ISSN 0105-8517

MAPPING INTEGERS AND HENSEL CODES ONTO FAREY FRACTIONS

by

Peter Kornerup
and
R. T. Gregory

DAIMI PB-149
July 1982

Computer Science Department
AARHUS UNIVERSITY
Ny Munkegade – DK 8000 Aarhus C – DENMARK
Telephone: 06 – 12 83 55

MAPPING INTEGERS AND HENSEL CODES ONTO FAREY FRACTIONS

Peter Kornerup
Aarhus University, Denmark

R. T. Gregory
University of Tennessee, Knoxville

Abstract

The order-N Farey fractions, where N is the largest integer satisfying $N \leqq \sqrt{(p-1)/2}$, can be mapped onto a proper subset of the integers $\{0,1,\cdots,p-1\}$ in a one-to-one and onto fashion. However, no completely satisfactory algorithm for affecting the inverse mapping (the mapping of the integers back onto the order-N Farey fractions) appears in the literature. See Krishnamurthy, Rao and Subramanian [1975] and Gregory [1981] where this mapping is employed.

A new algorithm for the inverse mapping problem is described which is based on the Euclidean Algorithm. This algorithm solves the inverse mapping problem for both integers and the Hensel codes of Krishnamurthy et. al.

1. Introduction

In a recent paper [2] a method is proposed for error-free computation using rational operands. It involves a one-to-one mapping of the reduced order-N Farey fractions

$$F_N = \left\{\frac{a}{b} : \gcd(a,b) = 1,\ 0 \leqq a \leqq N, \text{ and } 0 < |b| \leqq N\right\} \tag{1.1}$$

into the set of integers

$$I_p = \{0,1,\cdots,p-1\} \tag{1.2}$$

where N is the largest integer satisfying the inequality

$$N \leqq \sqrt{\frac{p-1}{2}}\ . \tag{1.3}$$

Recall that $(I_p, +, \cdot)$, where addition and multiplication are modulo p, is a finite field, if p is a prime, and a finite commutative ring, if p is a composite. The basic idea is to map the operands from F_N into I_p, carry out the computation (free of rounding errors) in $(I_p, +, \cdot)$, and then map the results back into F_N.

If $\hat{I}_p \subset I_p$ denotes the set of images of the elements of F_N, then the mapping $F_N \to \hat{I}_p$ is both one-to-one and onto, and thus it has an inverse mapping $\hat{I}_p \to F_N$. The procedure described in [2] for

2. Mapping Rational Numbers Onto Integers

Let $|\cdot|_p : I \to I_p$ be the mapping of the integers I onto their least non-negative residues modulo p. If we define, for $\gcd(b,p) = 1$,

$$\left|\frac{a}{b}\right|_p = |ab^{-1}|_p \tag{2.1}$$

where the integer b^{-1} is the multiplicative inverse of b modulo p, then $|\cdot|_p : Q \to I_p$ maps those rational numbers $\frac{a}{b} \in Q$ for which $\gcd(b,p) = 1$, onto integers in I_p.

For $k \neq 0$, let Q_k denote the set of rational numbers mapped onto $k \in I_p$. The set Q_0 (the rational numbers mapped onto zero) consists of those numbers $\frac{a}{b}$, with $\gcd(b,p) = 1$, for which a is an integral (including zero) multiple of p. We call the disjoint subsets $Q_0, Q_1, \cdots, Q_{p-1}$ <u>generalized residue classes</u>, since they contain the ordinary residue classes (of integers) as proper subsets.

If $x = \frac{a}{b}$ and $y = \frac{c}{d}$, where b^{-1} and d^{-1} exist, then $|x|_p = |y|_p$ if and only if

$$ad \equiv bc \pmod{p}. \tag{2.2}$$

Thus, two distinct rational numbers x and y belong to the same generalized residue class Q_k if and only if (2.2) is satisfied.

tiplication. Since I_p is a homomorphic image of $\hat{Q}$, arithmetic operations in $(\hat{Q}, +, \cdot)$ correspond to arithmetic operations in $(I_p, +, \cdot)$.

3. The Inverse Mapping

The mapping $|\cdot|_p : \hat{Q} \rightarrow I_p$ is onto but it is not one-to-one, since each integer $k \in I_p$ is the image of the infinite set Q_k. Hence, the mapping has no inverse. With N given by (1.3) it is easy to show that distinct order-N Farey fractions belong to distinct sets Q_k and, since the number of order-N Farey fractions is less than p, not every generalized residue class contains an element of F_N.

If we select the set of images of the elements of F_N,

$$\hat{I}_p = \left\{ \left|\frac{a}{b}\right|_p : \frac{a}{b} \in F_N \right\}, \tag{3.1}$$

then $\hat{I}_p \subset I_p$ and the mapping

$$|\circ|_p : F_N \rightarrow \hat{I}_p \tag{3.2}$$

is both one-to-one and onto and so an inverse mapping $\hat{I}_p \rightarrow F_N$ exists. <u>It is this inverse mapping which we wish to consider</u>.

4. A New Look at the Forward Mapping

Suppose we select four integers a, b, c, and d, and any sequence of integers $\{q_0, q_1, q_2, \cdots\}$ and generate the sequence of integer pairs $\{(a_i, b_i)\}$ by the recursion

$$\text{(4.1)} \qquad \begin{cases} a_i = a_{i-2} - q_i\, a_{i-1} \\ b_i = b_{i-2} - q_i\, b_{i-1} \end{cases} \qquad i = 0, 1, 2, \cdots$$

where the <u>seed</u> matrix is

$$\text{(4.2)} \qquad \begin{bmatrix} a_{-2} & b_{-2} \\ a_{-1} & b_{-1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then the following is true.

<u>LEMMA 1</u> If $ad \equiv bc \pmod p$, then, for $i = 0, 1, \cdots,$

$$a_i b_{i-1} \equiv a_{i-1} b_i \pmod p.$$

<u>PROOF</u>

$$\begin{aligned} a_i b_{i-1} - a_{i-1} b_i &= (a_{i-2} - q_i a_{i-1}) b_{i-1} - a_{i-1}(b_{i-2} - q_i b_{i-1}) \\ &= (a_{i-2} b_{i-1} - a_{i-1} b_{i-2}) + q_i \cdot 0 \\ &\;\;\vdots \\ &= (-1)^i (a_{-2} b_{-1} - a_{-1} b_{-2}) \\ &= (-1)^i (ad - bc) \end{aligned}$$

<u>Algorithm 1</u> (Extended Euclidean Algorithm)
For any four integers a, b, c, and d, where a and c are non-negative, let

$$\begin{bmatrix} a_{-2} & b_{-2} \\ a_{-1} & b_{-1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

For $i = 0, 1, \cdots, n$, while $a_{i-1} \neq 0$, determine q_i as the quotient and a_i as the non-negative remainder in the division of a_{i-2} by a_{i-1}. Then

$$a_i = a_{i-2} - q_i a_{i-1}.$$

Likewise, define

$$b_i = b_{i-2} - q_i b_{i-1}.$$

Terminate when $a_n = 0$. At this point $a_{n-1} = \gcd(a,c)$. □

This algorithm can be used to carry out the mapping

$$\left|\frac{r}{s}\right|_p = |r \cdot s^{-1}|_p$$

described in (2.1). We sometimes call $\left|\frac{r}{s}\right|_p$ the least non-negative residue of $\frac{r}{s}$ modulo p. For this application we need another lemma.

PROOF Since $ad = pd$ and $bc = 0$, it follows that $ad \equiv bc \pmod{p}$. By Lemma 1

$$a_0 d \equiv b_0 c \pmod{p}$$

and, since

$$\left|\frac{u}{v}\right|_p = \left|\frac{r}{s}\right|_p,$$

if and only if

$$us \equiv vr \pmod{p},$$

the result follows. □

THEOREM 1 Given any rational number $\frac{r}{s}$ and an integer p such that $\gcd(s,p) = 1$, the Euclidean Algorithm seeded with the matrix

$$\begin{bmatrix} p & o \\ s & r \end{bmatrix}$$

will terminate (for some n such that $a_n = 0$). At this point

$$\left|\frac{r}{s}\right|_p = |b_{n-1}|_p.$$

<u>EXAMPLE 1</u> If we want to find

$$\left|\frac{10}{13}\right|_{625}$$

we use the seed matrix

$$\begin{bmatrix} 625 & 0 \\ 13 & 10 \end{bmatrix}$$

in Algorithm 1. Observe that $p = 625$ implies $N = 17$, and so $\frac{10}{13}$ is an order-N Farey fraction. Observe, also that $p = 625$ is not a prime. However, $\gcd(13, 625) = 1$ and so Theorem 1 applies. We record the computation in the table

i	q_i	a_i	b_i
-2	-	625	0
-1	-	13	10
0	48	1	-480
1	13	0	6250

from which we conclude that

$$\left|\frac{10}{13}\right|_{625} = |-480|_{625}$$

5. A New Algorithm for the Inverse Mapping

Observation 2 Lemmas 1 and 2 taken together (as in Theorem 1) state that with the seed

$$\begin{bmatrix} a_{-2} & b_{-2} \\ a_{-1} & b_{-1} \end{bmatrix} = \begin{bmatrix} p & 0 \\ r & s \end{bmatrix},$$

and *any* sequence $\{q_0, q_1, q_2, \cdots\}$, we can generate an infinite sequence of integer pairs

$$\{(a_0, b_0),\ (a_1, b_1), \cdots\}$$

such that, for $i = 0, 1, \cdots$,

$$\left|\frac{b_i}{a_i}\right|_p = \left|\frac{s}{r}\right|_p .$$

Hence, it is possible to generate an infinity of members of the same generalized residue class Q_k, $0 \leq k < p$, by choosing $(r,s) = (k,1)$. Thus, we can "invert" the mapping (3.2) by selecting among the elements of Q_k the (unique) order-N Farey fraction. □

EXAMPLE 2 Continuing Example 1,

i	q_i	a_i	b_i
-2	-	625	0
-1	-	145	1
0	4	45	-4
1	3	$\boxed{10}$	$\boxed{13}$
2	4	5	-56
3	2	0	125

Notice that $\frac{10}{13}$ is recovered. Notice also that 145 and 625 are not relatively prime and that

$$a_{n-1} = 5 = \gcd(625,\ 145)$$

as described in Algorithm 1. $\square$

To see that the recovery of $\frac{10}{13}$ in Example 2 is not accidental, let

$$\begin{bmatrix} a_{-2} & b_{-2} & c_{-2} \end{bmatrix} \qquad \begin{bmatrix} p & 0 & -1 \end{bmatrix}$$

$$(5.2) \qquad q_i = \left\lfloor \frac{a_{i-2}}{a_{i-1}} \right\rfloor \quad \text{and} \quad \begin{cases} a_i = a_{i-2} - q_i\, a_{i-1} \\ b_i = b_{i-2} - q_i\, b_{i-1} \\ c_i = c_{i-2} - q_i\, c_{i-1} \end{cases} \qquad i = 0,1,\ldots,n.$$

It is well known [3] that the sequence

$$(5.3) \qquad \left\{ \frac{|b_0|}{|c_0|}, \frac{|b_1|}{|c_1|}, \ldots, \frac{|b_n|}{|c_n|} \right\}$$

is the complete sequence of continued fraction convergents of $\frac{p}{k}$. It is also easy to see that, for $i = 0,1,\cdots,n$,

$$(5.4) \qquad a_i = k\, b_i - p\, c_i.$$

These continued fraction convergents are the so-called "best rational approximations", for which the following theorem holds.

<u>THEOREM 2</u> Every fraction $\frac{r}{s}$ that satisfies the inequality

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}$$

is a continued fraction convergent of α.

<u>PROOF</u> See, for example, [3] page 153. □

where $k \in \hat{I}_p$ and

$$0 < r \leqq N$$

$$0 < |s| \leqq N,$$

then there exists an i such that

$$(r,s) = (a_i, b_i),$$

where $\{(a_j, b_j)\}$, $j = 0,1,\cdots,n$ is the sequence of integer pairs generated by the Extended Euclidean Algorithm seeded with the matrix

$$\begin{bmatrix} p & 0 \\ k & 1 \end{bmatrix}.$$

PROOF If we extend the seed matrix as in (5.1) and define the sequence $\{c_i\}$, $i = 0,1,\cdots,n$, as in (5.2), then (5.3) is the complete sequence of convergents of $\frac{p}{k}$ whenever $k \neq 0$.

From our hypothesis

$$\left|\frac{r}{s}\right|_p = |k|_p = k \in \hat{I}_p.$$

Therefore,

This allows us to write

$$\begin{aligned}\left|\frac{k}{p}-\frac{t}{s}\right| &= \left|\frac{ks-pt}{ps}\right| \\ &= \left|\frac{r}{ps}\right| \\ &\leqq \frac{1}{s^2}\cdot\frac{|s|\cdot N}{2N^2+1} \\ &\leqq \frac{1}{s^2}\cdot\frac{N^2}{2N^2+1} \\ &< \frac{1}{2s^2}.\end{aligned}$$

Therefore, using Theorem 2, we deduce that either $\frac{t}{s}$ or $\frac{-t}{-s}$ is a convergent of $\frac{k}{p}$.

Since (5.3) is the sequence of convergents of $\frac{p}{k}$, it follows that

$$\left\{\frac{0}{1}, \frac{|c_0|}{|b_0|}, \ldots, \frac{|c_n|}{|b_n|}\right\}$$

is the sequence of convergents of $\frac{k}{p}$. Hence, there exists an i, where $0 \leqq i \leqq n$, such that

$$\frac{t}{s} = \frac{c_i}{b_i} \quad \text{and} \quad |s| = |b_i|.$$

Hence,

$$\frac{a_i}{b_i} = \frac{r}{s},$$

and so

$$(r,s) = (a_i,b_i),$$

since both r and a_i are positive. $\square$

<u>COROLLARY 1</u> Let k be any integer such that $0 \leqq k \leqq p-1$, and let $\{(a_i,b_i)\}$ $i = 0,1,\cdots,n$ be the sequence generated by the Extended Euclidean Algorithm, seeded with:

$$\begin{bmatrix} a_{-2} & b_{-2} \\ a_{-1} & b_{-1} \end{bmatrix} = \begin{bmatrix} p & 0 \\ k & 1 \end{bmatrix}.$$

Then $k \in \hat{I}_p$ if and only if

(5.5) $\exists i,\ -1 \leqq i \leqq n$ such that $\frac{a_i}{b_i} \in F_N$

in which case:

$$\gcd(b_i,p) = 1 \quad \text{and} \quad \left|\frac{a_i}{b_i}\right|_p = k.$$

where the signs of r and s may be chosen such that $r > 0$. Then (5.5) follows from Theorem 3.

To prove the other part, notice from (5.4) that $\gcd(b_i,p)$ must be a divisor of a_i; but from (5.5), $\gcd(a_i,b_i) = 1$. Hence $\gcd(b_i,p) = 1$, and by Lemma 2

$$\left|\frac{a_i}{b_i}\right|_p = \left|\frac{k}{1}\right|_p = k,$$

thus $k \in \hat{I}_p$. □

<u>Observation</u> For practical purposes it may be worth noticing from the proof of Corollary 1 that (5.5) may be substituted by:

(5.6) $\exists i,\ -1 \leqq i \leqq n$ such that $|a_i| \leqq N$, $|b_i| \leqq N$ and $\gcd(b_i,p) = 1$.

Hence with p prime it is not necessary to check $\gcd(b_i,p)$ as $|b_i| \leqq N < p$. For p composite it is necessary to check either $\gcd(a_i,b_i)$ or $\gcd(b_i,p)$, where the latter may be the simplest, as in the case of the Hensel codes discussed in the next section. □

<u>6. The Conversion of Hensel Codes to Rational Numbers</u>

To get the unique Hensel code for $\frac{a}{b} \in F_N$, where, as in [2], N is the largest integer satisfying

$$N \leqq \sqrt{\frac{m-1}{2}}$$

$$= \sqrt{\frac{p^r-1}{2}},$$

two steps are involved. First, we compute

$$\left|\frac{a}{b}\right|_m = |ab^{-1}|_m$$

where the multiplicative inverse of b modulo m exists if and only if $\gcd(b,p) = 1$. Second, we convert the integer $|ab^{-1}|_m \in I_m$ to its radix-p representation and then reverse the order of the digits.

<u>EXAMPLE 3</u> Let $p = 5$ and $r = 4$, so that $m = 625$ and $N = 17$. To get the Hensel code for $\frac{a}{b} = \frac{2}{3}$ we use the method of Section 4 to obtain

$$\left|\frac{2}{3}\right|_{625} = 209.$$

Then, since

$$209_{ten} = 1314_{five},$$

the Hensel code is

First, the digits of the Hensel code are reversed, and the value of the resulting radix-p integer is computed. From this point on the procedure is the same.

<u>EXAMPLE 4</u> Suppose we are given the Hensel code

$$H(5,4,\frac{a}{b}) = .4131$$

and we want to find $\frac{a}{b}$. We reverse the order of the digits and obtain

$$1314_{five} = 209_{ten}.$$

We now use the algorithm of Section 5 and record the computation in the following table

i	q_i	a_i	b_i
-2	-	625	0
-1	-	209	1
0	2	207	-2
1	1	$\boxed{2}$	$\boxed{3}$
2	103	1	-311
3	2	0	625

References

1. R. T. Gregory, The use of finite-segment p-adic arithmetic for exact computation, BIT 18(1978), 282 - 300.

2. R. T. Gregory, Error-free computation with rational numbers, BIT 21(1981), 194 - 202.

3. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Fourth Ed. (1960), Clarendon Press, Oxford.

4. E. V. Krishnamurthy, T. M. Rao and K. Subramanian, Finite segment p-adic number systems with applications to exact computation, Proc. Indian Acad. Sci., 81A (1975), 58 - 79.

Errata and additions to

"Mapping Integers and Hensel Codes onto Farey Fractions"

by

Peter Kornerup

and

R. T. Gregory

<u>Page 1</u> line 4 from below: Delete "Extended"

<u>Page 5</u> reformulate LEMMA 2 as follows:

<u>LEMMA 2</u> If, in (4.2), we choose $a = p$, $b = 0$, and $0 < c < p$ such that $\gcd(c,p) = 1$, then, for $i = 0,1,\cdots, n-1$

$$\left|\frac{b_i}{a_i}\right|_p = \left|\frac{d}{c}\right|_p$$

and alternatively, if $\gcd(d,p) = 1$,

$$\left|\frac{a_i}{b_i}\right|_p = \left|\frac{c}{d}\right|_p .$$

<u>Page 11</u> line 1, and line 5 from below:
Change "I_p" into "$\hat{I}_p$"

<u>Page 12</u> line 5 from below, add: "and $|s| = |b_i|$."
(Observation to explain the implication on top of page 13)

<u>Page 13</u> line 9 should read:
"maps the order-N Farey fractions <u>in</u>to the ...."

<u>Page 15</u> line 4 from below: change "Section 4" into "Section 5"

To clarify Theorem 3 add the following corollary and observation:

in which case:

$$\gcd(b_i,p) = 1 \quad \text{and} \quad \left|\frac{a_i}{b_i}\right|_p = k.$$

<u>PROOF</u> Recall that the fractions in F_N are irreducible by definition, and notice that the corollary is trivially true for $k = 0$, with $n = -1$.

If $0 \neq k \in \hat{I}_p$ then by definition of $\hat{I}_p$ there exists an order-N Farey fraction $\frac{r}{s}$ such that:

$$\gcd(s,p) = 1 \quad \text{and} \quad \left|\frac{r}{s}\right|_p = k$$

where the signs of r and s may be chosen such that $r > 0$. Then (5.5) follows from Theorem 3.

To prove the other part, notice from (5.4) that $\gcd(b_i,p)$ must be a divisor of a_i; but from (5.5), $\gcd(a_i,b_i) = 1$. Hence $\gcd(b_i,p) = 1$, and by Lemma 2

$$\left|\frac{a_i}{b_i}\right|_p = \left|\frac{k}{1}\right|_p = k,$$

thus $k \in \hat{I}_p$. □