The next example illustrates once more that, when solving a problem modulo a composite number, it can be useful to use the Chinese remainder theorem.

Example 90. Determine the modular inverse of $17 \pmod{42}$.

Solution. (direct) Of course, we can use the Euclidean algorithm directly modulo $n = 42$.

Solution. (using Euler's theorem) Another option is to use Euler's theorem: since $\phi(42) = \phi(2 \cdot 3 \cdot 7) = 12$, we have $17^{12} \equiv 1 \pmod{42}$. Hence, $17^{-1} \equiv 17^{11} \pmod{42}$ (which we then compute using binary exponentiation).

But. However, as Example 92 illustrates, computing $\phi(n)$ is just as difficult as factoring n. So, we can only use Euler's theorem if we know the factorization of n. (Recall that we are not able to factorize very large numbers.)

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

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

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

Comment. For large n, using the CRT might be a little faster than using the Euclidean algorithm directly, but only if we already know the factorization of n.

Example 91. (homework) Compute $7^{111} \pmod{90}$ in the following three different ways:

(a) Directly, using binary exponentiation.

(b) With the help of Euler's theorem.

(c) With the help of the Chinese remainder theorem (as well as Euler's theorem).

Solution.

(a) Modulo 90, we have $7^2 = 49$, $7^4 = 49^2 \equiv 61$, $7^8 \equiv 61^2 \equiv 31$, $7^{16} \equiv 31^2 \equiv 61$, $7^{32} \equiv 31$, $7^{64} \equiv 61$. Therefore, $7^{111} = 7^{64} \cdot 7^{32} \cdot 7^8 \cdot 7^4 \cdot 7^2 \cdot 7 \equiv 61 \cdot 31 \cdot 31 \cdot 61 \cdot 49 \cdot 7 \equiv 73 \pmod{90}$.

(b) Since $90 = 2 \cdot 3^2 \cdot 5$, we find $\phi(90) = 90\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 24$ so that Euler's theorem tells us that $7^{24} \equiv 1 \pmod{90}$. Since $111 \equiv 15 \pmod{24}$, we have $7^{111} \equiv 7^{15} = 7^8 \cdot 7^4 \cdot 7^2 \cdot 7 \equiv 31 \cdot 61 \cdot 49 \cdot 7 \equiv 73 \pmod{90}$.

(c) Notice that $90 = 2 \cdot 3^2 \cdot 5$, where $2, 9, 5$ are pairwise coprime.

Computing 7^{111} modulo each of $2, 9, 5$ is much easier (note that $\phi(9) = 9\left(1 - \frac{1}{3}\right) = 6$ so that, by Euler's theorem $7^6 \equiv 1 \pmod{9}$; on the other hand, $7^4 \equiv 1 \pmod{5}$):

$$7^{111} \equiv 1^{111} \equiv 1 \pmod{2}, \quad 7^{111} \equiv 7^3 \equiv (-2)^3 \equiv 1 \pmod{9}, \quad 7^{111} \equiv 7^3 \equiv 2^3 \equiv 3 \pmod{5}.$$

By the Chinese remainder theorem,

$$7^{111} \equiv 1 \cdot 9 \cdot 5 \cdot \underbrace{[(9 \cdot 5)^{-1}_{\bmod 2}]}_{1} + 1 \cdot 2 \cdot 5 \cdot \underbrace{[(2 \cdot 5)^{-1}_{\bmod 9}]}_{1} + 3 \cdot 2 \cdot 9 \cdot \underbrace{[(2 \cdot 9)^{-1}_{\bmod 5}]}_{2} \equiv 45 + 10 + 108 \equiv 73 \pmod{90}.$$

Comment. While this might seem like the most involved approach (it certainly requires the most expertise), observe that the actual computations are much simpler than in the other cases (because we are operating modulo very small numbers).

Example 92. (bonus challenge) Find the factors of the following number $M = pq$:

8932028005743736339360838638746936049507991577307359908743556942810827\
0761514611650691813353664018876504777533577602609343916545431925218633\
75114106509563452970373049082933244013107347141654282924032714311

As indicated in Example 78, this is difficult. Through some sort of espionage, however, you have learned that $\phi(M)$ is:

8932028005743736339360838638746936049507991577307359908743556942810827\
0761514611650691813353664018867572649527833866269983077906684989169125\
75956375773572578614678768000225628866990840223520746283867797512

In general, if $M = pq$ is a product of two large primes p, q, given $\phi(M)$, how can we factor M?

Comment. Even if we don't know the number of prime factors of M (in the above case we know that M is a product of two primes), we can "efficiently" factor M if we know the value of $\phi(M)$.

Definition 93. The **multiplicative order** of an invertible residue a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Lemma 94. If $a^r \equiv 1 \pmod{n}$ and $a^s \equiv 1 \pmod{n}$, then $a^{\gcd(r,s)} \equiv 1 \pmod{n}$.

Proof. By Bezout's identity, there are integers x, y such that $xr + ys = \gcd(r, s)$.
Hence, $a^{\gcd(r,s)} = a^{xr+ys} = a^{xr}a^{ys} = (a^r)^x(a^s)^y \equiv 1 \pmod{n}$. □

Corollary 95. The multiplicative order of a modulo n divides $\phi(n)$.

Proof. Let k be the multiplicative order, so that $a^k \equiv 1 \pmod{n}$. By Euler's theorem $a^{\phi(n)} \equiv 1 \pmod{n}$. The previous lemma shows that $a^{\gcd(k,\phi(n))} \equiv 1 \pmod{n}$. But since the multiplicative order is the smallest exponent, it must be the case that $\gcd(k, \phi(n)) = k$. Equivalently, k divides $\phi(n)$. □

Example 96. Compute the multiplicative order of 2 modulo $7, 11, 9$.

Solution.

- $2 \pmod{7}$
  $2^2 \equiv 4, 2^3 \equiv 1$. Hence, the order of 2 modulo 7 is 3.
  (From Fermat, we know that $2^6 \equiv 1$. Indeed, 3 divides 6.)

- $2 \pmod{11}$
  First approach (too much unnecessary work). $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 5, 2^5 \equiv 2 \cdot 5 = 10, 2^6 \equiv 2 \cdot 10 \equiv 9, 2^7 \equiv 2 \cdot 9 \equiv 7, 2^8 \equiv 2 \cdot 7 \equiv 3, 2^9 \equiv 2 \cdot 3 = 6, 2^{10} \equiv 2 \cdot 6 \equiv 1$. Thus, the order of 2 mod 11 is 10.
  Better approach. Since $\phi(11) = 10$, the only possible orders are $2, 5, 10$. Hence, checking that $2^2 \not\equiv 1$ and $2^5 \not\equiv 1$ is enough to conclude that the order must be 10.

- $2 \pmod{9}$
  Since $\phi(9) = 6$, the only possible orders are $2, 3, 6$. Hence, checking that $2^2 \not\equiv 1$ and $2^3 \not\equiv 1$ is enough to conclude that the order must be 6. (Indeed, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$.)