Example of a Disaster caused by Subtractive Cancellation

From http://www.netlib.org/na-digest-html/92/v92n22.html:

From: David Keaton <dmk@dmk.com>
Date: Thu, 28 May 92 11:12 MDT
Subject: Patriot Missle Bug Report


The report is quite well done and includes pictures that show the exact process used to track a Scud. It contains the level of technical detail needed for us to understand what happened, yet presents it so that a non-technical person has a fighting chance at understanding it too.

The problem began to manifest itself as roundoff error, but the real problem was precision error instead. They put the "real time since boot" clock in a single precision floating point number. To calculate a time interval, they took two snapshots of the clock and subtracted them. When the system had been up for more than eight hours, the absolute uptime started to get bigger than the mantissa and calculations got less and less accurate. Eventually, the Patriot would miss the window for tracking an incoming Scud.

The field fix was just to reboot the Patriots every eight hours until a software fix arrived. However, the people manning the Patriots didn't get the word.

The first copy of each GAO report is free. Additional copies are $2 each. Orders may be placed by calling (202) 275-6241, or by mail to U.S. General Accounting Office P.O. Box 6015 Gaithersburg, MD 20877 Make checks or money orders payable to Superintendent of Documents.

David Keaton
dmk@dmk.com

From http://www.netlib.org/na-digest-html/92/v92n24.html#4:

From: Murli Gupta <MMG@gwuvm.gwu.edu>
Date: Wed, 10 Jun 92 14:43:24 EDT
Subject: GAO Report-"Patriot Missile Defence"

A couple of weeks ago, David Keaton gave a brief description of the GAO report "Patriot Missile Defence: Software Problem Led to System Failure at Dhahran, Saudi Arabia".

I acquired a copy of the report and found it to be very interesting from a numerical analysis perspective; many others seem to be interested in further details contained in the report.
Further details of the GAO Report

The Patriot missile defence battery uses a 24 bit arithmatic which causes the representation of real time and velocities to incur roundoff errors; these errors became substantial when the patriot battery ran for 8 or more consecutive hours.

As part of the search and targeting procedure, the Patriot radar system computes a "Range Gate" that is used to track and attack the target. As the calculations of real time and velocities incur roundoff errors, the range gate shifts by substantial margins, especially after 8 or more hours of continuous run.

The following data on the effect of extended run time on patriot operations from Appendix II of the report would be of interest to numerical analysts everywhere.

<table>
<thead>
<tr>
<th>Hours</th>
<th>Real time (seconds)</th>
<th>Calculated Time (seconds)</th>
<th>Inaccuracy (seconds)</th>
<th>Approximate shift in range gate (meters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>3600</td>
<td>3599.9966</td>
<td>.0034</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>28800</td>
<td>28799.9725</td>
<td>.0275</td>
<td>55</td>
</tr>
<tr>
<td>20a</td>
<td>72000</td>
<td>71999.9313</td>
<td>.0687</td>
<td>137</td>
</tr>
<tr>
<td>48</td>
<td>172800</td>
<td>172799.8352</td>
<td>.1648</td>
<td>330</td>
</tr>
<tr>
<td>72</td>
<td>259200</td>
<td>259199.7528</td>
<td>.2472</td>
<td>494</td>
</tr>
<tr>
<td>100b</td>
<td>360000</td>
<td>359999.6667</td>
<td>.3333*</td>
<td>687</td>
</tr>
</tbody>
</table>

a: continuous operation exceeding 20 hours-target outside range gate
b: Alpha battery [at Dhahran] ran continuously for about 100 hours

* corrected value [GAO report lists .3433]

On February 21, 1991 the Patriot Project Office sent a message to all patriot sites stating that very long run times "could cause a shift in the range gate, resulting in the target being offset". However, the message did not specify "what constitutes very long run times. According to the Army officials, they presumed that the users would not run the batteries for such extended periods of time that the Patriot would fail to track targets. Therefore, they did not think that more detailed guidance was required".

The air fields and seaports of Dhahran were protected by six Patriot batteries. Alpha battery was to protect the Dhahran air base. On February 25, 1991, Alpha battery had been in operation for over 100 consecutive hours. That's the day an incoming Scud struck an Army barracks and killed 28 American soldiers.

On February 26, the next day, the modified software, which compensated for the inaccurate time calculation, arrived in Dhahran.