Math 437/537—Group Work #2
Tuesday, September 24, 2024

1. Two moduli:

(a) *Find an integer that is congruent to* $0 \pmod{13}$ *and also congruent to* $1 \pmod{23}$.
(b) *Find an integer that is congruent to* $0 \pmod{23}$ *and also congruent to* $1 \pmod{13}$.
(c) *Given two integers* a_1 *and* a_2*, find a formula for an integer that is congruent to* $a_1 \pmod{13}$ *and also congruent to* $a_2 \pmod{23}$. *(Hint: use your answers to (a) and (b).)*
(d) *Why is there no integer that is congruent to* $2 \pmod{15}$ *and also congruent to* $3 \pmod{25}$*? What could you change about the* 2 *and* 3 *so that there is such an integer?*

(a) Such an integer must be of the form $13x$; we want to choose x so that $13x \equiv 1 \pmod{23}$. The extended Euclidean algorithm gives us the Bézout identity $4\cdot 23 - 7\cdot 13 = 1$; reducing modulo 23 yields $-7 \cdot 13 \equiv 1 \pmod{23}$. Therefore one such integer is $-7 \cdot 13 = -91$.
(b) On the other hand, reducing $4\cdot 23 - 7\cdot 13 = 1$ modulo 13 yields $4\cdot 23 \equiv 1 \pmod{13}$. Since clearly $4 \cdot 23$ is congruent to 0 modulo 23, one such integer is $4 \cdot 23 = 92$.
(c) Since $-91 \equiv 0 \pmod{13}$ and $92 \equiv 1 \pmod{13}$, we see that $-91a_2 + 92a_1 \equiv 0a_2 + 1a_1 = a_1 \pmod{13}$. Similarly, since $-91 \equiv 1 \pmod{23}$ and $92 \equiv 0 \pmod{23}$, we see that $-91a_2 + 92a_1 \equiv 1a_2 + 0a_1 = a_2 \pmod{13}$. Therefore $-91a_2 + 92a_1$ is a formula with the desired properties.
(d) Since $5 \mid 15$, the congruence $n \equiv 2 \pmod{15}$ implies the weaker congruence $n \equiv 2 \pmod{5}$. Similarly, $n \equiv 3 \pmod{25}$ implies $n \equiv 3 \pmod{5}$. But $2 \not\equiv 3 \pmod{5}$, so no integer n can simultaneously satisfy $n \equiv 2 \pmod{5}$ and $n \equiv 3 \pmod{5}$. This problem would go away if we changed the 2 and 3 to integers that were congruent modulo 5, such as 2 and 7. (It's not immediately clear whether this is the only problem—for example, whether the congruences $n \equiv 2 \pmod{15}$ and $n \equiv 7 \pmod{25}$ must have a simultaneous solution. We'll return to this point later in the course.)

(continued on next page)

2. *Three moduli:*

(a) *Find an integer that is congruent to* $1 \pmod 5$*, congruent to* $0 \pmod 7$*, and congruent to* $0 \pmod 9$.

(b) *Find an integer that is congruent to* $0 \pmod 5$*, congruent to* $1 \pmod 7$*, and congruent to* $0 \pmod 9$.

(c) *Find an integer that is congruent to* $0 \pmod 5$*, congruent to* $0 \pmod 7$*, and congruent to* $1 \pmod 9$.

(d) *What is the smallest positive integer that leaves a remainder of* 3 *when divided by* 5*, leaves a remainder of* 2 *when divided by* 7*, and leaves a remainder of* 1 *when divided by* 9*?*

(e) *Why must every integer satisfying the three conditions in part (d) be congruent, modulo* $5 \cdot 7 \cdot 9$*, to your answer to part (d)?*

(a) Such an integer must be of the form $7 \cdot 9 \cdot x$ (since $(7, 9) = 1$, any multiple of both 7 and 9 must also be a multiple of $7 \cdot 9$); we want to choose x so that $63x \equiv 1 \pmod 5$—that is, we want x to be the multiplicative inverse of 63 modulo 5. The extended Euclidean algorithm, or inspection, gives $x \equiv 2 \pmod 5$, and so $63 \cdot 2 = 126$ is a solution.

(b) Similarly, we need an integer $5 \cdot 9 \cdot x$ where $x \equiv (5 \cdot 9)^{-1} \pmod 7$; a calculation shows that $x = 5$ works, so that $5 \cdot 9 \cdot 5 = 225$ is a solution.

(c) Since $(5 \cdot 7)^{-1} \equiv 8 \pmod 9$, the integer $5 \cdot 7 \cdot 8 = 280$ is a solution.

(d) Given our answers to parts (a)–(c), the linear combination $3 \cdot 126 + 2 \cdot 225 + 1 \cdot 280 = 1108$ is one such integer. However, we may subtract $5 \cdot 7 \cdot 9 = 315$ without changing any of the congruences modulo 5, 7, or 9; subtracting 315 three times yields $1108 - 3 \cdot 315 = 163$ as the smallest such integer. (Part (e) below justifies why it is the smallest one.)

(e) Suppose n_1 and n_2 are two integers satisfying the simultaneous congruences $n \equiv 3 \pmod 5$, $n \equiv 2 \pmod 7$, and $n \equiv 1 \pmod 9$. Then $n_1 - n_2 \equiv 3 - 3 = 0 \pmod 5$, so that $5 \mid (n_1 - n_2)$. By the same argument, $7 \mid (n_1 - n_2)$; since $(5, 7) = 1$, we conclude that $5 \cdot 7 \mid (n_1 - n_2)$. Similarly, $9 \mid (n_1 - n_2)$ and $(9, 5 \cdot 7) = 1$, and so $5 \cdot 7 \cdot 9 \mid (n_1 - n_2)$, which is to say $n_1 \equiv n_2 \pmod{5 \cdot 7 \cdot 9}$.

(continued on next page)

3. Given moduli $m_1, m_2, \ldots, m_k$ and integers $a_1, a_2, \ldots, a_k$, write down a formula for an integer that is congruent to $a_j \pmod{m_j}$ for each $1 \le j \le k$. What hypothesis (if any) is necessary on the moduli $m_1, m_2, \ldots, m_k$? on the integers $a_1, a_2, \ldots, a_k$?

The answer is known as the **Chinese remainder theorem**: Let $m_1, m_2, \ldots, m_k$ be nonzero integers such that $(m_i, m_j) = 1$ for all $1 \le i < j \le k$, and let $a_1, a_2, \ldots, a_k$ be any integers. Then the integers satisfying the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

consist of a single residue class modulo $m_1 m_2 \cdots m_k$. One such integer is given by the formula

$$n = b_1 M_1 a_1 + \cdots + b_k M_k a_k, \tag{1}$$

where $M_j = m_1 \cdots m_{j-1} m_{j+1} \cdots m_k$ is the product of all of the m_i except for m_j, and $b_j \equiv M_j^{-1} \pmod{m_j}$.

Note that for $k \ge 3$, there is a difference between the m_k being *pairwise coprime*—meaning that $(m_i, m_j) = 1$ for all $1 \le i < j \le k$—and the k-tuple $(m_1, \ldots, m_k)$ having greatest common divisor equal to 1; the former condition implies the latter condition, but not conversely as the triple $(6, 10, 15)$ shows. EXERCISE: Verify that the proof of the Chinese remainder theorem requires the stronger condition of pairwise coprimality.

(continued on next page)

Notation: Let $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ be the set of all residue classes modulo m, and let $\mathbb{Z}_m^\times = (\mathbb{Z}/m\mathbb{Z})^\times$ be the set of reduced residue classes modulo m.

Structural comments (with a payoff at the end): Whenever $d \mid m$, there is a well-defined projection map $\pi_d : \mathbb{Z}_m \to \mathbb{Z}_d$ given by $\pi_d(a \bmod m) = a \bmod d$. (EXERCISE: Verify that this map is *not* well-defined when $d \nmid m$. For example, it doesn't make sense to talk about whether elements of $\mathbb{Z}_7$ are even or odd.) Now, let $m_1, m_2, \dots, m_r$ be pairwise coprime. The map between sets

$$\pi : \mathbb{Z}_{m_1 m_2 \cdots m_r} \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r},$$

is given in each component $\mathbb{Z}_{m_i}$ by π_{m_i}. The Chinese remainder theorem gives a map

$$\rho : \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \longrightarrow \mathbb{Z}_{m_1 m_2 \cdots m_r},$$

given by the formula in equation (1); the statement of the theorem is equivalent to saying that $\pi \circ \rho$ is the identity map. Since both sets are finite, we conclude that π and ρ are set bijections.

One can check (EXERCISE) that π *and* ρ *respect addition and multiplication* (indeed, that was part of how we deduced general formulas such as 1(c) and 2(d) from specific cases such as 1(a)–(b) and 2(a)–(c). In other words, π *and* ρ *are ring isomorphisms*.

Moreover, one can check (EXERCISE) that π *and* ρ *respect coprimality*: an element $a \in \mathbb{Z}_{m_1 m_2 \cdots m_r}$ is coprime to $m_1 \cdots m_r$ if and only if the jth coordinate of $\pi(a)$ is coprime to m_j for each $1 \le j \le r$. In other words, π and ρ induce *isomorphisms of multiplicative groups*

$$\pi^\times : (\mathbb{Z}_{m_1 m_2 \cdots m_r})^\times \longrightarrow \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \times \cdots \times \mathbb{Z}_{m_r}^\times$$
$$\rho^\times : \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \times \cdots \times \mathbb{Z}_{m_r}^\times \longrightarrow (\mathbb{Z}_{m_1 m_2 \cdots m_r})^\times.$$

In particular, these maps are set bijections; since $\phi(n)$ is, by definition, the cardinality of $\mathbb{Z}_n^\times$, we conclude that the Euler phi-function is *multiplicative*, meaning that

$$\phi(m_1 m_2 \cdots m_r) = \phi(m_1)\phi(m_2)\cdots\phi(m_r) \text{ whenever } m_1, \dots, m_r \text{ are pairwise coprime.} \qquad (2)$$

One important special case of all this is when n is factored (uniquely, by the fundamental theorem of arithmetic) into a product of powers of distinct primes,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

with $\alpha_i > 0$ and $p_i \ne p_j$ for all $i \ne j$; verify that $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ are indeed pairwise coprime.

We are thus motivated to compute $\phi(p^\alpha)$ for prime p; but the only integers $1 \le k \le p^\alpha$ with $(p^\alpha, k) > 1$ must have $(p^\alpha, k) = p^\beta$ for some $1 \le \beta \le \alpha$, and in particular must be multiples of p. We deduce that the integers in the range $1 \le k \le p^\alpha$ that are not coprime to p^α are precisely the $p^{\alpha-1}$ multiples of p in that range; consequently, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$.

Consequently, we may write down a *formula for* $\phi(n)$*, for any integer* n*, in terms of its prime factorization*, thanks to the multiplicative property (2):

$$\phi\big(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\big) = \big(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\big) \cdots \big(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\big) = \prod_{j=1}^{r} p_j^{\alpha_j}\big(1 - \tfrac{1}{p_j}\big),$$

or equivalently

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right),$$

where the product runs over all (distinct) prime divisors p of n.