Minimal Fractional Representations of Integers mod M

David Greve
david@thegreves.com

We say that the fraction $\frac{N}{D}$ *represents* $x \in \mathbf{Z}/m\mathbf{Z}$ when $x * D \equiv N \pmod{M}$. Our definition admits many possible fractional representations. We say that $\frac{N}{D}$ is a *minimal* representation of x if no smaller denominator (D) results in a numerator with a magnitude less than the magnitude of N. We introduce a function for computing such fractional representations and prove that it generates minimal fractions. We also prove that every $x \in \mathbf{Z}/m\mathbf{Z}$ has a minimal fractional representation in which the magnitude of N and D are less or equal to $\sqrt{M}$.

1 Introduction

We say that the fraction $\frac{N}{D}$ *represents* $x \in \mathbf{Z}/m\mathbf{Z}$ when $x * D \equiv N \pmod{M}$. We denote this relationship[1] as $x \cong \frac{N}{D} \pmod{M}$. This definition admits many possible fractional representations of x, some possibly not reduced. For example, 7 (mod 17) has the following representations:

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

In this work we consider both positive and negative residues in the numerator. A positive residue is defined as $(x * D \bmod M)$ for $0 < D \leq Q$ while a negative residue is defined as $(x * D \bmod M) - M$ for $0 \leq D < Q$. Using the negative residue the fractional representations of 7 (mod 17) are:

{-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}

Within the same residue class (positive or negative), we say that $\frac{N}{D}$ is a *minimal* representation of x if no denominator smaller than (D) results in a numerator with a magnitude less than the magnitude of N. (7/1) is minimal for 7 (mod 17) simply because we don't consider positive residues with denominators less than 1. The fraction (-3/2) is also minimal because |-3| is less than the magnitude of the numerators of both negative fractions with denominators less than 2, $(-17/0)$ and $(-10/1)$. (-6/4), however, is not minimal because (-3/2) has both a smaller magnitude numerator and a smaller denominator.

Our proof of correctness actually requires a stronger, more general notion of minimality that is invariant over our algorithm for computing minimal fractions. This more general invariant is expressed with respect to a pair of fractions: one negative residual and one positive residual. The pair is considered minimal if, for all possible denominators (d), if the magnitude of either the positive or negative residual of $d * x$ is less than the *sum* of the magnitudes of the numerators of the pair of fractions, then d must be greater than or equal to the denominator of the fraction with the same residual sign. Under this generalization the pair of fractions (-3/2, 4/3) is considered minimal because no denominator less than 3 has a positive residual and no denominator less than 2 has a negative residual less than $|\text{-}3| + |4| = 7$.

[1] We might say "congruent to" when $D \perp M$ but we don't require this condition.

G. Passmore, R. Gamboa (Eds.): ACL2 Workshop 2020
EPTCS ??, 2020, pp. 1–2, doi:10.4204/EPTCS.??.??

Our computation of minimal fractions relies on the following property of the mediant computation[2]:

$$x \cong \frac{N_1}{D_1} \wedge x \cong \frac{N_2}{D_2} \implies x \cong \frac{N_1 + N_2}{D_1 + D_2} \pmod{M}$$

Our algorithm takes as input two minimal fractions with differing signs, initially $(x-M)/0$ and $x/1$ (which are trivially minimal). It then recursively replaces the fraction with the larger magnitude numerator with the mediant of the two original fractions until one of the numerators is zero. The key to the termination of our algorithm is the observation that the mediant of two fractions whose numerators differ in sign is a fraction whose numerator is smaller in magnitude than the larger of the magnitudes of the two original numerators. We prove that this algorithm preserves our notion of minimal fractional pairs. The minimal fractional pairs generated by our algorithm for 7 (mod 17) are listed below.

(-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)

In addition to our minimality invariant we prove that every x has a fractional representation in which both $|N|$ and D are less than or equal to $\sqrt{M}$. This result follows from the fact that $N_1 * D_2 - N_2 * D_1 = M$ where $N_1, D_1, D_2 >= 0 \wedge N2 < 0$ is also an invariant of our algorithm. Consider the case where $D_1 < \sqrt{M}$ and $D_2 < \sqrt{M}$ but $D_1 + D_2 \geq \sqrt{M}$. If both $N_1 > \sqrt{M}$ and -$N_2 > \sqrt{M}$, then in the following step, $|(D_1 + D_2) * N_i|$ will be greater than M, violating our invariant. Thus, at least one $|N_i| \leq \sqrt{M}$.

It is possible for a number to have more than one representation whose coefficients are less than $\sqrt{M}$. For example, 12 (mod 17) is represented by both (-3/4) and (2/3), both of whose coefficient magnitudes are less than $\sqrt{17}$. Deciding which is *the minimum* is a judgment call. We say that the minimum fraction is the one with the smallest maximum coefficient, resolving ties with the smaller denominator. Under those conditions the minimum fractional representation of 12 (mod 17) is (2/3). Using this minimality criteria the minimum fractional representations for each of the numbers 1...16 (mod 17) are:

{1, 2, 3, 4, -2/3, 1/3, -3/2, -1/2, 1/2, 3/2, -1/3, 2/3, -4, -3, -2, -1}

2 Conclusion

The properties presented in this paper were verified usng ACL2 and are distributed along with the ACL2 source code in the directory `/books/workshops/2020/greve`. In that book we verify an algorithm for computing minimal fractional representations $\frac{N}{D}$ of numbers $x \in \mathbf{Z}/m\mathbf{Z}$. We also prove that all such numbers have a representation in which the magnitude of both N and D are less than or equal to $\sqrt{M}$. In the cryptographic community there is interest in finding smooth numbers that result from specific computations. The quadratic sieve algorithm [2], for example, attempts to find small numbers (numbers on the order of $\sqrt{M}$) in hopes of factoring them into a smooth factor base. We show that any residue relatively prime to M can be represented as a quotient of two numbers less than or equal to $\sqrt{M}$.

References

[1] (2020): *Farey Sequence*. Available at `https://en.wikipedia.org/wiki/Farey_sequence`.

[2] (2020): *General Number Field Sieve*. Available at `https://en.wikipedia.org/wiki/General_number_field_sieve`.

[2] As used in the generation of Farey sequences [1] except that, in our case, $N_1 * D_2 - N_2 * D_1$ is equal to M rather than 1