

# Re: Finding minimum in arithmetic series modulo N

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2008-04/msg02056.html>

---

- *From:* Tim Little <[tim@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:tim@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 11 Apr 2008 00:29:47 -0500
- 

On 2008-04-10, 3130@xxxxxxxx <3130@xxxxxxxx> wrote:

$$x(k) = (A + kD) \bmod N$$

[...]

k takes values 0, 1, 2 ... M-1.

[ Find minimum  $x(k)$  ]

I'm guessing you mean the ordering in which  $n-1 < n$  for  $n \neq 0 \bmod N$ . Yes, there certainly are methods of search that are much better than brute force. Think of where the successive values of the sequence "land".

You start at A and increment by D, eventually exceeding N and wrapping around to some value  $m_1 < D$  at  $k = k_1$ . If  $k_1 \geq M$  then A is the smallest value.

Now consider only every  $\text{floor}(N/D)$  iterations from then on. Obviously none of the intermediate values can be a minimum. Successive values in this sequence increase by some amount  $r < D$ . If  $r > 0$  you can now reduce the problem to be that of finding the minimum value of  $x'(k') = (m_1 + k' r) \bmod D$ , for  $0 \leq k' < M / \text{floor}(N/D)$ .

- Tim

.