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

A comb \( C := T + M \)Z is coprime if \( T \perp M \).

Divisibility Conundra

Here is a soln to LeVeque’s \#tP63: Fix a coprime comb \( C := T + M \)Z and positn L. Prove there exists \( x \in \mathbb{C} \) st. \( x \perp L \).

Short solution. Let \( F \) be the maximum factor of \( L \) such that \( F \perp M \). Letting \( Q \coloneqq \frac{L}{F} \), then,

\[
\begin{align*}
1: & \quad \text{Primes}(Q) \subset \text{Primes}(M) . \\
2: & \quad x \equiv_M T \quad \text{and} \quad x \equiv_F 1 .
\end{align*}
\]

So in order to show that \( x \perp L \), we need show that \( x \perp Q \). FTOSB, suppose \( p \) is a prime with \( p \mid x \) and \( p \mid Q \). This latter forces \( p \mid M \), by (1). Now LHs(2) forces \( T \nmid p \). This contradicts that \( T \perp M \).

Longer solution. Use nested combs.

3: Lemma. Fix a coprime comb \( C := T + M \)Z. Each positn L yields a coprime subcomb \( \hat{C} \subset C \), where

\[
\hat{C} \coloneqq \hat{T} + \hat{M} \cdot Z ,
\]

with \( \hat{M} \coloneqq \text{lcm}(M, L) \).

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

\[
\text{Remark.} \quad \text{The above proof is entirely constructive. We actually could avoid the “square-free” step, at the cost of verbiage.}
\]

4: Very weak Dirichlet Thm \( \odot \). Each coprime comb \( C \coloneqq T + M \)Z includes an infinite pairwise coprime subset \( \{ T_j \}_{j=1}^{\infty} \) of (distinct) integers.

Proof. Let \( T_1 \coloneqq T \) and \( T_0 \coloneqq M \) and \( C_1 \coloneqq T_1 + T_0 \)Z. ISTProduce nested combs

\[
C_j \supsetneq C_j \supsetneq C_j \supsetneq \ldots \quad \text{of the form}
\]

\[
C_j = T_j + [T_{j-1} \cdots T_1 \cdot T_0] \cdot Z ,
\]

each a coprime comb.

Ok, at stage \( j \), apply Lemma 3 to \( C_j \) with \( N \coloneqq T_j \).

It hands us a translation amount \( T_{j+1} \coloneqq \hat{T} \) which is coprime to

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

Looks like a wrap, Folks. \( \diamond \)

---

\( \odot \) Chinese Remainder Thm: Given arb. “targets” \( s, t \in Z \), \( \exists_x \)

with \( x \equiv_M s \) and \( x \equiv_F t \).

\( \odot \) A much stronger result, Dirichlet’s Theorem, asserts that every coprime comb includes infinitely many prime numbers.
5: Two Comb Lemma. Two combs \( C_j := T_j + M_j \mathbb{Z} \) intersect IFF \\
\[ \vdash \quad \gcd(M_1, M_2) \mid [T_1 - T_2] \]

**Proof.** A integer \( x \) is in \( C_1 \cap C_2 \) means there exist integers \( z_i \) with \( x + z_i M_i = T_i \). Subtracting yields \( z_1 M_1 - z_2 M_2 = T_1 - T_2 \). This has a soln \( (z_1, z_2) \) exactly when \( (\vdash) \). When it does, use either \( z_i \) to determine \( x \).

Two remarks. Suppose \( (\vdash) \). 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 \( L := \gcd(M_1, M_2) \), the algorithm fuses the pair \( y \equiv M_j T_j \) of congruences, into a single \( y \equiv V \) congruence.

The next result, the Pairwise-comb Thm, reminds me of Helly’s theorem on convex sets.

\[ 6: \text{Pairwise-comb Thm.} \quad \text{Consider combs} \ C_1, \ldots, C_N, \text{where} \ C_j := T_j + M_j \mathbb{Z}. \text{Then the combs mutually intersect IFF each pair intersects. The nonvoid intersection} \ \bigcap_1^N C_j \text{has form} \ T + L \mathbb{Z}, \text{where} \ L = \gcd(M_1, \ldots, M_N). \]

Since \( x \in C_j \) means

\[ C_j: \quad x \equiv_{M_j} T_j. \]

Then the combs mutually intersect, producing a comb \( T + L \mathbb{Z} \), where \( L \) is \( \gcd(M_1, \ldots, M_N) \).

Indeed, the combs mutually intersect IFF

\[ \vdash: \quad \text{For each pair} \ j < k \ \text{in} \ [1..N]: \quad \gcd(M_j, M_k) \mid [T_j - T_k]. \]

Reduction. Courtesy \( (5 \vdash) \), condition \( (\vdash) \) 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 \( \sigma: \ x \equiv_K S \), our goal has become:

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

\[ \ddagger\ddagger: \quad \text{Write} \ \text{Fuse(C1,C2)} \text{as} \ x \equiv_L V, \text{where} \ L := \gcd(M_1, M_2). \text{Thus each} \ T_j \equiv_{M_j} V. \text{Hence} \ V - S \equiv_{M_j} T_j - S. \text{With} \ \hat{M}_j := \gcd(M_j, K), \text{then,}

\[ V - S \equiv_{\hat{M}_j} T_i - S, \]

since \( \hat{M}_i \mid M_i \). By hyp., \( (Ci) \) and \( (\sigma) \) can fuse, i.e

\[ T_i - S \equiv_{\hat{M}_i} 0. \]

Together, these give \( [V - S] \equiv \hat{M}_i \). The upshot is

\[ \gcd(\hat{M}_1, \hat{M}_2) \mid [V - S]. \]

Thus \( \gcd(L, K) \) divides \( [V - S] \), as desired.

**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

\[ 7: \quad AZ, \ BZ, \ T' + M' \mathbb{Z}. \]

Let \( D := \gcd(T', M') \), \( T := \frac{T'}{D} \) and \( M := \frac{M'}{D} \). ISTFind a point

\[ z \in ABZ \cap [T + M \mathbb{Z}], \]

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

So now \( T \perp M \). By hypothesis, Whoal jk: Proof is broken.

\[ \ddagger\ddagger\ddagger: \quad \text{Write} \ \text{Fuse(C1,C2)} \text{as} \ x \equiv_L V, \text{where} \ L := \gcd(M_1, M_2). \text{Thus each} \ T_j \equiv_{M_j} V. \text{Hence} \ V - S \equiv_{M_j} T_j - S. \text{With} \ \hat{M}_j := \gcd(M_j, K), \text{then,}

\[ V - S \equiv_{\hat{M}_j} T_i - S, \]

since \( \hat{M}_i \mid M_i \). By hyp., \( (Ci) \) and \( (\sigma) \) can fuse, i.e

\[ T_i - S \equiv_{\hat{M}_i} 0, \]

Together, these give \( [V - S] \equiv \hat{M}_i \). The upshot is

\[ \gcd(\hat{M}_1, \hat{M}_2) \mid [V - S]. \]

Thus \( \gcd(L, K) \) divides \( [V - S] \), as desired.

\[ \ddagger\ddagger\ddagger: \quad \text{Write} \ \text{Fuse(C1,C2)} \text{as} \ x \equiv_L V, \text{where} \ L := \gcd(M_1, M_2). \text{Thus each} \ T_j \equiv_{M_j} V. \text{Hence} \ V - S \equiv_{M_j} T_j - S. \text{With} \ \hat{M}_j := \gcd(M_j, K), \text{then,}

\[ V - S \equiv_{\hat{M}_j} T_i - S, \]

since \( \hat{M}_i \mid M_i \). By hyp., \( (Ci) \) and \( (\sigma) \) can fuse, i.e

\[ T_i - S \equiv_{\hat{M}_i} 0, \]

Together, these give \( [V - S] \equiv \hat{M}_i \). The upshot is

\[ \gcd(\hat{M}_1, \hat{M}_2) \mid [V - S]. \]

Thus \( \gcd(L, K) \) divides \( [V - S] \), as desired.

\[ \ddagger\ddagger\ddagger: \quad \text{Write} \ \text{Fuse(C1,C2)} \text{as} \ x \equiv_L V, \text{where} \ L := \gcd(M_1, M_2). \text{Thus each} \ T_j \equiv_{M_j} V. \text{Hence} \ V - S \equiv_{M_j} T_j - S. \text{With} \ \hat{M}_j := \gcd(M_j, K), \text{then,}

\[ V - S \equiv_{\hat{M}_j} T_i - S, \]

since \( \hat{M}_i \mid M_i \). By hyp., \( (Ci) \) and \( (\sigma) \) can fuse, i.e

\[ T_i - S \equiv_{\hat{M}_i} 0, \]

Together, these give \( [V - S] \equiv \hat{M}_i \). The upshot is

\[ \gcd(\hat{M}_1, \hat{M}_2) \mid [V - S]. \]