Example 134. Compute $3^{29} \pmod{77}$ using the Chinese remainder theorem.

Solution. We determine $x = 3^{29}$ both modulo 7 and 11:

- $3^{29} \equiv 3^5 \equiv 3 \cdot 4 \equiv -2 \pmod 7$ [Here, we used $29 \equiv 5 \pmod{\phi(7)}$ and $3^2 \equiv 2$, $3^4 \equiv 4 \pmod 7$.]
- $3^{29} \equiv 3^{-1} \equiv 4 \pmod{11}$ [Here, we proceeded unusually and used $29 \equiv -1 \pmod{\phi(11)}$.]

Therefore, $x \equiv -2 \pmod 7$ and $x \equiv 4 \pmod{11}$.
Using the Chinese remainder theorem, $x = -2 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{2} + 4 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{-3} \equiv -128 \equiv 26 \pmod{77}$.

Comment. Alternatively, we can proceed modulo $n = 77$ directly and use binary computation. However, if we already know the factorization of n (that's a big "if" for large n), then applying the CRT is a little faster.

13.1 More on Euler's theorem

Example 135. Compute $7^{100} \pmod{60}$.

Solution. $\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$. Since $\gcd(7, 60) = 1$, we obtain that $7^{16} \equiv 1 \pmod{60}$ by Euler's theorem. Since $100 \equiv 4 \pmod{16}$, we have $7^{100} \equiv 7^4 \pmod{60}$.
It remains to notice that $7^2 = 49 \equiv -11$ and hence $7^4 \equiv (-11)^2 = 121 \equiv 1 \pmod{60}$. So, $7^{100} \equiv 1 \pmod{60}$.
Comment. See the next example, which shows that we actually have $a^4 \equiv 1 \pmod{60}$ for all integers a coprime to 60.

Example 136. Euler's theorem doesn't necessarily provide an optimal exponent. For instance, show that $a^4 \equiv 1 \pmod{60}$ for all integers a coprime to 60.

Note. Since $\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$, Euler's theorem shows that $a^{16} \equiv 1 \pmod{60}$.

Proof. By the Chinese remainder theorem, $a^4 \equiv 1 \pmod{60}$ is equivalent to

$$a^4 \equiv 1 \pmod 4, \quad a^4 \equiv 1 \pmod 3, \quad a^4 \equiv 1 \pmod 5.$$

All three of these congruences are true:

- $a^4 \equiv 1 \pmod 5$ is true by Fermat's little theorem.
- $a^4 \equiv 1 \pmod 3$ is true, because $a^2 \equiv 1 \pmod 3$ by Fermat's little theorem.
- $a^4 \equiv 1 \pmod 4$ is true, because $a^2 \equiv 1 \pmod 4$ by Euler's theorem ($\phi(4) = 2$).

(Note that a is coprime to 60 if and only if a is coprime to each of 4, 3, 5.) □

A brute-force verification in Sage. The following computation also proves the claim. Even if you have never coded yourself, you can surely figure out what the following code is doing:

```
Sage] [1..59]
```

$[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59]$

```
Sage] [ x for x in [1..59] if gcd(x,60)==1 ]
```

$[1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59]$

```
Sage] [ x^4 % 60 for x in [1..59] if gcd(x,60)==1 ]
```

$[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]$

Example 137. As in the previous example, show that $a^6 \equiv 1 \pmod{42}$ for all integers a coprime to 42.

Note. Since $\phi(42) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12$, Euler's theorem shows that $a^{12} \equiv 1 \pmod{42}$.

Proof. By the Chinese remainder theorem, $a^6 \equiv 1 \pmod{42}$ is equivalent to

$$a^6 \equiv 1 \pmod{2}, \quad a^6 \equiv 1 \pmod{3}, \quad a^6 \equiv 1 \pmod{7}.$$

But these congruences all follow from Fermat's little theorem (because 6 is a multiple of $2-1=1$, $3-1=2$ and $7-1=6$)! (Note that a is coprime to 42 if and only if a is coprime to each of 2, 3, 7.) □

Advanced. Based on these ideas, can you formulate a general strengthening of Euler's theorem?
https://en.wikipedia.org/wiki/Carmichael_function

14 Primality testing

Recall that it is extremely difficult to factor large integers (this is the starting point for many cryptosystems). Surprisingly, it is much simpler to tell if a number is prime.

Example 138. The following is the number mentioned earlier, for which RSA Laboratories, until 2007, offered $100,000 to the first one to factorize it. To this day, nobody has been able to do so.

Has the thought crossed your mind that the challengers might be tricking everybody by choosing M to be a huge prime that cannot be factored further? Well, we'll talk more about primality testing soon. But we can actually quickly convince ourselves that M cannot be a prime. If M was prime then, by Fermat's little theorem, $2^{M-1} \equiv 1 \pmod{M}$. Below, we compute $2^{M-1} \pmod{M}$ and find that $2^{M-1} \not\equiv 1 \pmod{M}$. This proves that M is not a prime. It doesn't bring us any closer to factoring it though.

Comment. Ponder this for a while. We can tell that a number is composite without finding its factors. Both sides to this story (first, being able to efficiently tell whether a number is prime, and second, not being able to factor large numbers) are of vital importance to modern cryptography.

```
Sage] rsa = Integer("135066410865995223349603216278805969938881475605667027524485143851\
                     525510604859533833940287150571909441798207282164471551373680419703\
                     964191743046496589274256239341020864383202110372958725762358509643\
                     110564073501508187510676594629205563685529475213500852879416377328\
                     533906109750544334999811150056977236890927563")

Sage] power_mod(2, rsa-1, rsa)

    120939094432033615867650595352956996867540098463588951238902808367556733932202059338 53\
    348534147116662841968124107288512373904071077139405352848835710498409193003137847878 95\
    226029615123284879513798127406300472693925500331497519103479951096634123177725212482 97\
    950196643140069546889855131459759160570963857373851
```

Comment. Just for giggles, let us emphasize once more the need to compute $2^{N-1} \pmod{N}$ without actually computing 2^{N-1}. Take, for instance, the 1024 bit RSA challenge number $N = 135...563$ in this example. The number 2^{N-1} itself has $N - 1 \approx 2^{1024} \approx 10^{308.3}$ binary digits. It is often quoted that the number of particles in the visible universe is estimated to be between 10^{80} and 10^{100}. Whatever these estimates are worth, our number has WAY more digits (!) than that. Good luck writing it out! [Of course, the binary digits are a single 1 followed by all zeros. However, we need to further compute with that!]

Comment. There is nothing special about 2. You could just as well use, say, 3.