Example 8. Find the modular inverse of 17 modulo 23.

Solution. We determine $17^{-1} \pmod{23}$ using the extended Euclidean algorithm:

$$\begin{aligned} &\gcd(17,23) && \boxed{23} = 1\cdot\boxed{17} + 6 && \text{or:} && \boxed{A} \quad 6 = 1\cdot\boxed{23} - 1\cdot\boxed{17} \\ &= \gcd(6,17) && \boxed{17} = 3\cdot\boxed{6} - 1 && && \boxed{B} \quad 1 = -1\cdot\boxed{17} + 3\cdot\boxed{6} \\ &= 1 \end{aligned}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$1 \;=\; \underset{\boxed{B}}{-1\cdot\boxed{17} + 3\cdot\boxed{6}} \;=\; \underset{\boxed{A}}{3\cdot\boxed{23} - 4\cdot\boxed{17}}$$

Reducing $1 = 3\cdot 23 - 4\cdot 17$ modulo 23, we get $-4\cdot 17 \equiv 1 \pmod{23}$.
Hence, $17^{-1} \equiv -4 \pmod{23}$. [Or, if preferred, $17^{-1} \equiv 19 \pmod{23}$.]

Example 9. (homework) For further practice with the extended Euclidean algorithm:

(a) Determine $46^{-1} \pmod{99}$.

(b) Solve $81x \equiv 4 \pmod{101}$.

Solution.

(a) The final answer is $46^{-1} \equiv 28 \pmod{99}$.

(b) The final answer is $x \equiv 20 \pmod{101}$.

1.2 Application: credit card numbers

Have you ever thought about the numbers on your credit card? Usually, these are 16 digits. For instance, 4266 8342 8412 9270.

No worries (or false hopes...). While close, this is not exactly my credit card number.

- The first digit(s) of a credit card identify the issuer of the card. For instance, a leading 4 is typically Visa, 51 to 55 indicate Mastercard, and 34, 37 indicate American Express. The above credit card is indeed a Visa card.

  More information at: https://en.wikipedia.org/wiki/Payment_card_number

- The last digit is a **check digit**, and a valid credit card number must pass the **Luhn check** (patented by IBM scientist Hans Peter Luhn in 1954/60; now in public domain). This works as follows: every second digit, starting with the first, is doubled. If that results in a two-digit number, we take the sum of those two digits.

$$\begin{bmatrix} & 4 & 2 & 6 & 6 & 8 & 3 & 4 & 2 & 8 & 4 & 1 & 2 & 9 & 2 & 7 & 0 \\ \times 2 & 8 & & 12 & & 16 & & 8 & & 16 & & 2 & & 18 & & 14 & \\ & 8 & 2 & 3 & 6 & 7 & 3 & 8 & 2 & 7 & 4 & 2 & 2 & 9 & 2 & 5 & 0 \end{bmatrix}$$

  The other half of the digits is left unchanged. We then add all these digits and reduce modulo 10:

$$8+2+3+6+7+3+8+2+7+4+2+2+9+2+5+0 \equiv 0 \pmod{10}$$

  The result of that computation must be 0. Otherwise, the credit card number fails the Luhn check and is invalid.

Example 10. (homework)

(a) Check that the number 4266 8342 8412 9280 fails the Luhn check.

(b) How do we have to change the last digit to turn this into a valid credit card number?

The purpose of the Luhn check is to detect accidental errors.

[A random number has a 90% chance of failing the Luhn check. Why?!]

On the other hand, as the previous example shows, it provides basically no protection against malicious attacks (except against amateur thiefs not aware of the Luhn check).

Note that it was designed before online banking. So a special focus is on detecting accidental errors that occur frequently when writing down (things like) credit card numbers by hand.

- For instance, it is common that a single digit gets messed up. Every such error is detected by the Luhn check. (Why?!)
- Another common error is to transpose two digits. Every such error (with the exception of 09 versus 90) is detected.

  For instance. A 82 at the beginning contributes $7+2=9$ to the check sum, while a 28 contributes $4+8\equiv 2$ to the sum. Hence, replacing one with the other will result in the Luhn check failing.

Example 11. The doubling and sum-of-digits procedure permutes the digits as follows:

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{bmatrix}$$

Example 12. The Luhn check has the somewhat complicated feature that every second digit has to be doubled. Why do we not just add all the original digits and reduce the sum modulo 10?

Solution. One reason is that this simplified check does not catch the transposition of two digits. Why?!

[On the other hand, that simplified check does also detect if just a single digit is incorrect.]

1.3 An encrypted message

Example 13. (bonus challenge!) You find a post-it with the following message:

$$ITGGVKPIUUVTCPIGT$$

Can you make any sense of it?