Example 104. By the Chinese remainder theorem there is a bijective correspondence

$$x \pmod{nm} \mapsto \begin{bmatrix} x \pmod{n} \\ x \pmod{m} \end{bmatrix}.$$

Here's a graphical representation for $n=3$, $m=5$. Do you see the pattern?

		$\pmod 5$ 0	1	2	3	4
$\pmod 3$	0	0	6		3	
	1		1	$\ddots$		4
	2	5		2	$\ddots$	

$\rightsquigarrow$

		$\pmod 5$ 0	1	2	3	4
$\pmod 3$	0	0	6	12	3	9
	1	10	1	7	13	4
	2	5	11	2	8	14

Example 105. Solve $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.

Solution. $x \equiv 1 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)^{-1}_{\bmod 4}]}_{3} + 2 \cdot 4 \cdot 7 \cdot \underbrace{[(4 \cdot 7)^{-1}_{\bmod 5}]}_{2} + 3 \cdot 4 \cdot 5 \cdot \underbrace{[(4 \cdot 5)^{-1}_{\bmod 7}]}_{-1}$
$\equiv 105 + 112 - 60 = 157 \equiv 17 \pmod{140}$.

Silicon slave labor. Once you are comfortable doing it by hand, you can easily let Sage do the work for you:

```
Sage] crt([1,2,3], [4,5,7])
```

17

Example 106. Solve $x \equiv 2 \pmod 3$, $3x \equiv 2 \pmod 5$, $5x \equiv 2 \pmod 7$.

Solution. Note that $3^{-1} \equiv 2 \pmod 5$ and $5^{-1} \equiv 3 \pmod 7$.
Hence, we can simplify the congruences to $x \equiv 2 \pmod 3$, $x \equiv 2 \cdot 2 \equiv -1 \pmod 5$, $x \equiv 2 \cdot 3 \equiv -1 \pmod 7$.
Using the CRT, $x \equiv 2 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)^{-1}_{\bmod 3}]}_{2} - 1 \cdot 3 \cdot 7 \cdot \underbrace{[(3 \cdot 7)^{-1}_{\bmod 5}]}_{1} - 1 \cdot 3 \cdot 5 \cdot \underbrace{[(3 \cdot 5)^{-1}_{\bmod 7}]}_{1}$
$\equiv 140 - 21 - 15 = 104 \equiv -1 \pmod{105}$.
Note. Can you see how we could have totally gotten that answer without the CRT computation?

Example 107. (extra)

(a) Solve $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod{25}$.

(b) Solve $x \equiv -1 \pmod 4$, $x \equiv 2 \pmod 7$, $x \equiv 0 \pmod 9$.

Solution. (final answer only)

(a) $x \equiv 78 \pmod{100}$

(b) $x \equiv 135 \pmod{252}$

Example 108. How many solutions does $x^2 \equiv 9 \pmod{M}$ have for $M = 55$? For $M = 385$? For $M = 110$? For $M = 105$?

Solution.

(a) $M = 55 = 5 \cdot 11$. There are 2 solutions modulo 5 and 2 solutions modulo 11. By the CRT, these combine to $2 \cdot 2 = 4$ solutions modulo 55.

(b) $M = 385 = 5 \cdot 7 \cdot 11$. There are 2 solutions modulo 5, 2 solutions modulo 7, and 2 solutions modulo 11. By the CRT, these combine to $2 \cdot 2 \cdot 2 = 8$ solutions modulo 385.

(c) $M = 110 = 2 \cdot 5 \cdot 11$. There is 1 solution modulo 2 (why?!), 2 solutions modulo 5, and 2 solutions modulo 11. By the CRT, these combine to $1 \cdot 2 \cdot 2 = 4$ solutions modulo 110.

(d) $M = 105 = 3 \cdot 5 \cdot 7$. There is 1 solution modulo 3 (why?!), 2 solutions modulo 5, and 2 solutions modulo 7. By the CRT, these combine to $1 \cdot 2 \cdot 2 = 4$ solutions modulo 105.

Example 109. (extra) Determine all solutions to $x^2 \equiv 9 \pmod{110}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 9 \pmod{110} \\ \iff\ & x^2 \equiv 9 \pmod{2} \text{ and } x^2 \equiv 9 \pmod{5} \text{ and } x^2 \equiv 9 \pmod{11} \\ \iff\ & x \equiv \pm 3 \pmod{2} \text{ and } x \equiv \pm 3 \pmod{5} \text{ and } x \equiv \pm 3 \pmod{11} \\ \iff\ & x \equiv 1 \pmod{2} \text{ and } x \equiv \pm 3 \pmod{5} \text{ and } x \equiv \pm 3 \pmod{11} \end{aligned}$$

Let us write down all possible four combinations:

solution #1	solution #2	solution #3	solution #4
$x \equiv 1 \pmod{2}$	$x \equiv 1 \pmod{2}$	$x \equiv 1 \pmod{2}$	$x \equiv 1 \pmod{2}$
$x \equiv 3 \pmod{5}$	$x \equiv 3 \pmod{5}$	$x \equiv -3 \pmod{5}$	$x \equiv -3 \pmod{5}$
$x \equiv 3 \pmod{11}$	$x \equiv -3 \pmod{11}$	$x \equiv 3 \pmod{11}$	$x \equiv -3 \pmod{11}$
$x \equiv 3 \pmod{110}$	$x \equiv a \pmod{110}$	$x \equiv -a \pmod{110}$	$x \equiv -3 \pmod{110}$

To get the non-obvious solution a, we solve $x \equiv 1 \pmod{2}$, $x \equiv 3 \pmod{5}$, $x \equiv -3 \pmod{11}$.

$$x \equiv 1 \cdot 55 \cdot \underbrace{55^{-1}_{\bmod 2}}_{1} + 3 \cdot 22 \cdot \underbrace{22^{-1}_{\bmod 5}}_{-2} - 3 \cdot 10 \cdot \underbrace{10^{-1}_{\bmod 11}}_{-1} \equiv 55 - 132 + 30 \equiv -47 \pmod{110}$$

Hence, the solutions are $x \equiv \pm 3 \pmod{110}$ and $x \equiv \pm 47 \pmod{110}$.

11 Euler's phi function

Definition 110. **Euler's phi function** $\phi(n)$ denotes the number of integers in $\{1, 2, ..., n\}$ that are relatively prime to n.

[For $n > 1$, we might as well replace $\{1, 2, ..., n\}$ with $\{1, 2, ..., n-1\}$.]

Important comment. In other words, $\phi(n)$ counts how many numbers are invertible modulo n.

Example 111. Compute $\phi(n)$ for $n = 1, 2, ..., 8$.

Solution. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$.

Observation 1. $\phi(n) = n - 1$ if and only if n is a prime.

This is true because $\phi(n) = n - 1$ if and only if n doesn't share a common factor with any of $\{1, 2, ..., n-1\}$.

Observation 2. If p is a prime, then $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

This is true because, if p is a prime, then $n = p^k$ is coprime to all $\{1, 2, ..., p^k\}$ except $p, 2p, ..., p^k$.

Theorem 112.

(a) $\phi(n) = n - 1$ if and only if n is a prime.

(b) If p is a prime, then $\phi(p^k) = p^k - \frac{p^k}{p} = p^k\left(1 - \frac{1}{p}\right)$.

(c) ϕ is multiplicative, that is, $\phi(nm) = \phi(n)\phi(m)$ whenever n, m are coprime.

(d) $\boxed{\text{If the prime factorization of } n \text{ is } n = p_1^{k_1} \cdots p_r^{k_r}, \text{ then } \phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).}$

Proof.

(a) $\phi(n) = n - 1$ if and only if n doesn't share a common factor with any of $\{1, 2, ..., n-1\}$. That's true for n precisely when it is a prime.

(b) If p is a prime, then $n = p^k$ is coprime to all $\{1, 2, ..., p^k\}$ except $p, 2p, ..., p^k$.

(c) Note that a is invertible modulo nm if and only if a is invertible modulo both n and m.
The claim therefore follows from the Chinese remainder theorem which provides a bijective (i.e., 1-1 and onto) correspondence

$$x \pmod{nm} \mapsto \left[\begin{array}{c} x \pmod{n} \\ x \pmod{m} \end{array}\right].$$

Alternatively, our book contains a direct proof (page 133).

(d) Using the two previous parts, we have
$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$. □

Example 113. Compute $\phi(1000)$.

Solution. $\phi(1000) = \phi(2^3 \cdot 5^3) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$.

Alternatively. $\phi(1000) = \phi(2^3) \cdot \phi(5^3) = (8 - 4)(125 - 25) = 400$

Example 114. **(extra)** Compute $\phi(980)$.

Solution. $\phi(980) = \phi(2^2 \cdot 5 \cdot 7^2) = 980\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 336$.

Armin Straub
straub@southalabama.edu