Ruby master - Bug #1934

Segmentation fault

08/13/2009 06:20 AM - jeheine (Julia Heine)

Status:	Closed		
Priority:	Normal		
Assignee:	authorNari (Narihiro Nakamura)		
Target version:	2.0.0		
ruby -v:	ruby 1.9.1p129 (2009-05-12 revision 23412) [i386-darwin9]	**Backport:**	

Description

=begin
When executing the program attached, I get the following segmentation fault. The segmentation fault is reproducible, but not at a deterministic point in the evaluation (so far somewhere between the 170th and the 205th prime). On previous patch-levels, I also got the segmentation fault.

/Users/julia/Ruby/Euler/euler060a.rb:85: [BUG] Segmentation fault
ruby 1.9.1p129 (2009-05-12 revision 23412) [i386-darwin9]

-- control frame ----------
c:0018 p:0014 s:0064 b:0062 l:000534 d:000061 BLOCK /Users/julia/Ruby/Euler/euler060a.rb:85
c:0017 p:---- s:0059 b:0059 l:000058 d:000058 FINISH
c:0016 p:---- s:0057 b:0057 l:000056 d:000056 CFUNC :each
c:0015 p:0056 s:0054 b:0054 l:000534 d:000053 BLOCK /Users/julia/Ruby/Euler/euler060a.rb:85
c:0014 p:---- s:0049 b:0049 l:000048 d:000048 FINISH
c:0013 p:---- s:0047 b:0047 l:000046 d:000046 CFUNC :each
c:0012 p:0153 s:0044 b:0044 l:000534 d:000043 BLOCK /Users/julia/Ruby/Euler/euler060a.rb:82
c:0011 p:---- s:0039 b:0039 l:000038 d:000038 FINISH
c:0010 p:---- s:0037 b:0037 l:000036 d:000036 CFUNC :call
c:0009 p:0018 s:0033 b:0033 l:000025 d:000032 BLOCK /opt/local/lib/ruby1.9/1.9.1/prime.rb:265
c:0008 p:---- s:0031 b:0031 l:000030 d:000030 FINISH
c:0007 p:---- s:0029 b:0029 l:000028 d:000028 CFUNC :loop
c:0006 p:0049 s:0026 b:0026 l:000025 d:000025 METHOD /opt/local/lib/ruby1.9/1.9.1/prime.rb:264
c:0005 p:0045 s:0021 b:0021 l:000020 d:000020 METHOD /opt/local/lib/ruby1.9/1.9.1/prime.rb:137
c:0004 p:0023 s:0015 b:0015 l:000014 d:000014 METHOD (eval):3
c:0003 p:0104 s:0010 b:0010 l:000534 d:000e04 EVAL /Users/julia/Ruby/Euler/euler060a.rb:58
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:000534 d:000534 TOP :26660

-- Ruby level backtrace information----------
/Users/julia/Ruby/Euler/euler060a.rb:85:in block (3 levels) in <main>'
/Users/julia/Ruby/Euler/euler060a.rb:85:ineach'
/Users/julia/Ruby/Euler/euler060a.rb:85:in block (2 levels) in <main>'
/Users/julia/Ruby/Euler/euler060a.rb:82:ineach'
/Users/julia/Ruby/Euler/euler060a.rb:82:in block in <main>'
/opt/local/lib/ruby1.9/1.9.1/prime.rb:265:incall'
/opt/local/lib/ruby1.9/1.9.1/prime.rb:265:in block in each'
/opt/local/lib/ruby1.9/1.9.1/prime.rb:264:inloop'
/opt/local/lib/ruby1.9/1.9.1/prime.rb:264:in each'
/opt/local/lib/ruby1.9/1.9.1/prime.rb:137:ineach'
(eval):3:in each'
/Users/julia/Ruby/Euler/euler060a.rb:58:in'

-- C level backtrace information ---

[NOTE]
You may encounter a bug of Ruby interpreter. Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html
=end

History

#1 - 12/05/2009 11:49 AM - yugui (Yuki Sonoda)

=begin
I could reproduce the bug, but with ruby 1.9.2dev (2009-11-17 trunk 25805) [i386-darwin9.8.0], can't reproduce.
It seems a 1.9.1 specific bug.
=end

#2 - 06/02/2010 02:43 PM - runpaint (Run Paint Run Run)

=begin
I can reproduce this on trunk by running euler060a.rb:

run@paint:/tmp → ruby 475
# of primes: 2 results: [] prime: 7 process time: 0.1
# of primes: 3 results: [] prime: 11 process time: 0.1
# of primes: 4 results: [] prime: 13 process time: 0.1
# of primes: 5 results: [] prime: 17 process time: 0.1
# of primes: 6 results: [] prime: 19 process time: 0.1
# of primes: 7 results: [] prime: 23 process time: 0.1
# of primes: 8 results: [] prime: 29 process time: 0.1
# of primes: 9 results: [] prime: 31 process time: 0.1
# of primes: 10 results: [] prime: 37 process time: 0.1
# of primes: 11 results: [] prime: 41 process time: 0.11
# of primes: 12 results: [] prime: 43 process time: 0.11
# of primes: 13 results: [] prime: 47 process time: 0.11
# of primes: 14 results: [] prime: 53 process time: 0.11
# of primes: 15 results: [] prime: 59 process time: 0.11
# of primes: 16 results: [] prime: 61 process time: 0.11
# of primes: 17 results: [] prime: 67 process time: 0.12
# of primes: 18 results: [] prime: 71 process time: 0.12
# of primes: 19 results: [] prime: 73 process time: 0.12
# of primes: 20 results: [] prime: 79 process time: 0.13
# of primes: 21 results: [] prime: 83 process time: 0.13
# of primes: 22 results: [] prime: 89 process time: 0.14
# of primes: 23 results: [] prime: 97 process time: 0.14
# of primes: 24 results: [] prime: 101 process time: 0.14
# of primes: 25 results: [] prime: 103 process time: 0.14
# of primes: 26 results: [] prime: 107 process time: 0.15
# of primes: 27 results: [] prime: 109 process time: 0.16
# of primes: 28 results: [] prime: 113 process time: 0.16
# of primes: 29 results: [] prime: 127 process time: 0.16
# of primes: 30 results: [] prime: 131 process time: 0.17
# of primes: 31 results: [] prime: 137 process time: 0.18
# of primes: 32 results: [] prime: 139 process time: 0.19
# of primes: 33 results: [] prime: 149 process time: 0.2
# of primes: 34 results: [] prime: 151 process time: 0.21
# of primes: 35 results: [] prime: 157 process time: 0.22
# of primes: 36 results: [] prime: 163 process time: 0.23
# of primes: 37 results: [] prime: 167 process time: 0.24
# of primes: 38 results: [] prime: 173 process time: 0.26
# of primes: 39 results: [] prime: 179 process time: 0.26
# of primes: 40 results: [] prime: 181 process time: 0.27
# of primes: 41 results: [] prime: 191 process time: 0.28
# of primes: 42 results: [] prime: 193 process time: 0.29
# of primes: 43 results: [] prime: 197 process time: 0.3
# of primes: 44 results: [] prime: 199 process time: 0.32
# of primes: 45 results: [] prime: 211 process time: 0.33
# of primes: 46 results: [] prime: 223 process time: 0.34
# of primes: 47 results: [] prime: 227 process time: 0.36
# of primes: 48 results: [] prime: 229 process time: 0.38
# of primes: 49 results: [] prime: 233 process time: 0.38
# of primes: 50 results: [] prime: 239 process time: 0.4
# of primes: 51 results: [] prime: 241 process time: 0.41
# of primes: 52 results: [] prime: 251 process time: 0.43
# of primes: 53 results: [] prime: 257 process time: 0.44
# of primes: 54 results: [] prime: 263 process time: 0.46
# of primes: 55 results: [] prime: 269 process time: 0.47
# of primes: 56 results: [] prime: 271 process time: 0.5
# of primes: 57 results: [] prime: 277 process time: 0.52
# of primes: 58 results: [] prime: 281 process time: 0.54
# of primes: 59 results: [] prime: 283 process time: 0.56
# of primes: 60 results: [] prime: 293 process time: 0.58
# of primes: 61 results: [] prime: 307 process time: 0.6
# of primes: 62 results: [] prime: 311 process time: 0.62

# of primes: 63 results: [] prime: 313 process time: 0.64
# of primes: 64 results: [] prime: 317 process time: 0.65
# of primes: 65 results: [] prime: 331 process time: 0.7
# of primes: 66 results: [] prime: 337 process time: 0.72
# of primes: 67 results: [] prime: 347 process time: 0.75
# of primes: 68 results: [] prime: 349 process time: 0.78
# of primes: 69 results: [] prime: 353 process time: 0.81
# of primes: 70 results: [] prime: 359 process time: 0.87
# of primes: 71 results: [] prime: 367 process time: 0.9
# of primes: 72 results: [] prime: 373 process time: 0.98
# of primes: 73 results: [] prime: 379 process time: 1.01
# of primes: 74 results: [] prime: 383 process time: 1.06
# of primes: 75 results: [] prime: 389 process time: 1.09
# of primes: 76 results: [] prime: 397 process time: 1.14
# of primes: 77 results: [] prime: 401 process time: 1.17
# of primes: 78 results: [] prime: 409 process time: 1.2
# of primes: 79 results: [] prime: 419 process time: 1.24
# of primes: 80 results: [] prime: 421 process time: 1.28
# of primes: 81 results: [] prime: 431 process time: 1.32
# of primes: 82 results: [] prime: 433 process time: 1.36
# of primes: 83 results: [] prime: 439 process time: 1.4
# of primes: 84 results: [] prime: 443 process time: 1.44
# of primes: 85 results: [] prime: 449 process time: 1.54
# of primes: 86 results: [] prime: 457 process time: 1.59
# of primes: 87 results: [] prime: 461 process time: 1.64
# of primes: 88 results: [] prime: 463 process time: 1.68
# of primes: 89 results: [] prime: 467 process time: 1.81
# of primes: 90 results: [] prime: 479 process time: 1.86
# of primes: 91 results: [] prime: 487 process time: 1.92
# of primes: 92 results: [] prime: 491 process time: 1.99
# of primes: 93 results: [] prime: 499 process time: 2.14
# of primes: 94 results: [] prime: 503 process time: 2.22
# of primes: 95 results: [] prime: 509 process time: 2.29
# of primes: 96 results: [] prime: 521 process time: 2.37
# of primes: 97 results: [] prime: 523 process time: 2.44
# of primes: 98 results: [] prime: 541 process time: 2.63
# of primes: 99 results: [] prime: 547 process time: 2.73
# of primes: 100 results: [] prime: 557 process time: 2.96
# of primes: 101 results: [] prime: 563 process time: 3.06
# of primes: 102 results: [] prime: 569 process time: 3.17
# of primes: 103 results: [] prime: 571 process time: 3.27
# of primes: 104 results: [] prime: 577 process time: 3.39
# of primes: 105 results: [] prime: 587 process time: 3.5
# of primes: 106 results: [] prime: 593 process time: 3.61
# of primes: 107 results: [] prime: 599 process time: 3.72
# of primes: 108 results: [] prime: 601 process time: 3.84
# of primes: 109 results: [] prime: 607 process time: 4.14
# of primes: 110 results: [] prime: 613 process time: 4.46
# of primes: 111 results: [] prime: 617 process time: 4.92
# of primes: 112 results: [] prime: 619 process time: 5.09
# of primes: 113 results: [] prime: 631 process time: 5.28
# of primes: 114 results: [] prime: 641 process time: 5.46
# of primes: 115 results: [] prime: 643 process time: 5.64
# of primes: 116 results: [] prime: 647 process time: 5.84
# of primes: 117 results: [] prime: 653 process time: 6.03
# of primes: 118 results: [] prime: 659 process time: 6.21
# of primes: 119 results: [] prime: 661 process time: 6.42
# of primes: 120 results: [] prime: 673 process time: 6.96
# of primes: 121 results: [] prime: 677 process time: 7.18
# of primes: 122 results: [] prime: 683 process time: 7.44
# of primes: 123 results: [] prime: 691 process time: 7.69
# of primes: 124 results: [] prime: 701 process time: 8.3
# of primes: 125 results: [] prime: 709 process time: 8.56
# of primes: 126 results: [] prime: 719 process time: 9.25
# of primes: 127 results: [] prime: 727 process time: 9.59
# of primes: 128 results: [] prime: 733 process time: 10.42
# of primes: 129 results: [] prime: 739 process time: 11.37
# of primes: 130 results: [] prime: 743 process time: 11.8
# of primes: 131 results: [] prime: 751 process time: 12.25
# of primes: 132 results: [] prime: 757 process time: 12.78
# of primes: 133 results: [] prime: 761 process time: 13.22
# of primes: 134 results: [] prime: 769 process time: 13.66
# of primes: 135 results: [] prime: 773 process time: 14.11
# of primes: 136 results: [] prime: 787 process time: 14.55
# of primes: 137 results: [] prime: 797 process time: 15.0

```
# of primes: 138 results: []  prime: 809  process time: 15.42
# of primes: 139 results: []  prime: 811  process time: 15.87
# of primes: 140 results: []  prime: 821  process time: 16.32
# of primes: 141 results: []  prime: 823  process time: 17.48
# of primes: 142 results: []  prime: 827  process time: 17.99
# of primes: 143 results: []  prime: 829  process time: 18.69
# of primes: 144 results: []  prime: 839  process time: 19.19
# of primes: 145 results: []  prime: 853  process time: 19.82
475:83: [BUG] Segmentation fault
ruby 1.9.3dev (2010-06-01 trunk 28120) [i686-linux]

-- control frame ----------
c:0018 p:---- s:0060 b:0060 l:000059 d:000059 CFUNC  :combination
c:0017 p:---- s:0058 b:0058 l:000057 d:000057 CFUNC  :each
c:0016 p:---- s:0056 b:0056 l:000055 d:000055 CFUNC  :to_a
c:0015 p:0025 s:0053 b:0053 l:001ee4 d:000052 BLOCK  475:83
c:0014 p:---- s:0048 b:0048 l:000047 d:000047 FINISH
c:0013 p:---- s:0046 b:0046 l:000045 d:000045 CFUNC  :each
c:0012 p:0155 s:0043 b:0043 l:001ee4 d:000042 BLOCK  475:82
c:0011 p:---- s:0038 b:0038 l:000037 d:000037 FINISH
c:0010 p:---- s:0036 b:0036 l:000035 d:000035 CFUNC  :call
c:0009 p:0018 s:0032 b:0032 l:000024 d:000031 BLOCK  /usr/local/lib/ruby/1.9.1/prime.rb:270
c:0008 p:---- s:0030 b:0030 l:000029 d:000029 FINISH
c:0007 p:---- s:0028 b:0028 l:000027 d:000027 CFUNC  :loop
c:0006 p:0052 s:0025 b:0025 l:000024 d:000024 METHOD /usr/local/lib/ruby/1.9.1/prime.rb:269
c:0005 p:0045 s:0020 b:0020 l:000019 d:000019 METHOD /usr/local/lib/ruby/1.9.1/prime.rb:137
c:0004 p:0025 s:0014 b:0014 l:000013 d:000013 METHOD /usr/local/lib/ruby/1.9.1/forwardable.rb:182
c:0003 p:0086 s:0009 b:0009 l:001ee4 d:000e90 EVAL   475:58
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:001ee4 d:001ee4 TOP
```

```
-- Ruby level backtrace information ----------------------------------------
475:58:in <main>'
/usr/local/lib/ruby/1.9.1/forwardable.rb:182:ineach'
/usr/local/lib/ruby/1.9.1/prime.rb:137:in each'
/usr/local/lib/ruby/1.9.1/prime.rb:269:ineach'
/usr/local/lib/ruby/1.9.1/prime.rb:269:in loop'
/usr/local/lib/ruby/1.9.1/prime.rb:270:inblock in each'
/usr/local/lib/ruby/1.9.1/prime.rb:270:in call'
475:82:inblock in '
475:82:in each'
475:83:inblock (2 levels) in '
475:83:in to_a'
475:83:ineach'
475:83:in `combination'

-- C level backtrace information -------------------------------------------
ruby(rb_vm_bugreport+0xa5) [0x8161375]
ruby() [0x81a0069]
ruby(rb_bug+0x28) [0x81a0118]
ruby() [0x80f4088]
[0xd9a410]
ruby() [0x817300c]
ruby() [0x817512d]
ruby() [0x81520b9]
ruby() [0x8157895]
ruby(rb_iterate+0xac) [0x814d11c]
ruby(rb_block_call+0x3f) [0x814d2af]
ruby() [0x819da59]
ruby() [0x81520b9]
ruby() [0x8157895]
ruby(rb_iterate+0xac) [0x814d11c]
ruby(rb_block_call+0x3f) [0x814d2af]
ruby() [0x819952d]
ruby() [0x814cf55]
ruby() [0x8158541]
ruby() [0x815a8e8]
ruby() [0x815e2c6]
ruby(rb_yield+0x50) [0x815f6c0]
ruby(rb_ary_each+0x41) [0x8170dc1]
ruby() [0x8158541]
ruby() [0x815a8e8]
ruby() [0x815e2c6]
ruby(rb_vm_invoke_proc+0x76) [0x8151ba6]
```

ruby() [0x8064394]
ruby() [0x814cf55]
ruby() [0x8158541]
ruby() [0x815a8e8]
ruby() [0x815e2c6]
ruby() [0x815fc3e]
ruby(rb_rescue2+0x141) [0x805e1e1]
ruby() [0x814de04]
ruby() [0x8158541]
ruby() [0x815a8e8]
ruby() [0x815e2c6]
ruby(rb_iseq_eval_main+0x1c7) [0x815e697]
ruby() [0x805e432]
ruby(ruby_run_node+0x32) [0x805fc42]
ruby(main+0x5a) [0x805d66a]
/lib/tls/i686/cmov/libc.so.6(__libc_start_main+0xe6) [0x14cbd6]
ruby() [0x805d571]

[NOTE]
You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html

Aborted

=end

#3 - 06/27/2010 11:47 PM - mame (Yusuke Endoh)

- Status changed from Open to Assigned

- Assignee set to authorNari (Narihiro Nakamura)

- Target version set to 2.0.0

=begin
Hi,

I confirmed this issue at r28115 of trunk.
This issue has been fixed at r28191 in ruby_1_9_2, but not in trunk
because the code is quite different between 1_9_2 and trunk because
of lazy sweep feature, which is included only in trunk.
Narihiro, who is the author of lazy sweep, is assigned.

Here is a log by valgrind:

...
# of primes: 129 results: [] prime: 739 process time: 189.97
# of primes: 130 results: [] prime: 743 process time: 197.16
# of primes: 131 results: [] prime: 751 process time: 205.02
==24732==
==24732== Invalid read of size 4
==24732==   at 0x8068492: rb_newobj (gc.c:1049)
==24732==   by 0x817CDFB: ary_new (array.c:297)
==24732==   by 0x817EA16: rb_ary_combination (array.c:331)
==24732==   by 0x815AC61: vm_call0 (vm_eval.c:78)
==24732==   by 0x815B98F: iterate_method (vm_eval.c:234)
==24732==   by 0x81557C7: rb_iterate (vm_eval.c:851)
==24732==   by 0x815595E: rb_block_call (vm_eval.c:931)
==24732==   by 0x81A95FA: enumerator_each (enumerator.c:317)
==24732==   by 0x815AC61: vm_call0 (vm_eval.c:78)
==24732==   by 0x815B98F: iterate_method (vm_eval.c:234)
==24732==   by 0x81557C7: rb_iterate (vm_eval.c:851)
==24732==   by 0x815595E: rb_block_call (vm_eval.c:931)
==24732== Address 0x501c4d4 is 116 bytes inside a block of size 16,384 free'd
==24732==   at 0x4022B8A: free (vg_replace_malloc.c:323)
==24732==   by 0x806375C: free_unused_heaps (gc.c:1869)
==24732==   by 0x816E2C4: rb_threadptr_execute_interrupts_rec (thread.c:1295)
==24732==   by 0x816E58E: rb_thread_check_ints (thread.c:968)
==24732==   by 0x81A616E: collect_all (enum.c:379)
==24732==   by 0x8159C67: vm_yield_with_cfunc (vm_insnhelper.c:724)
==24732==   by 0x8165CDE: rb_yield (vm.c:587)
==24732==   by 0x817EA75: rb_ary_combination (array.c:4078)
==24732==   by 0x815AC61: vm_call0 (vm_eval.c:78)
==24732==   by 0x815B98F: iterate_method (vm_eval.c:234)

==24732== by 0x81557C7: rb_iterate (vm_eval.c:851)
==24732== by 0x815595E: rb_block_call (vm_eval.c:931)

--
Yusuke Endoh mame@tsg.ne.jp
=end

#4 - 06/29/2010 12:17 PM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

=begin
This issue was solved with changeset r28472.
Julia, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

=end

Files

euler060a.rb	3.47 KB	08/13/2009	jeheine (Julia Heine)