/2$, such that $r \equiv k \pmod{a}$. If we want to develop modular approaches for the rational field, we need to go in the other direction, that is, given a residue $k \pmod{a}$, can we compute a rational number $r = u/v$ such that $r \equiv k \pmod{a}$?

In 1981, P. Wang [9] introduced an algorithm for reconstructing a rational number from a modular image. Given integers $a, b > 0$, Wang's algorithm finds, if it exists, a pair of integers α, β, satisfying

$$\alpha \equiv \beta b \pmod{a} \tag{1}$$

and

$$0 \leq |\alpha|, \beta < \sqrt{a/2}, \qquad \beta \neq 0. \tag{2}$$

The algorithm is a modification of the extended Euclidean algorithm (for the greatest commom divisor). Wang also observed, in his original paper, that if such a rational representation exists and if, additionally, $\gcd(\alpha, \beta) = 1$, then the representation is unique.

Such a representation, however, may not exist. As an example, modulo 15, we have representations 0=0/1, 1= 1/1, 2=2/1, 7=-1/2. It's worth noticing that 3, 4, 5 and 6 are not rational images (modulo 15) of fractions with numerator and denominator between -2 and 2.

If the bound $\sqrt{a/2}$ is relaxed, then more rational numbers can be represented. For instance, if we allow rational fractions with denominator bigger than 2 (but smaller than 5) then, modulo 15, we have 3=3/1, 6=-3/2. Uniqueness, however, may not be assured. For instance, $4 = 4/1 = 1/4 \pmod{15}$.

We study a more general situation in this paper, fixing an arbitrary bound c for the denominator β and, as a consequence, adjusting the size of the numerator α in such a way that the product $\alpha\beta$ is as large as the modulo a. The problem is also generalized for a rational reconstruction that simultaneously satisfy several modular relations.

In section 2, we discuss the existence of the rational representation in this new set of conditions. We discuss the nature of the solutions and make a conjecture about the number of solutions that are relatively prime.

In section 3, we restrict the problem so that we obtain unique representation of a modular number as a rational number. We point out, however, that we may not assure existence of solutions.

Algorithms for recovering the rational numbers are introduced in section 4. We discuss Wang's algorithm, modifying it to obtain the rational representation in this new situation. We finally point out several applications appearing in the literature that make use of rational reconstruction.

2. The Existence

The material of this section is inspired by the statement of lemma 3 given in [4]. We rectify here some mistakes that appear in the result, and generalize its content, adding an extra parameter.

Let a_i, b_i be positive integers for $1 \leq i \leq n$, where a_i and a_j are relatively prime for $i \neq j$. Let $A = \prod_{k=1}^{n} a_i$. Given positive integers c and m, with $1 \leq m \leq c$, consider the following

Problem 1: Find integers α, β, such that

$$1 \leq \beta \leq c, \tag{3}$$

$$0 \leq |\alpha| \leq \left\lceil \frac{Am}{2c} \right\rceil, \tag{4}$$

$$\beta b_i \equiv \alpha \pmod{a_i} \text{ for } 1 \leq i \leq n. \tag{5}$$

The following result holds.

Theorem 1. *If $m \geq 2$, then there exists a pair (α, β) solving problem 1.*

Proof. First we prove theorem 1 for $n = 1$. Let $a = a_1$, $b = b_1$. Without loss of generality we assume $m = 2$. Consider all pairs (γ, δ) where $-\lceil \frac{a}{2c} \rceil < \gamma \leq \lceil \frac{a}{2c} \rceil$, $1 \leq \delta \leq c$. There are $2\lceil \frac{a}{2c} \rceil c \geq 2\frac{a}{2c}c = a$ such pairs. Let us assume there is no pair (γ, δ) such that $a|(\gamma - \delta b)$. Then by the pigeon hole principle there are two different pairs (γ_1, δ_1) and (γ_2, δ_2) such that $\gamma_1 - \delta_1 b \equiv \gamma_2 - \delta_2 b \pmod{a}$, $\delta_1 > \delta_2$, i.e

$$a|(\gamma_1 - \gamma_2) - (\delta_1 - \delta_2)b.$$

What remains to be shown is that $0 \leq |\gamma_1 - \gamma_2| \leq \lceil \frac{a}{c} \rceil$.

Without loss of generality we assume $\gamma_1 > 0$, $\gamma_2 < 0$. We know $\gamma_1 \leq \lceil \frac{a}{2c} \rceil < \frac{a}{2c} + 1$. Furthermore, $|\gamma_2| \leq \lceil \frac{a}{2c} \rceil - 1 < \frac{a}{2c}$. Both γ_1 and γ_2 are integers, so $|\gamma_1 - \gamma_2| \leq |\gamma_1| + |\gamma_2| \leq \lceil \frac{a}{c} \rceil$.

For $n > 1$, we can compute a nonnegative integer $B < A$ such that $B \equiv b_i \pmod{a_i}$ for $1 \leq i \leq n$, using the Chinese Remainder Algorithm. Let (α, β) be a solution to $\alpha \equiv \beta B \pmod{A}$. Then $a_i|(\alpha - \beta b_i)$ for $1 \leq i \leq n$. So, theorem 1 is proved.

□

Note: A special case of this result appears in Sorensen [7] (lemma 2.2) for $n = 1, m = 2$ and $c = \sqrt{a}$.

We observe that the existence of solutions for problem 1 is not granted for $m = 1$. As a counter example, take $a = 27, b = 4$ and $c = 5$. There are no solutions $0 < \beta \leq c$, $|\alpha| \leq 3$ to the congruence $4\beta \equiv \alpha \pmod{a}$.

In some applications, obtaining any solution to problem 1 is enough to benefit from the rational reconstruction technique. New integer GCD algorithms, for example, use the following reduction to improve efficiency. Given integers $u > v$, relatively prime to a, find integers α, β satisfying $\alpha u + \beta v \equiv 0 \pmod{a}$, with $|\alpha|, |\beta| < \sqrt{a}$ and replace u by $u' = |\alpha u + \beta v|/a$, whose size is smaller than u (actually the size of u is reduced by roughly $\log_2(a)/2$ bits). Notice now that $\gcd(u, v)$ can be recovered from $\gcd(u', v)$ (see [7, 11]). The operation $\alpha u + \beta v \equiv 0 \pmod{a}$ is equivalent to reconstructing a rational number from the residue $r = u/v \pmod{a}$. In this case, the existence of multiple solutions are of no importance, as long as the bound $\sqrt{a}$ is observed, guaranteeing the size reduction.

When dealing with other applications, however, certain properties of the solutions are some times required, beyond its simple existence. For example, if $m = 2$, $a = 12$, $b = 4$ and $c = 3$, then the only solutions to $4\beta \equiv \alpha \pmod{12}$ with the constraints $1 \leq \beta \leq 3$ and $-4 \leq \alpha \leq 4$ are the pairs (α,β)=(4,1),(-4,2),(0,3). As *rational numbers*, the second and third pairs do not represent solutions, for we can not say that $0/3 \equiv 4 \pmod{12}$ or that $-4/2 \equiv 4 \pmod{12}$ since 3 and 2 are not invertible modulo 12. Also, $0/3 = 0 \not\equiv 4 \pmod{12}$ and $-4/2 = -2 \not\equiv 4 \pmod{12}$. The problem is that these two pairs are not *relatively prime*.

A relatively prime solution pair, that is, a solution (α, β) to problem 1 with $m = 2$ and $\gcd(\alpha, \beta) = 1$ does not always exist. As an example, notice that the only solutions to $7\beta \equiv \alpha \pmod{24}$ with the constraints $1 \leq \beta \leq 5$ and $|\alpha| \leq 5$ are (-3,3) and (4,4).

Another issue is the uniqueness of solutions. For $m \geq 2$, the above examples show that problem 1 has no chance of having a unique solution. If only the relatively prime pairs are sought, neither existence is attained (as example above shows), nor uniqueness. To see the this, observe that, modulo 24, $b = 5 = 5/1 = -4/4 = 1/5$. That is, there are two relatively prime solutions to problem 1, for $a = 24, b = 5, c = 5$ and $m = 2$.

We believe to be true the following conjecture regarding the number of solutions (α, β) with $\gcd(\alpha, \beta) = 1$.

Conjecture: Problem 1 has at most m relatively prime solution pairs.

This result is proven for $m = 1$ in the next section. In other words, to guarantee uniqueness of relatively prime solutions, we need to restrict the size of numerator (as function of the denominator). The existence of solutions, however, is no longer assured.

3. The Uniqueness

Let a_i, b_i be positive integers for $1 \leq i \leq n$, where a_i and a_j are relatively prime for $i \neq j$. Let $A = \prod_{k=1}^{n} a_i$. Given a positive integer c, consider the following

Problem 2: Find integers α, β, such that

$$1 \leq \beta \leq c, \tag{6}$$

$$-\frac{A}{2c} < \alpha \leq \frac{A}{2c}, \tag{7}$$

$$\beta b_i \equiv \alpha \pmod{a_i} \text{ for } 1 \leq i \leq n. \tag{8}$$

$$\gcd(\alpha, \beta) = 1, \tag{9}$$

The following result holds.

Theorem 2. *If there is a pair (α, β) satisfying problem 2, then it is unique.*

Proof. Let (α_1, β_1) and (α_2, β_2) be two solutions of problem 2. Then, the relation

$$\alpha_1\beta_2 \equiv \alpha_2\beta_1 \pmod{a_i} \qquad i = 1, \ldots, n$$

holds, which implies that

$$\alpha_1\beta_2 \equiv \alpha_2\beta_1 \pmod{A},$$

that is, there exists an integer k

$$\alpha_1\beta_2 - \alpha_2\beta_1 = kA.$$

On the other hand,

$$|\alpha_1\beta_2 - \alpha_2\beta_1| \leq |\alpha_1\beta_2| + |\alpha_2\beta_1| \leq A.$$

The only possibility for equality above is when $\beta_1 = \beta_2 = c$ and $\alpha_1 = -\alpha_2 = \pm A/2c$ and this is impossible for either α_1 or α_2 is out of the range given by equation (7).

It follows that

$$|\alpha_1\beta_2 - \alpha_2\beta_1| = kA < A,$$

implying that $k = 0$ and because the pairs are relatively prime, $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$, which proves the result.

$\square$

We now turn to the problem of recovering rational numbers by presenting algorithms for Problems 1 and 2.

4. Recovering Rational Numbers

Wang's original problem may be viewed as a restriction of problem 2 with $c = \sqrt{A/2}, n = 1$. As observed by Wang, a modification on the Euclidean extended algorithm can be used to compute such pair (α, β). The difference between his algorithm and the Euclidean is that it has a distinct stop condition.

Collins & Encarnación [2], using multiple-precision techniques for integer gcd computations, presented a more efficient version of Wang's algorithm for rational reconstruction.

Consider now finding an integer solution (α, β) to problem 1. Because of the Chinese Remainder Theorem and observation at the end of theorem 1, it is sufficient to consider $n = 1$. The algorithm RATCON of figure 1, a slight modification of Wang's [9], may be used to find (α, β), satisfying conditions (3), (4) and (5).

The algorithm differs from Wang's in the stopping condition (step 3.1), since it considers an adjustable bound for the denominator and numerator, depending on two parameters (c and m).

The correctness of the algorithm has been proved in [10] and in [6] for the special case $c = \sqrt{a/2}$ and $m = 1$ in the sense that the solution (if there is any) to $\alpha \equiv \beta b \pmod{a}$, with constraints $\alpha < \frac{a}{2c}, \quad 0 < \beta \leq c$ is generated by the algorithm. Both proofs can be extended for the general case presented here. Since we are using $m \geq 2$, theorem 1 assures the existence of solutions, so RATCON will return a pair (α, β) satisfying conditions (3), (4) and (5).

RATCON (a, b, c, m)
INPUT : Integers, a, b, c and m, with $2 \leq m \leq c < a$.
OUTPUT: A solution (α, β) for problem 1.

0. Let check:=$\lceil \frac{a*m}{2*c} \rceil$, $i := 1$
1. Let $(\alpha_0, \alpha_1) := (a, b)$
2. Let $(\beta_0, \beta_1) := (0, 1)$
3. While $\beta_i \leq c$ do
   - 3.1 if $|\alpha_i| <=$ check then return $(\text{sign}(\beta_i)\alpha_i, |\beta_i|)$;
   - 3.2 $q_i := \lfloor \alpha_{i-1}/\alpha_i \rfloor$;
   - 3.3 $\alpha_{i+1} := \alpha_{i-1} - q_i\alpha_i$;
   - 3.4 $\beta_{i+1} := \beta_{i-1} - q_i\beta_i$
   - 3.5 $i := i + 1$

Figure 1: Algorithm for computing a solution to **Problem 1**

Let us now examine the output (α, β) of algorithm RATCON. As the examples of the previous section show, we can say neither that it is the unique solution to problem 1 nor that $\gcd(\alpha, \beta) = 1$.

Theorem 3. *Let (α, β) be the output of algorithm RATCON. Then the following properties are satisfied.*

1. *If an integer k divides* $\gcd(\alpha, \beta)$ *then k divides a.*
2. $\gcd(a, \beta) = \gcd(\alpha, \beta)$.

Proof.

Property 2 is given in [2]. Clearly, property 1 may be seen as a consequence of of property 2. However, it is also a consequence of the following loop invariant [11], that is interesting by itself.

$$\alpha_i\beta_{i+1} - \alpha_{i+1}\beta_i = (-1)^i a, \quad \text{for} \quad i = 0, 1, \ldots \tag{10}$$

This can be easily proven by induction on i. Now, since $(\alpha, \beta) = (\alpha_{i+1}, \beta_{i+1})$

for some i and k divides both α_{i+1} and β_{i+1}, it follows from (10) that k divides a.

□

It is worth noticing that algorithm RATCON would not be able to generate all solutions to problem 1, even if we let stop condition (step 3.1) go to zero. For example, consider the congruence $8\beta \equiv 8 \pmod{27}$. The only possible outputs returned by the algorithm (depending on the stop condition) are $(8,1), (-3,3), (2,7)$ and $(-1,10)$. The pair $(5,4)$, a solution to problem 1 with parameters $a = 27, b = 8, c = 4$ and $m = 2$, is not returned, and may be considered "better" then the non-relatively prime pair $(-3,3)$, the output of the algorithm ran with these parameters.

Consider now finding a solution to problem 2. The obvious use of algorithm RATCON with $m = 1$ is not enough, since there could be no solutions. An additional problem is that there is at most one satisfying $\gcd(\alpha, \beta) = 1$ (theorem 2), but there may exist solutions that are non-relatively prime and if the algorithm RATCON above is used with $m = 1$, it could return such a solution.

The first difficulty is easily fixed, adding an extra stopping condition. The following modification, introduced in [2], corrects the second problem. As above, we consider $n = 1$. The algorithm of figure 2 finds, when it exists, the solution to problem 2.

The extra condition $\gcd(\alpha, \beta) = 1$ at step 3.2 guarantees the co-primeness of α and β and is equivalent to saying that β is invertible in the ring of integers modulo a; in other words, that the rational $\frac{\alpha}{\beta}$ is well defined or that

$$\frac{\alpha}{\beta} = b \pmod{a}.$$

5. Applications

The problems usually dealt in computer algebra that use rational reconstruction are polynomial factorization, partial fraction decomposition and Gröbner basis determination. It is feasible to use rational reconstruction for isolating polynomial roots. Actually, in [5], there is a modular version of the Sturm the-

RATCONUN (a, b, c)
INPUT : Integers, a, b and c, $c < a$.
OUTPUT: A solution (α, β) for problem 2, if it exists, NIL otherwise.

1. Let $(\alpha_0, \alpha_1) := (a, b)$;
2. Let $(\beta_0, \beta_1) := (0, 1)$;
3. For $i = 1, 2, \ldots$,do
   3.1 if $|\beta_i| > c$ then return NIL;
   3.2 if $|\alpha_i| \leq a/2c$ then
       if $\gcd(\alpha_i, \beta_i) = 1$ then return $(\text{sign}(\beta_i)\alpha_i, |\beta_i|)$;
   3.3 $q_i := \lfloor \alpha_{i-1}/\alpha_i \rfloor$;
   3.4 $\alpha_{i+1} := \alpha_{i-1} - q_i\alpha_i$;
   3.5 $\beta_{i+1} := \beta_{i-1} - q_i\beta_i$

Figure 2: Algorithm for computing the solution to **Problem 2**

orem that counts the number of zeros of a real polynomial in an interval with rational endpoints.

As explained in section 2, rational reconstruction has also been used for reducing the input size in the computation of integer gcd. It should be noted that, in this case, the inputs for the rational reconstruction are small, since it is itself a gcd computation.

In other applications where large inputs are needed, the multi precision arithmetic algorithm given in [2] is recommended. Special care should be given to the extra condition $\gcd(\alpha, \beta) = 1$, since the numbers α and β can also be large. Most applications require working modulo a product of prime numbers (or prime powers), therefore the modulo a has a known form and, because of theorem 3, it is possible to efficiently undertake the step. Collins & Encarnación [2] discuss ways to avoid or at least improve the efficiency for computing this condition.

Most applications look for the unique solution in the rational reconstruction problem. Some problems, like polynomial factorization, have a trial step at the end so it may be possible to use the algorithm RATCON, that is to say to find a solution to our problem 1, which would be more efficient, requiring fewer lifting steps or chinese remaindering recoveries.

Even if the unique solution is sought, the generalization presented here improves Wang's original problem, in the sense that more rational numbers may be reconstructed from the same residues modulo a. For example, if solutions to $\frac{\alpha}{\beta} \equiv 10 \bmod 24$ are to be found, Wang's algorithm returns nil, since for $\alpha, \beta < \lfloor\sqrt{12}\rfloor = 3$ there are no solutions. If, however, solutions to problem 2 with $c = 5$ are sought, the pair $(\alpha, \beta) = (2, 5)$ is returned by algorithm RATCONUN. The improvement is more significant when a bound c for the denominator is known in advance.

References

[1] Beauzamy, B., Trevisan. V. and Wang, P., *Polynomial Factorization: Sharp Bounds, Efficient Algorithms*, J. Symbolic Comp. 15, (1993), 393-413.

[2] Collins, G. E. and Encarnación, M. J., *Efficient Rational Number Reconstruction*, J. Symbolic Comp. 20, (1995), 287-297.

[3] Davenport, J. H., Siret, Y. and Tournier, E., *Computer Algebra - Systems and Algorithms for Algebraic Computation*, Academic Press, (1988).

[4] Chistov, A. L., Grigoryev, D. Yu., *Subexponential Time Solving Systems of Algebraic Equations I*, Ussr Academy of Sciences, Steklov Mathematical Institute, Leningrad Department, LOMI Preprints E-9-83, Leningrad 1983.

[5] Jacobs, D. P., Trevisan, V. and Weber, K. E., *Modular Sturm Sequences*, UFRGS - CPGMAp Technical Report TR12-96 (http://www.mat.ufrgs.br).

[6] Sasaki, T. and Sasaki, M., *On Integer-to-Rational Conversion Algorithm*, SIGSAM Bulletin 26, No. 2, (1992), 19-21.

[7] Sorenson, J., *Two Fast GCD Algorithms*, Journal of Algorithms 16, (1994), 110-144.

[8] Traverso, C., *Gröbner Trace Algorithms*, Proc. of ISSAC'88, LNCS 358, Springer-Verlag, (1988), 125-138.

[9] Wang, P. S., *A p-Adic Algorithm for Univariate Partial Fractions*, Proceedings of 1981 ACM SYMSAC, 212-217.

[10] Wang, P. S., Guy, M. J. T. and Davenport, J. H., *p-Adic Reconstruction of Rational Numbers*, SIGSAM Bulletin, Vol. 16, (1982), 2-3.

[11] Weber, K., *The Accelerated Integer GCD Algorithm*, ACM TOMS 21, (1995), 111-122.

Technikum Joanneum
Fachhochschulgang Industrielle Elektronik
Werk VI Strasse 46
A-8605 Kapfenberg - Austria

UFRGS-Instituto de Matemática
Porto Alegre, RS
91509-900, Brazil
e-mail: trevisan@mat.ufrgs.br