6 Fermat's little theorem

Example 62. (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, $3^9 = 3^8 \cdot 3^1 \equiv 2 \cdot 3 \equiv -1 \pmod{7}$.

By the way, this approach of computing powers via exponents that are $2, 4, 8, 16, 32, \ldots$ is called **binary exponentiation**. It is crucial for efficiently computing large powers (see below).

Corrected calculation (using Fermat). $3^6 \equiv 1 \pmod{7}$ just like $3^0 = 1$. Hence, we are allowed to reduce exponents modulo 6. Consequently, $3^9 \equiv 3^3 \equiv -1 \pmod{7}$.

Theorem 63. (Fermat's little theorem) Let p be a prime, and suppose that $p \nmid a$. Then

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

Proof. The first $p-1$ multiples of a,

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

are all different modulo p. (Otherwise, $ra \equiv sa \pmod{p}$ for some $r, s \in \{1, 2, \ldots, p-1\}$. Since p is prime, this implies $r \equiv s \pmod{p}$.) 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).

Comment. An alternative proof based on induction is given in our book (bottom of page 88).

Example 64. What is 2^{100} modulo 3? That is, what is the remainder upon division by 3?

Solution. $2 \equiv -1 \pmod{3}$. Hence, $2^{100} \equiv (-1)^{100} = 1 \pmod{3}$.

Careful! Once more, it is incorrect to reduce the exponent modulo 3! $100 \equiv 1 \pmod{3}$ but $2^{100} \not\equiv 2^1 \pmod{3}$.

Comment. However, since we are working modulo a prime, $p = 3$, Fermat's little theorem does allow us to reduce the exponent modulo $p - 1 = 2$. Indeed, $2^{100} \equiv 2^0 \equiv 1 \pmod{3}$.

Example 65. Compute $3^{1003} \pmod{101}$.

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

Therefore, $3^{1003} = 3^{10 \cdot 100} \cdot 3^3 \equiv 3^3 = 27 \pmod{101}$.

Important comment. Note that, because of Fermat's little theorem, we can reduce the exponent modulo 100 when calculating modulo 101. In particular, since $1003 \equiv 3 \pmod{100}$, we have $3^{1003} \equiv 3^3 = 27 \pmod{101}$.

7 Binary exponentiation

Example 66. Compute $3^{32} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.

$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, $3^{32} \equiv 16^2 \equiv 54$, all modulo 101

Armin Straub
straub@southalabama.edu

Example 67. Compute $3^{25} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.
Instead, we do what is called **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
Since $25 = 16 + 8 + 1$, we have $3^{25} = 3^{16} \cdot 3^8 \cdot 3^1 \equiv 16 \cdot (-4) \cdot 3 = -192 \equiv 10 \pmod{101}$.

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**.

Because $25 = \boxed{1} \cdot 2^4 + \boxed{1} \cdot 2^3 + \boxed{0} \cdot 2^2 + \boxed{0} \cdot 2^1 + \boxed{1} \cdot 2^0$, we will write $25 = (11001)_2$.

8 Representations of integers in different bases

Example 68. 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 69. Express 25 in base 2.

Solution. We already noticed that $25 = 16 + 8 + 1 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$. Hence, $25 = (11001)_2$.
Alternatively, here's how we could have determined the digits without prior knowledge:

- $25 = 12 \cdot 2 + \boxed{1}$. Hence, $25 = (\ldots 1)_2$ where … are the digits for 12.
- $12 = 6 \cdot 2 + \boxed{0}$. Hence, $25 = (\ldots 01)_2$ where … are the digits for 6.
- $6 = 3 \cdot 2 + \boxed{0}$. Hence, $25 = (\ldots 001)_2$ where … are the digits for 3.
- $3 = 1 \cdot 2 + \boxed{1}$, with $\boxed{1}$ left over. Hence, $25 = (11001)_2$.

Example 70. Express 49 in base 2.

Solution.

- $49 = 24 \cdot 2 + \boxed{1}$. Hence, $49 = (\ldots 1)_2$ where … are the digits for 24.
- $24 = 12 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 01)_2$ where … are the digits for 12.
- $12 = 6 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 001)_2$ where … are the digits for 6.
- $6 = 3 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 0001)_2$ where … 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? $49 = (100)_7$.