

Re: question: random number in residue number representation

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-02/msg00068.html>

- *From:* hkrubin@xxxxxxxxxxxxxxxxxxxxxxxx (Herman Rubin)
 - *Date:* 5 Feb 2008 13:48:05 -0500
-

In article <df03304-b08c-48ed-bac9-865aeba6b05d@xx>, jiangwu.mail@xxxxxxxxxx <jiangwu.mail@xxxxxxxxxx> wrote:

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

Herman Rubin wrote:

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

Let p_1, \dots, p_n be n prime numbers. Let $g = p_1 p_2 \dots p_n$. Any number $0 \leq x < g$ can be represented as x_1, \dots, x_n , where $x_i = x \bmod p_i$.

The question is to generate a random number r in residue number representation (r_1, \dots, r_n) and $0 \leq r < g$ 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 range $0 \leq x < \sqrt{g}$.

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 $l < n$.

Re: question: random number in residue number representation

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.

—

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

hrubin@xxxxxxxxxxxxxxxxx Phone: (765)494-6054 FAX: (765)494-0558

.