

Re: Finding minimum in arithmetic series modulo N

Source: <http://sci.tech-archive.net/Archive/sci.math/2008-04/msg02199.html>

- *From:* Ilmari Karonen <usenet2@xxxxxxxxxxxxxxxx>
 - *Date:* 12 Apr 2008 01:31:11 GMT
-

On 11.04.2008, James Waldby <no@xxxxx> wrote:

On Thu, 10 Apr 2008 15:33:03 -0700, 3130 wrote:

Consider the sequence of values generated by:

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

where A, D and N are positive non-zero integers, and k takes values 0, 1, 2 ... M-1.

Other than brute force search, is there is a way to determine the minimum value for x(k) and the value of k for which that minimum value occurs.

Here's an idea to consider; still a brute force search, but with a good chance of terminating much earlier than when just stepping k=1,2,3... -- Suppose $\gcd(D,N) = 1$. From Euclid's algorithm, let a,b be such that $1 = aD + bN$, so that $aD \equiv 1 \pmod N$. Let i be the smallest integer such that $0 < -a + iN < N$. (i exists since $(D,N) = 1$.) Let $c = -a + iN$ and $k = Ac \pmod N$. (Now $A + kD \equiv 0 \pmod N$.) Until k is in range, set k to $k + a \pmod N$. Afterward, compute $\min = A + kD \pmod N$. (I haven't figured out how to adapt this if $\gcd(D,N) > 1$.)

Hmm... if $d = \gcd(D,N) > 1$, surely you could just take $D' = D/d$, $N' = N/d$ and $A' = \text{floor}(A/d)$, so that $\gcd(D',N') = 1$, and apply your method (or any other) to these reduced values?

Anyway, let me see if I understood your suggestion correctly:

1. Assume $\gcd(D,N) = 1$ and $A > 0$.
2. Choose $0 < a < N$ such that $aD \pmod N = 1$ using Euclid's algorithm.
3. Let $k := -aA \pmod N (= (N-a)A \pmod N)$.
4. If $k < M$, let $k_{\min} := k$ and stop.

Re: Finding minimum in arithmetic series modulo N

5. Otherwise, let $k := k+a \bmod N$ and return to step 4.

The loop over steps 4 and 5 can take no more than N/a iterations. The number of iterations may be further reduced, especially if a is small, by changing step 5 to let $k := k-N \bmod a$ ($= k-N+aN \bmod a$). This makes the loop terminate in at most $\min(a, N/a)$ iterations (and in particular, if $a < M$, in at most one iteration). The expected number of iterations should in any case be roughly inversely proportional to M ; for very low M , it may be faster to just check all possible $0 \leq k < M$ instead.

—

Ilmari Karonen

To reply by e-mail, please replace ".invalid" with ".net" in address.

.