A Polynomial Diophantine Generator Function for Integer Residuals

Charles Sauerbier

January 2010

Abstract: Two Diophantine equation generator function for integer residuals produced by integer division over closed intervals are presented. One each for the closed intervals \( [1, \sqrt[3]{n}] \) and \( [[\sqrt[3]{n}], n] \), respectively.

1. Preliminaries

In this paper we address the problem of determining residual values in integer division by mathematical computation more amenable to analytic methods than iterative division, as well as the values of the corresponding integer quotient. Diophantine generator functions derived from empirical observation of the pattern present in integer values as a result of sequential execution of the division operation over each of the respective closed integer intervals is presented that admits the direct computation of corresponding residual and quotient by means of polynomial functions. Unlike the process of simple iterative division the resulting generator functions admit application of mathematical tools to analysis of applicable problems not otherwise admitted by the sequential division process.

We have not found the results presented addressed by others in available literature. The focus of the literature of general relation to the problem and problems it impacts having taken avenues premised on more conventional methods, such as algebraic structures and numeric sieves. The approach taken in derivation of the generator functions is by way of difference expression\(^{[1]}\) on the 3-tuple \(<x, y, r>\) in context of the commonly known relation \( n = (x * y) + r \).

2. Generator Functions

The observed behavior of the integer values in the two intervals leads us to produce distinct generator functions for each interval. This dichotomy works to benefit the objective of locating the zeros of the function \( \frac{n^3}{3} |_{x=1}^{n} \), as the interval \( [[\sqrt[3]{n}], n] \) contains precisely one value for ‘x’ such that ‘x’ divides ‘n’.

2.1. Conditions

We consider the following conditions: Given a value ‘n’, 3-tuples \(<x_0, y_0, r_0>\) where \(<x_0, y_0, r_0> = (\lceil \sqrt[3]{n} \rceil, \lceil n/\sqrt[3]{n} \rceil, n - (\lceil \sqrt[3]{n} \rceil * \lceil n/\sqrt[3]{n} \rceil))\). The values of \(x_0, y_0\) have the relation \(x_0 \leq y_0\). For our purpose here we define on the values \(i = x_0\) and \(j = y_0\) the following delta: \(\delta_{ij} = \begin{cases} 1 & \text{where } i \neq j \\ 0 & \text{where } i = j \end{cases}\)

\(^{[1]}\) (Kelley & Peterson, 1990) (Elaydi, 2005) (Goldberg, 1986)
2.2. X Decrement \([1, x_0]\)

The generator functions here are premised on decrementing ‘\(x\)’ over the interval \([\frac{3}{\sqrt{n}}] \geq x \geq 1\), where ‘\(x\)’ is an integer index value. The generator function is derived from \(n = (x \ast y) - r\). We obtain the set of difference expressions of Lemma 2.2.1 for the respective values of \(x, y, r\) from that relation.

**Lemma 2.2.1**

*Given the conditions as stated, above in 2.1, for all values \(k\) in the closed interval \([1, x_0]\) over integers:*

\[
\begin{align*}
x_k &= x_{k-1} - 1 \\
y_k &= y_{k-1} + \left((r_{k-1} + y_{k-1}) \div x_k\right), \text{ and;} \\
r_k &= (r_{k-1} + y_{k-1}) \mod x_k.
\end{align*}
\]

The difference expressions follow by basic algebra from the relations \(n = (x \ast y) - r\), as any amount by which \(x\) is reduced needs be account for in the other terms of the equation to maintain the equality relation between the left and right sides. The expressions for computing the resultant values of ‘\(y\)’ and ‘\(r\)’ distribute the subtracted value of ‘\(x\)’ in the context of the equation across those variables in accordance with the algebraic manipulation:

\[
n = (x - 1) \ast y + (r + y)
\]

\[
n = ((x - 1) \ast y + ((r + y) \div (x - 1))) + ((r + y) \mod (x - 1))
\]

**Theorem 2.2.1**

*Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.2.1, where \(x_k = x_{k-1} - 1\), the residual value \(r_k = r'_{k} \mod x_k\) where*

\[
r'_{k} = r_0 + (k \ast \delta_{ij}) + \left(\frac{(k-1)k}{2}\right) + \left(\frac{(k+1)k}{2}\right);
\]

*which reduces to*

\[
r'_{k} = r_0 + (k \ast \delta_{ij}) + k^2.
\]

We observe that under the given conditions the value \(\frac{2}{\sqrt{n}}\) will be either an integer or real number with a non-zero decimal component. The result of the assignment of values to \(x_0, y_0\) is such that either \(x_0 = y_0\) or \(x_0 = y_0 - 1\) for any given value of ‘\(n\)’. With \(\delta_{ij}\) representing \(|y_0 - x_0|\) we have then the follow sequence:

\[
\begin{align*}
   r_0 &= n - |x_0 \ast y_0| \\
   r_1 &= r_0 + (y_0 - x_1) = (r_0 + y_0) \mod x_1 \\
   r_2 &= r_1 + (y_1 - x_2) = (r_1 + y_1) \mod x_2
\end{align*}
\]
The sequence of relations above only hold where \((y_{i-1} - x_i) = (r_{i-1} + x_{i-1}) \mod x_i\). However, in foregoing the application of the mod and div operations we arrive at the following:

\[
\begin{align*}
    r'_0 &= r_0 \\
    r'_1 &= r_0 + (y_0 - x'_1), \quad x'_1 = x_0 - 1, \quad y'_1 = y_0 + 1
\end{align*}
\]

Which then leads to the following:

\[
\begin{align*}
    r'_1 &= r_0 + (y_0 - (x_0 - 1)) = r_0 + (y_0 - x_0) + 1 \\
    r'_2 &= r'_1 + (y'_1 - x'_2) = r_0 + (y_0 - x_0) + 1 + (y'_1 - x'_2) \\
        &= r_0 + (y_0 - x_0) + 1 + ((y_0 + 1) - (x_0 - 2)) \\
        &= r_0 + (y_0 - x_0) + 1 + (y_0 - x_0) + (1 + 2)
\end{align*}
\]

Observing that \((y_0 - x_0)\) is equal to 0 or 1 and present in each iteration we have for any \(r'_k\) the product \((k * \delta_{ij})\). This leaves the summation of \(y_{i-1} - x_i\) for each \(r'_k\) giving us

\[
\sum_{i=1}^{k-1} i + \sum_{i=1}^{k} i.
\]

From which we can thus derive:

\[
r'_k = r_0 + (k * \delta_{ij}) + \left(\frac{(k-1)k}{2}\right) + \left(\frac{(k+1)k}{2}\right),
\]

which by algebraic operations on the summations reduces to

\[
r'_k = r_0 + (k * \delta_{ij}) + k^2.
\]

Testing this hypothesis for base values 0 and 1 we obtain the following results:

\[
\begin{align*}
    r'_0 &= r_0 + (0 * \delta_{ij}) + 0^2 = r_0 \\
    r'_1 &= r_0 + (1 * \delta_{ij}) + 1^2 = r_0 + \delta_{ij} + 1.
\end{align*}
\]

By induction we then assume that the expression holds for all \(k\), for \(k+1\) we then have

\[
\begin{align*}
    r'_{k+1} &= r_0 + (k + 1) * \delta_{ij} + (k + 1)^2 \\
    r'_{k+1} &= r_0 + (k * \delta_{ij}) + \delta_{ij} + (k^2 + 2k + 1) \\
    r'_{k+1} &= r_0 + (k * \delta_{ij}) + k^2 + (2k + 1) + \delta_{ij} \\
    r'_{k+1} &= r_k + (2k + 1) + \delta_{ij}
\end{align*}
\]

Observing that absent application of the quotient of \(r'_k \div x_k\) that the difference between the corresponding values of \(x'_{k+1}, y'_k\) increase with \(k\) by 2, including the constant 1 resulting from the decrementing action of \(x_k = x_{k-1} - 1\) the above then reduces to

\[
r'_{k+1} = r'_k + (y'_k - x'_{k+1}),
\]

proving the theorem.
Theorem 2.2.2

Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.2.1, as applied in Theorem 2.2.1:

\[ ax_k' = r_k' \text{ only where } x_k' \text{ divides } n \text{ for all values of } a. \]
\[ by_k' = r_k' \text{ only where } y_k' \text{ divides } n \text{ for all values of } b. \]

Let us assume \( x_k' \not\mid n \) and \( ax_k' = r_k' \); then \( n = (x_k' * y_k') + ax_k' = x_k'(y_k' + a) \) implies \( x_k' \) divides \( 'n' \), in contradiction of the assumption.

Similarly, assume \( y_k' \not\mid n \) and \( by_k' = r_k' \); then \( n = (x_k' * y_k') + ay_k' = y_k'(x_k' + a) \) implies \( y_k' \) divides \( 'n' \), in contradiction of the assumption.

Corollary 2.2.1

Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.2.1, as applied in Theorem 2.2.1:

\[ ax_0 = r_k' + ak \text{ only where } x_k \text{ divides } n \text{ for all values of } a. \]

This corollary follows from Theorem 3 by substitution of \( x_k = x_0 - k \); where the equality follows from the definition of \( x_k \) as the \( k^{th} \) subtraction of the value 1.

Lemma 2.2.2

Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.2.1, as applied in Theorem 2.2.1:

\[ y_k' = y_0 + k \]

Lemma 2.2.3

Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.2.1, as applied in Theorem 2.2.1 and using the result of Lemma 2.2.2:

\[ y_k = y_k' + r_k' \text{ div } x_k \]

Noting that the value computed as \( y_k' \) is absent the addition of integer quotient of \( \left\lceil \frac{r_k'}{x_k} \right\rceil \) (i.e. “\( \text{r \ div } \text{x}' \)”) and that \( r_k' \) accounts for that integer quotient in the absence of the mod operation being applied, from Lemma 2.2.1 it follows that \( y_k = y_k' + r_k' \text{ div } x_k \), producing a generator function for the quotient of integer division of \( 'n' \) by \( 'x' \).

2.3. Y-Increment \([y_0, n]\)

The generator functions here are premised on incrementing \( 'y' \) over the interval \( \left\lceil \sqrt{n} \right\rceil \leq y \leq n \), where \( 'y' \) is an integer index value. The generator function is derived from \( n = (x * y) - r \). We obtain the set of difference expressions of Lemma 2.1.1 for the respective values of \( x, y, r \) from that relation.
The generator functions presented in this section operate over the interval \( \lceil \sqrt{n} \rceil \leq y \leq n \). Computation of ‘x’ without modular normalization of values will cause ‘x’ to become negative, which in computer applications may become problematic.

**Lemma 2.3.1**

*Given the conditions as stated, above in 2.1, for all values k in the closed interval \([y_0, n]\) over integers:*

\[
\begin{align*}
y_k &= y_{k-1} + 1 \\
x_k &= x_{k-1} + \left((r_{k-1} - x_{k-1}) \text{ div } y_k\right), \text{ and} \\
r_k &= (r_{k-1} - x_{k-1}) \text{ mod } y_k.
\end{align*}
\]

The difference expressions follow by basic algebra from the relations \( n = (x \ast y) - r \), as any amount by which \( y \) is increases needs be account for in the other terms of the equation to maintain the equality relation between the left and right sides. The expressions for computing the resultant values of ‘x’ and ‘r’ absorb the added value of ‘y’ in the context of the equation across those variables in accordance with the algebraic manipulation:

\[
\begin{align*}
n &= \left((y + 1) \ast x\right) + (r - x) \\
n &= \left((y + 1) \ast (x + ((r - x) \text{ div } (y + 1)))\right) + ((r - x) \text{ mod } (y + 1))
\end{align*}
\]

**Theorem 2.3.1**

*Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.3.1, where \( y_k = y_{k-1} + 1 \), for all values \( k \) in the closed interval \([y_0, n]\) over integers the residual value \( r_k = r'_{k} \text{ mod } y_k \) where*

\[
r'_{k} = r_0 + \left(k \ast \delta_{ij}\right) + \left(\frac{(k-1)k}{2}\right) + \left(\frac{(k+1)k}{2}\right);
\]

*which reduces to*

\[
r'_{k} = r_0 + \left(k \ast \delta_{ij}\right) + k^2.
\]

We observe that under the given conditions the value \( \sqrt{n} \) will be either an integer or real number with a non-zero decimal component. The result of the assignment of values to \( x_0, y_0 \) is such that either \( x_0 = y_0 \) or \( x_0 = y_0 - 1 \) for any given value of ‘n’. With \( \delta_{ij} \) representing \(|y_0 - x_0|\) we have then the follow sequence:

\[
\begin{align*}
r_0 &= n - |x_0 \ast y_0| \\
r_1 &= r_0 + (x_0 - y_1) = (r_0 + x_0) \text{ mod } y_1 \\
r_2 &= r_1 + (x_1 - y_2) = (r_1 + x_1) \text{ mod } y_2
\end{align*}
\]
The sequence of relations above only hold where \((x_{i-1} - y_i) = (r_{i-1} + x_{i-1}) \mod y_i\). However, in foregoing the application of the mod and div operations we arrive at the following:

\[
r'_{0} = r_0 \\
r'_{1} = r_{0} + (x_0 - y'_{1}), \ x'_{1} = x_{0} - 1, \ y'_{1} = y_{0} + 1
\]

Which then leads to the following:

\[
r'_{1} = r_{0} + (x_0 - (y_0 + 1)) = r_{0} + (x_0 - y_0) + 1 \\
r'_{2} = r_{1} + (x_{1}' - y_{2}') = r_{0} + (x_0 - y_0) + 1 + (x_{1}' - y_{2}') \\
= r_{0} + (x_0 - y_0) + 1 + ((x_0 - 1) - (y_0 - 2)) \\
= r_{0} + (x_0 - y_0) + 1 + (x_0 - y_0) + (1 + 2)
\]

Observing that \((y_0 - x_0)\) is equal to 0 or 1 and present in each iteration we have for any \(r'_{k}\) the product \((k \cdot \delta_{ij})\). This leaves the summation of \(x_{i-1} - y_i\) for each \(r'_{k}\) giving us

\[
\sum_{i=1}^{k-1} i + \sum_{i=1}^{k} i.
\]

From which we can thus derive:

\[
r'_{k} = r_{0} + (k \cdot \delta_{ij}) + \left(\frac{(k-1)k}{2}\right) + \left(\frac{(k+1)k}{2}\right),
\]

which by algebraic operations on the summations reduces to

\[
r'_{k} = r_{0} + (k \cdot \delta_{ij}) + k^2.
\]

The proof then follows in consequence of Theorem 2.2.1.

**Theorem 2.3.2**

*Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.3.1, as applied in Theorem 2.3.1, for all values \(k\) in the closed interval \([y_0, n]\) over integers:*

\[
a x'_{k} = r'_{k} \text{ only where } x'_{k} \text{ divides } n \text{ for all values of } a. \\
b y'_{k} = r'_{k} \text{ only where } y'_{k} \text{ divides } n \text{ for all values of } b.
\]

Let us assume \(x'_{k} \nmid n\) and \(a x'_{k} = r'_{k}\); then \(n = (x'_{k} \cdot y'_{k}) + a x'_{k} = x'_{k} (y'_{k} + a)\) implies \(x'_{k}\) divides ‘n’, in contradiction of the assumption.

Similarly, assume \(y'_{k} \nmid n\) and \(b y'_{k} = r'_{k}\); then \(n = (x'_{k} \cdot y'_{k}) + a y'_{k} = y'_{k} (x'_{k} + a)\) implies \(y'_{k}\) divides ‘n’, in contradiction of the assumption.

**Corollary 2.3.1**

*Given the foregoing conditions under the difference expressions of Lemma 2.3.1, as applied in Theorem 2.3.1, for all values \(k\) in the closed interval \([y_0, n]\) over integers:*

\[
a y_0 = r'_{k} - a k \text{ only where } y'_{k} \text{ divides } n \text{ for all values of } a.
\]
This corollary follows from Theorem 3 by substitution of \( y'_k = y_0 + k \); where the equality follows from the definition of \( y_k \) as the \( k^{th} \) addition of the value 1.

**Lemma 2.3.2**

*Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.3.1, as applied in Theorem 2.3.1, for all values \( k \) in the closed interval \([y_0, n]\) over integers:*

\[
x'_k = x_0 + k
\]

Follows directly from definition of difference expressions, with the exception that where \( k \geq x_0 \), the relation does not hold.

**Lemma 2.3.3**

*Given the conditions as stated, above in 2.1, under the difference expressions of Lemma 2.3.1, as applied in Theorem 2.3.1 and using the result of Lemm2.3.2, for all values \( k \) in the closed interval \([y_0, n]\) over integers:*

\[
x_k = x'_k + r'_k \text{div} \ y_k
\]

Noting that the value computed as \( x'_k \) is absent the addition of integer quotient of \( \left\lfloor \frac{r}{y} \right\rfloor \) (i.e. “\( r \text{ div} \ y \)” and that \( r'_k \) accounts for that integer quotient in the absence of the mod operation being applied, from Lemma 2.3.1 it follows that \( x_k = x'_k + r'_k \text{div} \ y_k \), producing a generator function for the quotient of the integer division of ‘\( n \)’ by ‘\( y \).’

3. Conclusion

As a result of observation of empirical data sets a Diophantine generator function of integer quotient and residual in integer division was derived. The generator functions admits the computation of both quotient and residual values using continuous polynomial functions on basis of an index in either of the closed integer intervals \([1, \left\lfloor \sqrt{n} \right\rfloor]\) or \([\left\lceil \sqrt{n} \right\rceil, n]\). The generator functions provide means to determine the zeros within either closed interval where ‘\( n \)’ is the dividend. The results presented have potential application in determining the factors of an integer value, as well as implications for other applications.

4. References

Elaydi, S. (2005). *An Introduction to Difference Equations*. Springer.

Goldberg, S. (1986). *Introduction to Difference Equations*. Dover Publications.

Kelley, W. G., & Peterson, A. C. (1990). *Difference Equations : An introduction with Applications*. Academic Press.