Minimal Fractional Representations of Integers mod M

David Greve

ACL2 Workshop
May, 2020

Integers mod M

- Whole numbers 0 .. M-1
- Integers mod 17:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Signed Representations

- Negative numbers: (- x)
  - The number added to x to make zero (0) (mod M)
  - The number added to 7 to make zero (0) (mod 17)
    - 7 + 10 == 0 % 17
    - 10 == -7
    - 7 == -10

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1

Is there a “best” signed representation for each number?

Signed Representations

- Negative numbers: (- x)
  - The number added to x to make zero (0) (mod M)
  - The number added to 7 to make zero (0) (mod 17)
    - 7 + 10 == 0 % 17
    - 10 == -7
    - 7 == -10

Is there a “best” signed representation for each number?

Reciprocals

- Reciprocals: (1/x)
  - The number multiplied by x to make one (1) (mod M)?
  - The number multiplied by 7 to make one (1) (mod 17)?
    - 7 * 5 = 1 % 17
    - 5 = 1/7
    - 7 = 1/5
  - Not every x has a reciprocal mod M

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1	1/9	1/6	1/13	1/7	1/3	1/5	1/15	1/2	1/12	1/14	1/10	1/4	1/11	1/8	1/16

Fractional Representations

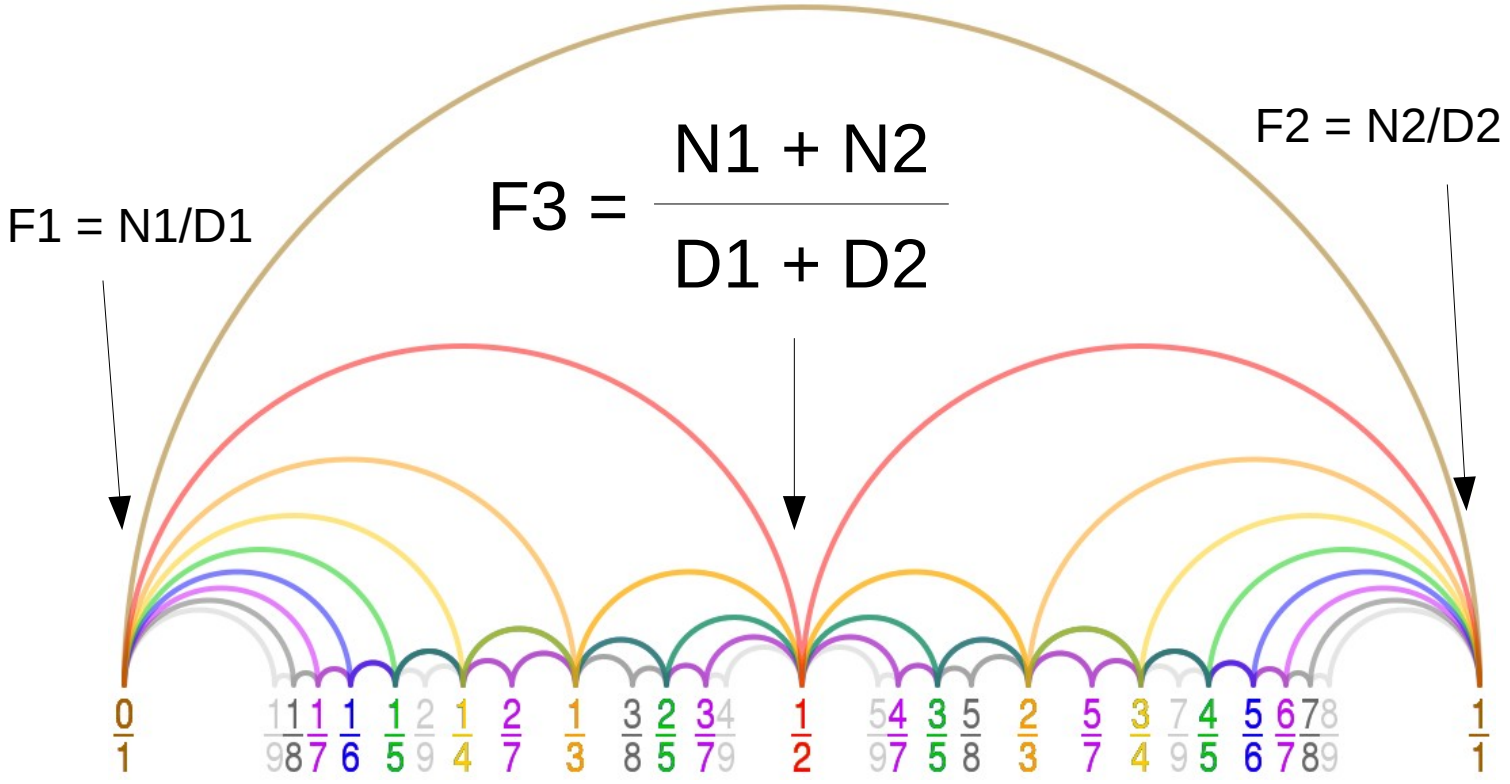
- Fractional Representation (x ~= N/D) mod M
  - x * D == N % M
  - Fractional Representations for 7 mod 17:

$$7/1, 14/2, 4/3, 11/4, 1/5, 8/6, 15/7, 5/8, 12/9, 2/10, 9/11, 16/12, 6/13, 13/14, 3/15, 10/16, 0/17$$

$$-17/0, -10/1, -3/2, -13/3, -6/4, -16/5, -9/6, -2/7, -12/8, -5/9, -15/10, -8/11, -1/12, -11/13, -4/14, -14/15, -7/16$$

Is there a “best” fractional representation for each number?

Farey Sequences



“Neighbors”

N2*D1 – N1*D2 = 1

Fractional Representations

- Fractional Representation (x ~= N/D) mod M
  - x * D == N % M
  - Fractional Representations for 7 mod 17:

$$7/1, 14/2, 4/3, 11/4, 1/5, 8/6, 15/7, 5/8, 12/9, 2/10, 9/11, 16/12, 6/13, 13/14, 3/15, 10/16, 0/17$$

$$-17/0, -10/1, -3/2, -13/3, -6/4, -16/5, -9/6, -2/7, -12/8, -5/9, -15/10, -8/11, -1/12, -11/13, -4/14, -14/15, -7/16$$

Is there a “best” fractional representation for each number?

Fractional Representations

- Fractional Representation (x ~= N/D) mod M
  - x * D == N % M
  - Fractional Representations for 7 mod 17:

7/1, 14/2, 4/3, 11/4, 1/5, 8/6, 15/7, 5/8, 12/9, 2/10, 9/11, 16/12, 6/13, 13/14, 3/15, 10/16, 0/17

-17/0, -10/1, -3/2, -13/3, -6/4, -16/5, -9/6, -2/7, -12/8, -5/9, -15/10, -8/11, -1/12, -11/13, -4/14, -14/15, -7/16

Is there a “best” fractional representation for each number?

Fractional Representations

- Fractional Representation (x ~= N/D) mod M
  - x * D == N % M
  - Fractional Representations for 7 mod 17:

7/1, 14/2, 4/3, 11/4, 1/5, 8/6, 15/7, 5/8, 12/9, 2/10, 9/11, 16/12, 6/13, 13/14, 3/15, 10/16, 0/17

-17/0, -10/1, -3/2, -13/3, -6/4, -16/5, -9/6, -2/7, -12/8, -5/9, -15/10, -8/11, -1/12, -11/13, -4/14, -14/15, -7/16

Is there a “best” fractional representation for each number?

Fractional Representations

- Fractional Representation (x ~= N/D) mod M
  - x * D == N % M
  - Fractional Representations for 7 mod 17:

7/1, 14/2, 4/3, 11/4, 1/5, 8/6, 15/7, 5/8, 12/9, 2/10, 9/11, 16/12, 6/13, 13/14, 3/15, 10/16, 0/17

-17/0, -10/1, -3/2, -13/3, -6/4, -16/5, -9/6, -2/7, -12/8, -5/9, -15/10, -8/11, -1/12, -11/13, -4/14, -14/15, -7/16

Is there a “best” fractional representation for each number?

Minimal Fractional Representation

- A Fractional Representation is “minimal” if :
  - No smaller denominator results in a smaller numerator
    - Sadly: Not sufficiently general

Minimal Fractions Pair

$$X \sim= \frac{N}{K} \quad (N < 0)$$

$$X \sim= \frac{P}{M}$$

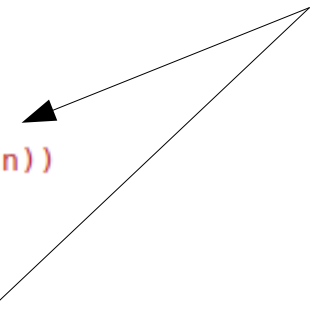
```
;; Our generalized universally quantified minimal fractions invariant
;; can be represented logically as:
;;
;; (implies
;;  (and
;;   (equal n (nmod (* k x) q))
;;   (equal p (pmod (* m x) q)))
;;  (forall (z)
;;    (and
;;     (implies
;;      (< (- (nmod (* z x) q)) (- p n))
;;      (<= k z))
;;     (implies
;;      (and
;;       (not (equal (pmod z q) 0))
;;       (< (pmod (* z x) q) (- p n)))
;;      (<= m z)))))
```

Minimal Fractions Pair

$$X \sim= \frac{N}{K} \quad (N < 0)$$

$$X \sim= \frac{P}{M}$$

```
;; Our generalized universally quantified minimal fractions invariant
;; can be represented logically as:
;;
;; (implies
;;  (and
;;   (equal n (nmod (* k x) q))
;;   (equal p (pmod (* m x) q)))
;;  (forall (z)
;;    (and
;;     (implies
;;      (< (- (nmod (* z x) q)) (- p n))
;;      (<= k z))
;;     (implies
;;      (and
;;       (not (equal (pmod z q) 0))
;;       (< (pmod (* z x) q) (- p n)))
;;      (<= m z)))))
```



No smaller denominator results in a numerator whose magnitude is smaller than the sum of the two numerator magnitudes

Step Minimal Fractions Pair

$$X \sim= \frac{N}{K} \qquad X \sim= \frac{P}{M} \qquad X \sim= \frac{N + P}{K + M}$$

```
(def::un step-minimal-fractions-pair (k n m p)
  (declare (xargs :signature ((natp negp natp natp) natp negp natp natp)))
  (if (< p (- n)) (mv (+ k m) (+ n p) m p)
    (mv k n (+ k m) (+ n p))))
```

$(-17/0, 7/1), (-10/1, 7/1), (-3/2, 7/1), (-3/2, 4/3), (-3/2, 1/5), (-2/7, 1/5), (-1/12, 1/5), (-1/12, 0/17)$

Step Minimal Fractions Pair

$$X \sim= \frac{N}{K} \qquad X \sim= \frac{P}{M} \qquad X \sim= \frac{N + P}{K + M}$$

```
(def::un step-minimal-fractions-pair (k n m p)
  (declare (xargs :signature ((natp negp natp natp) natp negp natp natp)))
  (if (< p (- n)) (mv (+ k m) (+ n p) m p)
    (mv k n (+ k m) (+ n p))))
```

$$(-17/0, 7/1), (-10/1, 7/1), (-3/2, 7/1), (-3/2, 4/3), (-3/2, 1/5), (-2/7, 1/5), (-1/12, 1/5), (-1/12, 0/17)$$

Step Minimal Fractions Pair

$$X \sim= \frac{N}{K} \qquad X \sim= \frac{P}{M} \qquad X \sim= \frac{N + P}{K + M}$$

```
(def::un step-minimal-fractions-pair (k n m p)
  (declare (xargs :signature ((natp negp natp natp) natp negp natp natp)))
  (if (< p (- n)) (mv (+ k m) (+ n p) m p)
    (mv k n (+ k m) (+ n p))))
```

$$(-17/0, 7/1), (-10/1, 7/1), (-3/2, 7/1), (-3/2, 4/3), (-3/2, 1/5), (-2/7, 1/5), (-1/12, 1/5), (-1/12, 0/17)$$

Minimal Coefficient Bound

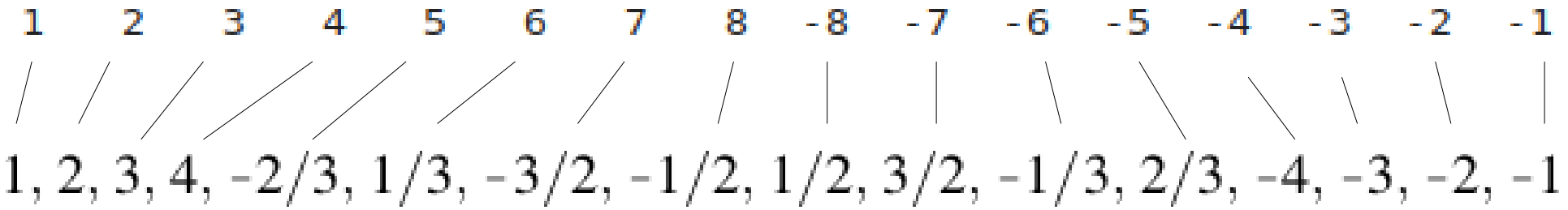
2/20/2020
6:30 pm →

2/20/2020
9:30 pm →

```
;; We also prove that our algorithm preserves the following invariant:
;;
;; (implies
;;   (and
;;     (equal n (nmod (* k x) q))
;;     (equal p (pmod (* m x) q)))
;;   (equal (- (* k p) (* m n)) q))
;;
;; We use this invariant to prove that every number has a minimal
;; fractional representation in which the coefficients are less than
;; the square root of the modulus (unless the resulting numerator is
;; exactly the square root of the modulus)

;; (defthm lt-sqrt-minimum-fraction
;;   (implies
;;    (and
;;     (integerp x)
;;     (non-trivial-modulus q))
;;    (mv-let (n d) (minimum-fraction x q)
;;      (or (and (equal (* n n) q)
;;               (lt-sqrt d q))
;;          (and (lt-sqrt n q)
;;               (lt-sqrt d q))))))
```

Minimal Fractions mod 17



- smallest maximum coefficient
- smallest denominator

Also a Floor Wax ..

- Computes Modular Inverses/GCDs ..
  - Generates Same “coefficients” as Euclidean Algorithm
    - If you use “division” instead of ”repeated subtraction”
  - Like “Extended GCD”
    - All computations are in “M”

```
(def::un inv-rec (k n m p)
  (declare (xargs :signature ((natp negp natp natp) natp natp)
                  :measure (+ (nfix (- (ifix n))) (nfix p))))
  (if (not (and (< (ifix n) 0) (< 0 (nfix p)))) (mv p m)
    (mv-let (k1 n1 m1 p1) (step-minimal-fractions-pair k n m p)
      (if (zp p1) (mv p m)
        (inv-rec k1 n1 m1 p1)))))
```

```
(def::und inv (x q)
  (declare (xargs :signature ((natp posp) natp natp)))
  (let ((k 0)
        (n (- q))
        (m 1)
        (p (nfix x)))
    (inv-rec k n m p)))
```

.. and A Dessert Topping!

- Performs Modular “Long Division”
  - Traditionally “Division” means multiply by reciprocal

```
(def::und div (n d q)
  (declare (xargs :signature ((natp natp posp) natp natp)))
  (let ((k n)
        (n (nmod d q))
        (m n)
        (p (pmod d q)))
    (mv-let (g r) (inv-rec k n m p)
      (mv g (pmod r q)))))
```

Conclusion

- Algorithm for finding minimal fractional representations
  - Also performs long division!
- Verified sqrt(M) bound on numerator/denominator
- Culmination of Several Years of .. Contemplation