Exercises and Solutions

Exercise 1

Show that if a and b are positive integers, then

$$(2^a - 1) \bmod (2^b - 1) = 2^{\,a \bmod b} - 1.$$

Solution

Let $a, b \in \mathbb{N}^*$ and write the Euclidean division of a by b:

$$a = qb + r, \quad \text{where } 0 \leq r < b.$$

Then

$$2^a - 1 = 2^{qb+r} - 1 = (2^b)^q \cdot 2^r - 1.$$

We rewrite:

$$(2^b)^q \cdot 2^r - 1 = \big((2^b)^q - 1\big)2^r + (2^r - 1).$$

Observe that $2^b - 1$ divides $(2^b)^q - 1$, since

$$(2^b)^q - 1 = (2^b - 1)\left((2^b)^{q-1} + \cdots + 1\right).$$

Hence,

$$2^a - 1 \equiv 2^r - 1 \pmod{2^b - 1}.$$

Since $r = a \bmod b$, we conclude:

$$(2^a - 1) \bmod (2^b - 1) = 2^{\,a \bmod b} - 1.$$

□

Exercise 2

Use Exercise 1 to show that if a and b are positive integers, then

$$\gcd(2^a - 1,\, 2^b - 1) = 2^{\gcd(a,b)} - 1.$$

Solution

We apply the Euclidean algorithm:

$$\gcd(2^a - 1,\, 2^b - 1) = \gcd(2^b - 1,\ (2^a - 1) \bmod (2^b - 1)).$$

By Exercise 1:

$$(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1.$$

Thus,

$$\gcd(2^a - 1,\, 2^b - 1) = \gcd(2^b - 1,\ 2^{a \bmod b} - 1).$$

This shows that each step of the Euclidean algorithm applied to $(2^a - 1, 2^b - 1)$ produces numbers of the form $2^r - 1$, where r is the corresponding remainder in the Euclidean algorithm applied to (a, b).

Continuing this process, we eventually reach:

$$\gcd(2^a - 1,\, 2^b - 1) = 2^{\gcd(a,b)} - 1.$$

□

Clarification of the Euclidean Algorithm Step

Let $a, b \in \mathbb{N}^*$ with $a \geq b$. Define the sequence (r_k) by the Euclidean algorithm:

$$r_0 = a, \quad r_1 = b,$$

and for $k \geq 1$,

$$r_{k-1} = q_k r_k + r_{k+1}, \quad 0 \leq r_{k+1} < r_k.$$

Since the sequence (r_k) is strictly decreasing and consists of nonnegative integers, there exists an index p such that

$$r_p = 0.$$

Then $r_{p-1} > 0$, and by the fundamental property of the Euclidean algorithm,

$$\gcd(a, b) = r_{p-1}.$$

Equivalently, if one prefers to index the last nonzero remainder by r_p, one may write:

$$r_p = \gcd(a, b),$$

with $r_{p+1} = 0$.

Clarification of the Key Step

We use the fundamental identity:

$$\gcd(x, y) = \gcd\big(y,\ x \bmod y\big).$$

Applying this with $x = 2^a - 1$ and $y = 2^b - 1$, we obtain:

$$\gcd(2^a - 1,\ 2^b - 1) = \gcd\big(2^b - 1,\ (2^a - 1) \bmod (2^b - 1)\big).$$

By Exercise 1,

$$(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1.$$

Hence,

$$\gcd(2^a - 1,\ 2^b - 1) = \gcd(2^b - 1,\ 2^{a \bmod b} - 1).$$

Structure Preservation Along the Algorithm

Define a new sequence (R_k) by

$$R_k = 2^{r_k} - 1,$$

where (r_k) is the sequence of remainders from the Euclidean algorithm applied to (a, b).

We claim that the Euclidean algorithm applied to $(2^a-1, 2^b-1)$ produces exactly the sequence (R_k).

Indeed:

$$R_{k-1} \bmod R_k = (2^{r_{k-1}}-1) \bmod (2^{r_k}-1) = 2^{\,r_{k-1} \bmod r_k}-1 = 2^{r_{k+1}}-1 = R_{k+1}.$$

Thus, the remainders are preserved under the transformation

$$r \longmapsto 2^r - 1.$$

Conclusion

Since the Euclidean algorithm terminates with

$$r_p = \gcd(a, b),$$

we obtain

$$R_p = 2^{r_p} - 1 = 2^{\gcd(a,b)} - 1.$$

Therefore,

$$\gcd(2^a - 1,\, 2^b - 1) = 2^{\gcd(a,b)} - 1.$$

□