

# Congruences in Number Theory

Jonathan L.F. King  
 University of Florida, Gainesville FL 32611-2082, USA  
 squash@ufl.edu  
 Webpage <http://www.math.ufl.edu/~squash/>  
 23 September, 2014 (at 12:24)

**Entrance.** Let  $\text{Primes}(L)$  mean the set of primes that divide  $L$ . An **arithmetic progression** means a set  $T + \mathbf{M}\mathbb{Z}$  of integers, where the **gap** (or **modulus**)  $\mathbf{M}$  is a posint and **translation** (or **target**)  $T$  an integer. Use **comb**, also, for “arithmetic progression”.

A comb  $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$  is **coprime** if  $T \perp \mathbf{M}$ .

## Divisibility Conundra

Here is a soln to LeVeque’s #7P:63: Fix a coprime comb  $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$  and posint  $L$ . Prove there exists  $x \in \mathcal{C}$  st.  $x \perp L$ .

**Short solution.** Let  $F$  be the maximum factor of  $L$  such that  $F \perp \mathbf{M}$ . Letting  $Q := \frac{L}{F}$ , then,

$$1: \quad \text{Primes}(Q) \subset \text{Primes}(\mathbf{M}).$$

Since  $F \perp \mathbf{M}$ , the CRT<sup>♥1</sup> applies to produce an integer  $x$  with

$$2: \quad x \equiv_{\mathbf{M}} T \quad \text{and} \quad x \equiv_F 1.$$

So in order to show that  $x \perp L$ , we need show that  $x \perp Q$ . FTSOC, suppose  $p$  is a prime with  $p \mid x$  and  $p \mid Q$ . This latter forces  $p \mid \mathbf{M}$ , by (1). Now LhS(2) forces  $T \mid p$ . This contradicts that  $T \perp \mathbf{M}$ . ♦

**Longer solution.** We use nested combs.

**3: Lemma.** Fix a coprime comb  $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$ . Each posint  $L$  yields a coprime subcomb  $\widehat{\mathcal{C}} \subset \mathcal{C}$ , where

$$*: \quad \widehat{\mathcal{C}} := \widehat{T} + \widehat{\mathbf{M}} \cdot \mathbb{Z}, \quad \diamond$$

with  $\widehat{\mathbf{M}} := \text{Lcm}(\mathbf{M}, L)$ .

**Proof.** Each integer  $\widehat{T} \in \mathcal{C}$  is  $\perp \mathbf{M}$  and defines a subcomb via (\*). So ISTProduce a  $\widehat{T} \in \mathcal{C}$  with

$$\forall: \quad \widehat{T} \perp L,$$

<sup>♥1</sup>Chinese Remainder Thm: Given arb. “targets”  $s, t \in \mathbb{Z}$ ,  $\exists x$  with  $x \equiv_{\mathbf{M}} s$  and  $x \equiv_F t$ .

for then, automatically,  $\widehat{T}$  will be  $\perp \text{Lcm}(\mathbf{M}, L)$ .

Consider  $L = p_1^{k_1} \cdots p_K^{k_K}$ , the prime factorization. If we find a  $\widehat{T} \in \mathcal{C}$  coprime to  $p_1 \cdots p_K$  then certainly  $\widehat{T} \perp L$ . So WLOG  $L$  is square-free.

We’ll now show that, WLOG,

$$\pounds: \quad L \text{ is coprime to } \mathbf{M}.$$

Letting  $D := \text{Gcd}(\mathbf{M}, L)$ , necessarily,  $\frac{L}{D} \perp \mathbf{M}$ , since  $L$  is square-free. And each  $\widehat{T} \in \mathcal{C}$  is  $\perp D$ , so we just need to find one which is coprime to  $\frac{L}{D}$ .

Courtesy ( $\pounds$ ), we can pick a mod- $G$  reciprocal, call it  $\beta$ , of  $L$ . I.e.  $\beta L \equiv_{\mathbf{M}} 1$ . Our goal ( $\forall$ ) [we have a **yen** for it (...no, I’m not sorry)] is certainly satisfied by a  $\widehat{T} \in \mathcal{C}$  with  $\widehat{T} \equiv_N 1$ . So we want an integer  $y$  with

$$\widehat{T} := 1 + Ny \stackrel{\text{Want}}{\in} \mathcal{C},$$

i.e. with  $1 + Ny \equiv_{\mathbf{M}} T$ , i.e. with  $Ny \equiv_{\mathbf{M}} T - 1$ . It looks like  $y := \beta[T - 1]$  will do the trick. So we *define*

$$\widehat{T} := 1 + N\beta[T - 1]. \quad \blacklozenge$$

**Remark.** The above proof is entirely constructive. We actually could avoid the “square-free” step, at the cost of verbiage. □

**4: Very weak Dirichlet Thm<sup>♥2</sup>.** Each coprime comb  $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$  includes an infinite pairwise coprime subset  $\{T_j\}_{j=1}^{\infty}$  of (distinct) integers. ♦

**Proof.** Let  $T_1 := T$  and  $T_0 := \mathbf{M}$  and  $\mathcal{C}_1 := T_1 + T_0\mathbb{Z}$ . ISTProduce nested combs

$$\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3 \supset \dots \quad \text{of the form}$$

$$\mathcal{C}_j = T_j + [T_{j-1} \cdots T_1 \cdot T_0]\mathbb{Z},$$

each a coprime comb.

Ok, at stage  $j$ , apply Lemma 3 to  $\mathcal{C}_j$  with  $N := T_j$ . It hands us a translation amount  $T_{j+1} := \widehat{T}$  which is coprime to

$$\text{Lcm}(T_j, [T_{j-1} \cdots T_1 \cdot T_0]) \stackrel{\text{note}}{=} T_j \cdot T_{j-1} \cdots T_1 \cdot T_0.$$

*Looks like a wrap, Folks.* ♦

<sup>♥2</sup>A much stronger result, Dirichlet’s Theorem, asserts that every coprime comb includes infinitely many prime numbers.

**5: Two Comb Lemma.** Two combs  $\mathcal{C}_j := T_j + \mathbf{M}_j\mathbb{Z}$  intersect IFF

$$\dagger: \quad \text{Gcd}(\mathbf{M}_1, \mathbf{M}_2) \bullet [T_1 - T_2] \quad \diamond$$

*Proof.* An integer  $x$  is in  $\mathcal{C}_1 \cap \mathcal{C}_2$  means there exist integers  $z_i$  with  $x + z_i\mathbf{M}_i = T_i$ . Subtracting yields  $z_1\mathbf{M}_1 - z_2\mathbf{M}_2 = T_1 - T_2$ . This has a soln  $(z_1, z_2)$  exactly when  $(\dagger)$ . When it does, use either  $z_i$  to determine  $x$ .  $\blacklozenge$

*Two remarks.* Suppose  $(\dagger)$ . The above gives an algorithm to compute an  $x$ . I call this **fusing** two (linear) congruences into a single congruence. Renaming this  $x$  to  $V$  and setting  $L := \text{Lcm}(\mathbf{M}_1, \mathbf{M}_2)$ , the algorithm fuses the pair  $y \equiv_{\mathbf{M}_j} T_j$  of congruences, into a single  $y \equiv_L V$  congruence.

The next result, the Pairwise-comb Thm, reminds me of Helly's theorem on convex sets.  $\square$

**6: Pairwise-comb Thm.** Consider combs  $\mathcal{C}_1, \dots, \mathcal{C}_N$ , where  $\mathcal{C}_j := T_j + \mathbf{M}_j\mathbb{Z}$ . Then the combs mutually intersect IFF each pair intersects. The non-void intersection  $\bigcap_1^N \mathcal{C}_j$  has form  $T + L\mathbb{Z}$ , where  $L$  is  $\text{Lcm}(\mathbf{M}_1, \dots, \mathbf{M}_N)$ .

Since  $x \in \mathcal{C}_j$  means

$$\mathcal{C}_j: \quad x \equiv_{\mathbf{M}_j} T_j.$$

Then the combs mutually intersect, producing a comb  $T + L\mathbb{Z}$ , where  $L$  is  $\text{Lcm}(\mathbf{M}_1, \dots, \mathbf{M}_N)$ .

Indeed, the combs mutually intersect IFF

$$\ddagger: \quad \text{For each pair } j < k \text{ in } [1..N]: \quad \text{Gcd}(\mathbf{M}_j, \mathbf{M}_k) \bullet [T_j - T_k]. \quad \diamond$$

*Reduction.* Courtesy  $(5\dagger)$ , condition  $(\ddagger)$  is necessary, so we will just show sufficiency.

It suffices to prove the  $N=3$  case, since a simple induction on  $N$  handles the general case. Considering a congruence  $\boxed{\sigma: x \equiv_K S}$ , our goal has become:

$$\ddagger\dagger: \quad \text{If each pair of } (C1), (C2) \text{ and } (\sigma) \text{ can fuse, then } \text{Fuse}(C1, C2) \text{ can be fused with } (\sigma). \quad \square$$

*Pf of  $(\ddagger\dagger)$ .* Write  $\text{Fuse}(C1, C2)$  as  $x \equiv_L V$ , where  $L := \text{Lcm}(\mathbf{M}_1, \mathbf{M}_2)$ . Thus each  $T_j \equiv_{\mathbf{M}_j} V$ . Hence  $V - S \equiv_{\mathbf{M}_j} T_j - S$ . With  $\widehat{\mathbf{M}}_j := \text{Gcd}(\mathbf{M}_j, K)$ , then,

$$V - S \equiv_{\widehat{\mathbf{M}}_j} T_j - S,$$

since  $\widehat{\mathbf{M}}_i \bullet \mathbf{M}_i$ . By hyp.,  $(Ci)$  and  $(\sigma)$  can fuse, i.e

$$T_i - S \equiv_{\widehat{\mathbf{M}}_i} 0,$$

Together, these give  $[V - S] \bullet \widehat{\mathbf{M}}_i$ . The upshot is

$$\text{Lcm}(\widehat{\mathbf{M}}_1, \widehat{\mathbf{M}}_2) \bullet [V - S].$$

The last ingredient is that Gcd distributes over Lcm. Here,

$$\text{Gcd}(L, K) = \text{Lcm}(\widehat{\mathbf{M}}_1, \widehat{\mathbf{M}}_2).$$

Thus  $\text{Gcd}(L, K)$  divides  $[V - S]$ , as desired.  $\blacklozenge$

*Proof (unfinished).* ISTProve that the  $N$  combs intersect. By induction on  $N$ , IStEstablish the  $N=3$  case.

Given three pairwise-intersecting combs, translate all three so that two intersect at the origin. So we may write these three combs as

$$7: \quad A\mathbb{Z}, \quad B\mathbb{Z}, \quad T' + \mathbf{M}'\mathbb{Z}.$$

Let  $D := \text{Gcd}(T', \mathbf{M}')$ ,  $T := \frac{T'}{D}$  and  $\mathbf{M} := \frac{\mathbf{M}'}{D}$ . IStFind a point

$$z \in AB\mathbb{Z} \cap [T + \mathbf{M}\mathbb{Z}],$$

since then  $zD$  is in each comb of (7).

So now  $T \perp \mathbf{M}$ . By hypothesis, **Whoa! jk: Proof is broken.**  $\blacklozenge$

Filename: Problems/NumberTheory/congruences.latex  
As of: Saturday 04Mar2006. Typeset: 23Sep2014 at 12:24.