iratrecon

September 24, 2021 8:17 AM

Rational Reconstruction (Wang 1981)

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

Suppose we have computed $u = \frac{n}{d} \bmod m$. where $0 \le u < m$.
and $\gcd(d,m)=1$. Context: $m = p_1 p_2 p_3 \cdots$ or $m = p^k$.

How can we recover n/d from u, m?

E.g. $m = 5 \cdot 7 = 35$ $\frac{n}{d} = -\frac{2}{3}$ $u = -2 \cdot 12 = -24 = +11 \bmod 35$

How big does m need to be?

Can we recover $\frac{114}{109}$ from $\frac{114}{109} \bmod 35 = 11$?

$\Rightarrow m > 2 \cdot 114 \cdot 109$.

Run EEA with input $m, u \ge 0$.

$r_0, r_1 \leftarrow m, u$ $s_0, s_1 \leftarrow 1, 0$ $t_0, t_1 \leftarrow 0, 1$
$i \leftarrow 1$.
while $r_i \ne 0$ do
  $q_{i+1} \leftarrow \lfloor \frac{r_{i-1}}{r_i} \rfloor$
  $r_{i+1} \leftarrow r_{i-1} - q_{i+1} r_i$
  $s_{i+1} \leftarrow s_{i-1} - q_{i+1} s_i$
  $t_{i+1} \leftarrow t_{i-1} - q_{i+1} t_i$
end while
$N \leftarrow i-1$. // $r_N = \gcd(r_0, r_1)$. $r_{N+1} = 0$.

The integers r_i, s_i and t_i satisfy

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

(mod m) $t_i \cdot u \equiv r_i \pmod m$

$\gcd(m, t_i) = 1 \Rightarrow u \equiv r_i / t_i \pmod m$

$i=0$ $i=N+1$
$t_0 = 0$ $t_{N+1} = m$
$s_{N+1} = u$

i.e. the EEA gives us a sequence of rationals $r_i/t_i \equiv u \pmod m$.

Is $r_i/t_i = \frac{n}{d}$ for some $0 < i < N+1$?
Yes provided $m > |2nd|$ and $\gcd(d,m) = 1$.
Which index i?

Theorem (Fu, Davenport, Wang). 1982.

Which make c.

Theorem (Guy, Davenport, Wang). 1982.

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

$2^{-1} = 7$.

(i) if $m > 2ND$ then u is unique in $\mathbb{Z}_m$.

$m = 13$
$\boxed{N = 3,\ D = 2}$
$2 \cdot N \cdot D = 12$

$\frac{n}{d}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{-1}{1}$	$\frac{2}{1}$	$\frac{-2}{1}$	$\frac{3}{1}$	$\frac{-3}{1}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{3}{2}$	$-\frac{3}{2}$
u	0	1	12	2	10	3	9	7	6	8	5

$\frac{2}{3} \bmod 13 = 5$

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

If we have good bounds $N \ge |n|$ and $D \ge d$ e.g. $N = 10n$ and $D = 10d$. then compute $m = p^k$ until $m > 2ND$. and apply (ii).

If we don't have good bounds?
E.g. Solve $Ax = b$ where $[\ \ ]\begin{bmatrix} 1/2 \\ 1/3 \end{bmatrix} = [\ \ ]$

Wang: Set $N = D = \lfloor \sqrt{m/2} \rfloor$.
Try (ii) to get y
Check if $Ay = b$.

$\boxed{\text{EEA Cost. } O((\log_B m)^2).}$

Maximal Quotient Rational Reconstruction. Monagan 2004.

Algorithm. Output $\frac{r_i}{t_i}$ with $\underline{q_{i+1}}$ maximal.

Lemma. 1.

$$\frac{m}{3} < q_{i+1} \boxed{|t_i| r_i} < \underline{m} \quad \text{for } 1 \le i \le N.$$

If $m \gg 2|n|d$ then q_{i+1} must be large.

If $m \gg 2|n|d$ then q_{i+1} must be large.

Maple: iratrecon(u, m) $\longrightarrow$ FAIL or n/d.

iratrecon($\begin{bmatrix} x \\ x \\ x \\ x \end{bmatrix}$, m) $\qquad N = D = \sqrt{\frac{m}{2}}$ default

$\cdot x^3 + \cdot x^2 + \cdot xy + \cdot$

iratrecon(u, m, maxquo=$\underline{1000000}$).