Example 98. Determine the modular inverse of $17 \pmod{88}$.

Solution. (direct) We can use the extended Euclidian algorithm directly. Left as an exercise!

Solution. (Chinese remainder theorem) $88 = 8 \cdot 11$. Hence, we instead solve $17x \equiv 1 \pmod{8}$, $17x \equiv 1 \pmod{11}$. Simplified: $x \equiv 1 \pmod{8}$, $6x \equiv 1 \pmod{11}$.

The inverting on that level is easy: $x \equiv 1 \pmod{8}$, $x \equiv 2 \pmod{11}$.

$x \equiv 1 \pmod{8}$, $x \equiv 0 \pmod{11}$: $x = 11 \cdot \underbrace{(11)^{-1}}_{\bmod 8} = 11 \cdot 3 = 33$

$x \equiv 0 \pmod{8}$, $x \equiv 1 \pmod{11}$: $x = 8 \cdot \underbrace{(8)^{-1}}_{\bmod 11} = 8 \cdot (-4) = -32$

Combined $x \equiv 1 \cdot 33 + 2 \cdot (-32) = -31 \equiv 57 \pmod{88}$.

Comment. Now that we are used to it some more, we can immediately write down the solution to $x \equiv 1 \pmod{8}$, $x \equiv 2 \pmod{11}$ as $x \equiv 1 \cdot 11 \cdot \underbrace{(11)^{-1}}_{\bmod 8} + 2 \cdot 8 \cdot \underbrace{(8)^{-1}}_{\bmod 11} \equiv 1 \cdot 11 \cdot 3 + 2 \cdot 8 \cdot (-4) = -31 \equiv 57 \pmod{88}$.

Comment. It is not so convincing in this small example, but the Chinese remainder theorem is important for practical purposes when working with very large numbers.

Example 99. Determine the modular inverse of $17 \pmod{42}$.

Solution. (Chinese remainder theorem) $42 = 2 \cdot 3 \cdot 7$.

Inverting modulo $2, 3, 7$ is easy: $17^{-1} \equiv 1^{-1} \equiv 1 \pmod{2}$, $17^{-1} \equiv 2^{-1} \equiv 2 \pmod{3}$, $17^{-1} \equiv 3^{-1} \equiv 5 \pmod{7}$.

$17^{-1} \equiv 1 \cdot 3 \cdot 7 \cdot \underbrace{(3 \cdot 7)^{-1}}_{\bmod 2} + 2 \cdot 2 \cdot 7 \cdot \underbrace{(2 \cdot 7)^{-1}}_{\bmod 3} + 5 \cdot 2 \cdot 3 \cdot \underbrace{(2 \cdot 3)^{-1}}_{\bmod 7} \equiv 21 \cdot 1 + 28 \cdot 2 + 30 \cdot (-1) = 47 \equiv 5 \pmod{42}$

Example 100. Compute $3^{100} \pmod{60}$.

Solution. (direct) We could use binary exponentiation directly. Do it as an exercise! (But note that we cannot reduce the exponent 100 using Fermat's little theorem because 60 is not a prime; however, there exists a generalization, known as Euler's theorem, that we could use instead. This will be discussed next class.)

Solution. (Chinese remainder theorem) Notice that $60 = 4 \cdot 3 \cdot 5$, where $4, 3, 5$ are pairwise coprime.

By the Chinese remainder theorem, determining $x \equiv 3^{100} \pmod{60}$ is the same as finding $x \equiv 3^{100} \pmod{4}$, $x \equiv 3^{100} \pmod{3}$, $x \equiv 3^{100} \pmod{5}$. It is now super easy to reduce 3^{100} in each case:

$$3^{100} \equiv (-1)^{100} = 1 \pmod{4}, \quad 3^{100} \equiv 0 \pmod{3}, \quad 3^{100} \equiv (3^4)^{25} \equiv 1 \pmod{5}$$

(Note that we are using Fermat's little theorem in the modulo 5 case.)

Thus, $3^{100} \equiv 1 \cdot 3 \cdot 5 \cdot [(3 \cdot 5)^{-1}_{\bmod 4}] + 1 \cdot 4 \cdot 3 \cdot [(4 \cdot 3)^{-1}_{\bmod 5}] \equiv 15 \cdot (-1) + 12 \cdot 3 = 21 \pmod{60}$.

Definition 101. Euler's phi function $\phi(n)$ denotes the number of integers in $\{1, 2, \ldots, n\}$ that are relatively prime to n.

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

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

Example 102. Compute $\phi(n)$ for $n = 1, 2, \ldots, 8$.

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 $\{1, 2, \ldots, n-1\}$.

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 $\{1, 2, \ldots, p^k\}$ except $p, 2p, \ldots, p^k$.