Ruby trunk - Bug #7242

Bignum mathematical accuracy regression in r31695

10/30/2012 07:34 AM - mhall (Matthew Hall)

Status:	Closed		
Priority:	Normal		
Assignee:	mrkn (Kenta Murata)		
Target version:	2.0.0		
ruby -v:	ruby 1.9.3dev (2011-05-22 trunk 31695) [x86_64-linux]	**Backport:**	

Description

We have some pure Ruby code which performs a DH (Diffie Hellman) cryptographic handshake.

If I upgrade to using the Ruby 1.9.3 interpreter instead of 1.9.2, the unit tests around the code fail, because the client and server can no longer compute matching secret keys. I would expect they could agree on matching keys as the DH algorithm expects. The code worked fine since May 2007 on Ruby 1.8 and 1.9 until the commit below was introduced.

Using svn-bisect, I was able to find that this commit from ruby-trunk in between Ruby 1.9.2 (27656) and Ruby 1.9.3 (32500) causes the problem:

r31695 | mrkn | 2011-05-22 08:37:00 -0700 (Sun, 22 May 2011) | 4 lines

- bignum.c (dump_bignum, bigmul1_balance, big_split, biglsh_bang, bigrsh_bang, big_split3, bigmul1_toom3, bigmul0): implement Toom3 (Toom-Cook) multiplication.
- include/ruby/defines.h: add format prefixes for BDIGIT and BDIGIT_DBL.

Attached to this bug I have a simplified example test case which will pass without this commit, and fail with this commit present.

Since this commit covers some relatively complex mathematical algorithms I'd appreciate some assistance in finding the root cause from the experts on how bignum.c works. I think the bug is relatively serious because it could cause inaccurate output for other mathematical code using Bignums since it was introduced in mid-2011.

This ruby -v comes from ruby trunk SVN at revision 31695, where the failure begins to happen. I hand-re-compiled at the bisection points on trunk from 27655 through 32501 to identify the one which caused the problem.

```
$ ruby -v
ruby 1.9.3dev (2011-05-22 trunk 31695) [x86_64-linux]

C Compiler: gcc (Ubuntu/Linaro 4.6.3-1ubuntu5) 4.6.3

configure params:

./configure \
--with-static-linked-ext \
--prefix=/usr/local/ruby192 \
--enable-shared \
--with-ruby-version=full
```

Related issues:

Related to Ruby trunk - Bug #6974: Functionality Loss in Bignum for Very Larg...	**Assigned**	
Related to Backport193 - Backport #7315: r37565 (bigmul1_toom3 □□□□□) □□□□□□□...	**Closed**	**11/09/2012**

Associated revisions

Revision 22767ffd - 11/08/2012 08:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): disable big_mul_toom3_temporalily. [ruby-core:48552] [Bug #7242]
- test/ruby/test_bignum.rb (test_mul_large_numbers): add a test for bigmul1_toom3 suggested in [Bug #7242].

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37565 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 37565 - 11/08/2012 08:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): disable big_mul_toom3_temporalily. [ruby-core:48552] [Bug #7242]
- test/ruby/test_bignum.rb (test_mul_large_numbers): add a test for bigmul1_toom3 suggested in [Bug #7242].

Revision 37565 - 11/08/2012 08:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): disable big_mul_toom3_temporalily. [ruby-core:48552] [Bug #7242]
- test/ruby/test_bignum.rb (test_mul_large_numbers): add a test for bigmul1_toom3 suggested in [Bug #7242].

Revision 37565 - 11/08/2012 08:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): disable big_mul_toom3_temporalily. [ruby-core:48552] [Bug #7242]
- test/ruby/test_bignum.rb (test_mul_large_numbers): add a test for bigmul1_toom3 suggested in [Bug #7242].

Revision 37565 - 11/08/2012 08:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): disable big_mul_toom3_temporalily. [ruby-core:48552] [Bug #7242]
- test/ruby/test_bignum.rb (test_mul_large_numbers): add a test for bigmul1_toom3 suggested in [Bug #7242].

Revision 37565 - 11/08/2012 08:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): disable big_mul_toom3_temporalily. [ruby-core:48552] [Bug #7242]
- test/ruby/test_bignum.rb (test_mul_large_numbers): add a test for bigmul1_toom3 suggested in [Bug #7242].

Revision 37565 - 11/08/2012 08:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): disable big_mul_toom3_temporalily.
  [ruby-core:48552] [Bug #7242]

- test/ruby/test_bignum.rb (test_mul_large_numbers):
  add a test for bigmul1_toom3 suggested in [Bug #7242].

Revision bb250b00 - 11/08/2012 10:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37567 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 37567 - 11/08/2012 10:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

Revision 37567 - 11/08/2012 10:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

Revision 37567 - 11/08/2012 10:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

Revision 37567 - 11/08/2012 10:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

Revision 37567 - 11/08/2012 10:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

Revision 37567 - 11/08/2012 10:38 PM - mrkn (Kenta Murata)

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

Revision 122b6dbc - 11/09/2012 02:21 AM - usa (Usaku NAKAMURA)

merge revision(s) 37565: [Backport #7315]

```
* bignum.c (bigmul0): disable big_mul_toom3_temporalily.
  [ruby-core:48552] [Bug #7242]

* test/ruby/test_bignum.rb (test_mul_large_numbers):
  add a test for bigmul1_toom3 suggested in [Bug #7242].
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@37570 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 995e4281 - 11/09/2012 04:16 AM - usa (Usaku NAKAMURA)

merge revision(s) 37567: [Backport #7315]

```
* bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

* bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

* bignum.c (bigmul0): disable big_mul_toom3 temporalily.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@37573 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 10/30/2012 08:36 PM - mame (Yusuke Endoh)

- File toom3-bug.py.rb added

- Status changed from Open to Assigned

- Priority changed from Normal to 6

- Target version set to 2.0.0

Hello,

2012/10/30, mhall (Matthew Hall) mhall@mhcomputing.net:

> Attached to this bug I have a simplified example test case which will pass
> without this commit, and fail with this commit present.

Good catch! I created a more simplified example.

```
$ ruby toom3-bug.py.rb
$ python toom3-bug.py.rb
```

Python seems to output the correct answer.
mrkn, could you check it out?

--
Yusuke Endoh mame@tsg.ne.jp

#2 - 11/04/2012 03:04 AM - mrkn (Kenta Murata)

- Category set to core

Although I'm trying to fix it for about two days, I found I need more time to find the direct causes of the bug.
I decide to disable Toom3 method until the bug is fixed.

#3 - 11/06/2012 09:44 AM - mhall (Matthew Hall)

I am curious, what can I do on my end to disable Toom3 in my own Ruby interpreter?

#4 - 11/07/2012 02:12 PM - phasis68 (Heesob Park)

After some inspections, I found the cause of this bug.

One omission of bigtrunc made a different result for the minus Bignum value.

Here is a patch:

diff --git a/bignum.c b/bignum.c.new
index 305a63d..8cf6160 100644
--- a/bignum.c
+++ b/bignum.c.new
@@ -2501,7 +2501,7 @@ bigmul1_toom3(VALUE x, VALUE y)
z2 = bigtrunc(bigadd(u2, u0, 0));

```
 /* z3 <- (z2 - z3) / 2 + 2 * z(inf) == (z2 - z3) / 2 + 2 * u4 */
```

- z3 = bigadd(z2, z3, 0);
- z3 = bigtrunc(bigadd(z2, z3, 0)); bigrsh_bang(BDIGITS(z3), RBIGNUM_LEN(z3), 1); t = big_lshift(u4, 1); /* TODO: combining with next addition */ z3 = bigtrunc(bigadd(z3, t, 1));

#5 - 11/08/2012 01:52 PM - mhall (Matthew Hall)

This patch appears to fix the issue for me. Could we try it on Bug 6974 to confirm the legitimacy of it?

#6 - 11/08/2012 09:25 PM - phasis68 (Heesob Park)

I confirmed this patch also solves Bug 6974.

#7 - 11/08/2012 10:37 PM - mame (Yusuke Endoh)

Awesome, thank you! Mrkn, could you review phasis68's patch?

BTW: I think that he should have a commit bit.

--
Yusuke Endoh mame@tsg.ne.jp

#8 - 11/09/2012 05:38 AM - mrkn (Kenta Murata)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r37565.

Matthew, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- bignum.c (bigmul0): disable big_mul_toom3_temporalily.
  [ruby-core:48552] [Bug #7242]

- test/ruby/test_bignum.rb (test_mul_large_numbers):
  add a test for bigmul1_toom3 suggested in [Bug #7242].

#9 - 11/09/2012 05:41 AM - mrkn (Kenta Murata)

- Status changed from Closed to Open

- Priority changed from 6 to 5

reopen because the bug of bigmul1_toom3 hasn't fixed yet.

#10 - 11/09/2012 07:16 AM - mrkn (Kenta Murata)

Thank you for your contribution, Matthew and Heesob.
I will confirm your patch and apply it asap.

#11 - 11/09/2012 07:38 AM - mrkn (Kenta Murata)

- Status changed from Open to Closed

This issue was solved with changeset r37567.
Matthew, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- bignum.c (bigmul0): enable big_mul_toom3.
  [ruby-core:48552] [Bug #7242]

- bignum.c (bigmul1_toom3): fix incorrect calculation.
  the patch is made by Heesob Park.
  [ruby-core:48552] [Bug #7242]

#12 - 11/09/2012 07:43 AM - mrkn (Kenta Murata)

Wrote by Yusuke Endoh:

> BTW: I think that he should have a commit bit.

I think so too.
He can confirm the calculation algorithms for large Bignum than me, I think.

Files

dhtest.rb	1.2 KB	10/30/2012	mhall (Matthew Hall)
dhtest.yaml	9.36 KB	10/30/2012	mhall (Matthew Hall)
toom3-bug.py.rb	3.64 KB	10/30/2012	mame (Yusuke Endoh)