Rational Number Reconstruction

September 28, 2023 8:44 AM

(Paul Wang 1981)

Suppose $\frac{n}{d} \in \mathbb{Q}$, $n, d \in \mathbb{Z}$ and $d > 0$, $\gcd(n,d) = 1$.

Suppose we have computed $u = n/d \bmod \underline{m}$ where $0 \le u < m$ and $\gcd(m,d) = 1$.

[Context: $m = p_1 p_2 p_3 \cdots p_k$ or $m = p^k$]

How can we recover $\frac{n}{d}$ from $u \bmod m$.? $\frac{-2}{3}$?

E.g. $m = 35$, $\frac{n}{d} = \frac{-2}{3}$ $u = -2 \cdot 12 = -24 = +11 \bmod 35$.

How big does m need to be to recover n/d?

Can we recover $\frac{114}{109}$ from $\frac{114}{109} \bmod 35 = 11 \bmod 35$. No

We need $m > 2|n| \cdot d$.

↑ ±

Run Ext. Euc. Alg. with input $m > u \ge 0$. (r_0, r_1)

We will obtain integers s_i, t_i, r_i satisfying

$$s_i \cdot m + t_i \cdot u = r_i \quad \text{for } 0 \le i \le N+1 \text{ where } r_{N+1} = 0.$$

(mod m) $\Rightarrow$ $t_i \cdot u \equiv r_i \bmod m$.

If $\gcd(t_i, m) = 1 \Rightarrow u \equiv \frac{r_i}{t_i} \bmod m$.

$i \ne 0$	$i \ne N+1$
$t_0 = 0$	$t_{N+1} = m$

i.e., the EEA gives us a sequence of rationals

$$\frac{r_i}{t_i} \equiv u \bmod m. \text{ for } 1 \le i \le N.$$

Is $\frac{n}{d} = \frac{r_i}{t_i}$ for some i? Yes provided $m > 2|n|d$.

Which one?

Theorem (Guy, Davenport, Wang) 1982.

Let $n, d \in \mathbb{Z}$, $d > 0$, $\gcd(n,d) = 1$.

Let $m \in \mathbb{Z}$, $m > 0$, $\gcd(m,d) = 1$

Let $n, d \in \mathbb{Z}$, $d > 0$, $\gcd(n,d) = 1$.
Let $m \in \mathbb{Z}$, $m > 0$, $\gcd(m,d) = 1$.
Let $u = \frac{n}{d} \bmod m$ with $0 \le u < m$.

Let $N \geq |n|$ and $D \geq d$. Then

(i) If $m > 2ND$ then $\phi_m\left(\frac{n}{d}\right)$ is one to one.

E.g. $\mathbb{Z}_{13}$

$m = 13$
$N = 3$
$D = 2$
$2ND = 12 < m$.

$\mathbb{Z}_{13}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{-1}{1}$	$\frac{2}{1}$	$\frac{-2}{1}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{3}{1}$	$\frac{-3}{1}$	$\frac{3}{2}$	$\frac{-3}{2}$
$\phi_{m=13}$	0	1	12	2	11	7	6	3	10	8	5

(ii) If $m > 2ND$ then on input of m, u there exists a unique index i in the EEA s.t. $\frac{r_i}{t_i} = \frac{n}{d}$.
Moreover i is the first index s.t. $r_i \le N$.

If we have good bounds $N \geq |n|$ and $D \geq d$ then we compute $m = p^k > 2ND$ and run RR.

Consider $Ax = b$ $k = 1$ is sufficient

$\rightarrow \begin{bmatrix} \text{[redacted]} & \text{[redacted]} \\ \text{[redacted]} & \text{[redacted]} \end{bmatrix} \begin{bmatrix} 1/2 \\ -1/2 \end{bmatrix} = \begin{bmatrix} \text{[redacted]} \\ \text{[redacted]} \end{bmatrix}$

Wang: Set $N = D = \left\lfloor \frac{\sqrt{m}}{2} \right\rfloor$ and try RR.
If it succeeds check: if $Ax = b$ then output x.