2.3 Some review of Fermat's little theorem and Euler's theorem

Example 24. (warmup) What a terrible blunder... Explain what is wrong!

$$\text{(incorrect!)} \quad 10^9 \equiv 3^2 = 9 \equiv 2 \pmod{7}$$

Solution. $10^9 = 10 \cdot 10 \cdot \ldots \cdot 10 \equiv 3 \cdot 3 \cdot \ldots \cdot 3 = 3^9$. Hence, $10^9 \equiv 3^9 \pmod{7}$.
However, there is no reason, why we should be allowed to reduce the exponent by 7 (and it is incorrect).
Corrected calculation. $3^2 \equiv 2$, $3^4 \equiv 4$, $3^8 \equiv 16 \equiv 2$. Hence, $3^9 = 3^8 \cdot 3^1 \equiv 2 \cdot 3 \equiv -1 \pmod{7}$.
Corrected calculation (using Fermat). $3^6 \equiv 1$ just like $3^0 = 1$. Hence, we are allowed to reduce exponents modulo 6. Hence, $3^9 \equiv 3^3 \equiv -1 \pmod{7}$.

Theorem 25. (Fermat's little theorem) Let p be a prime, and suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. (beautiful!) Since a is invertible modulo p, the first $p-1$ multiples of a,

$$a, 2a, 3a, \ldots, (p-1)a$$

are all different modulo p. Clearly, none of them is divisible by p.
Consequently, these values must be congruent (in some order) to the values $1, 2, \ldots, p-1$ modulo p. Thus,

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Cancelling the common factors (allowed because p is prime!), we get $a^{p-1} \equiv 1 \pmod{p}$. □

Remark. The "little" in this theorem's name is to distinguish this result from Fermat's last theorem that $x^n + y^n = z^n$ has no integer solutions if $n > 2$ (only recently proved by Wiles).

Recall that Fermat's little theorem is just the special case when n is a prime of Euler's theorem:

Theorem 26. (Euler's theorem) If $n \geqslant 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Example 27. Compute $3^{1003} \pmod{101}$.

Solution. Since 101 is a prime, $3^{100} \equiv 1 \pmod{101}$ by Fermat's little theorem.
Therefore, $3^{1003} = 3^{10 \cdot 100} 3^3 \equiv 3^3 = 27 \pmod{101}$.

Example 28. Compute $3^{25} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.
$25 = 16 + 8 + 1$. Hence, $3^{25} = 3^{16} \cdot 3^8 \cdot 3^1 \equiv 16 \cdot (-4) \cdot 3 = -192 \equiv 10 \pmod{101}$.

Every integer $n \geqslant 0$ can be written as a sum of distinct powers of 2 (in a unique way). Therefore our approach to compute powers always works. It is called **binary exponentiation**.

Example 29. (homework) What are the last two (decimal) digits of 3^{7082}?

Solution. We need to determine $3^{7083} \pmod{100}$. $\phi(100) = \phi(2^2 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

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

Armin Straub
straub@southalabama.edu

Example 30. (bonus challenge!) 2^{29} is a nine (decimal) digit number. Each digit occurs except one. Which digit is missing?

Well, $2^{29} = 536870912$, so 4 is missing. So the actual question is how to find out that 4 is missing without computing that large number (not fun by hand). Can you find a slick trick?

Hint. First, compute 2^{29} modulo 9. How does that help?

Example 31. (homework) Compute $2^{20} \pmod{41}$.

Final answer. $2^{20} \equiv 1 \pmod{41}$

Example 32. (homework) Compute $99^{307} \pmod{84}$.

Final answer. $99^{307} \equiv 15 \pmod{84}$

2.4 Historical ciphers, cont'd

Example 33. (affine cipher) A slight upgrade to the shift cipher, we encrypt each character as

$$E_{(a,b)}: \quad x \mapsto ax + b \pmod{26}.$$

How does the decryption work? How large is the key space?

Solution. Each character x is decrypted via $x \mapsto a^{-1}(x - b) \pmod{26}$.

The key is $k = (a, b)$. Since a has to be invertible modulo 26, there are $\phi(26) = \phi(2 \cdot 13) = 26\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{13}\right) = 12$ possibilities for a. There are 26 possibilities for b. Hence, the key space has size $12 \cdot 26 = 312$.

Example 34. (substitution cipher) In a substitution cipher, the key k is some permutation of the letters $A, B, \ldots, Z$. For instance, $k = FRA\ldots$. Then we encrypt $A \to F$, $B \to R$, $C \to A$ and so on. How large is the key space?

Solution. Key space has size $26! \approx 10^{26.6} \approx 2^{88.4}$, so a key can be stored using 89 bits. That's actually a fairly large key space. Too large to go through by brute force.

However, still easy to break. Since each letter is always replaced with the same letter, this cipher is susceptible to a **frequency attack**, exploiting that certain letters (and, more generally, letter combinations!) occur much more frequently in, say, English text than others.

Example 35. (homework) It seems convenient to add the space as a 27th letter in the historic encryption schemes. Can you think of a reason against doing that?