

# Re: question: random number in residue number representation

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-02/msg00462.html>

---

- *From:* "jiangwu.mail@xxxxxxxx" <jiangwu.mail@xxxxxxxx>
  - *Date:* Wed, 6 Feb 2008 05:03:44 -0800 (PST)
- 

On Feb 5, 1:48 pm, hru...@xxxxxxxxxxxxxxxxxxxxxx (Herman Rubin) wrote:

In article <dfc03304-b08c-48ed-bac9-865aeba6b...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>,

jiangwu.m...@xxxxxxxx <jiangwu.m...@xxxxxxxx> wrote:

On Feb 1, 10:21 pm, d...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx (David Wagner) wrote:

Herman Rubin wrote:

jiangwu.m...@xxxxxxxx  
<jiangwu.m...@xxxxxxxx> wrote:

Let  $p_1, \dots, p_n$  be  $n$  prime numbers. Let  $g = p_1 p_2 \dots p_n$ . Any number  $0 \leq x \leq g$  can be represented as  $x_1, \dots, x_n$ , where  $x_i = x \pmod{p_i}$ . The question is to generate a random number  $r$  in residue number representation  $(r_1, \dots, r_n)$  and  $0 \leq r \leq g$  where  $b \approx \sqrt{g}$ .

Just generate separately  $0 \leq x_i < p_i$ . This can be done in time  $O(\log p_i)$ , and so one gets  $O(\log g)$  altogether.

But that generates a random  $x$  in the range  $0 \leq x < g$ , whereas the poster asked to generate a random  $x$  in approximately the

Re: question: random number in residue number representation

range  
 $0 \leq x \leq \sqrt{g}$ .

Exactly. Actually the problem can be better formulated: to generate an  $x$  such that  $0 \leq x < p_1 p_2 \dots p_l$  for a given  $l < n$ .

In this case,  $x$  is determined by its residues mod  $p_1, \dots, p_l$ .

I do not see any solution other than getting the residues mod  $p_{l+1}, \dots, p_n$  from the result of those. One way of doing this, if the same  $p$ 's occur often, is to preset the constants needed to carry out the computation.

You mean in the case that  $p_i = p_j$ ? but all  $p_i, p_j$  need to be coprime here.

--

This address is for information only. I do not claim that these views are those of the Statistics Department or of Purdue University.  
Herman Rubin, Department of Statistics, Purdue University  
hru...@xxxxxxxxxxxxxxxxx Phone: (765)494-6054 FAX: (765)494-0558