Homework due 20Mar2000

Number Theory
MAS 4203

Jonathan L.F. King
University of Florida, Gainesville 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
3 August, 2016 (at *17:44*)

P1: On an arbitrary set X, let Id_X be the ***identity map*** $x \mapsto x$. Fix two (possibly infinite) sets X and Y and a map $f: X \to Y$. Please prove: a f is injective (1-to-1) *iff* $\exists g: Y \to X$ such that $g \circ f = Id_X$. b f is surjective (onto) *iff* $\exists g: Y \to X$ such that $f \circ g = Id_Y$.

P2: i For positive integers N and K, attempt to define a map $\theta: \mathbb{Z}_N \to \mathbb{Z}_K$ by

$$\theta(x) := \langle x \rangle_K \in [0 .. K).$$

Prove that θ is well-defined *iff* $N \bullet K$.

When θ is well-defined, prove that θ is a surjective ring-hom(omorphism).

ii Suppose that $\psi: G \to H$ is a bijective ring-hom. Prove that $\psi^{-1}: H \to G$ is a ring-hom. In consequence, ψ is a ring-iso(morphsim).

P3: Let $f(x) := x^3 - 13x^2 + 44x - 32$.

a Make a 3-column table listing all solutions to the congruence $f(x) \equiv_M 0$, for $M = 3, 5, 7$, successively. [*Hint:* Rather than randomly plug-in values, first find a small integer root R of h, then divide $x - R$ into $f(x)$. Now use the Q.F. to factor h as $f(x) = [x - R][x - S][x - T]$. Now work mod M.]

b Use the CRT to count the number of solutions to $f(x) \equiv_{105} 0$. (It goes without saying (but I'm going to say it anyway) that 105 equals $3 \cdot 5 \cdot 7$.) Use EuclAlg to compute some integers A, B, C so that

1: $$f\big((x, y, z)\big) := \langle Ax + By + Cz \rangle_{105}$$

is a ring-iso from $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ onto $\mathbb{Z}_{105}$.

c Use your ring-iso to calculate all twelve solutions to $f(x) \equiv_{105} 0$. (Check a few!) Try to exhibit the 3-dimensionality of the solution set.

P4: Let $h(\cdot)$ be the polynomial from the preceding problem. d Let $P(K)$ be the product of the first K primes. *How many* solutions does $f(x) \equiv 0$ have, mod $P(K)$? Call the number of solutions $s(K)$. [*Hint:* Recall the factoring from part (a).]

e Let P denote the product of all primes in $[1 .. 10^6]$. Use PNT (Prime Number Thm) to *estimate* the number of solutions to $h(x) \equiv_P 0$. Express your answer in the form $10^{\text{something}}$.

Chinese Remainder Thm

We work our way towards one version of CRT, in bitsy steps.

2: Lemma. *If $\psi_j: G \to H_j$ are ring-homs, for j in $[1 .. K]$, then $f: G \to H_1 \times H_2 \times \ldots \times H_K$ is a ring-hom, where*

2′: $$f(x) := \big(\psi_1(x), \ldots, \psi_K(x)\big) \qquad \diamond$$

3: Corollary. *Suppose $P, A_1, \ldots, A_K$ are posints. Then mapping*

$$x \overset{f}{\mapsto} \big(\langle x \rangle_{A_1}, \ldots, \langle x \rangle_{A_K}\big)$$

is a ring-hom from $\mathbb{Z}_P$ to $\mathbb{Z}_{A_1} \times \cdots \times \mathbb{Z}_{A_K}$ iff each A_j divides P. [*Exercise:* If some two of the A_j fail to be coprime, then f is not surjective.] $\diamond$

4: *Notation.* Let $\vec{A} = \big(A_1, \ldots, A_K\big)$ be a tuple of posints. Let $P := \prod_{j=1}^{K} A_j$ and let $\vec{M}$ be the tuple with $M_j := P/A_j$. Use $\mathbf{z}$ for a general point in $\mathbb{Z}_{A_1} \times \cdots \times \mathbb{Z}_{A_K}$. □

5: Lemma. *WNFrom (with notation from) immediately above: Tuple $\vec{A}$ is pairwise coprime iff* $\text{Gcd}(\vec{M}) = 1$. $\diamond$

6: Chinese Remainder Theorem (CRT). *WNFrom(4), suppose that $\vec{A}$ is pairwise coprime. Then:*

*i: There is a **unique** ring-iso $f: \mathbb{Z}_P \to \mathbb{Z}_{A_1} \times \cdots \times \mathbb{Z}_{A_K}$ specified by $f(x) := \big(\langle x \rangle_{A_1}, \ldots, \langle x \rangle_{A_K}\big)$.*

ii: *Let $g := f^{-1}$. Suppose $\vec{C}$ is a tuple satisfying these two conditions:*

6.1: $$\sum_{j=1}^{K} C_j \equiv_P 1\,;$$

6.2: *For all pairs $j \neq k$:* $C_j \bullet\!| A_k$.

Then $g(\mathbf{z}) = \left\langle \sum_1^K z_j C_j \right\rangle_P$. *(That is, $\vec{C}$ is a "magic tuple".)* ♢

Remark. Lemma 5 tells us that EuclAlg can provide us with a tuple $\vec{T}$ so that $\sum_1^K T_j M_j = 1$. Thus $C_j := T_j M_j$ defines a particular magic tuple.

An alternative $\vec{C}$ can be compute as follows (Steven Hicks): Let

7: $$C_j := M_j * \langle 1/M_j \rangle_{A_j}\,.$$

This immediately satisfies (**??**.2). Thus $S := \sum_1^K C_j$, taken mod A_1, is congruent to $M_1 \cdot \langle 1/M_1 \rangle_{A_1}$, i.e, to 1. For each j, then, $S \equiv_{A_j} 1$. Thus $S \equiv 1 \bmod P$, as needed by (6.2). □

Observation. Given a point $\mathbf{z}$, consider the sum $S := \sum_1^K z_j C_j$ modulo, say, A_5. By (**??**.2), then, A_5 divides C_j for each $j \neq 5$. Thus for y an arbitrary integer, the product $z_j C_j \equiv y C_j$ modulo A_5. In particular, $z_j C_j$ is congruent to $z_5 C_j$. Thus S is congruent mod A_5 to

$$\sum_{j=1}^{K} z_5 C_j = z_5 \cdot \sum_{j=1}^{K} C_j \equiv_{A_5} z_5 \cdot 1 = z_5\,.$$

Nothing is special about "5" in this argument. So we conclude:

8: *For for each index k and for each tuple $\mathbf{z}$ of integers:* $\sum_{j=1}^K z_j C_j \equiv_{A_k} z_k$. □

Proof that g and f are well-defined. Note that (6.2) together with UFT shows that $C_1 \bullet\!| A_2 A_3 \cdots A_K$. More generally,

∗: $$\forall\, j : \quad A_j C_j \equiv_P 0\,.$$

Now observe that

$$g(z_1 + A_1, z_2, \ldots, z_K) \equiv_P A_1 C_1 + \sum_1^K z_j C_j$$
$$\equiv_P 0 + \sum_1^K z_j C_j \equiv_P g(\mathbf{z}) \quad \text{by } (*).$$

Similarly, the g-value is unchanged if we add a multiple of A_j to z_j. Thus $g()$ is well-defined.

That f is well-defined follows from HW problem **P2**. ♦

Proof of (6), the CRT. Courtesy of **P1** and **P2**, we need but show that $f \circ g$ and $g \circ f$ are the appropriate identity maps.

Let $\mathbf{y} := f(g(\mathbf{z}))$. By definition, $y_1 \equiv_P \sum_1^K z_j C_j$. Thus

$$y_1 \equiv_{A_1} \sum_1^K z_j C_j\,, \quad \text{since } A_1 \bullet\!| P,$$
$$\equiv_{A_1} z_1\,, \quad \text{by (8).}$$

Similarly, each $y_j \equiv z_j \bmod A_j$, so $f(g(\mathbf{z})) = \mathbf{z}$.

Establishing that $g \circ f = Id$. Fixing x, our goal is

∗: $$x \equiv_P g(f(x))\,.$$

Let us first work mod A_1. Since A_1 divides P,

$$g(f(x)) \equiv_{A_1} \sum_{j=1}^{K} \langle x \rangle_{A_j} \cdot C_j$$
$$\equiv_{A_1} \langle x \rangle_{A_1}\,, \quad \text{by (8).}$$

That is, A_1 divides the difference $x - g(f(x))$ and, similarly, so does each A_j. By pairwise coprimeness of $\vec{A}$, then, the UFT tells us that the product $A_1 \cdots A_K$ also divides $x - g(f(x))$. And this is $(*)$, as desired. ♦

The Euler Phi function

For an element α of a commutative group $(G, \oplus, 0)$, let "$k\alpha$" be an abbreviation for

$$\underbrace{\alpha \oplus \alpha \oplus \cdots \oplus \alpha}_{k \text{ occurrences of } \alpha},$$

when k is a natural number. When k is negative, let "$k\alpha$" mean $-k \cdot \beta$, where β here means the additive inverse $\ominus\alpha$.

Let $\mathrm{Ord}(\alpha)$, the ***order*** of α, be the minimum of positive integers k so that $k\alpha = 0$. (If there is no such k, then the minimum is $\text{Ord}(\alpha) = +\infty$.) As an example, in $G := \mathbb{Z}_{15}$, the order of $\alpha := 10$ is 3. Evidently,

9: *In* $\mathbb{Z}_N$: $\text{Ord}(\alpha) = \dfrac{N}{\text{Gcd}(N,\alpha)}$, *which, for* $\alpha \neq 0$, *equals* $\frac{\text{Lcm}(N,\alpha)}{\alpha}$.

If the set of multiples, $\{k\alpha \mid \alpha \in \mathbb{Z}\}$, is all of G then we call α a **"*generator* of G"**. Easily, a group G *has* a generator exactly when G is a copy of some $\mathbb{Z}_N$ or of $\mathbb{Z}$.

Let $\Phi(G)$ denote the set of generators of G. So $\Phi(\mathbb{Z}) = \{\pm 1\}$ and $\Phi(\mathbb{Z}_N)$ equals "big Phi of N", the set of $k \in [1 .. N]$ which are coprime to N.

Product groups.

Exercise. If N not prime and $N \neq 4$, then $\prod([1 .. N]) \equiv_N 0$.

Generalizing Wilson's thm

Let $F(N)$ be the number of pairs $\pm R$ of mod-N square-roots of 1; $R^2 \equiv_N 1$.

10: Obs. *Suppose* $N \geqslant 3$ *and* $b \perp N$. ◊

11: Wilson's Thm. *For all* $N \geqslant 3$:

$$\prod(\Phi(N)) \equiv_N [-1]^F. \qquad \Diamond$$