Example 89. Compute $407^{37249} \pmod{101}$.

Solution. First, $407^{37249} \equiv 3^{37249} \pmod{101}$. Then, using Fermat, $3^{37249} \equiv 3^{49} \pmod{101}$.
We then use binary exponentiation:
$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, $3^{32} \equiv 16^2 \equiv 54$, all modulo 101
Since $49 = (110001)_2 = 2^0 + 2^4 + 2^5$, we have $3^{49} = 3^{32} \cdot 3^{16} \cdot 3^1 \equiv 54 \cdot 16 \cdot 3 \equiv 67 \pmod{101}$.
In conclusion, $407^{37249} \equiv 67 \pmod{101}$.

Example 90. (extra) Using binary exponentiation, compute $5^{49} \pmod{105}$.

Solution. Recall that $49 = (110001)_2 = 2^0 + 2^4 + 2^5$.
$5^1 = 5$, $5^2 = 25$, $5^4 = 25^2 = 625 \equiv -5$, $5^8 \equiv (-5)^2 = 25$, $5^{16} \equiv 25^2 \equiv -5$, $5^{32} \equiv (-5)^2 = 25$
Hence, $5^{49} = 5^{32} \cdot 5^{16} \cdot 5^1 \equiv 25 \cdot (-5) \cdot 5 \equiv 5$.

9 Chinese remainder theorem

Example 91. (warmup)

(a) If $x \equiv 3 \pmod{10}$, what can we say about $x \pmod 5$?

(b) If $x \equiv 3 \pmod 7$, what can we say about $x \pmod 5$?

Solution.

(a) If $x \equiv 3 \pmod{10}$, then $x \equiv 3 \pmod 5$.
[Why?! Because $x \equiv 3 \pmod{10}$ if and only if $x = 3 + 10m$, which modulo 5 reduces to $x \equiv 3 \pmod 5$.]

(b) Absolutely nothing! $x = 3 + 7m$ can be anything modulo 5 (because $7 \equiv 2$ is invertible modulo 5).

Example 92. If $x \equiv 3 \pmod 5$, what can we say about $x \pmod{15}$?

Solution. $x \equiv 3, 8, 13 \pmod{15}$

Example 93. If $x \equiv 32 \pmod{35}$, then $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$.

Why?! As in the first part of the warmup, if $x \equiv 32 \pmod{35}$, then $x \equiv 32 \pmod 5$ and $x \equiv 32 \pmod 7$.

The Chinese remainder theorem says that this can be reversed!

That is, if $x \equiv 2 \pmod 5$ and $x \equiv 4 \pmod 7$, then the value of x modulo $5 \cdot 7 = 35$ is determined.
[How to find the value $x \equiv 32 \pmod{35}$ is discussed in the next example.]

Example 94. Solve $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$.

Solution. $x \equiv 2 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 5}}_{3} + 4 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 7}}_{3} \equiv 42 + 60 \equiv 32 \pmod{35}$

Important comment. Can you see how we need 5 and 7 to be coprime here?

Brute force solution. Note that, while in principle we can always perform a brute force search, this is not practical for larger problems. Here, if x is a solution, then so is $x + 35$. So we only look for solutions modulo 35.
Since $x \equiv 4 \pmod 7$, the only candidates for solutions are $4, 11, 18, \ldots$ Among these, we find $x = 32$.
[We can also focus on $x \equiv 2 \pmod 5$ and consider the candidates $2, 7, 12, \ldots$, but that is even more work.]

Example 95. Solve $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 5$.

Solution. $x \equiv 2 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 3}}_{-1} + 1 \cdot 3 \cdot \underbrace{3^{-1}_{\bmod 5}}_{2} \equiv -10 + 6 \equiv 11 \pmod{15}$

Theorem 96. (Chinese Remainder Theorem) Let $n_1, n_2, \ldots, n_r$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad \ldots, \quad x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique modulo $n = n_1 \cdots n_r$.

In other words. The Chinese remainder theorem provides a bijective (i.e., 1-1 and onto) correspondence

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

For instance. Let's make the correspondence explicit for $n = 2$, $m = 3$:
$0 \mapsto \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$, $1 \mapsto \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$, $2 \mapsto \left[\begin{smallmatrix} 0 \\ 2 \end{smallmatrix}\right]$, $3 \mapsto \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, $4 \mapsto \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$, $5 \mapsto \left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right]$

Example 97.

(a) Let $p > 3$ be a prime. Show that $x^2 \equiv 9 \pmod p$ has exactly two solutions (i.e. ± 3).

(b) Let p, $q > 3$ be distinct primes. Show that $x^2 \equiv 9 \pmod{pq}$ always has exactly four solutions (± 3 and two more solutions $\pm a$).

Solution.

(a) If $x^2 \equiv 9 \pmod p$, then $0 \equiv x^2 - 9 = (x-3)(x+3) \pmod p$. Since p is a prime it follows that $x - 3 \equiv 0 \pmod p$ or $x + 3 \equiv 0 \pmod p$. That is, $x \equiv \pm 3 \pmod p$.

(b) By the CRT, we have $x^2 \equiv 9 \pmod{pq}$ if and only if $x^2 \equiv 9 \pmod p$ and $x^2 \equiv 9 \pmod q$. Hence, $x \equiv \pm 3 \pmod p$ and $x \equiv \pm 3 \pmod q$. These combine in four different ways.
For instance, $x \equiv 3 \pmod p$ and $x \equiv 3 \pmod q$ combine to $x \equiv 3 \pmod{pq}$. However, $x \equiv 3 \pmod p$ and $x \equiv -3 \pmod q$ combine to something modulo pq which is different from 3 or -3.

Why primes >3? Why did we exclude the primes 2 and 3 in this discussion?
Comment. There is nothing special about 9. The same is true for $x^2 \equiv a^2 \pmod{pq}$ for any integer a.

Example 98. Determine all solutions to $x^2 \equiv 9 \pmod{35}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 9 \pmod{35} \\ \iff\ & x^2 \equiv 9 \pmod 5 \text{ and } x^2 \equiv 9 \pmod 7 \\ \iff\ & x \equiv \pm 3 \pmod 5 \text{ and } x \equiv \pm 3 \pmod 7 \end{aligned}$$

The two obvious solutions modulo 35 are ± 3. To get one of the two additional solutions, we solve $x \equiv 3 \pmod 5$, $x \equiv -3 \pmod 7$. [Then the other additional solution is the negative of that.]

$$x \equiv 3 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 5}}_{3} - 3 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 7}}_{3} \equiv 63 - 45 \equiv 18 \pmod{35}$$

Hence, the solutions are $x \equiv \pm 3 \pmod{35}$ and $x \equiv \pm 18 \pmod{35}$. [$\pm 18 \equiv \pm 17 \pmod{35}$]