4 Euler's Totient Function

4.1 Euler's Function and Euler's Theorem

Recall Fermat's little theorem:

$$p \text{ prime and } p \nmid a \implies a^{p-1} \equiv 1 \pmod p$$

Our immediate goal is to think about extending this to *composite* moduli. First let's search for patterns in the powers a^k modulo 6, 7 and 8:

modulo 6

k	1	2	3	4	5
$a=1$	1	1	1	1	1
2	2	4	2	4	2
3	3	3	3	3	3
4	4	4	4	4	4
5	5	1	5	1	5

modulo 7

k	1	2	3	4	5	6
$a=1$	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

modulo 8

k	1	2	3	4	5	6	7
$a=1$	1	1	1	1	1	1	1
2	2	4	0	0	0	0	0
3	3	1	3	1	3	1	3
4	4	0	0	0	0	0	0
5	5	1	5	1	5	1	5
6	6	4	0	0	0	0	0
7	7	1	7	1	7	1	7

The column in red (modulo 7) represents Fermat's little theorem. Unfortunately there don't seem to be many 1's in the other tables: indeed the tables should suggest the following.

Lemma 4.1. *If $k \geq 1$ is such that $a^k \equiv 1 \pmod n$, then $\gcd(a, n) = 1$ (a is a unit modulo n).*

The proof is a (hopefully) straightforward exercise.
We turn now to the converse: if $\gcd(a, n) = 1$, can we find k such that $a^k \equiv 1 \pmod n$? Again, let's consider the tables and look for patterns:

Modulo 6 The units are $a \equiv 1, 5$. For such a we see that $a^2 \equiv 1 \pmod 6$.

Modulo 7 Every non-zero remainder is a unit, and $a^6 \equiv 1 \pmod 7$.

Modulo 8 The units are $a \equiv 1, 3, 5, 7$. For such a we see that $a^2 \equiv 1 \pmod 8$.

In each case, observe that $a^k \equiv 1$ whenever k is the *number of units*[1] *modulo n.* Given all this, we make a definition and a hypothesis:

Definition 4.2. *Euler's totient function* $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by[2]

$$\varphi(n) = \left|\{0 < a \leq n : \gcd(a, n) = 1\}\right|$$

Theorem 4.3 (Euler's Theorem). *If $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod n$.*

[1]Certainly $a^4 \equiv 1 \pmod 8$ satisfies this pattern, even though a lower power $k = 2$ does also.

[2]Whenever $n \geq 2$, Euler's function returns the number of units modulo n. The definition is constructed so as to include $\varphi(1) = 1$. In what follows, the $n = 1$ case is always trivial and uninteresting; to avoid tedium we'll assume that $n \geq 2$.

Here are the first few values of Euler's function; we also list the units.

$\varphi(1) = 1 = \lvert\{1\}\rvert$	$\varphi(7) = 6 = \lvert\{1,2,3,4,5,6\}\rvert$
$\varphi(2) = 1 = \lvert\{1\}\rvert$	$\varphi(8) = 4 = \lvert\{1,3,5,7\}\rvert$
$\varphi(3) = 2 = \lvert\{1,2\}\rvert$	$\varphi(9) = 6 = \lvert\{1,2,4,5,7,8\}\rvert$
$\varphi(4) = 2 = \lvert\{1,3\}\rvert$	$\varphi(10) = 4 = \lvert\{1,3,7,9\}\rvert$
$\varphi(5) = 4 = \lvert\{1,2,3,4\}\rvert$	$\varphi(11) = 10 = \lvert\{1,2,3,4,5,6,7,8,9,10\}\rvert$
$\varphi(6) = 2 = \lvert\{1,5\}\rvert$	$\varphi(12) = 4 = \lvert\{1,5,7,11\}\rvert$

Whenever p is prime, we clearly have $\varphi(p) = p - 1$, from which we see that Fermat's little theorem is merely a special case of Euler's. You should mentally check that the main result holds for several of the values listed above with composite moduli: e.g.

$$4^{\varphi(9)} \equiv 4^6 \equiv 16^3 \equiv (-2)^3 \equiv -8 \equiv 1 \pmod 9$$

Perhaps unsurprisingly, we can prove Euler's theorem analogously to how we proved Fermat's.

Proof. Let a be a unit and let $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n : \gcd(x,n) = 1\}$ be the set of units modulo n. Define $f_a(x) = ax \pmod n$. We claim that $f_a : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ is *bijection* (invertible). This requires two checks:

1. If $x \in \mathbb{Z}_n^\times$, then $f_a(x) = ax$ is also a unit: if neither a nor x have any common divisors with n, then neither does the product ax.
2. Since a is a unit, it has an inverse b. But then $f_a^{-1} = f_b$ as is readily checked: for any x,

$$(f_a \circ f_b)(x) \equiv f_a\big(f_b(x)\big) \equiv a(bx) \equiv (ab)x \equiv x \pmod n$$

Since $f_a : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ is bijective, we may list the units in two ways:

$$\mathbb{Z}_n^\times = \{x_1, x_2, \ldots, x_{\varphi(n)}\} = \{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}$$

Multiply these together to obtain

$$x_1 x_2 \cdots x_{\varphi(n)} \equiv ax_1 ax_2 \cdots ax_{\varphi(n)} \equiv a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \pmod n$$

Since the x_i are all relatively prime to n, we may divide out, thus obtaining the result. ∎

Example 4.4. It should be clear that $\gcd(a,35) = 1 \iff \gcd(a,5) = 1$ and $\gcd(a,7) = 1$, whence the set of units modulo 35 is

$$\mathbb{Z}_{35}^\times = \mathbb{Z}_{35} \setminus \{0,5,10,15,20,25,30,7,14,21,28\} \implies \varphi(35) = 35 - 11 = 24$$

We may now employ this to simplify congruences as we did with Fermat. For instance, suppose you wanted to solve the congruence equation

$$x^{49} \equiv 12 \pmod{35}$$

First observe that if x is a solution and $\gcd(x,35) = d$, then $d \mid 12$ and $d \mid 35$, whence $d = 1$: it follows that x is a unit and we may apply Euler's theorem.

$$x^{24} \equiv 1 \implies x^{49} \equiv x \equiv 12 \pmod{35}$$

Computing Euler's Function

Rather than a laborious direct computation, we follow the classic number-theory approach: worry about primes first, then powers of primes, then glue everything together.

$\varphi(p)$ where p is prime: Since $\mathbb{Z}_p^\times = \{1, \ldots, p-1\}$, we plainly have $\varphi(p) = p - 1$.

$\varphi(p^2)$: We want to count the remainders in the set $\{1, 2, 3, \ldots, p^2\}$ which are coprime to p^2: this means *deleting the multiples of* p:

$$\varphi(p^2) = \mathbb{Z}_{p^2}^\times = \left|\{1, 2, \ldots, p^2\} \setminus \{p, 2p, 3p, \ldots, (p-1)p, p^2\}\right| = p^2 - p$$

$\varphi(p^k)$: We again delete the multiples of p:

$$\left|\{1, \ldots, p^k\} \setminus \{ap : 1 \le a \le p^{k-1}\}\right| = p^k - p^{k-1} \implies \boxed{\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)}$$

It remains to investigate moduli n which are divisible by more than one prime. Start by looking for patterns in the table of small values on page 2 and observe that

$$\varphi(6) = \varphi(2)\varphi(3), \qquad \varphi(10) = \varphi(2)\varphi(5), \qquad \varphi(12) = \varphi(3)\varphi(4)$$

Moreover, recalling Example 4.4, we see that $\varphi(35) = 24 = 4 \cdot 6 = \varphi(5)\varphi(7)$ also satisfies the pattern! We therefore have a hypothesis.

Theorem 4.5. *Euler's function φ is* multiplicative:

$$\gcd(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$$

There are many simpler examples of multiplicative functions, for instance

$$f(x) = 1, \qquad f(x) = x, \qquad f(x) = x^2$$

though these satisfy the product formula even if m, n are not coprime. The Euler function is more exotic; it really requires the coprime restriction!
Using the unique prime decomposition, the theorem quickly tells us that

$$\varphi(n) = \varphi(p_1^{\mu_1} \cdots p_k^{\mu_k}) = \varphi(p_i^{\mu_1}) \cdots \varphi(p_n^{\mu_k}) = p_1^{\mu_1}(1 - p_1^{-1}) \cdots p_k^{\mu_k}(1 - p_k^{-1})$$

from which we conclude:

Corollary 4.6. $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \frac{p-1}{p}$

We don't need the entire decomposition, only the list of distinct primes dividing n.

Example 4.7.

1. $\varphi(72) = \varphi(8 \cdot 9) = \varphi(2^3 \cdot 3^2) = 72 \cdot \frac{1}{2} \cdot \frac{2}{3} = 24.$
2. $\varphi(1000000) = 1000000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400000$

Proving the multiplicative property is a little awkward. To help follow along, consider listing all the remainders modulo $36 = 9 \times 4$ in a rectangle:

$$\begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \\ 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 \end{array}$$

The units (coprime to 36) are distributed in six columns containing two each. By rewriting the table modulo 9 and 4 we can now make an argument for why $\varphi(36) = 12 = 6 \times 2 = \varphi(9)\varphi(4)$:

$$\begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \qquad \begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 \\ 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 \\ 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 \\ 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{array}$$

1. The columns being distinct modulo 9, all elements coprime to 9 lie in one of $\varphi(9) = 6$ columns.
2. Each column contains a complete set of remainders modulo 4; exactly $\varphi(4) = 2$ entries in each column are therefore coprime to 4.
3. A remainder is coprime to 36 if and only if it is coprime to both 9 and 4: such must be one of the $\varphi(4)$ entries in one of the $\varphi(9)$ columns of interest. We conclude that $\varphi(36) = \varphi(9)\varphi(4)$.

The proof of the multiplicative property is merely an abstraction of this example.

Proof of Theorem 4.5. If either of m, n are equal to 1, then $\varphi(mn) = \varphi(m)\varphi(n)$ is trivial. We therefore suppose that $\gcd(m, n) = 1$ where $m, n > 1$ and list all the elements of $\mathbb{Z}_{mn}$ in an $n \times m$ table:

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & m-1 \\ m & m+1 & m+2 & \cdots & m+(m-1) \\ 2m & 2m+1 & 2m+2 & \cdots & 2m+(m-1) \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)m & (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+(m-1) \end{array}$$

We count the $\varphi(mn)$ entries coprime to mn in a different way, by first observing that

$$\gcd(x, mn) = 1 \iff \gcd(x, m) = 1 = \gcd(x, n)$$

In the first row of the table there are $\varphi(m)$ entries coprime to m. Since each column is congruent modulo m, the entries coprime to m consist precisely of everything in these $\varphi(m)$ columns.

Now consider the j^{th} column: $j, m+j, 2m+j, \ldots, (n-1)m+j$. Since $\gcd(m, n) = 1$, no two of these elements are congruent modulo n:

$$km + j \equiv lm + j \implies km \equiv lm \implies k \equiv l \pmod{n}$$

Each column consists of a complete set of remainders modulo n, and so $\varphi(n)$ of the entries in each column are coprime to n.

Putting this together, we have $\varphi(m)$ columns coprime to m, each of which contains $\varphi(n)$ entries coprime to n: thus $\varphi(m)\varphi(n)$ entries in the full table are coprime to both m and n. ∎

Example 4.8. As a nice example of the formula, we find all n such that $\varphi(n) = 6 = 2 \cdot 3$.

Writing $n = p_1^{\mu_1} \cdots p_k^{\mu_k}$, we see that $2 \cdot 3 = p_1^{\mu_1 - 1} \cdots p_k^{\mu_k - 1}(p_1 - 1) \cdots (p_k - 1)$. The divisors of 6 are $1, 2, 3, 6$: if one greater than these is prime, that prime might also be a divisor of n: thus we need also consider *at most* one factor of 7: $n = 2^a 3^b 7^c$ where $a, b \geq 0$ and $c = 0, 1$. Now compute all the possibilities:

$$2 \cdot 3 = \varphi(n) = \begin{pmatrix} 2^{a-1} \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \cdot 3^{b-1} \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 1 \end{pmatrix}$$

where we must take one factor from each pair (the bottom row corresponds to $a, b, c = 0$). It is not hard to check that only ways to make 6 are

- $\varphi(n) = 1 \cdot 1 \cdot 6 \implies n = 2^0 3^0 7^1 = 7$
- $\varphi(n) = 2^{1-1} \cdot 1 \cdot 6 \implies n = 2^1 3^0 7^1 = 14$
- $\varphi(n) = 1 \cdot (2 \cdot 3^{2-1}) \cdot 1 \implies n = 2^0 3^2 7^0 = 9$
- $\varphi(n) = 2^{1-1} \cdot (2 \cdot 3^{2-1}) \cdot 1 \implies n = 2^1 3^2 7^0 = 18$

Counting residues Euler's function records how many integers in $\mathbb{Z}_n$ are relatively prime to n. What about counting residues with other gcd's with n? Euler's function does this as well.

Lemma 4.9. *If $d \mid n$, then $\varphi\left(\frac{n}{d}\right)$ residues a satisfy* $\gcd(a, n) = d$.

Proof. Start by observing that $\gcd(a, n) = d \iff \gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$. However, by definition, $\varphi\left(\frac{n}{d}\right)$ of the values $1 \leq \frac{a}{d} \leq \frac{n}{d}$ are coprime to $\frac{n}{d}$. ∎

Example 4.10. There are $\varphi\left(\frac{136}{4}\right) = \varphi(34) = 16$ integers $1 \leq a \leq 136$ for which $\gcd(136, a) = 4$. Indeed these are precisely

$$4, 12, 20, 28, 36, 44, 52, 60, 68, 76, 84, 92, 100, 108, 116, 132$$

More surprising perhaps is what happens when you sum the value of Euler's function over all divisors of an integer.

Theorem 4.11. *Summing over all* positive *divisors d of n, we obtain* $\sum_{d \mid n} \varphi(d) = n$

Proof. Partition $\{1, \ldots, n\}$ into subsets according to the gcd of each with n. By Lemma 4.9, this $\gcd(a, n) = d$ for exactly $\varphi\left(\frac{n}{d}\right)$ of the numbers. Hence

$$\sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = n$$

since we've counted the whole set! Since the values $\frac{n}{d}$ are simply the divisors of n listed in the reverse order to d, the sums must be identical: $\sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = \sum_{d \mid n} \varphi(d)$. ∎

Example 4.12. With $n = 28$, we verify that

$$\sum_{d|28} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(7) + \varphi(14) + \varphi(28)$$
$$= 1 + 1 + 2 + 6 + 6 + 12 = 28$$

Exercises 4.1 1. Find the values of $\varphi(97)$ and $\varphi(8800)$.

2. Prove Lemma 4.1.

3. (a) If $n \geq 3$, explain why $\varphi(n)$ is always even.
   (b) Find all values n for which $\varphi(n)$ is not divisible by 4.

4. Find all n such that $\varphi(n)$ is the indicated value:

   (a) $\varphi(n) = 10$ (b) $\varphi(n) = 12$ (c) $\varphi(n) = 20$ (d) $\varphi(n) = 100$

5. Find all values n that solve each of the following equations. If there are none, explain why.

   (a) $\varphi(n) = \frac{n}{2}$ (b) $\varphi(n) = \frac{n}{3}$ (c) $\varphi(n) = \frac{n}{6}$

   For an extra challenge, find all n for which $\varphi(n) \mid n$.

6. Show that if $d \mid n$ then $\varphi(d) \mid \varphi(n)$.

7. Suppose $\gcd(a, b) = d$. Use prime decompositions to prove that $\varphi(ab) = \dfrac{d\varphi(a)\varphi(b)}{\varphi(d)}$

8. (A challenge!) Show that $\sum_{d|n} (-1)^{n/d} \varphi(d) = \begin{cases} 0 & \text{if } n \text{ even} \\ -n & \text{if } n \text{ odd} \end{cases}$

   (*Hint: write $n = 2^k m$ where m is odd and take the $k = 0, \geq 1$ cases separately*)

9. A unit $x \in \mathbb{Z}_n$ (i.e. $\gcd(x, n) = 1$) is a *primitive root* modulo n if the *smallest* exponent k such that $x^k \equiv 1 \pmod{n}$ is $k = \varphi(n)$.

   (a) Find a primitive root modulo 7. Modulo 14.
   (b) Show that 8 does not have any primitive roots.
   (c) If x is a primitive root modulo n, prove that the set of units in $\mathbb{Z}_n$ is given by $\{x, x^2, \ldots, x^{\varphi(n)}\}$

10. Recall the discussion of riffle-shuffling from the previous chapter.

    (a) Show that repeatedly shuffling a pack of $2m$ cards always eventually returns the pack to its initial position.
    (b) Let $n \geq 1$ be the minimum number of shuffles required to return the deck to its original order.
       i. Compute n when $2m = 4, 6, 8, 10, 12, 14$.
       ii. Prove that $n \mid \varphi(2m + 1)$.
       (*Hint: apply the division algorithm to $\varphi(2m + 1)$ and n*)
    (c) Investigate what happens if you try to shuffle an odd number of cards. Or if you shuffle so that the bottom card (labelled 1) starts on the bottom?

4.2 The Chinese Remainder Theorem

In this section we see how to solve *simultaneous* congruence equations. This is straightforward to see with a small example.

Example 4.13. Solve the simultaneous congruences

$$\begin{cases} x \equiv 4 \pmod{50} \\ x \equiv 15 \pmod{33} \end{cases}$$

Any solution x simultaneously satisfies $x = 4 + 50k = 15 + 33l$ for some integers k, l. Applying the Euclidean algorithm (or invoking divine intervention), we see that

$$(k, l) = (22, -33) \quad \text{satisfies} \quad 50k + 33l = 11$$

whence $x = 4 + 50 \cdot 22 = 1104$ solves the congruences.
We can say a little more, since we know that all suitable k satisfy $k = 22 + 33t$ for some $t \in \mathbb{Z}$, and so all solutions x have the form

$$x = 4 + 50(22 + 33t) = 1104 + 50 \cdot 33t \equiv 1104 \pmod{1650}$$

We therefore have a *unique* solution modulo the product of the original moduli.

This pattern holds in general, *provided the moduli are coprime.*

- Suppose $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. Otherwise said,

  $$\exists k, l \in \mathbb{Z} \text{ such that } x = a + km = b + ln \implies km - ln = b - a$$

- Since $\gcd(m, n) = 1$, we can find suitable k, l using Bézout's identity: if $\kappa m + \lambda n = 1$, then

  $$\begin{aligned} &(b-a)\kappa m + (b-a)\lambda n = b - a \\ \implies &k = (b-a)\kappa + nt : t \in \mathbb{Z} \\ \implies &x = a + ((b-a)\kappa + nt)m \equiv a + (b-a)\kappa m \pmod{mn} \\ &\quad \equiv a(1 - \kappa m) + b\kappa m \equiv a\lambda n + b\kappa m \pmod{mn} \end{aligned} \tag{$*$}$$

Not only do we see that the simultaneous congruence has a unique solution modulo mn, but we have a nice formula for evaluating it. Before seeing the full result, note that our abstract expression $(*)$ for x really does satisfy both congruences:

$$\begin{cases} a\lambda n + b\kappa m \equiv a\lambda n \equiv a \pmod{m} \\ a\lambda n + b\kappa m \equiv b\kappa m \equiv b \pmod{n} \end{cases}$$

The observation is that $\lambda n \equiv 1 \pmod{m}$ and $\kappa m \equiv 1 \pmod{n}$; that is, we have *inverses* for m and n *modulo each other.*

Theorem 4.14 (Chinese Remainder Theorem). *Suppose that moduli $n_1, \dots, n_k$ are pairwise coprime*[a]. *Then the simultaneous congruences*

$$x \equiv b_1 \pmod{n_1}, \quad x \equiv b_2 \pmod{n_2}, \quad \dots \quad x \equiv b_k \pmod{n_k} \tag{†}$$

have a unique solution modulo $N := n_1 \cdots n_k$. Specifically, for each i, define $N_i = \frac{N}{n_i}$ and compute its inverse $\lambda_i N_i \equiv 1 \pmod{n_i}$, then

$$x \equiv b_1\lambda_1 N_1 + b_2\lambda_2 N_2 + \cdots + b_k\lambda_k N_k \pmod{N}$$

[a] $\gcd(n_i, n_j) = 1$ whenever $i \neq j$

Proof. Plainly $\gcd(N_i, n_i) = 1$ since $N_i = \frac{N}{n_i}$ is the product of all coprime moduli $n_1 \cdots n_k$ *except* n_i. Bézout's identity says N_i has an inverse λ_i modulo n_i. Moreover, since $j \neq i \implies n_j \mid N_i$, we have

$$\lambda_i N_i \equiv \begin{cases} 0 \pmod{n_j} & \text{if } i \neq j \\ 1 \pmod{n_i} \end{cases}$$

It is now immediate that the advertised x solves all the congruences (†).
Finally suppose that y also solves the congruences. Then $x - y \equiv 0 \pmod{n_i}$ for all i which, since the n_i are pairwise coprime, forces $x \equiv y \pmod{N}$. ∎

Examples 4.15. 1. First we revisit Example 4.13 in this language.

$$x \equiv 4 \pmod{50}, \qquad x \equiv 15 \pmod{33}$$

The moduli 50 and 33 are pairwise coprime so the theorem applies. We compute

$$N = 50 \cdot 33 = 1650, \qquad N_1 = 33, \qquad N_2 = 50 \qquad\qquad (N_1 = \tfrac{mn}{m} = n \text{ and } N_2 = m \text{ in } (*))$$

We must therefore solve:

$$\begin{cases} 33\lambda_1 \equiv 1 \pmod{50} \implies \lambda_1 \equiv -3 \\ 50\lambda_2 \equiv 1 \pmod{33} \implies \lambda_2 \equiv 2 \end{cases} \qquad\qquad (\lambda_1 = \lambda \text{ and } \lambda_2 = \kappa \text{ in } (*))$$

Finally,

$$x \equiv b_1\lambda_1 N_1 + b_2\lambda_2 N_2 \equiv 4 \cdot (-3) \cdot 33 + 15 \cdot 2 \cdot 50 \equiv 1500 - 396 \equiv 1104 \pmod{1650}$$

2. Find all solutions $x \in \mathbb{Z}$ to the simultaneous congruences

$$x \equiv 3 \pmod{5}, \quad x \equiv 5 \pmod{7}, \quad x \equiv 2 \pmod{8}$$

Since the moduli 5, 7 and 8 are pairwise coprime the theorem applies and we compute:

$$N = 5 \cdot 7 \cdot 8 = 280, \qquad N_1 = 56, \qquad N_2 = 40, \qquad N_3 = 35$$

$$\implies \begin{cases} 56\lambda_1 \equiv 1 \pmod{5} & \implies \lambda_1 \equiv 1 \\ 40\lambda_2 \equiv 1 \pmod{7} & \implies \lambda_2 \equiv 3 \\ 35\lambda_3 \equiv 1 \pmod{8} & \implies \lambda_3 \equiv 3 \end{cases}$$

$$\implies x \equiv 3 \cdot 1 \cdot 56 + 5 \cdot 3 \cdot 40 + 2 \cdot 3 \cdot 35 \equiv 978 \equiv 138 \pmod{280}$$

Non-coprime moduli?

We state without proof the following generalization of the Chinese Remainder Theorem.

Corollary 4.16. *A system of congruences* (†) *may be solved if and only if* $\gcd(n_i, n_j) \mid (b_i - b_j)$ *for all* $i \neq j$. *In such a case, all solutions are congruent modulo* $\operatorname{lcm}(n_1, \ldots, n_k)$.

The method is essentially to remove superfluous congruences so that we can apply the Chinese Remainder Theorem.

Example 4.17. The corollary applies to the simultaneous congruences

$$x \equiv 1 \pmod 3, \qquad x \equiv 2 \pmod 4, \qquad x \equiv 8 \pmod{10}$$

the only divisor property we need to check being $\gcd(4, 10) \mid (2 - 8)$.
The final congruence holds if and only if $x \equiv 0 \pmod 2$ and $x \equiv 3 \pmod 5$. The first condition is unnecessary since it follows from $x \equiv 2 \pmod 4$. We therefore solve the congruence system

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases} \implies x \equiv 58 \pmod{60} \tag{‡}$$

using the standard Chinese remainder theorem. Note that the modulus is $60 = \operatorname{lcm}(3, 4, 10)$.

Exercises 4.2

1. Find the solutions to the following simultaneous congruences using the Chinese remainder theorem.
   (a) $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 9$
   (b) $x \equiv 1 \pmod 4$, $x \equiv 4 \pmod{15}$
2. (a) Do the calculations to solve the simultaneous triple congruence (‡) in Example 4.17.
   (b) Solve the triple congruence
   $$x \equiv 3 \pmod 4, \quad x \equiv 5 \pmod{21}, \quad x \equiv 7 \pmod{25}$$
   (c) Solve the triple congruence (*be careful!*)
   $$3x \equiv 9 \pmod{12}, \quad 4x \equiv 5 \pmod{35}, \quad 6x \equiv 2 \pmod{11}$$
3. Give x explicitly in terms of $b_1, \ldots, b_4$ if
   $$x \equiv b_1 \pmod 2, \qquad x \equiv b_2 \pmod 3, \qquad x \equiv b_3 \pmod 5, \qquad x \equiv b_4 \pmod 7$$
4. Find the solutions: note the generalized Corollary 4.16.
   (a) $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 7 \pmod{10}$
   (b) $x \equiv 1 \pmod{12}$, $x \equiv 4 \pmod{21}$, $x \equiv 18 \pmod{35}$
5. Solve $x^3 - x + 15 \equiv 0 \pmod{63}$.
   (*Don't just list solutions! Consider modulo 7 and 9 then use the Chinese remainder theorem*)
6. Prove the ($\Rightarrow$) direction of Corollary 4.16: if the system has a solution, then $\gcd(n_i, n_j) \mid (b_i - b_j)$.