Example 69. Compute the powers of 2 modulo 11.

Solution. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 5, 2^5 \equiv 2 \cdot 5 = 10, 2^6 \equiv 2 \cdot 10 \equiv 9, 2^7 \equiv 2 \cdot 9 \equiv 7, 2^8 \equiv 2 \cdot 7 \equiv 3,$ $2^9 \equiv 2 \cdot 3 = 6, 2^{10} \equiv 2 \cdot 6 \equiv 1$, and now the numbers we get will repeat...

Note. By **Fermat's little theorem**, it was clear from the beginning that $2^{10} \equiv 1 \pmod{11}$.

Also notice that the values $2^0, 2^1, \ldots, 2^9$, together with 0, form a complete set of residues modulo 11. For that reason, we say that 2 is a **primitive root** modulo 11.

Example 70. Is 2 a primitive root modulo 7?

Solution. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 1$, and now the numbers will repeat... The numbers $1, 2, 4$ we got, together with 0, do not form a complete set of residues modulo 7. Hence, 2 is not a primitive root modulo 7.

Note. From $2^3 \equiv 1$ it follows that $2^6 = (2^3)^2 \equiv 1$. As predicted by Fermat's little theorem.

Comment. It is an open conjecture to show that 2 is a primitive root modulo infinitely many primes. (This is a special case of Artin's conjecture which predicts much more.)

Example 71. Determine a primitive root modulo 7.

Solution. The previous example showed that 2 (as well as 4; why?!) is not a primitive root modulo 7. We therefore check whether 3 is a primitive root. Do it! It is a primitive root indeed.

Review. Fermat's little theorem, and its proof

Corollary 72. For any prime p and any integer a, we have $a^p \equiv a \pmod{p}$.

A freshman's dream. In particular, $(x + y)^p \equiv x^p + y^p \pmod{p}$, for any integers x, y and any prime p. [This follows from three applications of Fermat's little theorem: $(x + y)^p \equiv x + y \equiv x^p + y^p \pmod{p}$]

Example 73. What is 2^{100} modulo 3? That is, what's the remainder upon division by 3?

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

Careful! 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 74. 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 75. Compute $3^{32} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.
$3^2 = 9, 3^4 = 9 \cdot 9 \equiv -20, 3^8 \equiv (-20)^2 \equiv -4, 3^{16} \equiv (-4)^2 = 16, 3^{32} \equiv 16^2 \equiv 54$

Example 76. Compute $3^{25} \pmod{101}$.

Solution. $25 = 16 + 8 + 1$. 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**.

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 $25 = (11001)_2$.

Example 77. There is 10 types of people: those who understand binary, and those who don't.

People put that on their shirts... What's the joke?