Exercises

Exercise 1. Let $n \geq 1$, a and e two integers $< 2^n$. Consider the algorithm of Figure 1.

Algorithm 1: Algorithm P.

Function *P(a, e)*
Input : a, e two integers $< 2^n$
Output: ?
$g \leftarrow \gcd(a, e)$;
if $g = 1$ **then**
return $(1, a)$;
$G \leftarrow g^{2^k} \bmod a$ with $k = \lceil \log n / \log 2 \rceil$;
$u \leftarrow \gcd(G, a)$; $v \leftarrow a/u$;
return (u, v).

(a) Execute the algorithm on $(a, e) = (16, 210)$, $(a, e) = (5040, 231)$.

(b) What does this algorithm compute?

(c) Justify your claim.

Answer.

(a) One computes $(16, 1)$ for the first example and $(63, 80)$ for the second.

(b) Let us look at the prime factorizations of all the quantities used in function P:

a	e	$g = \gcd(a, e)$	u	v
$16 = 2^4$	$210 = 2 \cdot 3 \cdot 5 \cdot 7$	2	2^4	1
$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$	$231 = 3 \cdot 7 \cdot 11$	$3 \cdot 7$	$3^2 \cdot 7$	$2^4 \cdot 5$

Put

$$g = p_1^{\beta_1} \times \cdots \times p_r^{\beta_r}$$

with $\beta_i > 0$. Then we can write $a = uv$ in a unique way, with $\gcd(u, v) = 1$ and

$$u = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$$

with $\alpha_i \geq \beta_i$. We might infer that function P precisely computes (u, v).

(c) Let p be a prime factor of g. We put $\beta = \nu_p(g)$, $\alpha = \nu_p(a)$ and $\gamma = \nu_p(u)$ with $u = \gcd(G, a)$. The integer g^{2^k} is divisible by $p^{\beta 2^k}$. But

$$p^\alpha \mid a \Rightarrow p^\alpha \leq a < 2^n$$

or $\alpha < n \frac{\log 2}{\log p} \leq n \leq 2^k \leq \beta\, 2^k$. It follows that $\alpha < \beta 2^k$ and, in the euclidean division $g^{2^k} = aQ + G$, G (which might be 0) is divisible by p^α, hence $\gamma = \alpha$.