Modular Arithmetic

There are several concepts and theorems that were known in nearly every civilised culture (independently from each other!). Some examples are the Theorem of Pythagoras (see chapter *The Theorem of Pythagoras*), the number Pi (see chapter *Pi*) or modular arithmetic (with the Euclidean Algorithm as one example). Those were known to the ancient Greeks but also to the Indians and the Chinese.
The Chinese (like the other Islamic and Asian cultures, too) became familiar with modular arithmetic while discussing astronomical and calendrical problems, where they had to solve systems of indeterminate linear equations. However, there were also some simple congruence problems considered by the ancient Chinese, and "in fact probably the most famous mathematical technique coming from China is the techinque long known as the Chinese remainder theorem" ([Katz, p. 222]), which even has the word Chinese in it. This theorem was named "after a description of some congruence problems appeared in one of the first reports in the West on Chinese mathematics, articles by Alexander Wylie published in 1852 in the North China Herald, which were soon translated into both German and French and republished in European journals" [Katz, p. 222], so it wasn't the Chinese who gave this theorem its name. This theorem states the following:

> Let r and s be positive integers which are relatively prime and let a and b be any two integers. Then there is an integer N such that
>
> $N \equiv a \ (mod\ r)$ and $N \equiv b \ (mod\ s)$
>
> Moreover, N is uniquely determined modulo rs.

The earliest example of one dealing with this theorem dates back to Sun Zi. In his *Sunzi suanjing* (this can be translated to *Mathematical Classics of Master Sun*, written around the third century), he states:

> "We have things of which we do not know the number; if we count them by threes, the remainder is 2; if we count them by fives, the remainder is 3; if we count them by sevens, the remainder is 2. How many things are there?" [Katz, p. 222]

Here we can see the connection to the word remainder. If we rewrite this riddle using our modern modulo notation[1] this would be:

$$N \equiv 2 \ (mod\ 3) \ \ N \equiv 3 \ (mod\ 5), \ \ N \equiv 2 \ (mod\ 7),$$

or we could write it as well by finding an N such that it fulfills all of the following three conditions:

$$N = 3x + 2, \ \ N = 5y + 3, \ \ N = 7z + 2, \ with\ x, y, z \in \mathbb{Z}.$$

Moreover, Sun Zi was able to give the right solution (it is 23) as well as his strategy for it:

> "If we count by threes and there is a remainder 2, put down 140.
> If we count by fives and there is a remainder 3, put down 63.
> If we count by sevens and there is a remainder 2, put down 30.
> Add them to obtain 233 and subtract 210 to get the answer."
> [Stilwell, p. 71]

This task was the starting point of the Chinese remainder theorem, but it took many more years until it was advanced further. About two centuries after Sun Zi, in Zhang Quijian's *Mathematical Manual* there was a similar riddle posed, the problem of the "hundred fowls" (this task is famous because it also appears in various styles in other cultures like India or in Islamic and European countries). It originally is stated as follows:

> "A rooster is worth 5 coins, a hen 3 coins, and 3 chicks 1 coin. With 100 coins we buy 100 of the fowls. How many roosters, hens and chicks are there?"
> [Katz, p. 223]

He gave the correct answer but only hinted at his methods for obtaining it. All in all, we can see that the Chinese mathematicians were familiar with such remainder problems.
A strategy for the general solution of Sun Zi's problem was given only in 1247, in the Mathematical Treatise in Nine Sections by Qin Jiushao. This depended heavily on finding inverses by the Euclidean algorithm, a method he called "method of finding 1", [Stilwell, p. 73].
When the Chinese remainder theorem was finally discovered in Europe, Gauss and Euler utilized it frequently (see chapter *Gauss on congruences*).

[1] We say that $a \equiv b \ (mod\ n)$ if we can write b as $b = cn + a$ for some integer c or, equivalently, if n divides $(b - a)$.

References

[Katz] Victor Katz, A history of Mathematics - an introduction, Addison-Wesley, Boston, 2009

[Stilwell] John Stilwell, Mathematics and its History, Third Edition, Springer Verlag, New York, 2010