

3-parameter family of (integer) 4-tuples \vec{s} that satisfy $\vec{s}^3 \bullet \vec{J} = \text{Gcd}(\vec{J})$.

In other words, there is an injective (i.e, 1-to-1) function $f: \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ with the property that

$$f(a, b, c) \bullet \vec{J} = \text{Gcd}(\vec{J}),$$

for each triple a, b, c of integers. □

Solving a linear congruence

Having fixed a *modulus* $M \in \mathbb{Z}_+$, as well as a *coefficient* and *target* $B, T \in \mathbb{Z}$, our goal is to find all solutions x to

$$3: \quad B \cdot x \equiv_M T, \quad \text{where } x \in [0..M).$$

Our algorithm has three **STEPS**.

This congruence has a solution IFF there exists a *pair* (x, k) solving eqn

$$3*: \quad B \cdot x + M \cdot k = T, \quad \text{where } x, k \in \mathbb{Z}.$$

Evidently $D := \text{Gcd}(B, M)$ divides LhS(3*). Hence if $T \not\vdash D$, then (3*) has no soln-pair. Whence

STEP A: If $D := \text{Gcd}(B, M)$ fails to divide T , then (3) has no soln. Else, define

$$\beta := \frac{B}{D}, \quad \mu := \frac{M}{D} \quad \text{and} \quad \tau := \frac{T}{D}$$

and study this “reduced congruence”:

$$4: \quad \beta \cdot y \equiv_\mu \tau, \quad \text{where } y \in [0.. \mu).$$

We have gained that $\beta \perp \mu$.

STEP B: Use LBoI to compute a mod- μ multiplicative-inverse, I , of β ; so $I \cdot \beta \equiv_\mu 1$. Thus

$$y \equiv_\mu I \cdot \beta \cdot y \equiv_\mu I \cdot \tau.$$

Let y_0 be the unique value in $[0.. \mu)$ st. $y_0 \equiv_\mu I \cdot \tau$.

This y_0 is in the *unique* mod- μ residue class solving (4). But mod- M , this residue class splits into D many residue classes. So here is the last step:

STEP C: The D many solutions to (3) are

$$x = y_0, y_1, y_2, y_3, \dots, y_{D-2}, y_{D-1},$$

where $y_k := y_0 + [k\mu]$.

A worked example. I use an arrow over a letter to abbreviate a sequence, e.g

$$\vec{b} := (b_0, b_1, b_2, \dots).$$

We consider

$$35x \equiv_{21} 55.$$

Let’s apply **STEP A**. Since $\text{Gcd}(35, 21) \stackrel{\text{note}}{=} 7$ does not divide 55, the above congruence has no soln. [The same computation shows that congr. $21x \equiv_{35} 55$ has no solution.]

A congruence with solns. Consider congruence

$$3': \quad 33 \cdot x \equiv_{114} 18, \quad \text{where } x \in [0..114).$$

For **STEP A**, we compute just the \vec{r} and \vec{q} columns:

n	r_n	q_n
0	114	—
1	33	3
2	15	2
3	3	5
4	0	∞

Since $D := \text{Gcd}(33, 114) \stackrel{\text{note}}{=} 3$ divides the target, 18, we divide each of the numbers in (3') by $D=3$ to obtain the reduced congruence

$$4': \quad 11 \cdot y \equiv_{38} 6, \quad \text{where } y \in [0..38).$$

For **STEP B**, we compute (using \vec{q}) just^{♥1} the \vec{t} column. (Note: We have \vec{q} from the previous table.)

n	r_n	q_n	s_n	t_n
0	38	—	1	0
1	11	3	0	1
2	5	2	1	-3
3	1	5	-2	7
4	0	∞	11	-38

So the mod-38 reciprocal of 11 is 7. From **STEP B**, then,

$$y \equiv_{38} 7 \cdot 6 = 42 \equiv_{38} 4.$$

So we set $y_0 := 4$.

^{♥1}We do not need to compute \vec{s} nor \vec{r} . Of course, the new \vec{r} is just the old \vec{r} divided by D . I have grayed-out the superfluous columns.

Finally, **STEP C** tells us that these three,

$$4, \quad 4 + 38 \stackrel{\text{note}}{\equiv} 42, \quad 42 + 38 \stackrel{\text{note}}{\equiv} 80$$

are the $D=3$ many solutions to (3').

Checking. We calculate:

$$\begin{aligned} 33 \cdot 4 &= 132 = 1 \cdot 114 + 18; \\ 33 \cdot 42 &= 1386 = 12 \cdot 114 + 18; \\ 33 \cdot 80 &= 2640 = 23 \cdot 114 + 18. \end{aligned}$$

Copasetic!

Filename: Problems/NumberTheory/nt-algorithms.tex
As of: Thursday 24Sep2009. Typeset: 11Jul2018 at 17:37.