Example 30. (bonus challenge!) You intercept the following message from Alice:

WHCUHFWXOWHUQXOMOMQVSQWAMWHCUHFXOLNWXQMQVSQWAWMQLN

Your experience tells you that Alice is using a substitution cipher. You also know that this message contains the word "secret". Can you crack it?

Note. In modern practice, it is not uncommon to know (or suspect) what a certain part of the message should be. For instance, PDF files start with "%PDF" (0x25504446).

See https://en.wikipedia.org/wiki/Magic_number_(programming) for more such instances.

(Send me an email by 1/22 with the plaintext and how you found it to collect a bonus point.)

Example 31. Compute $3^{1003} \pmod{101}$.

Solution. Since 101 is a prime, $3^{100} \equiv 1 \pmod{101}$ by Fermat's little theorem.
Because $3^{100} \equiv 3^0 \pmod{101}$, this enables us to reduce exponents modulo 100.
In particular, since $1003 \equiv 3 \pmod{100}$, we have $3^{1003} \equiv 3^3 = 27 \pmod{101}$.

Example 32. Compute $3^{25} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.
Instead, we do **binary exponentiation**:
$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, all modulo 101
$25 = 16 + 8 + 1$ [Every integer $n \geqslant 0$ can be written as a sum of distinct powers of 2 (in a unique way).]
Hence, $3^{25} = 3^{16} \cdot 3^8 \cdot 3^1 \equiv 16 \cdot (-4) \cdot 3 = -192 \equiv 10 \pmod{101}$.

Euler's theorem

Recall that Fermat's little theorem is just the special case of Euler's theorem :

Theorem 33. (Euler's theorem) If $n \geqslant 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Euler's theorem can be proved along the lines of our earlier proof of Fermat's little theorem. The only adjustment is to only start with multiples ka where k is invertible modulo n. There is $\phi(n)$ such residues k, and so that's where Euler's phi function comes in. Can you complete the proof? □

Example 34. What are the last two (decimal) digits of 3^{7082}?

Solution. We need to determine $3^{7082} \pmod{100}$. $\phi(100) = \phi(2^2 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

Since $\gcd(3, 100) = 1$ and $7082 \equiv 2 \pmod{40}$, Euler's theorem shows that $3^{7082} \equiv 3^2 = 9 \pmod{100}$.

Example 35. (extra) Compute $2^{20} \pmod{41}$.

Solution. $2^2 = 4$, $2^4 = 16$, $2^8 = 256 \equiv 10$, $2^{16} \equiv 100 \equiv 18$. Hence, $2^{20} = 2^{16} \cdot 2^4 \equiv 18 \cdot 16 = 288 \equiv 1 \pmod{41}$.
Or: $2^5 = 32 \equiv -9 \pmod{41}$. Hence, $2^{20} = (2^5)^4 \equiv (-9)^4 = 81^2 \equiv (-1)^2 = 1 \pmod{41}$.

Comment. Write $a = 2^{20} \pmod{41}$. It follows from Fermat's little theorem that $a^2 \equiv 1 \pmod{41}$. The argument below shows that $a \equiv \pm 1 \pmod{41}$ [but we don't know which until we do the calculation].
The equation $x^2 \equiv 1 \pmod{p}$ is equivalent to $(x-1)(x+1) \equiv 0 \pmod{p}$ [b/c $(x-1)(x+1) = x^2 - 1$]. Since p is a prime and $p | (x-1)(x+1)$, we must have $p | (x-1)$ or $p | (x+1)$. In other words, $x \equiv \pm 1 \pmod{p}$.

Armin Straub
straub@southalabama.edu

Representations of integers in different bases

We are commonly using the **decimal system** of writing numbers:

$$1234 = 4 \cdot 10^0 + 3 \cdot 10^1 + 2 \cdot 10^2 + 1 \cdot 10^3.$$

10 is called the base, and $1, 2, 3, 4$ are the digits in base 10. To emphasize that we are using base 10, we will write $1234 = (1234)_{10}$. Likewise, we write

$$(1234)_b = 4 \cdot b^0 + 3 \cdot b^1 + 2 \cdot b^2 + 1 \cdot b^3.$$

In this example, $b > 4$, because, if b is the base, then the digits have to be in $\{0, 1, \ldots, b - 1\}$.

Example 36. $25 = \boxed{1} \cdot 2^4 + \boxed{1} \cdot 2^3 + \boxed{0} \cdot 2^2 + \boxed{0} \cdot 2^1 + \boxed{1} \cdot 2^0$. We write $25 = (11001)_2$.

Example 37. (extra) Express 49 in base 2.

Solution.

- $49 = 24 \cdot 2 + \boxed{1}$. Hence, $49 = (\ldots 1)_2$ where $\ldots$ are the digits for 24.
- $24 = 12 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 01)_2$ where $\ldots$ are the digits for 12.
- $12 = 6 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 001)_2$ where $\ldots$ are the digits for 6.
- $6 = 3 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 0001)_2$ where $\ldots$ are the digits for 3.
- $3 = 1 \cdot 2 + \boxed{1}$, with $\boxed{1}$ left over. Hence, $49 = (110001)_2$.

Other bases. What is 49 in base 3? $49 = 16 \cdot 3 + \boxed{1}$, $16 = 5 \cdot 3 + \boxed{1}$, $5 = 1 \cdot 3 + \boxed{2}$, $\boxed{1}$. Hence, $49 = (1211)_3$.
What is 49 in base 7? $49 = (100)_7$.

Example 38. Bases 2, 8 and 16 (binary, octal and hexadecimal) are commonly used in computer applications.

For instance, in JavaScript or Python, $0\mathrm{b}\ldots$ means $(\ldots)_2$, $0\mathrm{o}\ldots$ means $(\ldots)_8$, and $0\mathrm{x}\ldots$ means $(\ldots)_{16}$.
The digits $0, 1, \ldots, 15$ in hexadecimal are typically written as $0, 1, \ldots, 9, A, B, C, D, E, F$.
Example. FACE value in decimal? $(FACE)_{16} = 15 \cdot 16^3 + 10 \cdot 16^2 + 12 \cdot 16 + 14 = 64206$
Practical example. `chmod 664 file.tex` (change file permission)

664 are octal digits, consisting of three bits: $1 = (001)_2$ execute (x), $2 = (010)_2$ write (w), $4 = (100)_2$ read (r)
Hence, 664 means rw,rw,r. What is rwx,rx,-? 750
By the way, a fourth (leading) digit can be specified (setting the flags: setuid, setgid, and sticky).

Example 39. (terrible jokes, parental guidance advised)

There are I0 types of people... those who understand binary, and those who don't.
Ok, ok, of course you knew that. How about:
There are II types of people... those who understand Roman numerals, and those who don't.
It's not getting better:
There are I0 types of people... those who understand hexadecimal, and F the rest...