Exercise 1. Verify that the following Carmichael numbers satisfy the Korselt's criterion:

$$1105 = 5 \cdot 13 \cdot 17 \qquad 1729 = 7 \cdot 13 \cdot 19$$
$$2465 = 5 \cdot 17 \cdot 29 \qquad 2821 = 7 \cdot 13 \cdot 31$$
$$6601 = 7 \cdot 23 \cdot 41 \qquad 8911 = 7 \cdot 19 \cdot 67$$

Solution. As can be seen from corresponding factorizations, all the numbers are square-free. It can be shown that

$$5|1104, \quad 12|1104, \quad 16|1104 \qquad 6|1726, \quad 12|1726, \quad 18|1726$$
$$4|2464, \quad 16|2464, \quad 28|2464 \qquad 6|2820, \quad 12|2820, \quad 30|2820$$
$$6|6600, \quad 22|6600, \quad 40|6600 \qquad 6|8910, \quad 18|8910, \quad 66|8910$$

Exercise 2. Test the following numbers for primality using Euler-Jacobi primality test.

1105 1729 2465 2821 6601 8911

Solution. 601 is the witness of compositeness of 1105, since $601^{552} \bmod 1105 = 781 \neq \left(\frac{601}{1105}\right)$.

11 is a witness of the compositeness of 1729, since $11^{864} \bmod 1729 = 1 \neq \left(\frac{11}{1729}\right)$.

13 is a witness of the compositeness of 2465, since $13^{1232} \bmod 2465 = 1 \neq \left(\frac{13}{2465}\right)$.

2 is a witness of the compositeness of 2821, since $2^{1410} \bmod 2821 = 1520 \neq \left(\frac{2}{2821}\right)$.

13 is a witness of the compositeness of 6601, since $13^{3300} \bmod 6601 = 4509 \neq \left(\frac{13}{6601}\right)$.

2 is a witness of the compositiveness of 8911, since $2^{4455} \bmod 8911 = 6364 \neq \left(\frac{2}{8911}\right)$.

Exercise 3. Apply the Miller-Rabin test and check if the following integers are strong probable primes.

1105 1729 2465 2821 6601 8911

Solution. $1105 = 2^4 \cdot 69 + 1$. $a = 1101$ is a witness of compositeness of 1105, since

$$1101^{69} \bmod 1105 = 846 \neq 1$$
$$s = 0: \; 1101^{2^0 \cdot 69} \bmod 1105 = 846 \neq -1$$
$$s = 1: \; 1101^{2^1 \cdot 69} \bmod 1105 = 781 \neq -1$$
$$s = 2: \; 1101^{2^2 \cdot 69} \bmod 1105 = 1 \neq -1$$
$$s = 3: \; 1101^{2^3 \cdot 69} \bmod 1105 = 1 \neq -1$$

$1729 = 2^6 \cdot 27 + 1$. $a = 800$ is a witness of compositeness of 1729, since

$$800^{27} \bmod 1729 = 512 \neq 1$$
$$s = 0: \; 800^{2^0 \cdot 27} \bmod 1729 = 512 \neq -1$$
$$s = 1: \; 800^{2^1 \cdot 27} \bmod 1729 = 1065 \neq -1$$
$$s = 2: \; 800^{2^2 \cdot 27} \bmod 1729 = 1 \neq -1$$
$$s = 3: \; 800^{2^3 \cdot 27} \bmod 1729 = 1 \neq -1$$
$$s = 4: \; 800^{2^4 \cdot 27} \bmod 1729 = 1 \neq -1$$
$$s = 5: \; 800^{2^5 \cdot 27} \bmod 1729 = 1 \neq -1$$

$2465 = 2^5 \cdot 77 + 1$

$$501^{77} \bmod 2465 = 621 \neq 1$$
$$s = 0: \; 501^{2^0 \cdot 77} \bmod 2465 = 621 \neq -1$$
$$s = 1: \; 501^{2^1 \cdot 77} \bmod 2465 = 1101 \neq -1$$
$$s = 2: \; 501^{2^2 \cdot 77} \bmod 2465 = 1886 \neq -1$$
$$s = 3: \; 501^{2^3 \cdot 77} \bmod 2465 = 1 \neq -1$$
$$s = 4: \; 501^{2^4 \cdot 77} \bmod 2465 = 1 \neq -1$$

$2821 = 2^2 \cdot 705 + 1$. 19 is a witness of compositeness of 2821.

$$19^{705} \bmod 2821 = 993 \neq 1$$
$$s = 0: \; 19^{2^0 \cdot 705} \bmod 2821 = 993 \neq -1$$
$$s = 1: \; 19^{2^1 \cdot 705} \bmod 2821 = 1520 \neq -1$$

$6601 = 2^3 \cdot 825 + 1$. 17 is a witness of compositeness of 6601.

$$17^{825} \bmod 6601 = 5795 \neq 1$$
$$s = 0: \; 17^{2^0 \cdot 825} \bmod 6601 = 5795 \neq -1$$
$$s = 1: \; 17^{2^1 \cdot 825} \bmod 6601 = 2738 \neq -1$$
$$s = 1: \; 17^{2^1 \cdot 825} \bmod 6601 = 4509 \neq -1$$

$8911 = 2^1 \cdot 4455 + 1$. 17 is a witness of compositiveness of 8911, since

$$17^{4455} \bmod 8911 = 2547 \neq 1$$
$$s = 0: \; 17^{2^0 \cdot 4455} \bmod 8911 = 2547 \neq -1$$

Compare this result to some real prime integer, i.e., $1999 = 2 \cdot 999 + 1$.

$$\begin{aligned} 17^{999} \bmod 1999 &= 1998 \neq 1 \\ s = 0: \;\; 17^{999} \bmod 1999 &= 1998 = -1 \end{aligned}$$